PERIODICAL FOR THE PROOFPOINT CUSTOMER COMMUNITY

ISSUE 3 / AUTUMN 2021

THE INNOVATION EDITION

People-Centric Security
Threat Protection
Information & Cloud Security
Compliance

Are you ready to make your people the center of your cybersecurity strategy?
CONTENTS

P4 Identify user risk and its impact with Proofpoint Nexus People Risk Explorer

P7 Customer Spotlight: How INEOS rose to the challenge of a lifetime

P10 TAP URL isolation for VAPs

P13 Innovation: Raising the bar for detecting and responding to email fraud with Advanced BEC Defense

P19 Innovation: Identify email fraud from risky suppliers: Introducing Nexus Supplier Risk Explorer

Email Fraud with Advanced BEC Defense

P22 Innovation: Measuring security awareness success: For your CISO, and for your organization

P27 Innovation: Phishing Awareness Training: Best practices for your employees

P32 Practitioners’ update: Understanding threat actors and their objectives

P36 The first step: Initial access leads to ransomware

P40 How to raise the bar for your cloud security

P46 Innovation: Announcing new endpoint DLP capabilities: prevention and data classification

P50 Innovation: Proofpoint introduces advanced DLP for Microsoft Teams

P52 Customer Spotlight: Compliance in a post-pandemic world

P54 Innovation: How Proofpoint helps you stay compliant and secure on Microsoft Teams

P57 Ensure regulatory compliance with NexusAI machine learning

P62 Risky Business Live

P67 Working back from “Bang!” security metrics to help CEOs answer the tough questions

Magazine Contributors

Ryan Kalember
EVP, Cybersecurity Strategy, Proofpoint

Fabiola Fernandez
Product Marketing Manager, Proofpoint

Neko Papez
Product Marketing Manager, Proofpoint

Sara Pan
Product Marketing Manager, Proofpoint

Mike Bailey
Manager, Product Marketing, Proofpoint

David Knight
EVP & GM Cloud Security Group, Proofpoint

Elad Horn
VP Product Management Cloud Security, Proofpoint

Nirav Shah
Staff Product Manager, Proofpoint

Itir Clarke
Manager, Product Marketing, Proofpoint

Paige Adams
Group CISO, Zurich Insurance, Proofpoint

Andrew Rose
Resident CISO, EMEA, Proofpoint

Vincent Merlin
VP Marketing APJ & EMEA, Proofpoint

Adenike Cosgrove
Director, International Product Marketing, Proofpoint

Sophie Ree
Content Marketing Manager, EMEA, Proofpoint
Hello, and welcome once again to New Perimeters. In this, our third edition, we reflect on our recent Protect EMEA 2021 event.

In June, we welcomed over 4,000 Proofpoint customers and partners to our annual conference. We chose this year’s theme – ‘Ready’ – for two reasons. Our latest product innovations mean we can continue to offer the best defence against an evolving threat landscape, and we are more focused than ever on turning you, our customers, into security heroes within your organizations.

The goal of the Protect sessions, and indeed, this magazine, is to empower you with the tools and knowledge to implement robust security solutions, communicate their value to the C-suite, and make security preparedness a critical business priority.

Here are just a few of the key takeaways from this year’s sessions:

**Proofpoint is aligning protection to the risks that matter most**

In his opening keynote, Proofpoint CEO and Chairman Gary Steele covered the top company milestones from this year. He also offered a sneak peek into the newest innovations from the Proofpoint team, including Advanced BEC Defense powered by our Supernova engine and our new machine learning and AI capabilities.

**Leading CISOs share common pain points**

If we can’t take an honest look at our industry’s pain points, we cannot make productive changes. In this candid conversation, Patrick Gray, host of the world’s most influential cybersecurity podcast, Risky Business, interviewed our customers and expert CISOs, exploring major problem areas, including talent shortage and lack of diversity.

**Proofpoint is built for the “work from anywhere” world**

Proofpoint’s David Knight, EVP and GM of Cloud Security and Elad Horn, VP of Cloud Security Products, led a standout session, “Raise the Bar for your Cloud Security.” They covered how cloud security technologies from Proofpoint including – CASB, Isolation, ZTNA, and web security – integrate to provide secure access, stop threats, and enforce DLP.

**What’s next for information and threat protection at Proofpoint?**

Proofpoint’s Ashan Willy, Rajneesh Chopra, Rob Holmes, and Jeff Burstein revealed our latest innovations in ML/AI-based threat detection, user training, and supplier risks.

**Compliance in a post-pandemic world**

The move to remote work has altered the way we work, and many of the repercussions are likely to be here to stay. Maria Ringer, VP, WIM Social Media Program Manager at Wells Fargo and Sima Patel, Director of Digital Wealth Management at Merrill Lynch explained how they are planning for compliance in the post-pandemic era.

In this edition of New Perimeters, we dive into greater detail about the sessions above and explore the latest people-centric solution innovations across Threat Protection, Information and Cloud Security, and our Compliance Platforms released in the first half of 2021.

As always, this magazine should serve as the start of a conversation. The Proofpoint team is always available to answer your questions and discuss all things cybersecurity.
INNOVATION:
Identify user risk and its impact with Proofpoint Nexus People Risk Explorer

MITIGATING RISK IS EVERY SECURITY TEAM’S PRIMARY GOAL. BUT PRIORITISING SECURITY ALERTS AND KNOWING WHICH CONTROLS TO APPLY – AND TO WHOM – CAN BE A HUGE CHALLENGE.
To overcome this, many organisations take a threat-centric approach to determine which controls to protect their perimeter. While this can reduce the risk they see in their environments, it offers an incomplete view.

What’s more, digital transformation and accelerated adoption of cloud applications and platforms have added another layer of security complexity. Traditional network security approaches don’t provide the same level of protection because people bypass the network to access cloud apps. Having visibility into applications and traffic is vital. But gaining visibility into the risks impacting an organization becomes harder with more variables to track.

According to Verizon’s 2021 Data Breach Investigations Report, the most successful attacks originate from stolen credentials. To mitigate this all too common risk, Proofpoint introduced our VAP (Very Attacked People) model. Designed to help security teams assess risk based on user behavior, the VAP model focuses on user vulnerability, attack and privilege. The result is a people-centric risk view that helps organizations determine:

1. How people work in high-risk ways (vulnerability): whether they’re likely to fall for attacks
2. How people are attacked by threats (attack): what the probability is that they will be attacked
3. How people access valuable data (privilege): what is the impact on the rest of the organisation if a specific user is attacked

By measuring the intersection of probability, likelihood and impact, organizations can gain a more complete view of their people risk.

Introducing Proofpoint Nexus People Risk Explorer

To enhance this view of people risk, Proofpoint recently introduced Nexus People Risk Explorer – a unique dashboard available to all customers who adopt a Proofpoint solution bundle.

Nexus People Risk Explorer helps security teams gain visibility and actionable intelligence into the risks each user poses to the broader organization by:

Identifying vulnerability and privilege insight

Nexus People Risk Explorer analyses the vulnerabilities of user groups and the privileges they have based on their roles and associated activity. Each user is then assigned a risk score based on uncompleted or failed phishing simulation, clicker vulnerability, email and credential leaks, and more.

The integrated product data helps us surface vulnerabilities by breaking them down into logical categories and ranking them from most to least risk. Security teams can easily see the number of affected users for each vulnerability category, and the privileges individuals hold based on their business function.

“People are unquestionably the new perimeter – especially as organisations embrace hybrid work and increasingly adopt cloud applications. Our newest people-centric enhancements fortify the human element against a heightened combination of advanced threats, data loss, and compliance risks.”

“Backed by Proofpoint’s machine learning NexusAI and trillions of data points across all the digital channels that matter, our intelligence is unmatched in the industry. We are committed to developing security innovations that protect people from today’s toughest threats as they access applications and data, regardless of their location or the devices they use.”

Ryan Kalember
Executive Vice President of Cybersecurity Strategy for Proofpoint
Segmenting users based on profile similarities

By ranking and grouping users based on similar risk profiles, security teams can prioritize incident response actions.

Our integrated platform and synchronization with Active Directory allow for the segmentation of all users by business function, geography and department. This is an ongoing process, so when security teams click refresh, they can be confident they’re looking at the most up-to-date risk profiles.

Recommending security controls to mitigate risk, reduce costs and save time

Nexus People Risk Explorer suggests specific controls that security teams can apply within their existing tools to reduce risk in the desired user segmentation and manage the number of users to whom these controls are applied. If the organization has the integrated Proofpoint products related to these recommendations, security teams will receive additional, specific control instructions to protect their people.

Trending and risk calculation over time

Security teams are inundated with alerts. Nexus People Risk Explorer makes it easy to spot the most critical.

Proofpoint is the only vendor in the market that aggregates as much risk data and compiles it into an understandable visual for non-technical audiences and the board. And with data refreshed regularly, security teams can track their security controls and make changes in real-time based on what mitigates risk most effectively.

A people-centric view for a people-centric defense

Cyber-attacks are increasingly targeted at individuals. This makes user behavior the biggest risk factor facing your organization.

Nexus People Risk Explorer aggregates data insights from Proofpoint products to help you determine the level and scope of people risk facing your organization. This increased visibility allows security teams to prioritize resources and implement relevant adaptive controls based on the current threat landscape.

Ultimately, Nexus People Risk Explorer saves security teams time and money to protect what really matters: their people, networks, and data.
How INEOS rose to the challenge of a lifetime

A GLOBAL PETROCHEMICALS MANUFACTURER, INEOS OPERATES 194 SITES ACROSS 29 COUNTRIES, GENERATES $61 BILLION ANNUALLY AND EMPLOYS OVER 26,000 PEOPLE. THE LATTER FIGURE INCREASES TO AROUND 33,000 INCLUDING CONTRACTORS. AND, AS THE BUSINESS IS FEDERATED, EACH OF ITS 36 TEAMS HAS ITS OWN BOARD OF DIRECTORS, ITS OWN IT ORGANISATION, AND ITS OWN OBJECTIVES.

Complementing its core business, the company makes an impact across a range of elite sports, including cycling, football, and sailing. As a result, INEOS is becoming increasingly known to the everyday consumer.

Proofpoint Cybersecurity Strategist, Matt Cooke sat down with INEOS Group IT Director / CIO, Barry Pedley at this year’s Protect EMEA 2021 event. The pair discussed how the INEOS security team are rising to the challenge of protecting a diverse community of businesses, people, technology, and data – all while striving to nurture a safe and sustainable future for us all.
Protecting a brand on the rise

Despite being that UK’s largest private company and third largest chemical business, INEOS was little known outside its industry around a decade ago. So much so that it styled itself as “the biggest business you’ve never heard of”.

“If I go back a number of years, anonymity was our best defence. When I joined the company, you Googled INEOS and it came back with blank.”

Aside from a catchy tagline, this anonymity gave INEOS a defence against cybercriminals, whose sights remained largely on household names.

In the time since, however, thanks largely to sports advertising, INEOS brand recognition has increased significantly. And with greater recognition comes greater risk. Whereas once security was managed by individual business units, growing threats have called for a new approach. Today, cybersecurity is primarily overseen by the group CSO.

“Cybersecurity has been an evolution. It was handled in the business units. But as the security threat has grown, and as the need to respond to that has grown, it needs to be group coordinated.

…There’s nowhere to hide anymore and that’s meant we have to step up. We’re now a very known name and, as we see on a daily basis, we’re a target.”

So, what exactly does stepping up look like? For INEOS, it’s a matter of raising security awareness throughout the organisation.

“We’ve successfully transitioned [security] to the top of everyone’s agenda.”

This cybersecurity culture starts from the top. Back in 2018, INEOS chairman Jim Ratcliffe issued the “10 golden IT security rules”, instructing staff to follow them without exception. They included the following:

“If an email is at all suspicious then delete it.
There is no downside in doing this. Just delete it.
We cannot accept people opening suspicious emails and attachments. This threatens the integrity of our systems and harms INEOS.
If in doubt throw it out!”

