IDENTITY IS THE NEW ATTACK SURFACE

Break the attack chain with insight into your vulnerable and risky identities

Threat spotlight
Break the attack chain by detecting and preventing identity risk

Customer spotlight
Day in the life of a Business Information Security Analyst

Point of view
A CISO perspective on identity threat
The way we interact with corporate networks has forever changed and traditional perimeter security is no longer fit for purpose. ‘Work from anywhere’ is growing by the day, increasing reliance on cloud technology and leaving most organizations defending a disparate attack surface across locations, accounts and devices.

To infiltrate this vast network, cybercriminals do not need to breach the defences of an entire organization. They only need to compromise a single individual. In other words, identity is the new attack surface, and ultimately, your new perimeter.

Of course, attacks on individuals are not new. Recent years have seen heavy investment in tools to combat such threats, from Privileged Account Management (PAM) to Multi-Factor Authentication (MFA). But despite relatively widespread adoption of both, exploitable identity vulnerabilities are still present in one in six enterprise endpoints. This calls for a new set of tools tailored entirely to attacks on identity.

Identity Threat Detection and Response

To develop this new approach and ensure that Proofpoint can continue to offer innovative, advanced protection, we recently acquired Illusive, a market leader in Identity Threat Detection and Response (ITDR).

The resulting solution, Proofpoint Identity Threat Defense, is designed to detect, remediate and defend identity vulnerabilities. But, before you can place tools and protections where they are needed most, you must first understand the types of attacks you are defending against.

In this issue, discover how cybercriminals are attacking identities and how you can break the attack chain with insight into your risky and vulnerable identities.
We continue to use the term ‘people-centric’ to describe the modern threat landscape and the style of defence required to protect against it. Identity is now being used by threat actors to further their cybercriminal gains. Quite literally following a pattern, or an ‘attack chain’.

The threat actors start by targeting your people through attacks like credential phishing emails and by landing malware. Once they compromise an account, an identity, they win. They’re now inside your environment using that identity to move laterally through your organization to achieve their goals of ransomware or data exfiltration. Proofpoint Identity Threat Defense provides protection at this imperative middle section of the attack chain.

How are cybercriminals attacking identity?

Along with high-value targets such as administrators or finance contacts, modern threat actors also target great swathes of unmanaged and misconfigured identities that are often not afforded the same protections. This can include service accounts, local and shadow admins, cached credentials and many others that often slip through the net of privilege and password security tools.

By targeting identities like these, cybercriminals can bypass standard perimeter defenses with minimal effort or technical knowhow. And, as 87% of shadow admins are not enrolled in a PAM solution and 40% of shadow admins can be exploited in a single step, attacks of this nature are often successful. Very successful, in fact 84% of organizations fell victim to an identity-related breach in the past year (1).

Once an identity vulnerability is exploited, threat actors can move laterally through systems and networks, amassing intelligence, distributing malicious payloads and exfiltrating data.

The longer any malicious actor lays undetected, the greater their opportunity to traverse through identities – from privilege escalation to abuse of Active Directory and cloud environments. And the more potentially devastating the consequences.


(1) idsalliance.org/white-paper/2022-trends-in-securing-digital-identities
(2) proofpoint.com/us/resources/threat-reports/analyzing-identity-risks-air-research-report
Defending against such identity-focused attacks requires two distinct capabilities

Firstly, organizations must have the means to discover and fix identity vulnerabilities before they are exploited. And, as no single tool is 100% impenetrable, additional technology is required to detect and respond to identity threats and stop privilege escalation and lateral network movement.

Thanks to Proofpoint Spotlight™ and Proofpoint Shadow™ technologies, Identity Threat Defense can do both. Spotlight delivers unparalleled visibility into vulnerable identities by scanning directory structures, PAM solutions, endpoints, servers and services, revealing the gaps between the intention of your identity security policies and the reality of your environment.

Shadow is undefeated in over 150 red team exercises. It allows organizations to deterministically accelerate threat detection by identifying threats based on attacker interaction with deceptions, not probabilistic controls based on signatures or behaviours. So, with the acquisition of Illusive, Proofpoint has enhanced its market-leading threat and information protection platforms by adding proactive identity risk discovery and remediation as well as a robust post-breach defence capability.

The result is a unified solution that extends protection across the entire attack chain for critical threats like ransomware and data breaches, giving organizations unprecedented insights into their privileged access attack surface and helps security teams better protect those at most risk of attack.

Stop identity attacks in their tracks

Uncover value of Identity Threat Defense with our free assessment.

Proofpoint Identity Threat Defense discovers privileged identity risks on 1 in every 6 enterprise endpoints. Avoid dramatic compromise - discover and stop attackers before they move laterally in your organization.

Read more about breaking the attack chain with Identity Threat Defense on page 12.

Find out more in our SOLUTION BRIEFS

ILLUMINATE YOUR SECURITY BLINDSPOTS

Proofpoint Identity Threat Defense discovers privileged identity risks on 1 in every 6 enterprise endpoints. Avoid dramatic compromise - discover and stop attackers before they move laterally in your organization.
If the history of cyber threats has taught us anything, it’s that the game constantly changes: the bad actors show us a move. We counter the move. Then the bad actors show us a new one.

Today, that “new move” is the vulnerable state of identities. Attackers realize that even if the network and every endpoint and device are secured, they can compromise an enterprise’s resources once they gain access to just one privileged account. Within organizations, one in six endpoints has an exploitable identity risk, as noted in the AIR Research Report.\(^1\)

“Well, that escalated quickly.”

The 2023 Verizon DBIR Report 2023\(^2\) highlights the risks of complex attacks involving system intrusion and the need to disrupt the attacker once they are inside. “Once attackers have access to your environment, they will typically look for ways to escalate privileges, maintain persistence and locate paths to move across the organization to achieve their ultimate goal, whatever that may be.”

The problem has escalated because the management of enterprise identities, and the systems used to secure them, is quite complex. This complexity is further complicated by the constant changes made to accounts and their configurations.

Attackers are increasingly focused on privileged identity account takeover (ATO) attacks because they can compromise organizations much more easily and quickly this way, as compared to the time, effort and cost to exploit a software vulnerability (a common vulnerability and exposure or CVE). And we should not expect this trend to stop anytime soon, given that these ATOs have reduced attacker dwell times from months to merely days, with very little risk to attackers that they’ll be detected before completing their crime.

So, what should IT and security leaders and their teams do about this?

Take a “back to the basics” approach. Security teams work to protect their networks, systems and endpoints in their infrastructure, and have continued moving up the stack to secure applications. As identities have become the predominant attack vector, we now need to move to better protect identities. This makes for the foundational building blocks of a successful identity threat detection and response (ITDR) strategy, which is essential today (find out more about ITDR on page 12).

If we think of security in battle terms (as we often tend to do), identity is simply the next hill we need to defend. As we’ve done with the network, endpoint and application hills in the past, we should begin by applying good old-fashioned, basic cyber hygiene/security posture practices to prevent as much risk as possible. While there is value in both preventative and detective controls, preventative controls are preferred and are often less costly to deploy. In other words, as we take this next hill to secure identities, we should not forget that an ounce of prevention is worth a pound of cure.

Identity as a vulnerability management asset type

Organizations should consider managing the remediation of identity vulnerabilities (those most commonly exploited in today’s attacks) in the

\(^1\) proofpoint.com/us/resources/threat-reports/analyzing-identity-risks-air-research-report

\(^2\) verizon.com/business/resources/reports/dbir
A CISO perspective on identity threat

Compromised credentials and commandeered accounts can act as a skeleton key for your networks and corporate systems. With such a potentially lucrative reward on offer, cybercriminals are increasingly focusing their attacks squarely on your identities to unleash data exfiltration, take over IT environments and launch ransomware attacks.

YONESY NÚÑEZ
CISO, The Depository Trust & Clearing Corporation (DTCC)

The key factors for determining prioritization should include:
- The vulnerable asset’s importance to the business
- The threat likelihood of the vulnerability being exploited
- The strength and effectiveness of any compensating controls that mitigates the risk associated with the vulnerability.

