

# NEW PERIMETERS

## DATA DOESN'T LOSE ITSELF

Identify insider risk and protect data with a people-centric approach

**proofpoint.**

### Threat spotlight

Is the new 'work from anywhere' reality hiding insider threats?

### Customer spotlight

Aircastle – Grounding Insider Threats

### Point of view

The link between ransomware and data loss prevention

# CONTENTS

## What is data loss prevention and why does it matter?

### SPOTLIGHT 1

- P4 Redefining Data Loss Prevention
- P8 Is the new 'work from anywhere' reality hiding insider threats?
- P12 What is Data Loss Prevention and why do you need it?
- P16 Top 10 data breaches of 2021



## What should good data loss prevention look like?

### SPOTLIGHT 2

- P23 The Three Pillars of Data Loss Prevention
- P27 Envisioning the future of information protection; assessing your current capabilities
- P30 Ransomware and data loss prevention; shifting from detection to prevention
- P32 Proofpoint acquires Dathena; Strengthens Enterprise Information Protection Offering

## How to implement data loss prevention

### SPOTLIGHT 3

- P34 Grounding Insider Threats with Proofpoint Insider Threat Management
- P38 The way we access data has changed; it's time to change the way we protect it too
- P40 How to implement people-centric data loss prevention for Microsoft Office 365
- P44 Taking a modern approach to data loss prevention
- P48 From manual to managed – the changing face of data loss prevention



## Magazine contributors

### Ryan Kalember

EVP, Cybersecurity Strategy, Proofpoint

### Mayank Choudhary

EVP and GM Cloud Security Products, Proofpoint

### Brian Reed

Product Evangelist, Proofpoint

### Ian Pugh

Senior Director, Information Protection at Proofpoint

### Jeremy Wittkop

Senior Director, Technology Services, Proofpoint

### Karen Letain

VP, Product Management, Proofpoint

### Andrew Rose

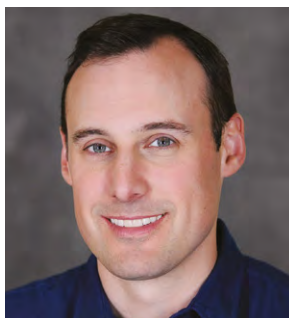
Resident CISO, EMEA, Proofpoint

### Itir Clarke

Manager, Product Marketing, Proofpoint

### Sophie Ree

Content Marketing Manager, EMEA, Proofpoint



# Welcome

---

WELCOME TO OUR FOURTH ISSUE OF NEW PERIMETERS – DATA DOESN'T LOSE ITSELF.

---

The ever-evolving threat landscape, along with our new 'work from anywhere' reality, means we are faced with new data protection challenges; how we gain visibility into and exercise control over how our most critical data moves and is accessed. In this issue, we'll explore why we must adapt to this new landscape by changing the way we prevent data loss and protect against insider threats.

## Data loss and insider risk in the new 'work from anywhere' reality

The global shift to hybrid working models has increased organizations' reliance on collaboration platforms and cloud technologies to maintain business continuity while employees are working from anywhere. In addition, organizations are creating and moving more data than ever. This in turn creates new forms of security risk for organizations, making it challenging to both understand when data is at risk and implement the proper control to mitigate that risk.

With the evaporation of the traditional network perimeter, the old way of protecting data doesn't work; we need to up our game and adapt data loss prevention (DLP) and insider risk solutions to protect the modern edge – endpoint, cloud apps, email, and the web.

## Data doesn't lose itself

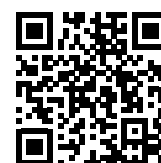
People lose data – it doesn't walk out of the door on its own. It's either stolen by an external attacker via compromised credentials, lost due to a careless user, or taken by a malicious employee, often to a competitor. It's important, now more than ever, to protect against insider threats by understanding context: What are users doing with information? What data do they have access to? How are they accessing it?

A modern approach to information protection must account for human behavior, whether in the office, at home, or in between. Unfortunately, legacy DLP and insider risk solutions fall far short in preventing, detecting, and investigating incidents in real time or immediately after they occur.

In this issue, we'll explore modern approaches to DLP that defend against new external and internal threats targeting your organization, its people, and your data.

## Find out more

If you'd like to find out more about any of the topics you read in this issue, please get in touch with your Account Manager, or use our online form to contact us.