A people-centric approach has remained at the heart of the company’s cyber defence strategy. People risk is highlighted at every board meeting, with hard statistics – number of email threats, number blocked, number of clicks. With such regular, tangible updates, cybersecurity – and most importantly, the human element of cybersecurity – is never far from the top of the agenda.
Defending in depth

Security awareness may be the cornerstone of an effective cyber defence, but it is not enough alone. Proofpoint’s Email Protection helps INEOS defend against the number one threat vector – email – keeping millions of potential threats at bay.

“Recently we’ve just had somebody very senior join us from another large organization. He reached out and said, ‘I don’t know what you’re doing, but [the email security] is far better than anywhere else I’ve worked.’ Working with a partner like Proofpoint, we’re seeing the benefits.”

Proofpoint also gives Barry and INEOS much greater visibility to quickly spot trends and highlight suspicious or malicious activity.

“We feed our Proofpoint logs into our SOC. We correlate that with our [Microsoft 365] logs and firewall logs. We correlate all the activity so that should something happen, we’re able to go back to source.”

The power of people-centric security

Through a combination of technology, process, and people, INEOS has implemented a broad, deep, and robust cyber defence. But Barry and his team know that no solution is 100% effective.

Threats new and old will penetrate defences, and when they do, every INEOS user must be ready to detect and deter. Vigilance is key.

“No tool is 100% effective, so something is going to get through. While we train, train, and train again, if somebody is busy, or somebody has a lapse of concentration, it’s that click that we want to try and avoid.”

Ultimately, behaviour is the biggest risk factor for any modern organisation. And changing that behaviour is paramount to a robust cyber defence.

This is only possible by creating a culture in which cybersecurity is not just a concern for IT. It is everyone’s responsibility. This culture is nurtured through regular, in-context awareness training.

“ONCE UPON A TIME, WE SAW MASS ATTACKS. WHAT WE NOW SEE IS DOWN IN THE DOZENS. IT’S VERY SPECIFIC. CYBERCRIMINALS WILL DO LOTS OF RESEARCH ON LINKEDIN AND VARIOUS PLATFORMS TO FIND OUT JOB TITLES, AND INSTEAD OF SEEING A WAVE, WE JUST SEE THESE LITTLE RIPPLES COMING AT US.”

As these attacks become increasingly targeted, INEOS knows that user behaviour, combined with effective email security, can be the difference between the success and failure of a cyber threat. And when users understand the link between reusing a password and a data breach or clicking a link from an unknown sender and ransomware, that behaviour changes.

Watch the interview: How INEOS have risen to the challenge of a lifetime

https://www.proofpoint.com/uk/resources/videos/protect-2021-threat-protection-sessions

In this video, Barry Pedley – Group IT Director / CIO explains how the INEOS security team are rising to the challenge of protecting a diverse community of businesses, people, technology and data whilst the company helps drives a safe and sustainable future for us all.
FOR YEARS, CISOs HAVE STRUGGLED TO PROTECT THEIR USERS AND IDENTIFY IF UNKNOWN URLS ARE MALICIOUS. EVEN TODAY, ORGANIZATIONS STILL DEPLOY A MYRIAD OF SECURITY TOOLS TO HELP SOLVE THESE CHALLENGES.

THREAT PROTECTION SPOTLIGHT

INNOVATION:
URL isolation for Very Attacked People

BY NEKO PAPEZ
Product Marketing Manager
Proofpoint

FOR YEARS, CISOs HAVE STRUGGLED TO PROTECT THEIR USERS AND IDENTIFY IF UNKNOWN URLS ARE MALICIOUS. EVEN TODAY, ORGANIZATIONS STILL DEPLOY A MYRIAD OF SECURITY TOOLS TO HELP SOLVE THESE CHALLENGES.

As the global pandemic continues to run rampant, CISOs are not only struggling to solve traditional cybersecurity challenges but are also faced with a new surge of pandemic themed phishing scams intended to deceive users and infiltrate organizations. Of these, credential phishing still remains one of the most common tactics used by threat actors. These attacks send an email with a URL that takes victims to a fake website designed to steal their credentials. Most of the time these fake sites are so well crafted that they look real and no matter how much training users have, sooner or later someone is going to click on a bad link and enter their credentials.

Operating from multiple countries, these threat actors have become increasingly sophisticated in their attempts to lure users into clicking a malicious link and divulging confidential account credentials, often targeting individuals with customized attacks through corporate and personal email.
With the shift to work from home and hybrid work environments, many of these people are now working outside the confines of a traditional corporate perimeter, increasing their vulnerability. For that very reason protection must start with people, protecting them from advanced threat tactics and arming them with knowledge and tools to help protect the organization. And protection must focus on email, which is the primary target of attackers.

Stopping a threat before the first point of infection is critical to prevent attackers from compromising an organization’s most important asset, the people. To properly defend against phishing attacks and targeted attacks requires a multi-layered solution that allows users to maintain continuity of their day-to-day operations, all while keeping the organization secure.

Understanding the impact of these credential phishing emails and socially engineered attacks is key to implementing a successful people-centric security strategy.

**Very Attacked People (VAPs)**

Modern email threats continue to exploit human nature because it’s simple and effective. We continue to see unique malicious URLs on the rise and a relentless focus on credential phish by bad actors. These attackers rely on users to activate the attack or provide their credentials for bad actors to gain access to their systems and launch their attacks from within.

We are excited to announce Targeted Attack Protection (TAP) URL Isolation for VAPs. This enables users to confidently browse unknown websites while still protecting them from URL and web-based attacks and is a critical component to basic email security. This new feature helps protect organizations from URL and web-based attacks for your VAPs. With this new integration, any URL that is clicked on within corporate email by your VAP users will be analyzed and isolated per configured policy. This will enable them to confidently access websites from their corporate email, knowing that the organization is secure.

Email Isolation can allow users to access risky or unknown URLs through their corporate and personal email by isolating sessions in a secure container. This technology helps prevent credential theft and protects users against things like malware and other malicious content. This is especially important for credential phishing emails which contain URLs and become unsafe post-delivery. Best of all, IT Teams can have peace of mind allowing users to navigate to links inside of their email without worrying about accidentally triggering a malicious link or file.
Visibility into isolated clicks through the TAP dashboard

Visibility into who your VAPs are, how they are being targeted and when they are interacting with potentially malicious URLs is key to protecting your organization today. In the Threat Detail page, you can now view the number of clicks isolated. If your organization has enabled TAP URL Isolation for VAPs, you can understand how many clicks are being protected through TAP’s Isolation integration and update your policies within the Proofpoint Isolation console to ensure protection against high-risk categories and activities like isolated user clicks on unknown or malicious URLs within corporate email.

How do these adaptive isolation controls protect my users?

These adaptive isolation capabilities draw on our expansive threat intelligence. We automatically isolate suspicious URLs based on two predictive scanning methods. First is a reputation check, in which Proofpoint’s Nexus Threat Graph helps determine whether a specific URL is subject to our condemned list or not by using a combination of NexusAI machine learning, advanced detection and human expertise. The second is our threat scan in which the HTML is sent to our static engine check to determine whether the page is malicious. During this time, all keyboard entry is disabled.

This adaptive control mechanism complements Proofpoint Email Protection and Targeted Attack Protection. Users can fully access and interact with most websites. For sites deemed suspicious by initial scans, they can view the site in read-only mode while a full threat analysis is performed behind the scenes. If anything comes back malicious then we would flag this browsing session and block the users from accessing this page.

Interested in adding TAP URL isolation for your VAPs?

Simply reach out to your Proofpoint account teams to get it enabled.

Customers already using our Proofpoint bundle (P0 and up) can take advantage of this protection with no additional cost.
INNOVATION:
Raising the bar:
Detecting and responding to email fraud with Advanced BEC Defense

Business Email Compromise (BEC)
Business email compromise (BEC) is a type of email cyber crime scam in which an attacker targets a business to defraud the company. Business email compromise is a large and growing problem that targets organizations of all sizes across every industry around the world.

SARA PAN
Product Marketing Manager
Proofpoint

Proofpoint has been stopping email fraud attacks for years, launching an ML-driven classifier as the attack category emerged over five years ago. Despite having stopped millions of fraud attempts, we haven’t rested on our laurels and have now launched an Advanced BEC Defense capability, powered by a completely new detection platform that we call Supernova.
Leveraging inbound and outbound gateway telemetry, supply chain risk analytics, and API data from cloud productivity platforms like Office 365 and Google Workspace, Advanced BEC Defense accurately uncovers even the most sophisticated email fraud attacks.

At its core, the new engine leverages a proven approach that we’ve applied to threat detection of all types over the years – the ensemble. Supernova leverages a combination of machine learning, stateful analytics, behavioral analytics, rulesets, and the work of researchers tracking threat actor tactics to deliver both high efficacy and the lowest false positive rate of any of our detection platforms. The ML components of Supernova are trained by our unmatched data set that comes from global scale and our deployments protecting the #1 threat vector at more of the Fortune 100, Fortune 1000, and Global 2000 than any other security provider.

The inputs to both the ML-driven and the other detection components work by analyzing multiple message attributes, including message header data, sender’s IP address (x-originating IP, reputation), and sender/recipient relationships, message body for sentiment and language and more to determine whether a message is a BEC threat. It effectively detects and blocks supplier invoicing fraud by analyzing messages for numerous tactics associated with supplier fraud, such as reply-to pivots, use of malicious IPs, use of impersonated supplier domains, and words or phrases commonly used in this type of attacks.

The Supernova engine is technically our third generation ML platform, but as the earlier models are all still operational, effective, and highly useful in training each other, it’s really just the newest member of the ensemble. That said, its other analytical capabilities make it both more effective and less false positive-prone than any ML-only approach. In recent head to head comparisons against several API-only tools, it has delivered both higher true positive detection rates and substantially lower false positive rates.

**Supernova leverages a combination of machine learning, stateful analytics, behavioral analytics, rulesets, and the work of researchers tracking threat actor tactics to deliver both high efficacy and the lowest false positive rate of any of our detection platforms.**
How does Advanced BEC Defense stop supplier invoicing fraud?

Here’s a real-world example that shows how an attacker leveraged compromised accounts and supplier impersonation jointly in a sophisticated supplier fraud attack.

In this attack, the attacker compromised the email accounts of both the target organization and of its suppliers. The attacker first compromised an email account of an accountant who works at the account payable department of the target organization. From there, he conducted extensive reconnaissance to gather information, such as billing cadence, approval chain, and email threads related to invoices.

The attacker also compromised an account at the target organization’s supplier. Using the compromised account of Sajid, who’s a salesperson from the supplier’s company, the attacker hijacked the original email thread and requested Afsal, who also works at the accounts payable department of the target organization, to STOP payment to the original bank account. He then pivoted to impersonation using a lookalike domain in the reply-to. By adding a bunch of lookalike accounts along with legitimate accounts from the approval chain to the cc field, the attacker made this email more creditable. (see Figure 1 - on the next page).
This is how sophisticated a supplier fraud attack is. With Proofpoint Advanced BEC Defense, we caught this attack in time and stopped a potential loss of millions of dollars. Advanced BEC Defense analyzed the header data and uncovered that the attacker was operating from a Nigerian IP space and that he utilized a compromised GoDaddy mail infrastructure to hijack the original thread posing as Sajid. Our enhanced BEC detection engine also identified the inconsistent reply-to pivot, as well as multiple lookalike accounts inserted in the CC field – both are emerging BEC tactics. Furthermore, in the message body, it detected words and phrases that implied urgency and that required financial transactions. Piecing every detail together, we detected and blocked this complex supplier invoicing fraud attack.
How is Advanced BEC Defense different?

Tackling payload-less threats like BEC requires more than ML algorithms. It requires a broad and deep set of data and human threat expertise to train those ML models to accurately detect and stop bad messages without misidentifying and blocking good messages. ML models trained with bad or incomplete data and no threat context generate high false positives, creating more work for security and messaging teams while delivering a poor user experience.

Proofpoint is uniquely positioned to address this hard-to-detect threat by combining our heritage in machine learning/AI with extensive threat data and threat analyst expertise. We see and analyze 2B+ messages daily and monitor hundreds of millions of domains and 16M+ cloud accounts. We correlate and aggregate everything we see, training our ML with rich threat data gathered across multiple threat vectors and a broad customer footprint. That coupled with our human expertise truly differentiates our BEC protection – providing the best detection effectiveness with minimum false positives.