Once these factors are considered, identity vulnerabilities associated with privileged identities often bubble up fairly high on the prioritization list. Privileged accounts can be used to create harm to the most important systems of a business. The threat likelihood of these accounts being exploited has increased as they’ve become the top focus of attackers. Additionally, since most ATOs go undetected, the risk of these vulnerabilities is clearly not mitigated by sufficient compensating controls.

Fortunately, many of the vulnerabilities discovered around these privileged identities are relatively easy to remediate, such as cleaning unsecured credentials off endpoints. Compare this to the effort associated with remediating software vulnerabilities (CVEs), for which remediation often requires costly potential code changes and the completion of full regression testing.

Identity vulnerability management is a compensating control for many un-remediated CVEs since many software vulnerabilities are leveraged to enable early tactics of an attack. Once attackers exploit these, they must still work to escalate privileges. As such, the remediation of identity vulnerabilities offers a compensating control for many un-remediated CVEs that, when left vulnerable, can stop the attacker from further progressing by escalating privilege.

Prioritizing remediation efforts across asset types including identity vulnerabilities

Since most organizations likely have millions of vulnerabilities across their different asset types, it is critical for vulnerability management efforts to be prioritized. Most vulnerabilities pose little risk for any number of reasons.

Proofpoint Spotlight™ provides this solution, enabling the continuous discovery of identity vulnerabilities, their automated prioritization based on the risk they pose, and visibility into the context of each vulnerability. Spotlight even enables fully automated remediation of vulnerabilities where the remediation creates no risk of interruption to the business.

Proofpoint Spotlight™ provides this solution, enabling the continuous discovery of identity vulnerabilities, their automated prioritization based on the risk they pose, and visibility into the context of each vulnerability. Spotlight even enables fully automated remediation of vulnerabilities where the remediation creates no risk of interruption to the business.

Identity is the New Attack Surface

Learn more and watch our cybersecurity experts discuss how IDTR can help your organization get ahead of identity vulnerabilities.

Watch the WEBINAR

Learn more and watch our cybersecurity experts discuss how IDTR can help your organization get ahead of identity vulnerabilities.
To gain a deeper understanding of how industry leaders are tackling this shift in the threat landscape, I recently participated in a webinar led by Proofpoint's Group VP Product Marketing, Tim Choi, and Group VP & GM Identity Threat Defense, Ofer Israeli.

We discussed why identity attacks are such a growing problem, the challenge of identifying vulnerable users and how to protect people and data from attacks leveraging compromised accounts.

**The ease offered by compromised identities**

Our industry uses the term people-centric a lot. We know that attacks are targeting people to launch ransomware or exfiltrate data. But, for today's cybercriminals, that is no longer the end of the matter.

Threat actors are now targeting people to compromise identities and then using those identities to further elevate their access and privileges. They then make lateral moves within organizations to gain intel, launch further attacks, and steal more data.

**Understanding high-risk identities**

Cybercriminals need to know two things to increase the chances of a successful attack: where is the data they want, and which identity will give them access to it.

Most of the time, the answer to the latter is a service account. There are not always protected in a privileged access management solution and often have access to many different files and systems with static passwords that can do nothing.

Regular users who are shadow administrators are also very high-risk identities. They’re not usually marked as privileged but have often inherited all kinds of access through complicated Active Directory group memberships, which are very hard to follow.

**Where are organizations most vulnerable to identity attacks?**

Most organizations have struggled with Identity and Access Management (IAM) for many years. Access has a way of becoming a living, breathing organism, so security teams need to make sure they understand what’s going on.

There are three main areas of concern: shared credentials, stored credentials and shared secrets.

Most users will have tens, if not hundreds, of usernames and passwords across various accounts.

And every are probably using credentials across at least some of them. This makes it easy for an attack, and those credentials can be sprayed across many more accounts.

When it comes to password leakage, organizations must be extremely careful with these service accounts, especially if they’re used in a distributed environment.

Unfortunately, many identity attacks originate from abuse by hacking, where cybercriminals get credentials from passwords dumped in data breaches and further use passwords to access corporate accounts.

**Protecting your identities**

Cybersecurity is like an arms race, and by the time we build a new control or defense mechanism, the bad guys have figured out a new way of circumventing it. That's what is happening right now.

There are plenty of statistics out there:

- There are plenty of statistics out there to prove that in a breach, attackers have a roughly 75% chance of becoming a victim.
- Attackers have begun to focus on compromised identities.
- Attackers are using compromised identities to enable data exfiltration, take over IT environments and launch ransomware attacks.

How [Proofpoint Spotlight™](https://www.proofpoint.com/us/resources/proofpoint-spotlight) and [Proofpoint Shadow™](https://www.proofpoint.com/us/resources/proofpoint-shadow) can help

Security is a layered defense, and Proofpoint Shadow™ can help. It gives you a new view of your environment and can dequote them into lateral movement. Shadow creates a hostile environment for cybercriminals by laying traps to deceive them into lateral movement.

Identities are a company's CROWN JEWELS

Attacker have begun to focus on compromised identities, and the largest breaches confirm this. To understand and remediate risky identities while taking steps to detect and deter privilege escalation and further harm to your data, systems and networks.

How Proofpoint Spotlight™ and Proofpoint Shadow™ can help
"The attacker only has to be right once. Defenders have to get it right every time."

This age-old saying has shaped countless cybersecurity strategies. The belief is that a single compromise of our defenses can lead to a catastrophic outcome. As new risks emerge and attackers develop tactics to evade our controls, defenders are burdened with the daunting task of safeguarding an ever-expanding array of connected identities. Many organizations are now embracing resilience strategies - it’s not a matter of “if” but “when” - accepting the inevitability of an incident.

The 3 best opportunities to break the links in the attack chain

First is stopping initial compromise. Preventing attackers getting into your organization through phishing, social engineering, imposter threats, business email compromise (BEC) and ransomware.

Aegis Threat Protection offers the best opportunity to stop the majority of these attacks.

Secondly, you must stop lateral movement. If an attacker does get in you have a small problem, but the attacker wants to make it a bigger problem by moving laterally and seeking identities that grant privileged escalation. They’ll try to get as much access as possible using Active Directory.

Identity Threat Defense provides visibility into identity attack paths to plant deceptions and prevent lateral movement and privilege escalation.

Thirdly, is the chance to protect data itself from loss or theft. Attackers will try to target valuable data and launch ransomware attacks. This is where information protection, insider threat management and data loss prevention solutions come into play.

Sigma Information Protection helps to defend data from data loss, accidental or otherwise.

Break the attack chain with Proofpoint Aegis, Proofpoint Identity Threat Defense and Proofpoint Sigma.
The enduring relevance of the attack chain in the evolving threat landscape

Since its inception in 2011, no other concept has captured the essence of successful cyberattacks quite like the attack chain (formerly known as the 'cyber kill chain'). Surprisingly, even after twelve years, the attack chain remains as relevant as ever, while defenders still struggle to prevent the most impactful incidents. One primary reason for this ongoing challenge is simple: defenders have been focused on the impossible task of protecting everything within their organizations. Instead, they should aim to neutralize the attacker's tactics, techniques, and procedures (TTPs) that cannot be easily replaced, effectively disrupting the completion of the attack chain.

**The challenge of initial compromise**

In today's dynamic threat landscape, cybercriminals employ an array of tactics to infiltrate organizations and inflict havoc on their cybersecurity. From the rise of Business Email Compromise (BEC) attacks to cloud account takeovers and ransomware infections, the frequency of such incidents continues to escalate. One trend is the exploitation of trusted third-party relationships to compromise organizations through their suppliers. What may appear as an innocuous initial email can rapidly escalate into a full-scale compromise, providing attackers unrestricted access to the organization's domain and enabling them to infiltrate email accounts for fraudulent activities.

Alarmingly, credential phishing emails leading to compromised accounts often evade detection, leaving behind no traces of compromise or evidence of malware. Even with the implementation of multifactor authentication (MFA), these attacks continue to surge. Once accounts are compromised either through a credential phishing email or malicious Remote Desktop Protocol access, organizations are faced with the next phase of the attack chain: privileged escalation and lateral movement within their networks.