Contact us  
[proofpoint.com/us/contact](https://proofpoint.com/us/contact)

RYAN KALEMBER  
 EVP, Cybersecurity Strategy  
 Proofpoint

# RED FINE LINE DATA LOSS PREVENTION

## A MODERN APPROACH FOR TODAY'S CHANGING WORKPLACE



Each of these real-world cases is unique. But they all resulted in data loss. Not to mention public-relations issues, remediation costs and the brand damage that comes with it.



While every setup is unique, one thing is always true: data doesn't move itself. People move, misuse and leak data. And while data loss may be the worst-case scenario, it is not the only potential consequence of poor information management.

**74% of finance  
leaders expect  
remote work  
to outlive the  
pandemic<sup>4</sup>**



## 85% of data breaches involve human interaction<sup>5</sup>

Compliance regulations are increasingly complex, and the penalties for non-compliance are more severe than ever before. Traditional data loss prevention (DLP) approaches are no longer up to the task. Solving this problem requires a new approach. One that is equipped to deal with the growing challenges of today's fast-evolving workplace and modern IT environments.

## 'Work from anywhere' is here to stay

The last few years have been a whirlwind of change for many organizations. An increasingly distributed workforce, new ways of doing business and a shift to the cloud have transformed the nature of work.

These trends have also made compliance much more challenging, especially for teams using security tools and processes built for an earlier era.

Even before the global COVID-19 pandemic upended business as usual, the nature of work was evolving. Terms such as “work from home” and “work from anywhere” are now a part of our regular lexicon. Once considered a perk, remote work and hybrid work schedules are now routine.

No longer are workers bound to their cubicle, protected by perimeter-based security tools or striving under the gaze of a manager. At the same time, work and personal lives have blurred. Personal devices are used for work, and employer-provided devices are used by the family and for leisure. This trend complicates even the most well-managed information protection and data privacy efforts.

## 30% of breaches involve malicious, careless or compromised insiders<sup>6</sup>

Careless users may make an honest mistake or take a shortcut to do their jobs. Compromised users may have their accounts taken over and misused by an outside cyber attacker. Malicious users can intentionally exfiltrate data for personal gain. In every case, the consequences can be severe.

## The wider your network...

Remote work has significantly increased our reliance on the cloud. Users rely on software-as-a-service (SaaS) platforms, cloud storage, collaboration tools, chat and videoconferencing.

Even classic industries such as government, healthcare, and manufacturing use infrastructure-as-a-service (IaaS) platforms to host services for customers, workforces, and citizens. With this “shared responsibility” model of security, cloud providers put the onus on organizations to protect their information, systems and apps.

On top of that, existing legacy infrastructure and applications may contain sensitive historical information. In such diverse application and cloud environments, security teams have struggled to see when data is leaving their environment, how it’s being lost and where it might be exposed.

The modern organization needs to manage not just external threats but malicious, careless and compromised users within their ranks.

### **...the more places for data to leak**

Beyond full-time employees, organizations have long relied on a virtual army of outside support: contractors, service providers, temporary workers, supply chain partners and others. Many have gone even further, refocusing on their core business and bringing in third parties to fill other pivotal roles.

Few security teams have the controls—let alone the resources—to manage and monitor third-party vendors. Nor can they ensure that these workers are well trained in security, data loss and insider risk-management issues.

Most organizations have third-party vendor compliance processes. They may even have perimeter-based access controls designed to ensure sensitive data stays within the network. What they don’t have is people-centric visibility or controls.

That means security teams cannot set access controls to critical applications and sensitive files. Nor do they have user-level visibility into contractors and outside partners as they move important files, interact with critical apps and use shared accounts on servers.

## **The modern organization needs to manage not just external threats but malicious, careless and compromised users within their ranks.**





## Bringing DLP up to date

As the world of work continues to evolve, it's time for a new, more modern approach to data loss.

Built on a cloud-based architecture, modern DLP helps reduce data loss from insider risks and external threats, streamline your team's workflow and speed up incident detection and response.

You should look for a solution that takes a holistic approach to data loss and includes several essential elements. Modern DLP must be multi-channel to protect email, cloud apps, and all data types and adapt to people misusing information, whether they are negligent, malicious or compromised.

It should also be based on cloud-native, flexible architecture that enables seamless integrations with other security solutions. With security and privacy built in by design, your solution must

be equipped to ensure that the right people—and only the right people—have access to the right data at the right time with well-defined data exclusion policies and strong access controls.

Finally, with people the number one risk factor for data loss, any effective strategy must put users at its heart. This means targeted and adaptive security awareness training that leaves every member of your team in no doubt about the part they can potentially play in exposing sensitive data and information.