Vendors who tout their ML/AI models often lack the extensive data across multiple threat vectors and expert threat intelligence required to accurately and effectively stop email threats. Finally, ML-only models suffer from high false positive rates that prevent any automation from being reliably built around their detections, introducing cost and complexity for security teams to manually chase down potential BEC risks rather than simply automating common workflows.

...UNLIKE OTHER EMAIL SECURITY SOLUTIONS THAT RELY ON STATIC RULE MATCHING AND MANUAL TUNING TO FIND BEC SCAMS, PROOFPOINT’S INTEGRATED PLATFORM UTILIZES ADVANCED BEC DEFENSE THAT LEARNS IN REAL-TIME
Unlike other email security solutions that rely on static rule matching and manual tuning to find BEC scams, Proofpoint’s integrated platform utilizes Advanced BEC Defense that learns in real-time. This learning enables dynamic classification of “good” and “bad” emails. It reacts to changes in attack tactics, stopping BEC variants that are often missed by legacy email security providers. Moreover, Advanced BEC Defense provides granular visibility into BEC threat details, revealing BEC themes such as gift carding, payroll redirect, invoicing, and more. It provides observations about why the message was suspicious as well as message samples. This insight allows the security team to better understand, communicate, and mitigate BEC risks.

**Figure 3:** Proofpoint identifies which users are mostly attacked by imposter threats and provides granular visibility into BEC threat details.

---

**Detect and stop BEC threats before they enter**

Only Proofpoint provides Advanced BEC Defense as an integral part of the Threat Protection Platform that:

- Accurately detects BEC threats without blocking good messages
- Provides visibility into who is being targeted with BEC and granular threat details
- Automates remediation of BEC threats
- Educates end users to identify and report potential threats
- Delivers insights into suppliers that may be compromised or impersonated

ALL EXISTING GATEWAY CUSTOMERS WILL BENEFIT FROM THIS NEW, IMPROVED DETECTION WITH NO ADDITIONAL COSTS.
INNOVATION:

Identify email fraud from risky suppliers:
Introducing Nexus Supplier Risk Explorer

SARA PAN
Product Marketing Manager
Proofpoint

EMAIL FRAUD OFTEN STARTS WITH AN EMAIL IN WHICH THE ATTACKER POSES AS SOMEONE THE VICTIM TRUSTS OR “ACTUALLY BECOMES” THAT PERSON BY COMPROMISING THEIR ACCOUNT. THE MESSAGE MAKES A SEEMINGLY LEGITIMATE BUSINESS REQUEST THAT OFTEN LEADS TO WIRE TRANSFER OR FINANCIAL PAYMENT.
Among various types of email fraud, supplier invoicing fraud often accounts for the biggest financial losses due to the nature of B2B payment. Attackers now target an organization’s suppliers and vendors to launch fraud, phishing and other attacks. These indirect attacks abuse the implicit trust relationship your organization has with its suppliers.

Proofpoint has observed that 98% of organizations have received a threat from a supplier domain with nearly three-quarters of those threats being phishing or impostor threats. Even world-class security organizations struggle with stopping these human-activated threats that don’t lend themselves to traditional defense in depth.

Unfortunately, most security teams don’t have visibility into who their suppliers are, let alone the risk posed by their trusted vendors.

Nexus Supplier Risk Explorer

To provide visibility into supplier vendor risk, Proofpoint recently introduced Nexus Supplier Risk Explorer, a unique feature in our Proofpoint Email Fraud Defense offering.

To help you overcome the challenge with complex supply chain attacks, Supplier Risk Explorer automatically identifies your suppliers and the domains they use to send email to your users. Integrated with Proofpoint’s industry-leading Threat Protection Platform, Supplier Risk Explorer analyzes your email communications and provides a supplier-centric view of threats. It reveals the message volume, the threats detected from supplier domains, as well as the messages blocked from malicious lookalikes of your suppliers’ domains.

Supplier Risk Explorer then assesses the risk level of these supplier domains by evaluating several dimensions, including:
- Threats sent to your organization
- Threats sent to other Proofpoint customers
- The lookalikes of supplier domains
- Whether it is recently registered
- Whether it has a DMARC reject policy

By ranking and prioritizing the risk level of your supplier domains, your security team can see and prioritize which suppliers that they should pay the most attention to. If a supplier’s domain is actively sending your users malicious email, it will pop to the top of the list. That way, your security team can focus their efforts on suppliers that pose the highest risk to your organization.
Drilling down into supplier domains

Supplier Risk Explorer unveils threats from impersonated and compromised suppliers. It identifies the malicious lookalikes of your suppliers’ domains, which is a common business email compromise (BEC) tactic. It shows the registration date of a supplier domain, which is an indicator of newly registered malicious lookalikes of supplier domains. It also validates the DMARC record of each domain. If a supplier domain is at P= reject, it won’t be vulnerable to domain spoofing.

Supplier Risk Explorer consumes and analyzes threat feeds from Proofpoint’s advanced email protection where our detection engines accurately identify and classify threats. With this shared threat intelligence, Supplier Risk Explorer shows you the count of unique threats sent from supplier domains, including phishing, impostor threats, malware, and spam. It also provides visibility into the threat spread – how many Proofpoint customers have also seen this threat. This insight indicates the severity and the prevalence of the threat, so you can better understand and communicate the risk. Your security analysts can automatically drill down into threat details in the Proofpoint Targeted Attack Protection dashboard, where they can investigate the threat actor, attack techniques, intended users and more.

Fraudsters are turning your suppliers against you by impersonating them or compromising their email accounts. Supplier Risk Explorer provides you with a supplier-centric view of threats targeting your users, so you know which suppliers are posing risk to your organization.

Figure 1: Supplier Risk Explorer identifies supplier domains and provides visibility into which suppliers pose risk to your organization.
If there’s one thing that I’ve learned about security awareness training, it’s that effective measurement can make or break a program. Unfortunately, security awareness is one of those items that is lower in budget priority than technical controls. So, getting the metrics right and communicating them correctly to your chief information security officer (CISO) and other stakeholders will help you to:

- Get sustained buy-in
- Avoid the time and frustration of restarting your security awareness training program

Depending on how your program is composed, there may be very different concerns from upper management. If your awareness program is primarily compliance-driven, it may be a checkbox “training completed.” For organizations with awareness and behavior metrics, it may be participation and metrics like click rate or reporting rate of simulations. And organizations with advanced programs may look even further. Let me explain.
Figure 1. Very Attacked People™ are users in your organization who receive a higher volume and more dangerous types of attacks from Proofpoint Targeted Attack Protection. Including these users in more frequent, targeted education efforts can help reduce your risk further and advance your program.

Figure 2. Our 2021 State of the Phish report shows the average “resilience factor,” or reporting rate divided by click rate. Organizations should aim to have a 14x resilience factor.

<table>
<thead>
<tr>
<th>Industry</th>
<th>Reporting Rate</th>
<th>Failure Rate</th>
<th>Resilience Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Services</td>
<td>20%</td>
<td>11%</td>
<td>1.8</td>
</tr>
<tr>
<td>Energy/Utilities</td>
<td>18%</td>
<td>11%</td>
<td>1.6</td>
</tr>
<tr>
<td>Insurance</td>
<td>17%</td>
<td>10%</td>
<td>1.7</td>
</tr>
<tr>
<td>Legal</td>
<td>17%</td>
<td>8%</td>
<td>2.1</td>
</tr>
<tr>
<td>Engineering</td>
<td>16%</td>
<td>16%</td>
<td>1.0</td>
</tr>
<tr>
<td>Automotive</td>
<td>15%</td>
<td>8%</td>
<td>1.9</td>
</tr>
<tr>
<td>Business Services</td>
<td>14%</td>
<td>11%</td>
<td>1.3</td>
</tr>
<tr>
<td>Technology</td>
<td>13%</td>
<td>12%</td>
<td>1.1</td>
</tr>
<tr>
<td>Government</td>
<td>13%</td>
<td>10%</td>
<td>1.3</td>
</tr>
<tr>
<td>Mining</td>
<td>13%</td>
<td>13%</td>
<td>1.0</td>
</tr>
<tr>
<td>Food &amp; Beverage</td>
<td>11%</td>
<td>11%</td>
<td>1.0</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>10%</td>
<td>10%</td>
<td>1.0</td>
</tr>
<tr>
<td>Healthcare</td>
<td>10%</td>
<td>10%</td>
<td>1.0</td>
</tr>
<tr>
<td>Entertainment/Media</td>
<td>10%</td>
<td>9%</td>
<td>1.0</td>
</tr>
<tr>
<td>Transportation</td>
<td>10%</td>
<td>12%</td>
<td>-1.2</td>
</tr>
<tr>
<td>Construction</td>
<td>9%</td>
<td>14%</td>
<td>-1.6</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>9%</td>
<td>11%</td>
<td>-1.2</td>
</tr>
<tr>
<td>Retail</td>
<td>9%</td>
<td>13%</td>
<td>-1.4</td>
</tr>
<tr>
<td>Education</td>
<td>6%</td>
<td>12%</td>
<td>-2.0</td>
</tr>
<tr>
<td>Hospitality/Leisure</td>
<td>5%</td>
<td>10%</td>
<td>-2.0</td>
</tr>
</tbody>
</table>

Measuring what matters for security awareness

As Gartner’s 2020 Market Guide for Security Awareness says, “Utilize additional information security metrics beyond phishing testing ‘click rates’ to determine program success.” We couldn’t agree with that statement more. We talk to a lot of customers that become laser-focused on the click rate of phishing simulations as the be-all and end-all of security awareness metrics. While a great starting point, it has a lot of flaws.

First, the click rate will be very variable based on the average failure rate of the template used and the audience it’s sent to. As programs get more advanced, you should consider more targeted templates for different audiences like Very Attacked People™ (VAPs). So, the click rate will vary, but it will only show employees are avoiding the bad – not “doing the good.”

When you include a metric like reporting rate with a phishing email add-in, you can start showing users are not only avoiding an attack, but they’re also taking action – and “doing the good” to help protect the company.

As a very high-level rule, we recommend having a phishing reporting rate of 70% or higher for phishing simulations and a click rate of under 5%. That means a resilience factor of 14x for top-performing customers.
Going a level deeper, it’s essential, and enlightening, to understand the real security impacts of your security awareness program. For instance, if users are reporting messages, are they reporting safe messages or malicious ones?

We use the Proofpoint threat detection stack to score user-reported emails. We can show you how much malicious email they’re reporting, and how that compares with other customers.

Additionally, if you’re able to gather other human-centric security impacts, such as:
- Successful phishing incidents
- Click rate of known malicious content
- Credential compromises
- Insider incidents
- Machine remediations due to malware and ransomware

…then, you can prove those key metrics have decreased and been influenced by your awareness program. And then, you’ll improve future investment and show how your program is changing behavior and driving culture.

**Figure 3.** Our new CISO Dashboard will show you different program areas and what percentile you are in compared with other customers. This provides context and allows you to focus on areas for improvement.

**Score calculation summary:**
**Reported email accuracy**
Reported email accuracy score is based on your performance in the last 90 days compared to all customers’ average reported email accuracy in the last 90 days.

**Reported email accuracy comparison**
- 43% - Your Organization’s Accuracy
- 0% - Lowest Performing Customer’s Accuracy
- 100% - Highest Performing Customer’s Accuracy

**Figure 4.** Security awareness impacts go beyond compliance and simulation metrics and can improve overall security through reducing the real click rate, reporting malicious messages and reducing human-driven security incidents.

**Training Completion**
**Reporting Rate of Simulations**
**Click Rate of Simulations**
**Real Click Rate**
**Real Impacts**
**Reported Message Types**
**Understanding user vulnerability**

Sometimes, it can be challenging to get buy-in to expand the awareness program. Stakeholders are worried that users are spending too much time in training, or they’ll become tired of the security awareness exercises.

One of the strategies we’ve seen customers use is to focus on vulnerable users at a more frequent cadence. That way, stakeholders know there’s a good reason for the additional education touchpoints with these users, and not all users require the same education. It’s a strategic way to advance your program that stakeholders can agree to.