**Detecting privilege escalation and lateral movement**

In the middle of the attack chain lies the threat actor's quest to breach an organization's defenses. Often, they accomplish this by compromising the identities of employees, contractors, service providers, or edge devices. Their primary objective is to leverage this initial access and elevate their privileges, typically targeting Active Directory (AD). AD, ubiquitous across organizations, is susceptible to compromise, granting attackers unparalleled control over the organization's computing infrastructure. This access gives them the ability to move laterally and spread malware intensively, causing even more harm.

**The risk of data loss**

Attackers don't merely rely on a single stroke of luck. Their success hinges on this series of precise maneuvers to achieve their ultimate objectives, often centered around monetary gains through data exfiltration. Once they have navigated through the intricate web of identities, they're able to target valuable data, skillfully orchestrating successful data theft operations. To counter the scenario of loss of intellectual property or customer identifiable data, we must disrupt this intricate chain of events so that defenders can gain the upper hand and steer the course of cybersecurity in their favor.

The best way to build a picture of the attack chain is to look at it in its entirety. The patterns become unmistakable: most initial compromises happen through phishing and compromised credentials, most privilege escalation and lateral movement happens through AD, and most data exfiltration happens through either those same compromised identities or the actions of an insider with that level of access already.

On the way to achieving their objective of data exfiltration, cybercriminals will have moved through your networks and systems from one identity to another, escalating their privileges as they go. A typical organization has almost infinite attack paths that result from the simple fact that AD connects almost every computing asset in the organization in practice. This could mean anything from using cached credentials on a compromised endpoint to finding a single server where the Domain User group is a local admin, enabling their tools for on-prem in that context, or innumerable other combinations.

How do attackers understand and choose between the multitude of attack paths available to them? In practice, it's often similar to how we navigate the real world—by using mapping applications. The same way you might use Google or Apple Maps upon arriving in a new city to find the quickest way from where you are to where you want to go. In the same way, cybercriminals will use conceptually similar tools (Bloodhound, Impacket, or Hping/Castle to name a few) to get to where they want to go, which is always the highest level of privilege in AD (Avam as a tier 0 entitlement, or simply Domain Administrator).

If an attacker gets into your ‘city’, you could remediate by closing roads to stop them getting where they want to go. But, if one road is used by your own people to real traffic flow, you can't do that. So, you need to set a trap wire on that road to detect attackers, what allowing your real traffic to pass through. Those traps could be deceptions or fake credentials which an attacker could use to log in to systems in your environment. When used, these will alert you when an attacker tries to use the road and with that visibility you can prevent the attacker from happening like ransomware or data exfiltration.

Ultimately, what really makes attackers insurable is when they can't get from where they are, to where they want to go. If they can't continue along the path their tools point them to, they'll give up and leave your environment.
Spotlight on Identity Threat Detection and Response (ITDR)

The role of ITDR solutions

To combat these escalating threats and safeguard organizational assets effectively, the adoption of proactive measures and comprehensive security controls is imperative. We must break the attack chain by implementing robust controls that block targeted phishing and malware attacks, swiftly detect and respond to account takeovers, identify and halt lateral movement, prevent privilege escalations, and fortify defenses against data exfiltration attempts.

Critical to breaking the attack chain is the utilization of Identity Threat Detection and Response (ITDR) solutions, which emerge as critical controls capable of thwarting attacks before they fully materialize into devastating incidents like ransomware or data theft. By actively monitoring and analyzing identity-related activities, ITDR solutions provide the necessary proactive defense measures to thwart threats at their earliest stages. Organizations can then effectively mitigate the risk of significant security breaches, safeguarding critical data and preserving operational continuity.

ITDR solutions scan each endpoint and identity repository to give both bottom-up and top-down views into risks related to unmanaged, misconfigured, and exposed identities. As a result, your security teams get the visibility required to take away the attack paths through Active Directory that are needed for attackers to deploy ransomware and steal large amounts of data.

In conclusion

By embracing ITDR and its associated practices, we empower ourselves to confront emerging threats head-on and ensure the resilience of our organizations in the face of ongoing identity-based challenges. With ITDR in combination with solutions in place across the attack chain that block initial compromise and tools to defend data, we are better armed to break the attack chain.

With identity as your new perimeter, you need a new set of tools to defend it. Proofpoint Aegis Threat Protection and Proofpoint Sigma Information Protection join forces with Proofpoint Identity Threat Defense to break the attack chain and provide a platform approach to protecting your people and defending your data.

The notable SolarWinds incident in 2020 was a grounding example of how threat actors get access to vulnerable environments and serves as a stark reminder of how we should be thinking about identities. While it is extremely challenging to prevent a well-resourced adversary from gaining initial access to an environment via a malicious software update or similar supply chain attack, the subsequent lateral movement, via Golden SAML, towards the ultimate target (often data in Microsoft 365) is much more detectable and preventable than the highly sophisticated method of initial compromise. Viewing the attack chain in its totality makes it clear where defenders should focus to mitigate the risk of similar incidents in the future.

As organizations embrace the pivotal role of identities in the cybersecurity landscape, the integration of ITDR solutions becomes paramount. By proactively defending against identity threats and investing in comprehensive identity management, organizations can holistically secure their environment and safeguard their most valuable assets. The rise of ITDR as a critical market category is a testament to the growing awareness of identity-centric risks and the collective commitment to bolstering defenses in an ever-evolving threat landscape.
Customer spotlight: Euan Doyle

A day in the life of a business information security analyst

The day-to-day experience can vary wildly from one security professional to the next. We may face similar threats and have many of the same tools at our disposal, but we’re shining a light on what the typical day looks like across the different job roles in the world of cybersecurity.

To kick off the New Perimeters job profile series, we spoke with Euan Doyle, a Business Information Security Analyst from Aberdeen, to discuss starting out, measuring success, and what makes up a ‘normal’ day. Here’s what he had to say:

Getting started in cybersecurity

I’m a musician. A bagpiper. It’s a strange one, I know, but that’s how I started my career. In a couple of years after leaving school, I taught and performed pipe music. But after finishing my music diploma, I knew that there are only so many hours in the week and only so many people you can teach, so perhaps I should look to learn another skill too.

It was my dad who suggested cyber. From my background, it looked interesting and seemed like an industry on the up and up, so I applied for a cybersecurity course at Robert Gordon University. At that time, I didn’t have much technical knowledge, but after a chance meeting with the head of the cybersecurity course on a university open day, I felt it was something I could potentially break into.

Within a few weeks, I had signed up to a five-year course with the option of a placement after the second year. Fast forward and here I am, 2 years into the job and I’ve just finished my third year at university. My work placement transitioned into a full-time role which I still balance with my full-time studies.

What does a ‘normal’ day look like?

No two days are ever the same. It’s common for people new to this role to ask, ‘what am I doing?’ and the honest answer is, they’re hard to define.

It depends on what’s going on in the business at that time and who you work with regularly. While we have great security tools in place to flag suspicious activity, a lot of the day-to-day experience can vary wildly from one security peer to another. We’ve got a shared spreadsheet that’s automatically tracked and always receive possible indicators internally from our ever-growing network of Security Champions. I just need to make sure that our email security and firewall security is all ticked off, blocked and managed.

Measuring success

Being part of the service organization forum means that we are constantly sharing information with our industry peers. We’ve got a shared spreadsheet that’s automatically tracked and always receive possible indicators internally from our ever-growing network of Security Champions. I just need to make sure that our email security and firewall security is all ticked off, blocked and managed.

A task I have grown into managing throughout my time here is the security training and phishing simulations across the company. Just yesterday, I issued approvals for a new training campaign that we were running for our operators team in Iraq. We aim to carry our largest team training quarterly in chatbot times, 20 minutes here and there, to try and keep people more engaged than once a year.

It’s usually a part of my day managing our external support teams and service providers, too. I manage our Security Exceptions process which involves vetting and approving requests from the business. For me, it’s a case of making sure we have the right information from our users, asking the right questions and finding out if there are possibly other, more secure, alternatives to providing a solution.