The modern threat landscape is rapidly evolving—with wider attack surfaces, more access points, and increasingly sophisticated cyberattacks. To stand any chance of keeping our organizations safe in this environment, our defences must evolve too. The sooner, the better.



### Redefining data loss prevention

For a deeper dive into the modern use cases for DLP and to learn how these capabilities can safeguard your organization.

#### Download our eBook

[proofpoint.com/us/resources/e-books/redefining-data-loss-prevention-dlp](https://proofpoint.com/us/resources/e-books/redefining-data-loss-prevention-dlp)

- 1 Trend Micro. "Trend Micro Discloses Insider Threat." November 2019.
- 2 Jessica Davis (Xtelligent Healthcare Media). "Massive SingHealth Data Breach Caused by Lack of Basic Security." January 2019.
- 3 Phil Muncaster (Infosecurity Magazine). "French Newspaper Le Figaro Leaks 7.4 Billion Records." May 2020
- 4 Verizon. "2020 Data Breach Investigations Report." June 2020.
- 5 Gartner. "Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently." April 2020.
- 6 Ibid



# Is the new 'work from anywhere' reality hiding insider threats?

INSIDER THREATS ARE NOTHING NEW. UNFORTUNATELY, THE CYBERSECURITY LANDSCAPE IS LITTERED WITH CAUTIONARY TALES OF BUSINESSES THAT HAVE FALLEN VICTIM TO ATTACKS FROM WITHIN. IN RECENT YEARS, HOWEVER, INSIDER INCIDENTS HAVE INCREASED RAPIDLY, UP BY ALMOST 50%.



**MAYANK CHOUDHARY**  
EVP and GM Cloud Security Products  
Proofpoint





**A**nd the consequences can be severe. The 2022 Ponemon Cost of Insider Threats Report, states that insider attacks are estimated to cost businesses around \$15.38 million per year.

While many organisations are waking up to the threat posed by insiders, the modern workplace makes prevention increasingly difficult. As many of us are now well-accustomed to remote and hybrid working, it is unlikely that we will ever return to the norms of the office environment.

The resulting reliance on cloud setups, changing work hours and behaviour, and a lack of visibility make insider threats, whether malicious or negligent, much harder to defend against.

Faced with this growing threat, the case for a comprehensive Insider Threat Management (ITM) solution is indisputable. Now more than ever, organisations must implement robust ITM programmes, combining tools, technology, process, and, perhaps most importantly, people.

## Understanding insider threats

Traditional cyber defences are perimeters, built to protect from the outside in. Insider threats require a defence capable of protecting your data, networks, and systems in a perimeter-less environment.

This requires a different approach, with tailored tools, strategies, and awareness training—a fact that worrying numbers of organisations continue to overlook.

To make matters worse, insider threats come in many forms. From those intentionally seeking to do your

organisation harm to those doing so by accident. And others who aren't really “insiders” at all.

The most common negligent threats account for almost two-thirds of all incidents. They occur when a user unintentionally allows a threat actor access to your data and systems. This could be by clicking on a malicious link, misusing their password or accidentally exposing sensitive data.

While less common, malicious threats are often more damaging—costing an average of \$648,000 per incident, compared to \$485,000 when caused by negligence (2022 Ponemon Cost of Insider Threats Report). Malicious threats can be driven by employees seeking revenge, financial gain, or by cybercriminals who have compromised legitimate accounts to get inside your networks.

The third type of insider threats are when accounts are compromised—costing an average of \$805,000 per incident. These involve an imposter or credential thief who targets users' login information to gain unauthorised access to applications and systems—these represent the costliest type of insider threat.

In any case, insider threats are notoriously difficult to detect and defend against. Negligent insiders with no motive may display few warning signs. Malicious attackers, meanwhile, will go to great lengths to cover their tracks and avoid arousing suspicion.

Add to this a relatively new way of working, a disparate workforce, and many more points of attack, and the challenge facing cybersecurity teams becomes abundantly clear.

**“...MALICIOUS THREATS ARE OFTEN MORE DAMAGING – COSTING AN AVERAGE OF \$648,000 PER INCIDENT, COMPARED TO \$485,000 WHEN CAUSED BY NEGLIGENCE”**

## The hybrid factor

Hybrid environments not only increase the risk of insider threats occurring, but without a comprehensive ITM programme in place, they also make them much harder to detect when they do.

Though many organisations are now accustomed to hybrid working, it still remains a relatively recent development. Cybersecurity teams are still learning about the telemetry of their logs, with users accessing networks from various locations and devices, and at times that may once have been considered unusual.