**Communicating effectively to your CISO and key stakeholders**

At Wisdom 2021, our annual security awareness event, many at the conference spoke to the overuse of fear, uncertainty and doubt (FUD). When communicating to security leaders, FUD can only get you so far.

So, how do you communicate security awareness performance to your CISO and other stakeholders? There are two important attributes: quantitative and qualitative components.

When talking about quantitative scores, understanding your overall performance and how you compare against others matters for context. When possible, focus on positive metrics instead of just the negative “click rate.” For example:

- Users reported more phishing simulations
- Security awareness knowledge improved
- Users became better at reporting real malicious messages
- More users participated in security awareness activities

Figure 5. Our User Vulnerability section of the CISO Dashboard will show you low performers and participators. If users are VAPs in Proofpoint Targeted Attack Protection, that data will be integrated as well for a better view of vulnerability.
Our new CISO Dashboard allows you to do this easily, with performance and participation scores that show you which percentile range you rank for each area, and how that score has changed overall. The overall score makes it simple to show quickly where you are at in a glance, and the stoplight-style icons can give you areas to focus on for program improvement.

While quantitative is important, it’s just as important to communicate the qualitative stories from users. For instance:

- Did a user stop a real phishing attack that was sophisticated?
- Did you get positive user sentiment from your awareness program? (Consider setting up an email alias or sending out a quick feedback survey.)
- Did an executive staff member or well-known person at your organization share something about security awareness with their staff?

**Figure 6.** The Security Program Score Summary helps you communicate program performance quickly to your CISO.

These stories combined with quantitative data help build a narrative that security awareness is more than a required compliance activity, users are changing their behavior, and the culture is actively shifting as users better understand the risks and help to protect the company.
INNOVATION: PHISHING AWARENESS TRAINING
BEST PRACTICES FOR YOUR EMPLOYEES

IF A USER AVOIDS CLICKING ON SIMULATED PHISHING ATTACKS – DOES IT MEAN THEY’RE LESS RISKY? ON THE SURFACE, YES, IT SHOULD MEAN THAT. BUT IT ISN’T THE FULL PICTURE.

The reality is what’s actually happening in your company’s environment matters more to your risk profile than simulations. Users could be engaging with real phishing messages – just avoiding simulated ones.

Attackers could be laser-focused on exploiting a user who isn’t considered risky through the lens of your security awareness training program. So there’s a mismatch of security awareness risk and real risk. Until today.
Finding the right people

All employees should have ongoing phishing simulations and education to keep their skills sharp. We recommend simulations at least every 4-6 weeks for all users. But sometimes, supplemental phishing education is needed for riskier users.

Traditionally, phishing awareness programs focus on the risk of users who have engaged with phishing simulations. That’s a good start. But when organizations understand data about who is being targeted or engaging with actual attacks, it means they can focus their program on real risk.

Proofpoint takes a new and fresh approach to security education initiatives by using real data from your email environment through our Targeted Attack Protection Guided Training integration. We employ the data from our advanced email security product to identify the riskiest people – or Very Attacked People (VAPs) – in your organization based on how they’re being targeted, threat actor sophistication, type of attack and overall attack volume. Each person gets a score and an overview of all the threats targeting them.

More than two-thirds of organizations surveyed for the “2021 State of the Phish” report said they have two hours or less per user per year to make an impact on their users’ behavior. And phishing is only one component of a security awareness program, with many compliance regulations, privacy laws and topics like cloud applications and data protection also needing attention.

That’s why making the best use of your limited training time is critical. Our annual “State of the Phish” survey shows that security awareness cadences are increasing each year. That’s good news, as phishing awareness skills tend to fade 4-6 months after education, according to a German study. Ongoing program engagements can help to improve the retention of phishing skills.

Let’s look at three areas of strategy – the right people, right education and right response – for increasing phishing awareness. With these core pillars driving your program, you can significantly and positively impact your organization’s risk posture.
Attacking are constantly using new templates, lures, and techniques to trick users. You can target users who are very attacked by real phishing attacks. In this way, you can focus your phishing awareness program on the people who need it most.

Provide relevant phishing education with impact.

Attacking are constantly using new templates, lures, and techniques to trick users. You can target users who are very attacked by real phishing attacks. In this way, you can focus your phishing awareness program on the people who need it most.

If this integration isn't available to you, work with your email security team to find data about people being attacked or those who have fallen for actual phishing attacks. That way, you can focus your phishing awareness program on the people who need it most.

Providing relevant phishing education with impact.

Providing relevant phishing education with impact.

This message was sent to you by John Davis who is using One Drive Electronic Signature Service.

Sincerely,

John Davis

John Wiles has shared a document with you. Please find herein the finalized contract details.

VIEW DOCUMENT

Microsoft OneDrive

OPEN

Figure 4. Examples of Proofpoint phishing simulation tool templates.
Phishing simulations are primarily assessments – and an indication to users that they’re vulnerable to these attacks. The landing page that prompts users when they engage with simulations usually stays open for no more than a few seconds.

An educational component can help improve retention and teach skills to spot phishing attempts, like double-checking the sender and hovering over and examining links for legitimacy. An example of this type of education is our Attack Spotlight content. We look at real phishing lures affecting organizations and then build a short educational module (about two to three minutes) around a specific threat.

Figure 5. Example of educational module in Proofpoint Attack Spotlight content

We can also help you maximize your annual security awareness time budget with education that focuses only on those users who fall for a phishing simulation or who have engaged with or been targeted by a real phishing threat.

Make sure the phishing awareness content you use suits your organization’s style, whether it’s more corporate or humorous. And customizing the content, so you can tailor wording and imagery and even add links to policies, will help improve the relevance and impact of your user education.

Finally, if your organization is multinational, be sure to provide localized and translated content for users in different countries. A best practice is to identify a reviewer in each region and have them review the content in advance to make sure the template or education will suit the target audience.

**Give users tools to respond to phishing attacks**

Avoiding phishing attacks is good, but having users actively reporting phishing attacks is even better. In phishing awareness programs, the “click rate” – or the percentage of users who click/fail a phishing simulation – is a popular reporting metric.

We highly recommend implementing a phishing reporting tool that lets users essentially become a part of the IT security team. Not only do these tools help reduce vulnerability, but they also provide a deeper understanding of user behavior. Accurate reporting of a potential phish means your users not only recognize what to avoid, but they also know what to do when they see a suspicious message.

### Failure/Click Rate

- **<5%**

### Reporting Rate

- **>70%**

<table>
<thead>
<tr>
<th>Subject Line</th>
<th>Template Style</th>
<th>Number of Messages Sent</th>
<th>Failure Rate</th>
<th>Reporting Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Someone has your password</td>
<td>Data Entry</td>
<td>798</td>
<td>&lt;1%</td>
<td>86%</td>
</tr>
<tr>
<td>Please DocSign this document Change</td>
<td>Attachment</td>
<td>441</td>
<td>2%</td>
<td>85%</td>
</tr>
<tr>
<td>COMPANY CONFIDENTIAL</td>
<td>Link</td>
<td>442</td>
<td>2%</td>
<td>83%</td>
</tr>
<tr>
<td>Toll Violation Notice</td>
<td>Link</td>
<td>676</td>
<td>4%</td>
<td>81%</td>
</tr>
<tr>
<td>Network Access Attempt</td>
<td>Data Entry</td>
<td>360</td>
<td>1%</td>
<td>80%</td>
</tr>
</tbody>
</table>

This is where we want to get your organisation to

**Figure 6. Examples of high reporting rates and low failure rates**

**There’s a lot to read about metrics and benchmarks for security awareness training. But a general rule of thumb for high-performing programs is to consistently have less than 5% of users fall for a simulation, but over 70% of users report it with the email reporting tool.**
Get the most from your Proofpoint investment and explore your own customised threat reports and product updates with our regular Customer Business Reviews.

Optimizing your security strategy starts with people.

Book your Customer Business Review now
https://go.proofpoint.com/customer-business-reviews.html
PRACTITIONERS’ UPDATE:

Understanding threat actors and their objectives

WE’VE DEVELOPED OUR INNOVATIVE TARGETED ATTACK PROTECTION (TAP) DASHBOARD TO HELP YOU UNDERSTAND THE HOW, WHAT AND WHY OF RANSOMWARE ATTACKS.

CRAIG HUITEMPA
Director Sales Engineering
Proofpoint
Ransomware is a type of malicious software (malware) that threatens to publish data or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. Ransomware is typically injected as a secondary payload following the installation of keylogging software, banking Trojans or other threats, which are also known as Initial Access Brokers.

According to research by Unit 42 of Palo Alto Networks, email phishing has become one of the top attack vectors for ransomware accounting for more than 75% of attack origins. Many attacks are now multistage campaigns, with malware used first to infect systems with ransomware.

In our analysis of data in our email security solutions, Proofpoint detected over 48 million malware samples last year that could have been used to launch ransomware.

**How Proofpoint stops ransomware**

It’s important to note that Proofpoint would have detected and blocked the messages shown above from delivery.

Proofpoint is the only vendor that provides an end-to-end, integrated solution to combat ransomware. We’ve built multilayered detection techniques to defend against constantly evolving threats. Known malicious documents are blocked automatically, while unknown attachments are analyzed and sandboxed, overcoming attempted evasions like password-protected documents, attachments with embedded URLs and zip files.

The machine learning components of URL and attachment protection are trained by our unmatched data set that comes from global scale and our deployments protecting the number one threat vector at more of the Fortune 100, Fortune 1000 and Global 2000 than any other security provider.
Threat actor tracking in Targeted Attack Protection (TAP)

Proofpoint recently released a new feature within TAP called Threat Actor Tracking. It helps you understand the dynamics of threat actors, their objectives, techniques and tools, and the people they’re targeting. You can also see how specific threat actors’ behaviors change over time based on how they are targeting people within the organization.

This visibility can help you ‘know your enemy’ - to know the ransomware gangs that may be targeting your people. For example, if a threat actor targets a specific user or group of users in your organization, you would know who those users are and who the threat actor is. And you’d be able to understand the following, as well:

- Objectives (e.g., trying to gain access to endpoints, collect user credentials, deploy ransomware)
- Techniques (e.g., Office VBA Macro, HTML, PowerShell)
- Attack progression (e.g., whether that click was blocked or isolated, people targeted, who clicked, trends)

Threat Actor Reporting is a free upgrade in the Targeted Attack Protection (TAP) dashboard. Let’s take a look how this feature appears in the TAP Dashboard.

To get started, go to threatinsight.proofpoint.com. From there, choose the “Reports” button on the left-hand side and then choose the “Threat Actor Tracking” tab inside the dashboard.

First, we’ll click on the “Reports” button located on the left and then click on the Actor tab above.

We’ve sorted based on Attack Index score, rather than by volume. Why? Volume unto itself is somewhat useless in telling us the true impact of an attack. We’re much more concerned with a single, well-targeted Remote Access Trojan (RAT) from a sophisticated state actor than we are about a few hundred, relatively innocuous spams from a somewhat pedestrian small crime gang. The Attack Index reflects the relative impact by considering the actor, the ‘targetedness’, and threat type – in addition to volume.

Figure 3 shows us that the Attack Index is very high for TA3546, despite low volume, especially in comparison to the second actor listed, TA569. This report allows us to quickly see that this actor has targeted two VIPs and has only very recently begun activity focused on us.

We can see from Figure 4 that TA3546 is also known as FIN7, one of the most successful and dangerous financially motivated threat groups around for the past half dozen years. There is considerable background info on each actor, sometimes including IOCs and C2 detail.
If you’d like more details, please reach out to your account team, or just dive into the TAP dashboard.
THE FIRST STEP: INITIAL ACCESS LEADS TO RANSOMWARE

Overview

Ransomware attacks still use email -- but not in the way you might think. Ransomware operators often buy access from independent cybercriminal groups who infiltrate major targets and then sell access to the ransomware actors for a slice of the ill-gotten gains. Cybercriminal threat groups already distributing banking malware or other trojans may also become part of a ransomware affiliate network. The result is a robust and lucrative criminal ecosystem in which different individuals and organizations increasingly specialize to the tune of greater profits for all – except, of course, the victims.