IOC-checks are always an ongoing task. We’re part of a service organization forum, so we often gather and share a lot of important information with our industry peers. We’ve got a shared spreadsheet that’s automatically tracked and always receive possible indicators internally from our ever-growing network of Security Champions. I just need to make sure that our email security and firewall security is all ticked off, blocked and managed.

As well as comparing ourselves to others, we also look back at how we have performed in these areas internally over the last few years to make sure we’re always improving.

We’re also passionate about data governance. We want to ensure our users understand risk, but also the appropriate management of company or client data, embed best practices and build an internal security culture from the ground up.

It’s like a football team. You’ve got 40,000 employees, and if one of them doesn’t follow what’s happening or business email compromise is, you’re at risk.

What advice would you give to anyone wanting a career in cybersecurity?

Firstly, I would say don’t worry if you don’t have a relevant degree. You can always take a CompTIA Security+ qualification, for example, to build your knowledge and get that start in the industry. If you do need or want to completely retrain, then rotational graduate roles over time can be a good option after completing a degree. Placements are also incredibly valuable, so if the opportunity to work whilst studying arises, I would always take it as early as possible. Networking is a must.

Ultimately though, it’s the insider knowledge that’s important. Learning all you can about the industry and your business is going to serve you better than any degree. So, if you have the opportunity to take on a junior cybersecurity role and work across different areas, absolutely take it. There’s nothing like learning on the job.

Whatever route you take, remember that you only know what you know in the moment, so, be honest about your understanding and don’t be afraid to ask questions.

So, get on LinkedIn, build connections, introduce yourself and ask questions. Ultimately though, it’s the insider knowledge that’s important. Learning all you can about the industry and your business is going to serve you better than any degree. So, if you have the opportunity to take on a junior cybersecurity role and work across different areas, absolutely take it. There’s nothing like learning on the job.

Whatever route you take, remember that you only know what you know in the moment, so, be honest about your understanding and don’t be afraid to ask questions.

If you could liken your role to a fictional spy or superhero, who would it be?

In the context of information security, it would have to be Sherlock Holmes. As soon as a phishing email comes through, just get Sherlock to find out who sent it!
Threat actors leverage numerous techniques to obtain account credentials for the simple reason that they open the door to a host of cyber attacks.

Ofer Israel
GVP & GM, Identity Threat Defense, Proofpoint

Without the need to break through perimeters, cybercriminals can lay in wait undetected, moving through networks, sowing multiple malicious payloads, exfiltrating data and targeting other high-value users along the way. As always, any effective defense against this style of attack requires an understanding of who is likely to be on the receiving end — your risky identities. These can be grouped into three categories:

Unmanaged identities
This includes service accounts that often go unmanaged by privileged access management as they were undiscovered during implementation. Another common unmanaged identity is the local admin. Set up to facilitate IT support requests, these identities are often forgotten after creation. Finally, many privileged accounts go unmanaged because they remained undiscovered during deployment.

Misconfigured identities
Shadow admins are commonly misconfigured due to the complexity of nested identity groupings, which can make it extremely difficult to see the complete rights and entitlements of all identities. As a result, shadow admins can be granted unintended excessive privileges.

Exposed identities
This category includes cached credentials, which are commonly stored on endpoints, memory, registry and disk, as they can be easily exploited.

Cloud access tokens stored on endpoints are also a common means for attackers to gain access to cloud assets.

Finally, remote application sessions may be improperly closed, allowing cybercriminals to compromise an open session and its privileges, often without the risk of detection.

While these are the riskiest identities in most organizations, it’s crucial to understand that any single identity can be compromised and should be protected accordingly. However, by gaining visibility into those most at risk, you can bolster training, tools and protocols where they are needed most.
Proofpoint Identity Threat Defense

A complete Identity Threat Detection and Response solution to defend and mitigate gaps in identity posture that can lead to exploitation.

More than half of surveyed enterprises had breaches because of exploited identities and credentials(1). Proofpoint Identity Threat Defense is undefeated in 150 red team exercises (and counting).

- Continuous discovery: discover and prioritize identity vulnerabilities.
- Automated remediation: automatically mitigate risks on endpoints and servers.
- Runtime detection: deploy deception for failsafe intruder detection.

Our preventative controls can discover and fix identity vulnerabilities before threat actors attempt to exploit them. At the same time, our detective controls alert security teams as soon as a threat actor attempts to compromise an identity.

As well as putting protections in place to keep cybercriminals out, our solution places lures to catch them should they get in. Planting deceptive content that only a threat actor would interact with gives your organization a viable and proven alternative to unreliable behavioral analytics for accurately detecting privilege escalation and lateral movement.

These tools and techniques combine to create an advanced solution that can prevent, detect and alert of attempted identity threats – and recover quickly from successful attacks before they can cause lasting damage.

(1) ESG Research: The Identity Security Paradox.

What Identities Are Risky Within an Organization?

**What are they?**
- Service Accounts
- Local Admin Accounts
- Shadow Admin Accounts
- Exposed Credentials & Cloud Tokens
- Legacy App Accounts
- Open Remote Desktop Sessions

**How are they risky?**
- Unchanged static passwords
- Full control over endpoint or server
- Unrecognized privileged access
- Accounts created in legacy systems
- Stored RDP session credentials

**Where do risky identities reside?**

- Service Accounts
- Local Admin Accounts
- Shadow Admin Accounts
- Exposed Credentials & Cloud Tokens
- Legacy App Accounts
- Open Remote Desktop Sessions
- Endpoints & Servers
- Enterprise Sessions
- Azure Active Directory

Illuminate your security BLINDSPOTS

Discover attackers and stop them before they move laterally in your environment. Proofpoint Identity Threat Defense discovers privileged identity risks on 1 in 6 enterprise endpoints.
Just as night follows day, cybercriminals get more creative with every passing year. In 2022, they focused their creativity firmly on the identities of your users.

In the face of greater adoption of security controls like multifactor authentication (MFA), threat actors had to find new and convincing ways to separate people from their credentials or convince them to unwittingly open the door to your organization by other means.

The result is a rapid rise in sophisticated identity-focused threats like MFA bypass and telephone-oriented attack delivery (TOAD), with the ultimate goal of account compromise.

What’s telephone-oriented attack delivery (TOAD)?

In a TOAD attack, targets receive a message often containing a fake invoice or alert. The message also contains a customer service number for anyone with questions. If the victim calls the number, they find themselves on the line with a cyber attacker.

At its peak last year, Proofpoint recorded over half a million attempted TOAD and MFA bypass attacks every day. So, it’s little wonder that account compromise was cited as a top concern by over a third of board members, behind only business email compromise (BEC).

Threats of this nature give cybercriminals a huge advantage, allowing them to circumnavigate protections that, up to now, have been trusted by many to protect users from common threats like phishing and credential theft. And once inside your organization, the veil of trust and privilege afforded by ‘legitimate’ accounts only serves to make matters much worse.

The State of the Phish: IMPROVING CYBER-RESILIENCE

Stop attackers gaining access to privileged identities

Take a discover, remediate and protect approach to identity risk management – make it difficult for attackers to evade your defenses.

Find out more about Proofpoint Identity Threat Defense

proofpoint.com/us/products/identity-threat-detection-response

Proofpoint

MATT CODE
Director, Cybersecurity Strategy, Proofpoint

THREAT UPDATE
ACCOUNT COMPROMISE

Just as night follows day, cybercriminals get more creative with every passing year. In 2022, they focused their creativity firmly on the identities of your users.

In the face of greater adoption of security controls like multifactor authentication (MFA), threat actors had to find new and convincing ways to separate people from their credentials or convince them to unwittingly open the door to your organization by other means.

The result is a rapid rise in sophisticated identity-focused threats like MFA bypass and telephone-oriented attack delivery (TOAD), with the ultimate goal of account compromise.

What’s telephone-oriented attack delivery (TOAD)?

In a TOAD attack, targets receive a message often containing a fake invoice or alert. The message also contains a customer service number for anyone with questions. If the victim calls the number, they find themselves on the line with a cyber attacker.