With flexible work patterns now commonplace, trends are much harder to spot. Behaviours traditionally considered suspicious may no longer raise alarm. Most organisations also now have many more access points, vastly increasing the potential attack surface.

Then there is the social and psychological impact of flexible and hybrid environments. Outside of the office, users may be more inclined to veer from best practice just to “get things done”. Whether this means using personal machines for convenience or corporate machines for personal tasks,

writing down passwords, or improperly accessing systems and data.

Most concerning of all, many users may not even be aware of the required security best practice when working from home. Working from outside the office also brings its fair share of distractions, from daily chores to home comforts. All of which can make users more prone to simple yet costly mistakes. While those with a sinister intent may feel they can operate more freely outside of the corporate atmosphere.

## Building an Insider Threat Management (ITM) programme

Effectively detecting and deterring insider threats in the modern workplace may be difficult, but it is by no means impossible.

The solution is a comprehensive ITM programme, combining controls, process, and people. This starts by building a dedicated insider threat monitoring practice tasked with monitoring and investigating suspicious activity.

A people-centric ITM programme requires specific resources such as monitoring tools capable of detecting

data exfiltration, privilege abuse, application misuse, unauthorised access, and risky and anomalous behaviours.

Allow this team to develop and deploy clear best practice policies for hybrid working, covering system and network access, user privileges, password hygiene, unauthorised applications, BYOD, data protection, and more.

Finally, the cornerstone of any robust ITM programme is knowledge. Your ITM team must have a rich understanding of your data activity. Essentially, who is accessing what data—when, why and through which platform. This contextual intelligence can help to establish motives and intent which is key to spotting early warning signs of insider threats.

Users must also be equipped with the knowledge to protect themselves and your organisation. This is only possible through ongoing and adaptive security awareness training. Training should go beyond multiple-choice tests and basic security hygiene, focusing on the importance of behaviour.

Whether at home, in the office, or in between, users must know the standards that are expected of them and the role they play in keeping your business safe.

## Pfizer insider threat solution flags employee who stole covid vaccine secrets

- Pfizer detected a potential data breach when a former employee transferred 12,000 files from their work laptop to an online Google Drive account.
- The company had implemented technology that monitors when employees upload files to cloud-based platforms, such as Google Drive.
- By having visibility into insider threats and identifying the breach early on, Pfizer were able to forensically investigate the breach, and prevent their sensitive, valuable data from being leaked by a malicious insider.

### Read more about the story



[news.bloomberglaw.com/ip-law/pfizer-says-employee-stole-files-with-covid-vaccine-secrets](https://news.bloomberglaw.com/ip-law/pfizer-says-employee-stole-files-with-covid-vaccine-secrets)



## The real cost of insider threats

External attackers aren't the only threats modern organizations need to consider in their cybersecurity planning. Malicious, negligent and compromised users are a serious and growing risk.

Read the full 2022 Ponemon Cost of Insider Threats Report

[proofpoint.com/us/resources/threat-reports/cost-of-insider-threats](https://proofpoint.com/us/resources/threat-reports/cost-of-insider-threats)



# Optimizing your security strategy starts with people



Get the most from your Proofpoint investment and explore your own customised threat reports and product updates with our regular Customer Business Reviews.



**Book your Customer  
Business Review now**

[go.proofpoint.com/customer-business-reviews.html](https://go.proofpoint.com/customer-business-reviews.html)

**proofpoint.**



# What is data loss prevention and why do you need it?

Data loss prevention (DLP) is a tool that ensures sensitive or critical data is not leaked outside your organization, either accidentally or maliciously. DLP software classifies and tracks data to prevent it from leaving the network via unauthorized channels. These solutions detect leakage and exfiltration by monitoring sensitive data while it's in use, in motion and at rest.



**N**ow more than ever, organizations across industries need a tool that effectively prevents data leakage and detects incidents quickly to minimize data loss (and the costs associated with it). According to a recent study, the average cost of an insider threat incident is nearly \$15 million (on average for one company, over the course of a 12-month period) and this cost climbs the longer it takes to resolve the incident.

Let's take a closer look at DLP benefits and limitations of traditional solutions, as well as best practices to reduce data loss at your organization using a more comprehensive insider threat management solution.

## Key DLP benefits and solutions

Data loss prevention is a billion-dollar industry, primarily due to the growing risk of data loss at the hand of company insiders. The core benefits of DLP solutions are:

- To adhere to Regulatory Compliance
- To monitor sensitive data movement
- To prevent critical files from leaving via specific egress points

Traditional DLP software keeps a close eye on sensitive data with a complex classification system, comprised of individualized policies and tags that are assigned to each file. Typically, these solutions constantly scan for the movement of tagged files and ultimately prevent them from being accessed by unauthorized users or leaving the network.