Typically, initial access brokers are understood to be opportunistic threat actors supplying affiliates and other cybercrime threat actors after the fact, for example by advertising access for sale on forums. But for the purposes of this report, we consider initial access brokers to be the groups who obtain initial access via first-stage malware payloads and may or may not work directly with the ransomware threat actors.

Key findings

- Preventing ransomware today largely has shifted from a direct email threat to an indirect threat where email is only part of the attack chain.
- Ransomware threat actors leverage cybercriminal enterprises – largely banking trojan distributors – for malware deployment. These access facilitators distribute their backdoors via malicious links and attachments sent via email.
- Banking trojans were the most popular malware distributed via email, representing almost 20% of malware seen in Proofpoint data the first half of 2021.
- Proofpoint currently tracks at least 10 threat actors acting as initial access facilitators or likely ransomware affiliates.
- Ransomware is rarely distributed directly via email. Just one ransomware strain accounts for 95% of ransomware as a first-stage email payload between 2020 and 2021.
- There is not a 1:1 relationship between malware loaders and ransomware attacks. Multiple threat actors use the same malware payloads for ransomware distribution.
These criminal threat actors compromise victim organizations with first-stage malware like The Trick, Dridex, or Buer Loader and will then sell their access to ransomware operators to deploy data theft and encryption operations. According to Proofpoint data, banking trojans – often used as ransomware loaders – represented almost 20% of malware observed in identified campaigns in the first half of 2021 and is the most popular malware type Proofpoint sees in the landscape. Proofpoint has also observed evidence of ransomware deployed via SocGholish which uses fake updates and website redirects to infect users, and via Keitaro traffic distribution system (TDS) and follow-on exploit kits which operators use to evade detection.

Proofpoint has unique visibility into initial access payloads – and threat actors that deliver them – often used by ransomware threat actors. It is important to note ransomware is not the only second-stage payload associated with the identified malware. In addition to email threat vectors, ransomware threat actors leverage vulnerabilities in software running on network devices exposed to the internet or insecure remote access services for initial access.

Map of the ransomware ecosystem

Proofpoint currently tracks around a dozen threat actors likely operating as initial access brokers, and many of the email threat campaigns distributing malware loaders observed by Proofpoint have led to ransomware infections. Confirmation of actor collaboration between access brokers and ransomware threat actors is difficult due to threat actors working hard to conceal their identity and evade detection. It is possible that initial access brokers and malware backdoor developers directly collaborate with – or operate as – ransomware-specific threat actors.

Initial access facilitators

The versatile and disruptive malware Emotet previously served as one of the most prolific distributors of malware enabling costly ransomware infections between 2018 and 2020. However, international law enforcement disrupted the malware in January 2021, wiping out its infrastructure and preventing further infections.

Since the Emotet takedown, Proofpoint observed consistent, ongoing activity from The Trick, Dridex, Qbot, IcedID, ZLoader, Ursnif, and many others in our data serving as first-stage malware payloads in attempts to enable further infections, including ransomware attacks. Proofpoint tracks these malware families under the “banking” family. Over the last six months, banking trojans were associated with more than 16 million messages, representing the most common malware type observed in our data.

Additionally, Proofpoint tracks downloaders such as Buer Loader and BazaLoader that are often used as an initial access vector for ransomware attacks. In the last six months, Proofpoint identified almost 300 downloader campaigns distributing almost six million malicious messages.

Proofpoint researchers track backdoor access advertised on hacking forums from various threat actors. Depending on the compromised organization and its profit margins, access can be sold anywhere from a few hundred to thousands of dollars. Access can be purchased with cryptocurrency, most commonly bitcoin.

Proofpoint observes overlap between various threat actors, malware, and ransomware deployments. Our data and third-party reporting indicate for example, Conti ransomware has been associated with multiple first-stage loaders including Buer, the Trick, Zloader, and IcedID. IcedID has also been associated with Sodinokibi, Maze, and Egregor ransomware events.

First-stage ransomware

Proofpoint still sees ransomware distributed via email directly, as attachments or links in email, at considerably lower volumes. For example, in 2020 and 2021 Proofpoint identified 54 ransomware campaigns distributing just over one million messages.

Of these, Proofpoint identified four Avaddon campaigns containing about a million messages in 2020, representing 95% of the total. In May 2021, the U.S. Federal Bureau of Investigation released details on an increase in Avaddon activity, noting the ransomware operators obtained initial access via remote access portals such as RDP and VPN, a pivot away from direct email access. This operational shift is consistent with Avaddon campaigns observed in Proofpoint data. Other ransomware leveraging email directly as an access vector and have appeared in Proofpoint data this year include Hentai OniChan, BigLock, Thanos, Demonware, and Xorist.
How hackers hunt

Ransomware threat actors currently carry out “big game hunting,” conducting open-source surveillance to identify high-value organizations, susceptible targets, and companies’ likely willingness to pay a ransom. Working with initial access brokers, ransomware threat actors can leverage existing malware backdoors to enable lateral movement and full domain compromise before successful encryption.

An attack chain leveraging initial access brokers could look like this:

1. A threat actor sends emails containing a malicious Office document
2. A user downloads the document and enables macros which drops a malware payload
3. The actor leverages the backdoor access to exfiltrate system information
4. At this point, the initial access broker can sell access to another threat actor
5. The actor deploys Cobalt Strike via the malware backdoor access which enables lateral movement within the network
6. The actor obtains full domain compromise via Active Directory
7. The actor deploys ransomware to all domain-joined workstations

Figure 2: Ransomware volumes as a first-stage malware
So far in 2021, Proofpoint continuously observes email-based threats including downloaders and bankers with multi-stage payloads that often lead to ransomware infections. The threat actors are conducting extensive reconnaissance, privilege escalation, and lateral movement within the environment before manually deploying the ransomware payload. One key metric to watch is dwell time. Over the last two years, multiple public reports from incident response companies point to a decrease in the amount of time threat actors spend within an environment before encryption activities. Some incidents are reporting two-day infection timelines between initial access and ransomware deployment compared to reported averages of 40 days in 2019.

Short dwell times, high payouts, and collaboration across cybercriminal ecosystems have led to a perfect storm of cybercrime that the world’s governments are taking seriously. In response to recent high-profile ransomware attacks, the United States government proposed new efforts to combat ransomware, and it was a hot topic at the 2021 G7 conference. It is possible with new disruptive efforts focused on the threat and growing investments in cyber defense across supply chains, ransomware attacks will decrease in frequency and efficacy.
The move to remote work and accelerated adoption of cloud applications has many IT security professionals playing catch up to secure their users and applications...
Proofpoint’s David Knight, EVP and GM Cloud Security Group, and Elad Horn, VP Product Management Cloud Security, sat down at Protect 2021 to discuss how Proofpoint’s cloud security technologies work together to provide secure access, stop threats, and enforce DLP in today’s work from anywhere world.

Here, we look at the key takeaways from that discussion and dive into the many features of Proofpoint’s cloud security platform.

What’s changed in a “work from anywhere” world?

Though many organisations are now well accustomed to hybrid setups, they are still a relatively new development. What’s more, in the rush to support such environments during the height of the pandemic, cybersecurity was often not the priority it should have been.

The result is a vast potential attack surface with users accessing networks and data from different locations at different times. All protected by a patchwork of solutions built to be “good enough”.

The challenge now is implementing a cyber defence strategy fit to protect disparate and hybrid workforces in the long term.

“We now have our employees working from anywhere, accessing data everywhere – in the cloud, on the web, behind the firewall. And this has fundamental implications on our security architectures for both threat protection and DLP. And we need an entirely different approach.”

David Knight, EVP and GM, Cloud Security Group, Proofpoint

The parent and baby analogy

Cybersecurity could once have been analogous to a parent protecting a baby. The parent sets up a playpen – the perimeter – ensuring that nothing harmful gets in and nothing valuable gets out.

While this may have been apt once upon a time, today, protecting an organisation is more like protecting a teenager.

You need to understand the risks they are exposed to outside the safety of the perimeter and equip them with the tools and the knowledge to keep those threats at bay.

So how exactly do you achieve this in the world of cybersecurity?

Firstly, you need to monitor your users wherever they are, gaining total visibility into their activity. Next, you need to educate them on how to defend against modern threats – phishing, social engineering, malware and the like.

Finally, you need to reassess your risk model. The days where anything outside the perimeter is bad and anything inside is good are over. You now need the tools to spot signs of malicious or suspicious activity wherever it happens.

This is only possible through people-centric controls. Here’s how Proofpoint can help.
The Proofpoint Cloud Security Platform

Cloud App Security Broker (CASB)

Proofpoint CASB helps you secure applications such as Microsoft 365, Google Workspace, Box, and more.

“CASB is the heart of our cloud security architecture.”

David Knight

CASB gives you people-centric visibility and control over your cloud apps, so you can deploy cloud services with confidence. Our powerful analytics help you grant the right levels of access to users and third-party add-on apps based on the risk factors that matter to you.

<table>
<thead>
<tr>
<th>People-centric visibility</th>
<th>Risk-Aware Data Security</th>
<th>Third-party Apps Controls and Shadow IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gain insight into cloud usage at global, app and user level</td>
<td>Stop employees from sharing sensitive company data broadly or with personal accounts</td>
<td>Define or automate actions based on analysis results for each app</td>
</tr>
<tr>
<td>Identify SaaS files at risk, including ownership, activity and who they were shared with</td>
<td>Speed up securing PCI, PII, PHI and GDPR compliance data with built-in smart identifiers and templates</td>
<td>Create policies for privileged users, defining read and write permissions for an access token</td>
</tr>
<tr>
<td>Check suspicious logins, activity, and DLP alerts via drill-down dashboards</td>
<td>Uncover orphaned and compromised accounts to protect corporate data</td>
<td>Deny a request from an app that exceeds defined thresholds</td>
</tr>
</tbody>
</table>

“More than 2,500 customers have connected their cloud APIs into our CASB, which gives us great visibility into the cloud threat landscape. Now combine that with the threat intelligence that you get from our protection suite, and it explains why we are the best in the market today in compromised account protection.”

Elad Horn
Proofpoint Web Security
Proofpoint Web Security protects users from all types of internet-based threats by applying dynamic access controls, advanced threat protection and data loss prevention policies.

“Proofpoint web security allows you to control web access and protect from malware and phishing using embedded Proofpoint threat protection.”

Elad Horn

Web Security uses a people-centric approach to protection regardless of where the users are or what network they belong to.
Proofpoint Zero Trust Network Access (ZTNA)

As applications move to the cloud and workers are increasingly mobile, enterprises need a better alternative for access than traditional VPN. Proofpoint Zero Trust Network Access (ZTNA) leverages a software-defined perimeter for cloud-delivered secure remote access to resources in the data centre and the cloud.

“With ZTNA, end users only see the applications and services they’re entitled to based on integration with their directory service. This is a people-centric approach to securing internal applications. We’re very excited about it, and we have a number of customers who have seen great value from it.”

David Knight

next generation
VPN alternative

Granular Access: Reduce exposure by granting each user explicit access to specific applications. The rest of the network is hidden from view.

Convenient User Experience: Enable access to authorised applications with a single, always-on connection wherever they are located. The cloud-native, encrypted overlay network features global PoPs to optimise performance.

Central Management and Total Visibility: The cloud-delivered secure access solution frees up IT from managing rules and troubleshooting problems across appliances in multiple locations.

API Automation: Automate cloud-related network workflow from policy definitions through dynamic access assignments, egress rules and more.

Secure Remote Access for Contractors

Reduced risk: Create an identity- and context-based boundary around applications and enforce a customised policy for each device.

Unauthorised resources are invisible, reducing the potential attack surface.

Application-specific access: Define policies and associate contractors with specific applications and services rather than providing access to entire network segments.

Easy onboarding: Manage remote access policies to all enterprise resources in the data centre or the cloud from a single cloud console.

Protect demo: Real-time DLP & access Governance for cloud apps
HOW IS YOUR ORGANIZATION BEING ATTACKED?
WHO IS BEING TARGETED?