At its peak last year, Proofpoint recorded over half a million attempted TOAD and MFA bypass attacks every day. So, it’s little wonder that account compromise was cited as a top concern by over a third of board members, behind only business email compromise (BEC).

Threats of this nature give cybercriminals a huge advantage, allowing them to circumnavigate protections that, up to now, have been trusted by many to protect users from common threats like phishing and credential theft. And once inside your organization, the veil of trust and privilege afforded by ‘legitimate’ accounts only serves to make matters much worse.

The State of the Phish: IMPROVING CYBER-RESILIENCE

Stop attackers gaining access to privileged identities

Take a discover, remediate and protect approach to identity risk management – make it difficult for attackers to evade your defenses.

Find out more about Proofpoint Identity Threat Defense

proofpoint.com/us/products/identity-threat-detection-response

Proofpoint

MATT CODE
Director, Cybersecurity Strategy, Proofpoint

THREAT UPDATE
ACCOUNT COMPROMISE

Just as night follows day, cybercriminals get more creative with every passing year. In 2022, they focused their creativity firmly on the identities of your users.

In the face of greater adoption of security controls like multifactor authentication (MFA), threat actors had to find new and convincing ways to separate people from their credentials or convince them to unwittingly open the door to your organization by other means.

The result is a rapid rise in sophisticated identity-focused threats like MFA bypass and telephone-oriented attack delivery (TOAD), with the ultimate goal of account compromise.

What’s telephone-oriented attack delivery (TOAD)?

In a TOAD attack, targets receive a message often containing a fake invoice or alert. The message also contains a customer service number for anyone with questions. If the victim calls the number, they find themselves on the line with a cyber attacker.

At its peak last year, Proofpoint recorded over half a million attempted TOAD and MFA bypass attacks every day. So, it’s little wonder that account compromise was cited as a top concern by over a third of board members, behind only business email compromise (BEC).

Threats of this nature give cybercriminals a huge advantage, allowing them to circumnavigate protections that, up to now, have been trusted by many to protect users from common threats like phishing and credential theft. And once inside your organization, the veil of trust and privilege afforded by ‘legitimate’ accounts only serves to make matters much worse.

The State of the Phish: IMPROVING CYBER-RESILIENCE

Stop attackers gaining access to privileged identities

Take a discover, remediate and protect approach to identity risk management – make it difficult for attackers to evade your defenses.

Find out more about Proofpoint Identity Threat Defense

proofpoint.com/us/products/identity-threat-detection-response

Proofpoint

MATT CODE
Director, Cybersecurity Strategy, Proofpoint

THREAT UPDATE
ACCOUNT COMPROMISE

Just as night follows day, cybercriminals get more creative with every passing year. In 2022, they focused their creativity firmly on the identities of your users.

In the face of greater adoption of security controls like multifactor authentication (MFA), threat actors had to find new and convincing ways to separate people from their credentials or convince them to unwittingly open the door to your organization by other means.

The result is a rapid rise in sophisticated identity-focused threats like MFA bypass and telephone-oriented attack delivery (TOAD), with the ultimate goal of account compromise.

What’s telephone-oriented attack delivery (TOAD)?

In a TOAD attack, targets receive a message often containing a fake invoice or alert. The message also contains a customer service number for anyone with questions. If the victim calls the number, they find themselves on the line with a cyber attacker.

At its peak last year, Proofpoint recorded over half a million attempted TOAD and MFA bypass attacks every day. So, it’s little wonder that account compromise was cited as a top concern by over a third of board members, behind only business email compromise (BEC).

Threats of this nature give cybercriminals a huge advantage, allowing them to circumnavigate protections that, up to now, have been trusted by many to protect users from common threats like phishing and credential theft. And once inside your organization, the veil of trust and privilege afforded by ‘legitimate’ accounts only serves to make matters much worse.

The State of the Phish: IMPROVING CYBER-RESILIENCE

Stop attackers gaining access to privileged identities

Take a discover, remediate and protect approach to identity risk management – make it difficult for attackers to evade your defenses.

Find out more about Proofpoint Identity Threat Defense

proofpoint.com/us/products/identity-threat-detection-response

Proofpoint

MATT CODE
Director, Cybersecurity Strategy, Proofpoint

THREAT UPDATE
ACCOUNT COMPROMISE

Just as night follows day, cybercriminals get more creative with every passing year. In 2022, they focused their creativity firmly on the identities of your users.

In the face of greater adoption of security controls like multifactor authentication (MFA), threat actors had to find new and convincing ways to separate people from their credentials or convince them to unwittingly open the door to your organization by other means.

The result is a rapid rise in sophisticated identity-focused threats like MFA bypass and telephone-oriented attack delivery (TOAD), with the ultimate goal of account compromise.

What’s telephone-oriented attack delivery (TOAD)?

In a TOAD attack, targets receive a message often containing a fake invoice or alert. The message also contains a customer service number for anyone with questions. If the victim calls the number, they find themselves on the line with a cyber attacker.

At its peak last year, Proofpoint recorded over half a million attempted TOAD and MFA bypass attacks every day. So, it’s little wonder that account compromise was cited as a top concern by over a third of board members, behind only business email compromise (BEC).

Threats of this nature give cybercriminals a huge advantage, allowing them to circumnavigate protections that, up to now, have been trusted by many to protect users from common threats like phishing and credential theft. And once inside your organization, the veil of trust and privilege afforded by ‘legitimate’ accounts only serves to make matters much worse.

The State of the Phish: IMPROVING CYBER-RESILIENCE

Stop attackers gaining access to privileged identities

Take a discover, remediate and protect approach to identity risk management – make it difficult for attackers to evade your defenses.

Find out more about Proofpoint Identity Threat Defense

proofpoint.com/us/products/identity-threat-detection-response

Proofpoint

MATT CODE
Director, Cybersecurity Strategy, Proofpoint

THREAT UPDATE
ACCOUNT COMPROMISE

Just as night follows day, cybercriminals get more creative with every passing year. In 2022, they focused their creativity firmly on the identities of your users.

In the face of greater adoption of security controls like multifactor authentication (MFA), threat actors had to find new and convincing ways to separate people from their credentials or convince them to unwittingly open the door to your organization by other means.

The result is a rapid rise in sophisticated identity-focused threats like MFA bypass and telephone-oriented attack delivery (TOAD), with the ultimate goal of account compromise.

What’s telephone-oriented attack delivery (TOAD)?

In a TOAD attack, targets receive a message often containing a fake invoice or alert. The message also contains a customer service number for anyone with questions. If the victim calls the number, they find themselves on the line with a cyber attacker.

At its peak last year, Proofpoint recorded over half a million attempted TOAD and MFA bypass attacks every day. So, it’s little wonder that account compromise was cited as a top concern by over a third of board members, behind only business email compromise (BEC).

Threats of this nature give cybercriminals a huge advantage, allowing them to circumnavigate protections that, up to now, have been trusted by many to protect users from common threats like phishing and credential theft. And once inside your organization, the veil of trust and privilege afforded by ‘legitimate’ accounts only serves to make matters much worse.

The State of the Phish: IMPROVING CYBER-RESILIENCE

Stop attackers gaining access to privileged identities

Take a discover, remediate and protect approach to identity risk management – make it difficult for attackers to evade your defenses.

Find out more about Proofpoint Identity Threat Defense

proofpoint.com/us/products/identity-threat-detection-response

Proofpoint

MATT CODE
Director, Cybersecurity Strategy, Proofpoint

THREAT UPDATE
ACCOUNT COMPROMISE

Just as night follows day, cybercriminals get more creative with every passing year. In 2022, they focused their creativity firmly on the identities of your users.

In the face of greater adoption of security controls like multifactor authentication (MFA), threat actors had to find new and convincing ways to separate people from their credentials or convince them to unwittingly open the door to your organization by other means.

The result is a rapid rise in sophisticated identity-focused threats like MFA bypass and telephone-oriented attack delivery (TOAD), with the ultimate goal of account compromise.

What’s telephone-oriented attack delivery (TOAD)?

In a TOAD attack, targets receive a message often containing a fake invoice or alert. The message also contains a customer service number for anyone with questions. If the victim calls the number, they find themselves on the line with a cyber attacker.

At its peak last year, Proofpoint recorded over half a million attempted TOAD and MFA bypass attacks every day. So, it’s little wonder that account compromise was cited as a top concern by over a third of board members, behind only business email compromise (BEC).

Threats of this nature give cybercriminals a huge advantage, allowing them to circumnavigate protections that, up to now, have been trusted by many to protect users from common threats like phishing and credential theft. And once inside your organization, the veil of trust and privilege afforded by ‘legitimate’ accounts only serves to make matters much worse.
As always, tools and protocols can only do so much, so sustainable security habits are crucial. To avoid handing over the keys to your accounts, networks and data, every user in your organization must have the knowledge to detect and deter threats to their identity. 

**Inside MFA bypass and TOAD attacks**

MFA bypass and TOAD attacks have made waves across the threat landscape, delivering a wake-up call to anyone still of the belief that protections such as multifactor authentication are a cybersecurity silver bullet. While we have seen MFA bypass attacks in the past, its relatively recent adoption by phishing-as-a-service providers puts it in the hands of almost anyone, for less than the price of a coffee.

Whether buying off-the-shelf or launching direct, cybercriminals can bypass MFA protections in a number of ways. Many threat actors rely on fatigue, using compromised credentials to repeatedly request access to an account. This is the most common method. But as always, tools and protocols can only deter threats to your organization, its people and its data. So, any effective defence requires visibility into those people and their behaviours. You must first understand who is most likely to face these threats, so you can apply identity-centric policies to your high-risk users.

When it comes to protecting identity, the person behind that identity can very quickly become your last line of defence. To avoid falling victim to an MFA bypass, TOAD attack or any other type of account compromise, threat actors can very simply intercept existing email chains, amend payment information and defraud unwitting victims. And, once again, from phishing and password spraying to keyloggers and other malware, most are available to anyone with some ill will and a few dollars.

To compound matters further, you can still experience this kind of attack even if your credentials and identities remain safe and secure. Should one of your suppliers fall victim to an MFA bypass, TOAD attack, or any other type of account compromise, threat actors can very simply intercept existing email chains, amend payment information and defraud both organizations in the process – not to mention causing lasting damage to your working relationship. The threat-reports/state-of-phish of companies experienced this style of supply chain attack in the past 12 months.

**Building an identity-focused defence**

Tools, protocols and other protections are an absolute requirement when defending against any method of cyber attack. But as the techniques described above show, they cannot be relied upon entirely. When it comes to protecting identity, the person behind that identity can very quickly become your last line of defence. And they must be equipped with the skills to spot suspicious communications to launch additional attacks such as invoice fraud, drop communications to launch additional attacks such as invoice fraud, drop

**Account compromise – the cyber skeleton key**

Legitimate credentials are among the most highly prized targets of today’s cybercriminals – and it’s no hard to see why. Once an account is compromised, threat actors gain access to a treasure trove of information that can be used to profile victims and pursue further misadventures. Compromised passwords and, most importantly, the session and capture usernames, only need a victim’s phone number. The target phone receives a take on the line, they are issued further instructions, usually to download malware, sign in to an account via a spoofed page, enable remote access or transfer money. As this style of attack puts cybercriminals in direct contact with potential victims, and doesn’t rely on the intermediary of malware or a malicious URL to be clicked, security awareness and education is the only thing standing in the way of account compromise and a raft of subsequent threats.

With such a bounty on offer, it’s little wonder that cybercriminals are constantly honing their techniques to trick and defraud unwitting victims. And, once again, from phishing and password spraying to keyloggers and other malware, most are available to anyone with some ill will and a few dollars.

To compound matters further, you can still experience this kind of attack even if your credentials and identities remain safe and secure. Should one of your suppliers fall victim to an MFA bypass, TOAD attack, or any other type of account compromise, threat actors can very simply intercept existing email chains, amend payment information and defraud both organizations in the process – not to mention causing lasting damage to your working relationship. The threat-reports/state-of-phish of companies experienced this style of supply chain attack in the past 12 months.

**Building an identity-focused defence**

Tools, protocols and other protections are an absolute requirement when defending against any method of cyber attack. But as the techniques described above show, they cannot be relied upon entirely. When it comes to protecting identity, the person behind that identity can very quickly become your last line of defence. And they must be equipped with the skills to spot suspicious communications to launch additional attacks such as invoice fraud, drop communications to launch additional attacks such as invoice fraud, drop

**Account compromise – the cyber skeleton key**

Legitimate credentials are among the most highly prized targets of today’s cybercriminals – and it’s no hard to see why. Once an account is compromised, threat actors gain access to a treasure trove of information that can be used to profile victims and pursue further misadventures. Compromised passwords and, most importantly, the session and capture usernames, only need a victim’s phone number. The target phone receives a take on the line, they are issued further instructions, usually to download malware, sign in to an account via a spoofed page, enable remote access or transfer money. As this style of attack puts cybercriminals in direct contact with potential victims, and doesn’t rely on the intermediary of malware or a malicious URL to be clicked, security awareness and education is the only thing standing in the way of account compromise and a raft of subsequent threats.

With such a bounty on offer, it’s little wonder that cybercriminals are constantly honing their techniques to trick and defraud unwitting victims. And, once again, from phishing and password spraying to keyloggers and other malware, most are available to anyone with some ill will and a few dollars.

To compound matters further, you can still experience this kind of attack even if your credentials and identities remain safe and secure. Should one of your suppliers fall victim to an MFA bypass, TOAD attack, or any other type of account compromise, threat actors can very simply intercept existing email chains, amend payment information and defraud both organizations in the process – not to mention causing lasting damage to your working relationship. The threat-reports/state-of-phish of companies experienced this style of supply chain attack in the past 12 months.

**Building an identity-focused defence**

Tools, protocols and other protections are an absolute requirement when defending against any method of cyber attack. But as the techniques described above show, they cannot be relied upon entirely. When it comes to protecting identity, the person behind that identity can very quickly become your last line of defence. And they must be equipped with the skills to spot suspicious communications to launch additional attacks such as invoice fraud, drop communications to launch additional attacks such as invoice fraud, drop
GENERAL AUTO FINANCE COMPANY EXPANDS VULNERABILITY PROGRAM TO ENCOMPASS IDENTITY RISKS

CHALLENGES
Incorporating identity risks into their vulnerability management program
Legacy applications can’t be feasibly supported by their Privileged Account Management (PAM) solution
Lack of continuous visibility into their privileged identity risks

SOLUTION
Deployed Illusive to regularly scan for identity risk
Incorporated results into existing vulnerability management and remediation

RESULTS
New awareness of substantial identity risks
Immediate improvement in risk posture
More comprehensive vulnerability program now addresses the #1 attack vector

“The Illusive tool has opened up new insights. Without it we knew we should look into these identity risks, but we just didn’t have a way to do it.”

AVP IT Vulnerabilities

Proofpoint POWER Series
Powering up the security community to protect people and defend data.

Watch on-demand go.proofpoint.com/PowerSeries

CUSTOMER STORY
The company

A global provider of auto finance solutions. Working with consumers and auto dealers, they offer retail financing and lease programs, as well as commercial lending products to dealers to help them finance and grow their businesses.

The challenge

The company has a large and diverse IT infrastructure, and challenges with legacy applications. Although they’ve implemented a Privileged Access Management (PAM) solution, it didn’t protect many legacy applications – especially ones that were too costly to upgrade or were scheduled to be decommissioned. There were also service accounts and exception administrative accounts that couldn’t be vaulted. The result was that the company couldn’t fully control privileged credentials and identities, or even have good visibility into potential identity risks. This was true for both IT administrators and also regular users.