Identify who the highly attacked users are in your organization and protect them against the threats they're most vulnerable to.

Request your Very Attacked People and Threat reports
https://go.proofpoint.com/VAP-Threat-Reports.html
INNOVATION:
Announcing new Endpoint Data Loss Prevention (DLP) capabilities:
Prevention and data classification

NIRAV SHAH
Staff Product Manager
Proofpoint
Data doesn’t move, people do. And your users – who could be negligent, compromised or malicious – interact with your sensitive data every day. Have you struggled with preventing people from exfiltrating sensitive data? You are not alone. Security teams around the globe are worried about losing intellectual property and sensitive business information on top of regulated data loss.

With insider threats on the rise, it’s more important than ever to get right the balance between the preventing of data loss risks and the pain of blocking legitimate business activities. We’ll discuss how our visibility and prevention capabilities help you get the balance right between risk prevention and business enablement.

**Enhanced Endpoint DLP capabilities and smoother incident response workflows**

Today, we’re excited to announce our enhanced Endpoint DLP capabilities which detect sensitive data movement and prevent such movement or exfiltration to USB devices attached to the endpoint. These features will be available to you with no change to your current workflow if you are an existing Proofpoint Insider Threat Management (ITM) SaaS customer.

Over the last year, many customers have expressed the complexity of tackling data loss through manually correlating disparate alerts and incomplete visibility from unconnected solutions. They ran the risk of catching potential data exfiltration late or leaving major gaps of evidence in insider investigations. That’s why Proofpoint built its ITM and Endpoint DLP within a modern, scalable, cloud-native information protection platform, shared with CASB and Email DLP under the Enterprise DLP suite.

**Microsoft Information Protection integration: increased data context, reduced alert fatigue**

Customers want to leverage their existing data classification to optimize their data loss and insider threat visibility and detection. Now, they can do that. Across the Proofpoint Enterprise DLP suite, including Endpoint DLP and ITM, we integrate with the customer’s Microsoft Information Protection (MIP) data classification. Classification labels provide more context about files.

When a file with a MIP label is downloaded to an endpoint, you can use the label to hunt for unknown risks, create rules for proactive alerting, and generate meaningful reports. We will detect MIP labels during any data movement, and optionally generate an alert using that label. This can be seen within the green box in the screenshot below.

**Figure 1:** MIP labels seen within the Explorations and Alerts tabs
On top of this visibility, you can detect the movement of sensitive data using new alert rules and conditions. For example, you may only want to detect the movement of data from your corporate CRM system if classified with sensitive labels and by specific user groups. The Proofpoint rule editor allows you to adapt an existing alert with two additional Boolean statements to select the relevant user groups and specify the labels to be tracked.

In the example below, you see a critical level data exfiltration rule for a specific classification label, “Company Confidential”, and for users within a specific business unit. Given the criticality of this alert, you will get a notification within one of your Slack channels and within your SOAR.

---

**Prevention of sensitive data movement to USB devices**

Customers can now prevent sensitive data movement to USB devices when the data movement is clearly out of policy or if a malicious user is trying to hide their tracks. You can define lists of permitted and prevented values for users, file extensions and devices. In addition, you can protect files from being exfiltrated to USB based on source URL or file content using MIP classification labels. The prevention rule will block the exfiltration even if the user attempts to first rename or in any way manipulate the file.

In this simplified example, the security team used our prevention rule template to specify the type of activities (“file write”), user groups (“domain users”), MIP classification labels (multiple, critical labels specific to the organization) and non-corporate USB devices (“sandisk”, “2Wire”, “3Com”). Once the rule is in place, the user will be blocked from moving files that meet the rule conditions with a simple blocking message.
Figure 4: Blocking message to the end-user

In the past, security teams had to get creative around blocking USB device usage either by blocking the USB hardware port or use legacy, heavyweight and productivity-sapping DLP solutions. With our proven lightweight endpoint agent and patented file driver, we provide prevention capabilities without creating more headaches for security teams.

Common use cases for MIP labels and USB prevention

Here are a few common use cases for detecting and preventing sensitive data movement:

- **User groups:** Prevent users, who’ve given their notice, from copying sensitive files from specific locations onto USB devices

- **Classification (MIP) label:** Prevent any file marked as confidential based on the MIP label from exfiltration through unlisted USB devices

- **Reduced alert triage:** Focus on detecting exfiltration of data marked as sensitive through MIP labels rather than all data downloads from sanctioned sites such as SharePoint or Salesforce

The start of the year has already been a busy time with a bounty of new product features. We look forward to rolling out additional endpoint DLP and ITM features in our platform and making your organizations more secure in this rapidly changing world.
Over the past year, chats and virtual calls through platforms like Microsoft Teams have almost entirely replaced in-person, workplace interactions. With travel restrictions leading to an abrupt drop in business travel, collaborative sessions with geographically dispersed groups have moved online. Teams grew from 20 million users at the end of 2019 to 145 million daily active users by April 2021.

Teams brings together meetings, chat, calls, collaboration, third-party apps and business processes into a seamless experience as people communicate, collaborate and co-author content. But adopting a powerful tool like Teams without governance presents risks – from security risks like data loss to regulatory compliance risk due to not capturing, retaining or supervising content appropriately.

ITIR CLARKE
Manager, Product Marketing
Proofpoint
Recent Proofpoint innovations, like our Advanced Data Loss Prevention and our Content Capture for Microsoft Teams, can help you mitigate data loss and comply with retention and supervision rules as you roll out Teams.

**Proofpoint’s advanced DLP for Microsoft Teams**

As employees share sensitive messages and files, you must protect regulated data such as personally identifiable information (PII), protected health information (PHI) and payment card industry (PCI) data to ensure compliance. You must also monitor sharing of confidential content such as source code, design documents, legal documents or engineering documents to protect your organization from internal and external threats seeking to steal or compromise that information.

Proofpoint Cloud App Security Broker (CASB) can help on both fronts. Proofpoint CASB is now a certified for Teams Data Loss Prevention (DLP) provider. Organizations can now use Proofpoint CASB to:

- Achieve near real-time Microsoft Graph APIs for Teams DLP. Proofpoint’s solution provides an additional option for DLP in Teams beyond the DLP capabilities in Microsoft 365. Apply DLP action to Teams messages as well as files shared in chat, channels and meetings
- Leave behind “tombstones” after removing sensitive content to notify and coach Teams users of a DLP violation
- Apply Microsoft Information Protection sensitivity labels to files and monitor the handling of confidential documents in Teams and across other cloud apps

Proofpoint CASB is also an integral part of the Proofpoint Information Protection Platform. The platform is a new people-centric approach to protecting against data loss across email, cloud apps and endpoints. It bridges across all DLP channels using a common data classification framework.

Combining content-, user behavior- and threat-based telemetry with sophisticated analytics, the Information Protection Platform addresses the full spectrum of data loss scenarios of malicious, negligent and compromised users. With our unified alerts and investigations interface, your security and compliance teams can better prioritize alerts, respond faster and achieve a shorter time to value.

**Capture and archive digital communications with Proofpoint Compliance Platform**

Proofpoint is also a certified Microsoft partner for compliant content capture and archiving for Microsoft OneDrive, Exchange Online and Yammer – available on the people-centric Proofpoint Compliance Platform. The platform enables end-to-end regulatory compliance, e-discovery, and supervision across more than 30 digital communications platforms.

“In today’s distributed work environment, Microsoft Teams enables employees to stay connected and productive,” said Hammad Rajjoub, Director, Product Marketing, Microsoft Compliance Ecosystem at Microsoft Corp. “The integrations with Proofpoint help ensure that our joint customers can address security and compliance needs while enabling employees to work from anywhere.”
How has the pandemic changed your industry?

Jasmine kicked off the conversation, asking – over the past 12 months, what shifts in behavior have you witnessed, specific to financial advisors and their client relationships?

“The shift has been the acceleration in the need for social media. So, where we had advisors who maybe were five or 10 years away from retirement they thought, you know, ‘I don’t need to embrace digital or social tools because I’m going to be retiring. They are now finding that, ‘Oh, no. I really did actually need to embrace all of those technologies.’” Maria Ringer, Wells Fargo

This is typical of a wider cross-industry trend. While the move to digital communication has moved at pace in recent years, the pandemic has rapidly accelerated this area of transformation.

The days of customers leaving voicemails or waiting a day for a response to an email are numbered. Wells Fargo’s advisors and others like them must now be present in digital spaces, ready to respond and engage with their customers.

Merrill Lynch’s Sima Patel echoed this sentiment.

“We made a big push in this direction. If we can’t meet in person and can’t have events anymore, we have to lift all the other efforts in terms of how to reach our clients. And social media was one of those big ones. Not just for maintaining existing relationships, but to grow the business.”

How are you staying compliant in the digital space?

Naturally, increasing use of digital channels brings with it concerns around compliance. Training is key in allaying these fears.
This training must be comprehensive, ensuring all users understand not just how to operate in the digital space, but also their responsibility in keeping their organisations and their clients safe.

Sima Patel: “Training is everything. We learned that very quickly. You go in thinking social media is common, everybody knows what they’re doing. But that’s not the case. It’s highly nuanced – especially in such a regulated world.”

Both Sima and Maria reflected the need for training to be tailored to those on the receiving end. Any effective training programme must not only account for a user’s skill and awareness level but also for their day-to-day circumstances.

Maria Ringer: “We try to bring the training to where the advisor is. I think for a long time we tried to train the advisors to move more towards social and digital. And they just weren’t there yet. So, now we’re trying to frame our training around how social is not other. Digital is not other. It’s complementary to what you are already doing.”

So, how do such heavily regulated businesses keep compliance teams on board when moving in such a fluid and fast-paced space like social media. The answer is collaboration – as early in the process as possible.

Maria Ringer: “The big thing for us has always been collaboration. We have to bring in our compliance partners right in the forefront. I probably talk to our compliance, risk and legal teams every day.”

Sima Patel: “Get everybody around the table as early as possible, and make sure that the team can think and brainstorm. Nothing’s really set in stone. Everybody has to be able to adapt quickly.”

What’s next for digital compliance?

Social media does not stand still. Myspace makes way for Facebook. Facebook makes way for TikTok – and so on. How are those in regulated industries preparing for faster, more real-time social networks? And do they always need to move with the times?

Naturally, any decisions require thorough consideration, with many factors coming into play. For Maria and Wells Fargo, any move into a new space needs clear business justification.

“We get pinged all the time about Instagram… and everybody wants to be on TikTok. But is the juice worth the squeeze? Is there technology that we need to sustain a new social media platform that we’re managing? Do the regulations need to evolve to support it in the future as well?

We’ve been using and defining this evaluation criteria over the last few years, and we’ll really utilise it over the next three to five years. To continue to ask, ‘does this new social network align with that evaluation criteria?’”

But as the digital realm continues to evolve, so too must the regulations policing its use. As digital media becomes more instantaneous, organisations must find a compliant way to operate in this world. Something that could prove challenging in the years ahead.

Sima Patel: “Live video and even podcasting – it’s interesting. In our world, anything real-time makes things hard. We can’t just send an advisor off to record whatever on their phone and publish it. It needs to be reviewed. It needs to be blessed by a lot of people.”

Regardless of the challenges it presents, the pace of digital transformation is unlikely to slow any time soon. And organisations and regulators alike will have little choice but to adapt.

Sima Patel: “It’s an evolving space. I think that it’s going to be hard for us to look the other way.

Watch the interview:
Compliance in a post-pandemic world

https://www.proofpoint.com/uk/resources/videos/protect-2021-compliance-sessions

As the public health landscape changes, employees are going to start returning to offices. Yet the move to remote work has altered the way we work, and many of the repercussions are likely here to stay. Watch this video to hear how Maria Ringer, VP, WIM Social Media Program Manager, Wells Fargo and Sima Patel, Director of Digital Wealth Management, Merrill Lynch are planning for compliance in the post-pandemic era.
How Proofpoint helps you stay compliant and secure on Microsoft Teams

Earlier this year, much of the world moved to remote work. And companies turned to chat and collaboration apps to sustain productivity. Microsoft Teams alone saw 70% growth in users over six weeks this spring.
Communication tools like Microsoft Teams are key for keeping businesses operating during this crisis. But they are not immune from risk, whether it’s security and compliance risk from data exfiltration or regulatory compliance risk if the content isn’t captured, retained, or supervised.