The solution

The company saw Illusive as a major expansion of their comprehensive vulnerability management strategy. Traditionally, the company’s approach to vulnerability management had been focused on common vulnerability and exposure (CVE) and common weakness enumeration (CWE). But they were aware that configuration missteps were also creating many potential risks, so they had started tracking those as well – basically anything in their environment that caused cybersecurity risk, regardless of whether or not it had an associated CVE. Using the ISO 7-layer model, as a guide, they reviewed their automated risk assessment approach to make sure it covered their entire IT environment – and identity risk management was the missing capability.

Driven by this realization, the company implemented the Illusive solution for identity risk management at the start of 2021. Illusive integrates with the company’s Active Directory (AD) infrastructure, and it also scans each endpoint regularly to produce a repository of identity risk findings, which the company retrieves using Illusive’s API. The IT security team reviews these findings and meets with the IT vulnerability remediation team regularly, where together they execute and track risk-reducing changes to their environment. It’s a collaborative effort and they do their best to work as a partner to IT.

Associated with their vulnerability remediation efforts are SLAs that vary depending on the level of criticality, so that more critical items are highly prioritized.

The results

Immediately after implementation, the company could see improvements in their risk posture. After using Illusive for over a year now, the company typically sees several new critical issues a week, and they resolve them quickly. It’s generally people not thinking rather than something malicious, just someone making a mistake or being in too much of a hurry.

“M&A is a great case – doing a scan before and after integration. With Illusive I can tell how clean their environment is, and the amount of technical debt.”

- SVP Global Cybersecurity Strategy & Operations

“If you have a large, on-premise infrastructure, where you’ve been using Active Directory for years, there are decisions made long ago, the forgotten landscape, where vulnerabilities often exist. There’s lots of technical debt also, cloud migration and M&A activity introduce complexity.”

SVP Global Cybersecurity Strategy & Operations

Based on the successes I’ve had, and knowing our direction, I would recommend this to everybody from a vulnerability standpoint. Being able to visualize everything – both traditional vulnerabilities and identity vulnerabilities and misconfigurations – that’s where this tool comes in.”

“It only takes one identity vulnerability, just one, to bring your entire environment down. Any way I can shine another light on something like that adds value, particularly when you can see the risk and be able to reduce it over time. There are hundreds of thousands of doors that are now locked – that’s huge.”

- SVP Global Cybersecurity Strategy & Operations
BANK ASSESSES IDENTITY RISK TO COMPLETE MERGER AND ACQUISITION (M&A) SAFELY

CHALLENGES
- Assessing the security posture of another bank they are acquiring
- Finding identity vulnerabilities - when they had no other solution
- Tight and inflexible deadlines for the closing of the acquisition

SOLUTION
- Deployed Illusive for a one-time assessment of the bank being acquired
- Comparison reporting against their own continuous assessments from Illusive

RESULTS
- Full identity assessment of the acquired bank in less than 30 days
- Discovered thousands of critical identity risks that were completely unknown
- Concrete, quantitative data persuaded executive team to delay full IT integration until issues were addressed

“I’M GLAD WE USED ILLUSIVE, EVERYONE SAW THE VALUE. IT’S A PLAYBOOK WE’LL CARRY FORWARD THROUGH THE NEXT M&A.”
Director of Cyber Security Engineering

The company
A bank holding company and its affiliates provide consumers, small and middle-market businesses, corporations, municipalities, and other organizations with a comprehensive suite of banking and other financial services.

“WE HAD AT MOST FOUR MONTHS, FROM THE ANNOUNCEMENT OF THE TRANSACTION TO THE CLOSING, TO EVALUATE THE OTHER BANK’S IT SECURITY POSTURE. WE NEEDED TO KNOW IF WE COULD TRUST THEM.”
Director of Cyber Security Engineering

The challenge
The company operates in an industry where consolidation is the norm. Over the last 20 years, the number of FDIC-insured commercial banks has dropped almost by half, primarily because of acquisitions. Each time this bank has gone through the process of a merger and acquisition (M&A), their IT department has needed to consolidate different systems, software, data, processes, and organizations. If any bank acquires an organization with a weaker IT security posture – or even one that’s unclear to them – it can put the company at risk. Conducting a security assessment is critical, and often it needs to be done under tight time constraints.
The rapid increase in identity-based attacks once again highlights the never-ending game of cat and mouse that persists between cybercriminals and security teams. As they adapt or augment a technique to breach our defences, we must implement a new tool or protocol to keep them at bay.

With the threat landscape evolving at such speed, it is not possible for a single security vendor to build a new solution for every style of attack, whether brand new or evolved. Instead, we must work with other providers to quickly complement our skills, experience and intelligence as required.

In some cases, as Proofpoint did with Illusive, this can be achieved through technology partnerships and technical integrations.

To find out what makes a partner the right match for Proofpoint and shine a light on what can be a long and complex process, we put six crucial questions to our Vice President, Strategic Alliances & Business Development, D.J. Long. Here’s a summary of what he had to say.

**Questions on the Power of Partnership**

**The solution**
Since identity security underpins their entire security posture, getting an understanding of potential identity vulnerabilities at the acquired bank was critical. As an Illusive customer, the acquiring bank was familiar with the solution and highly valued its insights:

"We’d been using Illusive to continuously scan our workstations for six months or more, so we were familiar with the insights it could provide." - Director of Cyber Security Engineering

With the help of the Illusive field engineering team, our customer had the acquired bank perform a wide-ranging identity assessment, a process which took less than 30 days from beginning to end.

**The results**
The Illusive evaluation of the acquired bank was critical in producing a risk scorecard comparing the two IT organizations, and in this case, there was enough risk to convince executives that the IT environments needed to be kept separate, at least initially. Although there were several identity risk areas, one quickly jumped out:

"The smoking gun on this was the number of domain admins on their workstations, 3000 of them! It just showed the state of their security hygiene. Anyone compromising one of those workstations would have had control of the whole environment. They didn’t know about it either, so they worked on cleaning that up." - Director of Cyber Security Engineering.

The overall results of the Illusive comparison were compelling.

"I’m glad we used Illusive. Everyone saw the value. It’s a playbook we’ll carry forward through the next M&A." - Director of Cyber Security Engineering.

In addition to M&A situations, the bank uses Illusive to continuously scan their own environment for identity vulnerabilities, as part of a complete solution for threat and vulnerability management.

"The Illusive evaluation of the acquired bank was critical in producing a risk scorecard comparing the two IT organizations, and in this case, there was enough risk to convince executives that the IT environments needed to be kept separate, at least initially. Although there were several identity risk areas, one quickly jumped out:

"The smoking gun on this was the number of domain admins on their workstations, 3000 of them! It just showed the state of their security hygiene. Anyone compromising one of those workstations would have had control of the whole environment. They didn’t know about it either, so they worked on cleaning that up." - Director of Cyber Security Engineering.

The overall results of the Illusive comparison were compelling.

"I’m glad we used Illusive. Everyone saw the value. It’s a playbook we’ll carry forward through the next M&A." - Director of Cyber Security Engineering.

In addition to M&A situations, the bank uses Illusive to continuously scan their own environment for identity vulnerabilities, as part of a complete solution for threat and vulnerability management.

"The Illusive evaluation of the acquired bank was critical in producing a risk scorecard comparing the two IT organizations, and in this case, there was enough risk to convince executives that the IT environments needed to be kept separate, at least initially. Although there were several identity risk areas, one quickly jumped out:

"The smoking gun on this was the number of domain admins on their workstations, 3000 of them! It just showed the state of their security hygiene. Anyone compromising one of those workstations would have had control of the whole environment. They didn’t know about it either, so they worked on cleaning that up." - Director of Cyber Security Engineering.

The overall results of the Illusive comparison were compelling.

"I’m glad we used Illusive. Everyone saw the value. It’s a playbook we’ll carry forward through the next M&A." - Director of Cyber Security Engineering.

In addition to M&A situations, the bank uses Illusive to continuously scan their own environment for identity vulnerabilities, as part of a complete solution for threat and vulnerability management.