Recent Proofpoint innovations help you mitigate data loss and comply with retention and supervision rules as you roll out Microsoft Teams.

**Mitigate people-centric compliance risk with Content Capture for Microsoft Teams**

Compliance risk starts with people. With Proofpoint Content Capture, compliance teams can rest assured that they are capturing and managing the content that employees create on the channel.

Our connector captures text-based content as well as multimedia: images, emojis, attachments and more. Our people-centric approach makes this content easy to search and supervise with a few key steps:

- Associate each message with an identity at the organization
- Capture the message together with conversational context, including metadata, threading information, and contextual details such as previous posts in a conversation
- Deliver the content and context to your repository, whether it is the Proofpoint Enterprise Archive or a third-party product.

**Capture, manage and track your digital communications with Content Capture**

Content Capture features 30+ connectors. These cover a wide set of the most popular communication platforms used within organizations. You get a single solution for capturing and managing your digital communications, including:

- Chat and collaboration apps
- Social media
- Text messaging
- File sharing applications
- And more

**Supported platforms include (but are not limited to):**

- Slack
- Microsoft Teams
- Zoom
- LinkedIn
- Twitter
- Facebook
- WhatsApp
- Bloomberg

With optional add-on products, we offer more compliance benefits that are unique in the market. You can pair Content Capture with Compliance Gateway to ensure that captured content is received by downstream services. While its accuracy is reconciled upstream via manifest from the original source (see next page).

And of course, it is easy to pair Content Capture with the full Proofpoint compliance suite to gain even more benefits across Microsoft Teams and other communication channels. This suite includes the award-winning Enterprise Archive, Intelligent Supervision and more. The full solution offers end-to-end compliance risk protection under a single pane of glass.
A people-centric approach to Data Loss Prevention (DLP) for Microsoft Teams

With the shift to remote working and increased adoption of collaboration tools like Microsoft Teams, it is more apparent than ever that people are the perimeter. Data loss also originates from people. They can be negligent, they can be compromised by an external threat actor, or they can be malicious for financial or political gain.

Proofpoint Cloud App Security Broker (CASB) extends our people-centric security and compliance to Microsoft Teams. CASB combines content, user behavior and threat telemetry for cloud apps to detect compromised accounts and monitor data handling. This allows you to address the full spectrum of people-centric data-loss scenarios comprehensively. With CASB, you can:

- Address the full range of data risk from negligent, compromised and malicious users
- Shorten time to discover and protect regulated cloud data with out-of-the-box DLP policies to stay in compliance with PCI, PII, PHI and GDPR
- Deploy consistent DLP across email, cloud apps and endpoint as part of Proofpoint’s people-centric Enterprise DLP solution
- Simplify day-to-day operations by unifying DLP incident management across multiple cloud apps and channels

Cross-platform integrations across advanced email security, security awareness training and CASB help you identify how users pose risk to your organization. Then you can segment your employees according to their risks and apply appropriate security and compliance controls for each group. This process helps you focus and prioritize your resources based on risk.

**CASB-supported cloud applications include (but are not limited to):**

- Microsoft 365 including Teams
- G Suite
- Slack
- Salesforce
- Box
- Dropbox
- ServiceNow
- Amazon Web Services
- Microsoft Azure
- Okta

The benefit of Content Capture + Content Patrol is the intersection of monitoring & remediating social media and enterprise collaboration tools for compliance, risk reduction, internal policy, brand reputation and regulatory requirements, all converging through a single platform.

You can also free up valuable resources by streaming review and approval workflows for social profiles. Integrations with social media publishing tools mean less resistance from advisors, who can continue to use the same tools they do now and our reports provide the data you need to demonstrate compliance to auditors.

Automatically detect compliance risks in real time across interactive social contact such as posts, comments, and replies, and limit damage by removing or editing problematic content right away.

**New features include:**

- New UI - Improved and more efficient review across large content in a dashboard framework.
- Classifications System - Documentation is now embedded for each classifier (e.g. “promissory” or “profanity”, etc.). Over 170+ classifiers
- User Management – Unlike competitive solutions where accounts are mapped to a user name (user identity), we offer a people centric view. User Management allows customers to automate identities by policies or provisioning (each channel account). A more 3-Dimensional view vs. Linear.

Content Patrol

With Content Patrol, you can monitor social media at scale and remediate risky content in real-time. You can manage the unique risks associated with these public channels while enabling employees to connect with customers.

Quote from Michael Rutty, Proofpoint PMM Compliance: “Proofpoint’s largest deployments of Content Patrol indicate that not only are Compliance buyers looking to reduce risk with Social Media. There is a significant need emanating from within internal Marketing departments, as well as HR and internal lines of business (LOB) looking to support compliance, as well as vanguard a corporate online presence, control outbound messaging, preserve brand reputation and mitigate risk.”
Ensure regulatory compliance with NexusAI machine learning

One of the most “must-attend” events at this year’s PROTECT EMEA 2021 explored the topic of machine learning and AI in compliance.

Reviewing false positives can be a major time drain. That’s why security teams across industries are always looking for ways to ensure efficient, intelligent regulatory compliance.

During the session, Proofpoint’s Director of Product Marketing, Rick Dales, and Director of Product Management, Dan Rapp, gave their view on the current state of play.

Below is an overview of their discussion, along with the key features of Proofpoint’s NexusAI Machine Learning offering.
Supervision is a growing challenge for financial services firms. We are seeing a growing set of data types and data sources, with volumes of communication increasing. On top of this, there is constant regulatory pressure to do a better job at detecting real issues – with a fixed set of resources.

Then there is perhaps the most considerable challenge – false positives.

Almost 90% of the review queue these days is false positives. And getting through them takes time. A lot of time.

It’s only natural then that people would start to ask whether machine learning can help streamline this process. After all, supervised machine learning is basically the art of classifying items by finding common characteristics between those labelled as a given type and those that aren’t labelled as that type.

The problem with doing this at scale successfully is that you need lots of examples of the problems you’re looking for. Those examples have to be similar to one another, and be different enough from everything else that the system can learn to tell the difference.

So, for example, if you are detecting disclaimers, you can build a model to find those – because most disclaimers have common characteristics. The same is true when finding newsletters or customer complaints.

But when adapted for something like insider trading, you begin to run into problems. Here, the type of inappropriate activity is so diverse, and it’s very rare to find smoking guns. So, it’s incredibly hard to build working models.

There’s a potential regulatory issue here too. FINRA’s guidance talks about having a model risk management program when trying to adopt new technologies. So, you have to do upfront model validation and think about how you’re going to carry out ongoing testing to ensure that that model remains correct and is applying the right decisions.

Essentially, you need to be able to explain, at least at the highest level, how the model works and its decision-making process. And, ultimately, you need some layer of human review.

Any solution must also integrate with your existing compliance program. So, what does that look like?

It starts by capturing all the data because you can’t monitor what you don’t have access to. That data is then stored in a compliant repository so that it can be monitored. And on top of this is supervision, which can be grouped into three areas.

You need a detection engine to identify the things that need to be looked at by a reviewer. You need an efficient review workflow that recognises that in a large organisation, you don’t have one big pool that everyone pulls from. And you need extensive reporting to monitor the progress of your review workflow and make sure you’re remaining as efficient as possible.

It’s not easy for machine learning to layer on top of this. But the NexusAI compliance solution is more than capable.

It supports the detection engine by detecting issues in a better way and by providing guidance on how to tweak the configuration of your existing capabilities. And on the workflow side, Nexus AI takes the place of some of your reviewers by siphoning out the obvious false positives.
Exploring NexusAI models

NexusAI for compliance optimises the configuration of supervision administrators by identifying disclaimer text and identifying senders of low-risk content. By doing so, the system avoids future flagging of false positives.

It also significantly automates the review process by auto-clearing, or auto-escalating flagged messages using secondary scoring. This drastically reduces the time spent in review of false positives that arrive in the queue. In many ways, the AI model acts as a member of the supervision review team – like a super-fast and incredibly consistent employee.

To give a little more detail on the process, the machine learning model takes messages in the review queue, looks at them paragraph by paragraph and identifies disclaimer text. It then feeds back to the intelligent supervision system and allows that disclaimer text to be presented as a suggestion to the supervision administrator. By observing commonalities, this disclaimer detection model allows the removal of that class of false positives in the future.

In the screenshot to the right, you’ll see example of NexusAI model scoring and the resulting actions that could be taken if thresholds are met, all within the context of Proofpoint Intelligent Supervision.

NexusAI also works to exclude senders by analysing the messaging that flows through intelligent supervision, looking out for low-value and low-impact content like newsletters, web advertisements, and automated system notifications. If, over time, it identifies that a given sender is only sending that type of content, it suggests that this sender could safely be excluded from the supervision process.

In these cases, suggestions are reviewed and approved or rejected by administrators. But once integrated in the configuration, these types of messages and classes of false positives will no longer show in the review flow.

Finally, there is review automation – one of the most complex areas of machine learning and compliance. In this instance, a given message that has been flagged for review will be looked at by the NexusAI compliance system. The system then scores that message – for ease, let’s say between zero and 100.

If a message scores close to zero, the machine learning model is highly confident that it is not a violation for the policy type that’s in play. The messages scored on the higher end are deemed by the model with a high degree of confidence to be a violation of policy.

We provide the model with a couple of configuration points – one on the auto-clear end of the scale and one on the auto-escalate end. When the configuration threshold is set and a message comes in below it, it will automatically be removed from the review queue. Likewise, if a message comes in and it’s deemed to be over the higher threshold, it is automatically escalated. To counter incorrect reviews and avoid issues with compliance, every new model is initially deployed in evaluation mode.

In this mode, the model scores a message, records that score, and passes it to the supervision system. The supervision system acknowledges the review but takes no action. This information is used to generate reports and decide on appropriate scoring thresholds. Once a threshold has been determined, the model is enabled. Only then will it begin auto-clearing or auto-escalating issues. However, even when enabled, messages suspected of being incorrectly reviewed must still be reviewed by supervision staff. So, you can continuously evaluate the performance of the model.

**Figure 1:** Screenshot of Nexus AI scoring and outcomes
Discover NexusAI for Compliance and rise above low-value supervision content

To get to meaningful content that can help you mitigate risk, you first need to plough through low-value content and disclaimers. This costs you time, money and effort. Proofpoint NexusAI for Compliance can help significantly reduce these false positives by using machine learning, giving you:

**Augmented supervision**
Extend your existing Proofpoint deployment with machine learning to significantly reduce low-value supervision content.

**People-centric compliance**
Combine advanced supervision with Proofpoint capture, archiving and e-discovery solutions to mitigate risk.

**Continuous improvement**
Train solutions on new scenarios relevant to your business, improving accuracy and machine learning model performance over time.

Protect demo:
Proofpoint Compliance Platform powered by NexusAI
https://youtu.be/VrX-3zZ4S4s
(N.B. This video contains more than just Nexus AI info)
Learn about roadmap innovations directly with our executive team

Meet our executive team and find out about our new products and services though our virtual Executive Briefing Centre.

Request a session to join now
https://go.proofpoint.com/virtual-EBC.html
RISKY BUSINESS IS ONE OF THE LONGEST-RUNNING AND MOST INFLUENTIAL INFORMATION SECURITY PODCASTS. EVERY WEEK, HOST PATRICK GRAY COVERS THE LATEST INDUSTRY NEWS AND SITS DOWN WITH EXPERTS IN THE FIELD TO PICK APART ALL THINGS CYBERSECURITY...
At this year’s Protect EMEA event, Patrick was joined by Paige Adams, Group CISO at Zurich Insurance, and David McLeod, VP and CISO at Cox Enterprises.

The panel discussed a host of issues currently facing our industry. Below are the key takeaways from their discussion.

**Skill gaps**

**Patrick Gray:**

This is not necessarily a new trend, but COVID has certainly worsened it – there are just not enough people to go around. So, how does the CISO address this? There may not be enough talent out there, but you still need to get your job done.

**David McLeod:**

Absolutely. I saw a recent ISC squared survey that found 42% of people working in cyber have less than three years of experience – and only 13% have a foremost cyber education. Around ten years ago, we hit a tipping point where there were too many computers and too much data. This leads to more demand for people.

To address it, you’ve got to make your own talent management engine. To figure out how to take on tools that create people leverage. Proofpoint is really good at that. Their threat intelligence dashboards are probably the most popular we’ve used in the last four years.

You also need to be able to find cyber potential anywhere. Many come out of IT as they have the technical understanding. But you also need to recruit teenagers, peers from other departments, and more.

**Paige Adams:**

It’s a universal problem. I think we’re all feeling this crunch of not enough people and not enough skills. And technology can solve problems for you, but it sometimes requires a lot of care and feeding.

One of the projects that I’ve been focusing on in my team over the last year or two is being diligent about quantification of the value that our tools are bringing. In the past, we tended to focus on the acquisition cost or the life cycle maintenance costs, but we didn’t necessarily factor in the people costs that it takes to acquire the skills.

Now, we’re investing more in things like automation because we want our tools and platforms to be multipliers and enablers. And because people and skills are in such short supply, I want a platform that can take my one smart analyst and multiply them times five.
Attracting new talent

PATRICK GRAY:
So, what needs to happen to solve that talent shortage? Do you think it involves universities? Do you think it involves private training courses or mentorship programs? How do you think we can keep feeding that pipeline and get more skilled people into this industry?

DAVID MCLEOD:
Simply put, teach it sooner and teach everyone. University can’t solve this. It doesn’t take four years to become an expert. Let’s get it into high schools. Let’s make it available to anyone, any age, any field.

PAIGE ADAMS:
Yes. I think we know it’s not going to be just one thing. It’s a holistic approach. But we definitely need to get the education out there and start younger.

There’s been a lot of talk about encouraging people that maybe wouldn’t traditionally be attracted to a STEM education. We need to do more too on diversity and inclusion. It’s a huge untapped resource.

We also need to focus on apprenticeship programs. Not everybody needs a four-year degree in computer science to go and be an effective security analyst. So, if we can look at non-traditional paths, that’s going to be a key way to get people in the door.

Ransomware

PATRICK GRAY:
Ransomware is everywhere right now – and it feels like particularly over the last six months that it’s got out of hand. So, I can’t imagine it’s currently difficult for you to get management buy-in to do things like build out programs that are designed to stop ransomware.

PAIGE ADAMS:
Yes, absolutely. My organisation is well aware of the risk. There have been a number of ransomware incidents that have hit pretty close to home. CNA, for example, recently paid a $40 million ransom.

These things catch people’s attention. If you’re a board of directors or senior management, you’re thinking, “Am I going to be in a position where I’m going to have to pay out a $40 million ransom?” Of course, nobody wants to be in that position. So, it makes you a little bit more amenable to wanting to invest more in your cyber capabilities. There’s a huge reputational piece, too, in the insurance business. Because we stake our reputation on trust, and we want to be able to demonstrate that we can protect the data that our customers trust us with.

That said, we’re beyond the days now where security is just a black hole you throw money into. So, yes, people are more willing to invest in it, but they really want to see the results.

Cloud evolution

PATRICK GRAY:
Are you noticing that a lot of our prior mistakes are following us into the cloud ecosystem? Earlier in the cloud movement, it was a more restrictive environment, and people couldn’t do really dumb things. But now, because we’ve needed to make it a bigger tent, it’s so much more configurable, so much more powerful, and there are so many more opportunities for bad things to happen.

DAVID MCLEOD:
I completely agree. If I put out a hundred workloads last year, I now have the ability to put up 4,000 workloads automated to serve a fast-moving business with the same error in it. So, it’s absolutely true. It’s a complexity problem.

PAIGE ADAMS:
A lot of companies rely on legacy IT, and when starting down the cloud path, there is a lift and shift mindset. So, you’re taking everything you have on-prem, including your problems, your security issues, and putting them in the cloud.

It’s a missed opportunity when migrating from on-premises to the cloud, to refactor your applications, rebuild things from scratch and take advantage of SaaS capabilities, containers, microservices, and all those things you can do in the cloud that you can’t or don’t do on-prem.
Changing regulation

PATRICK GRAY:
It feels like there’s momentum building in the United States for legislation that is going to be equivalent to GDPR. How will that affect cybersecurity?

DAVID MCLEOD:
For me, it’s going to mean that I have to scale up on information governance and life cycle management. Because I have to know where the data is to meet any particular notification or compliance requirement.

Separate from that, right after I finish talking to the lawyers about funds to stand up that program, then I’m going to go out to my big SaaS providers and say, “You guys already got this, right?” Because that’s why I bought SaaS, so I don’t have to worry about this everywhere.

PAIGE ADAMS:
GDPR is already a big concern. So, about a year and a half ago, we adopted the Zurich Data Commitment, which was our attempt to meet that high watermark.

After GDPR, we saw similar regulation coming, and, of course, we want to meet or exceed that. So, we established that as a global standard, with the expectation that even if we were in a jurisdiction that doesn’t have something as stringent as GDPR, we know it’s likely to be coming.

We’re starting to see some movement towards that in the US, with CCPA in California – although it’s not quite the same.

On that, I think that there’s a different attitude in general in the US around privacy. I still think that writ large privacy isn’t quite as big of a deal, or at least it’s not in the public conscious in the same way that it is in Europe. And I wonder if it’s going to take some major events to shake up things up.

Watch the interview:
Risky Business Live
https://www.proofpoint.com/uk/events/protect

Cybersecurity in a year that changed the world

Take a deep dive into how the recent global pandemic has changed the threat landscape, and what it means for the year ahead.

Read our Human Factor Report 2021
https://proofpoint.com/uk/resources/threat-reports/human-factor
Working back from ‘bang!’

SECURITY METRICS TO HELP CEOS ANSWER THE TOUGH QUESTIONS

For years, I’ve been on a quest to find the one effective security metric that chief information security officers (CISOs) can share with senior management and the board. Unfortunately, this singularly compelling metric has remained as elusive as the grail. And sadly, I’ve long given up on my Indiana Jones fantasies.

So, a little while ago, I decided to take a different approach to thinking about security metrics. I flipped the narrative, putting myself in the shoes of a CEO as they stepped up to the microphone to explain a security breach to an excitable crowd of reporters. My view is that this experience would most likely rate on a top five list of “things to avoid” for any CEO.

As security professionals, we can’t absolutely, 100% prevent attacks. But I thought if I could understand the questions a CEO might face, then I could build a series of metrics – and perhaps even a strategy – to ensure executives had robust, defensible answers during a crisis. And hopefully, these things would help protect the firm’s reputation and customer base, too.
Let’s work through some possible media questions and look at what information CISOs can provide to senior leadership to help ensure they can deliver solid answers:

1. **How did this happen?**

   The media will want to know how the breach happened. And in their response, many CEOs will roll out the phrase “a very advanced and sophisticated attack” – even when it’s anything but. However, that’s the key here. You need to be able to show your organization has taken care of the “usual” in terms of security, making it more likely that only an advanced and sophisticated attack could circumvent your robust security strategy.

   So, to help CEO’s supply that answer, you’ll want to arm them with independently validated evidence of your organization’s adherence to best practices, such as:
   
   - Certification to standards such as ISO27001, Cyber Essentials Plus, etc.
   - Recent bills of health from audits, regulatory reviews and red team tests.

2. **Why did this happen to you?**

   In search of the story, the media want an angle or reason why your firm has been affected. Your CEO doesn’t want to say it was because you were the weakest firm in your peer group. So, equip your CEO with sufficient details of the attack path, including:
   
   - Assurance relating to common cyber-hygiene factors such as up-to-date vulnerability management activities, involving patching, asset identification, anti-malware, security awareness training and email hygiene
   - Independent verification that the organization is in compliance with all relevant security policies and risk tolerances (see question 1).

3. **How long have you known about this?**

   Moving rapidly in these scenarios is perceived as best practice. Attacks that are undetected for long periods or slow responses to detected events can undermine confidence in the organization’s security controls and threat detection. To answer the above question from the media effectively, your CEO will need information about the discovery. Ideally, you should have:
   
   - A Security Operations Center (SOC) service running 24/7
   - Stats showing your “mean time to detection” and compare them to figures from peers and the industry so your CEO can discuss them with confidence.

4. **What data have you lost?**

   In the early days of any incident response, this can be a challenging question to answer. But rest assured, the question will come up. You can help your CEO address this question effectively by making sure they have:
   
   - Confirmation that the confidential data you hold is encrypted – this statement alone can defuse this question
   - Assurance about access controls, including least privilege, segregation of duties and timely updates of leavers and movers; this enables assurances regarding “limited data access” if the attack was via an account compromise.

5. **How will this impact your customers? The business?**

   This is another question with no defined answer. However, it’s also an opportunity to demonstrate that your organization was prepared for such an event and that a pre-existing plan is being put into place. In short, you’re not making this up as you go along. Provide your CEO with:
   
   - Knowledge of a documented incident response plan that is well-rehearsed and supported by external experts
   - Knowledge of well-documented and regularly tested business continuity plans that apply in these circumstances
   - Confirmation that the correct authorities have been advised of the event, in line with legal and regulatory requirements
6. Who was responsible for the attack?

This is yet another question where the media are likely to push for an answer that may, at best, be unclear. To help your CEO respond, give them:

- Assurance that your firm has a reliable threat intelligence program, which tracks threat actors who discuss or target your staff and brand
- Confirmation that the correct authorities have been engaged, in line with legal and regulatory requirements.

So, where does this exercise leave us? With a collection of measurement points and metrics that would be ideal to have to hand should the worst-case scenario occur. If we break them down into components and consider how to measure each one pragmatically, we end up with a table like this:

<table>
<thead>
<tr>
<th>Metric</th>
<th>Yes/No</th>
<th>RAG status</th>
<th>Policy compliance</th>
<th>% score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification status</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit and test schedule</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset identification and management</td>
<td>×</td>
<td>×</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability management</td>
<td></td>
<td>×</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Education and awareness</td>
<td></td>
<td>×</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Anti-malware</td>
<td></td>
<td>×</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Email hygiene</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24/7 SOC coverage</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mean time to detection of incidents, together with industry comparison</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% of sensitive data encrypted</td>
<td></td>
<td>×</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access control management</td>
<td>×</td>
<td>×</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident response plan</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business continuity plan</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection with authorities</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat intelligence program</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This is a great place to start building your executive-level metric set. If it becomes your monthly baseline, you’ll know you can provide insightful and useful security metrics to the CEO at a moment’s notice. That will be a great reassurance to all parties.

There are areas that would benefit from further focus – culture and behavior being a personal priority. However, this is where the individuality of each firm comes into play. So, assess your own industry and organization for particularly important and/or relevant metrics.

Finally, rework the “media interview” process in collaboration with your communications team and CEO to see what different questions they may expect. Then, use that information to inform and refine your core metric set. The model above isn’t flawless. But in my long quest to find perfection, I haven’t seen it. However, I have seen many CISOs worried by their own metric set, unsure if they’re doing enough or measuring what matters. This model aims to provide a solid foundation for security professionals to build upon with confidence and certainty.

---

**MOVING RAPIDLY IN THESE SCENARIOS IS PERCEIVED AS BEST PRACTICE. ATTACKS THAT ARE UNDETECTED FOR LONG PERIODS OR SLOW RESPONSES TO DETECTED EVENTS CAN UNDERMINE CONFIDENCE IN THE ORGANIZATION’S SECURITY CONTROLS AND THREAT DETECTION**

---

**Want to speak to a CISO directly?**

Our Proofpoint CISOs can review your metrics for you. Book a meeting today.

https://go.proofpoint.com/meet-with-a-CISO.html
ABOUT PROOFPOINT, INC.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations’ greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyberattacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.

NEW PERIMETERS

This magazine is provided as a statement of direction regarding our product development activities and is provided for discussion purposes only. It should not be relied upon in making a purchasing decision. The development, release and timing of any features or functionality for our products remains at Proofpoint’s sole discretion.