"The Illusive evaluation of the acquired bank was critical in producing a risk scorecard comparing the two IT organizations, and in this case, there was enough risk to convince executives that the IT environments needed to be kept separate, at least initially. Although there were several identity risk areas, one quickly jumped out:

"The smoking gun on this was the number of domain admins on their workstations, 3000 of them! It just showed the state of their security hygiene. Anyone compromising one of those workstations would have had control of the whole environment. They didn’t know about it either, so they worked on cleaning that up." - Director of Cyber Security Engineering.

The overall results of the Illusive comparison were compelling.

"I’m glad we used Illusive. Everyone saw the value. It’s a playbook we’ll carry forward through the next M&A." - Director of Cyber Security Engineering.
What role do you play in forming new partnerships at Proofpoint?

My responsibilities fall into several different categories, one of which is to lead all our technology alliances and ecosystem partnerships. That includes relationships that we have with major partners such as CrowdStrike, Okta, SailPoint, Palo Alto Networks, CyberArk, and others.

I also run Proofpoint’s outbound OEM business that sees over 70 organizations work with our Emerging Threats Pro solution on a subscription basis. On top of this, I work on many business development activities through which we seek to establish relationships with third-party companies that fall outside the scope of our standard programs.

I am frequently approached by senior leaders from a wide range of companies that would like to work with us. So, part of my job is to qualify, frame, rationalise, and ultimately negotiate these new relationships on behalf of Proofpoint so we choose to pursue these.

How do you decide which partners are the best fit for Proofpoint?

There are four critical factors in establishing a new partnership.

The number one is customer demand. For example, last year, we formed a new partnership with Ping Identity primarily due to a customer request that we integrate its Identity and Access Management (IAM) solution with our CASB product. That’s just one example of several that I could cite that illustrate the importance of these partnerships with respect to responding to specific customer demand. Another illustration of this is the over 750 customers that we support with CrowdStrike. We also have over 1,700 joint customers with Palo Alto and a similar number with Splunk as well.

The second criteria is technical viability. Simply put, is it possible to use our APIs or the APIs of a third party to develop a solution that will exploit the risk of relying too heavily on CrowdStrike as an endpoint vendor partnership.

Ultimately, we were able to develop a solution with competitive differentiation and invest together in integrations that could serve a broader base of customers.

Finally, the fourth factor is an acknowledgement that there are no successful cybersecurity companies in the industry today that do not have a healthy, vibrant technology partnership ecosystem. And the reason for that is that no single cybersecurity company is capable of addressing all of the requirements of an enterprise customer.

So, to give our customers what they need, we must continue to form new partnerships and integrated solutions.

The third is the value of that joint solution. What improvements in threat prevention and management performance will our customers recognise, and what value does that provide?

At the same time, we need to consider the value of reaching a wider audience that would use this new solution in conjunction with Proofpoint solutions. For example, when establishing our relationship with SentinelOne, we had to consider that they were competitive with CrowdStrike. But at the same time, the partnership would help us to mitigate the risk of relying too heavily on CrowdStrike as an endpoint vendor partnership.

Any use case should be unique, competitively differentiated and able to add value to our customers. It should also enable us to exploit the functional capabilities of our products in conjunction with a third-party product.

A great use case example is the work we do with CyberArk. At Proofpoint, we can identify a company’s Very Attacked People (VAPs) through our Targeted Attack Protection (TAP) solution. This also gives us a degree of predictive intelligence around what type of attack they are likely to face and when it is likely to occur.

We can then share that VAP information with CyberArk, who provide Privileged Access Management (PAM) capabilities and elevate the rights associated with those VAPs, identity so that they have even more protection in the context of their use of their PAM solution from CyberArk.

When we agree to work with a vendor, how do we decide how deep to make the integration?

All relationships that we establish with vendors, whether new partnerships or expansions of current partnerships, are based on use cases. Very simply, this means defining how our products work together as an integrated solution and exploring the ultimate benefits to a customer.

The second criteria is technical viability. Any use case should be unique, competitively differentiated and able to add value to our customers. It should also enable us to exploit the functional capabilities of our products in conjunction with a third-party product.

A great use case example is the work we do with CyberArk. At Proofpoint, we can identify a company’s Very Attacked People (VAPs) through our Targeted Attack Protection (TAP) solution. This also gives us a degree of predictive intelligence around what type of attack they are likely to face and when it is likely to occur.

We can then share that VAP information with CyberArk, who provide Privileged Access Management (PAM) capabilities and elevate the rights associated with those VAPs, identity so that they have even more protection in the context of their use of their PAM solution from CyberArk.
Who are Proofpoint’s major partners in the identity space, and what do they bring to our clients?

When it comes to protecting the identity perimeter, our big partners are Okta and Ping for IAM, CyberArk for PAM and SailPoint for Governance.

Each integration allows us to provide our customers with the added security of knowing that their identity protections are being used in conjunction with their email protection. So, they get an added level of comfort that their email vector is being protected and augmented by integration with identity capabilities, giving an added layer of security that they otherwise wouldn’t receive.

Finally, where is your focus right now and what are you looking forward to over the next 12 months?

When we acquired Illusive, we inherited a nascent ecosystem of partnerships, as well as a number of previous integrations. So, one of my key objectives is to reinforce that ecosystem and leverage the unique differentiation that we can provide with integrated Identity Threat Detection and Response (ITDR) solutions in conjunction with what we’re doing with other partnerships.

Illusive was already working with some of our current partners like Palo Alto, Splunk and CyberArk, so I’m also working on ways to leverage our broader range of solutions with partners where we have pre-existing relationships, which will bring us even closer together and expand our addressable market even more.

Finally, we’re reinforcing and restructuring how Illusive worked with its partners to expand our ecosystem further. We’re already close to forming agreements with two of these companies, Tanium for endpoint security, and Infoblox for DNS technology.

DID YOU KNOW?

HERE’S A FEW COMMON TERMS THROUGHOUT THIS ISSUE EXPLAINED

Active Directory (AD)
Active Directory is a centralized database that stores information about users, computers, and other resources in a networked environment. It provides authentication and authorization services, allowing users to access resources securely.

Account compromise
Also known as account takeover fraud, is the process by which an attacker gains access to a user’s account. This can lead to a range of risks, including data theft, identity theft, financial fraud, and damage to the victim’s reputation.

Identity Threat Detection and Response (ITDR)
Technology to help prevent identity-related risks in your environment and detect real-time identity threats with automated remediation. Many of these risks result from ordinary business/IT operations and can go undetected by administrators whilst being exploited by attackers.

MFA bypass
A technique used by attackers to bypass multi-factor authentication (MFA) measures and gain unauthorized access to an account or system, typically through social engineering, phishing, or exploiting vulnerabilities in the MFA implementation.

Multifactor authentication (MFA)
To increase the security of user accounts, multifactor authentication (MFA) adds a layer of protection from hackers, an example of which is ‘two-factor authentication’ or 2FA. This is a process where you log into your account using not only your password (known credential) but also provide a secondary factor or code to confirm it’s really you, such as a token generated by a smartphone app or a biometric.

Privileged Account Management (PAM)
PAM is the practice of securely managing and monitoring user accounts with elevated permissions, to prevent unauthorized access, misuse, and potential security breaches.

Red team
A red team is a group of security professionals who simulate real-world attacks on an organisation’s systems and infrastructure to identify vulnerabilities and improve the organisation’s security posture.

TOAD attack
TOAD stands for ‘telephone orientated attack delivery’. In a TOAD attack, targets receive a message often containing a fake invoice or an alert requiring action. The message also contains a customer service number for anyone with questions. If the victim calls the number, they find themselves on the line with a cyber attacker.
USEFUL CONTACT DETAILS

If you would like to contribute to a future issue of New Perimeters, or to give feedback, contact:
info@proofpoint.com

To view the digital version of New Perimeters, visit:
https://go.proofpoint.com/New-Perimeters.html

Technical Training:
www.proofpoint.com/us/support/technical-training
training@proofpoint.com

Proofpoint University:
www.proofpointlevelup.com

Proofpoint Community Support:
www.proofpoint.com/community

Professional Services:
services@proofpoint.com

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 cyber attacks. Leading organizations of all sizes, including 75 percent of the Fortune 100, 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, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. Proofpoint.com

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.