The problem is: DLP solutions only monitor files, but data doesn't exfiltrate itself. Organizations need to start monitoring and focusing on user activity to effectively prevent data loss.

## Common limitations of traditional DLP solutions

DLP solutions aren't new—they've been on the market since the early 2000s—yet in many cases, are proven ineffective at preventing and detecting data loss at the hands of insiders. There are many reasons for this, but most notably, traditional DLP solutions are heavy on the endpoint, are hard to deploy, and are difficult to maintain, due to the time-consuming classification process.



**60% to 70%** of all data breaches warrant public disclosure

This statistic can be harmful to the reputation of any company. A study conducted by Intel revealed that 70% of data loss incidents in smaller commercial organizations—SMEs or SMBs—warranted either public disclosure or had a negative financial impact.

Other challenges that reduce the effectiveness of these solutions include:



#### **The growth of unstructured & semi-structured data:**

DLPs have a hard time keeping up with the creation and modification of critical data. For this reason, data owners and DLP tech administrators have to be in constant communication. If there is ever a disconnect between these two parties, it would leave a critical piece of data untagged and therefore unmonitored. Many users also find workarounds for the barriers that tagging data and files put up, which is why a focus on user activity is paramount.



#### **Users are able to bypass the DLP solution:**

As mentioned above, even if users don't have malicious intent, many are able to use simple DLP bypass methods to get around existing controls to make their life easier and increase productivity—even something as simple as uploading information to a personal cloud storage account to work from home. The problem is, traditional DLP software isn't able to prevent every outcome and action users might take, malicious or not, and does not give insight into employee or third-party contractor activity.



#### **The need for context during security incidents:**

Investigating a security incident is overly complicated using a traditional DLP solution because it's time-intensive and requires multiple tools. Since DLP solutions lack the context about users and incidents to resolve issues quickly, there may also be false positives that send security teams on a chase to figure out the cause of an incident.



#### **The decentralization of IT:**

DLP solutions find it increasingly difficult to track critical data when increasing numbers of employees access data via SaaS applications, share with external vendors, and use personal devices to access corporate systems. This is because DLP solutions rely on tags, policies, and rules to track where data is located.

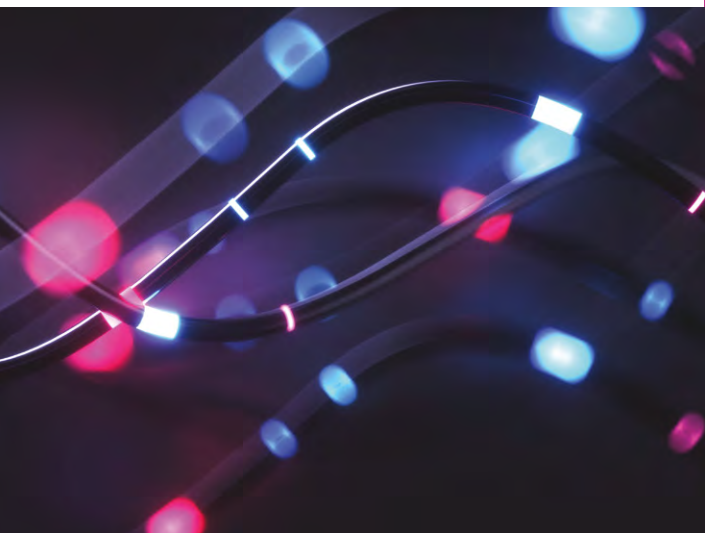
# 47%

## increase in data breaches since 2020

A common misconception is that data loss occurs mainly from malicious attackers. External breaches still account for over half of all data breaches. But internal data breaches are also increasing and account for nearly half of all data breaches. Many data breaches are not from outsiders, but from negligent or disgruntled employees.

## Final thoughts on Data Loss Prevention

The modern workplace, with remote employees and the prevalence of shared cloud applications, necessitates a more comprehensive solution than DLP to ensure data is secure. Stop data leakage in its tracks and diagnose the root of security incidents in minutes, not days, with constant monitoring of employees and authorized user behavior.



# Identify and prevent insider threats with a free trial



**As more companies face a 'work from anywhere' reality relying on cloud-applications to collaborate, insider threats are on the rise.**

Proofpoint's people-centric Insider Threat Management (ITM) solution can help your organisation manage the risk of insider threats by:

- Detecting potential insider threats
- Investigating incidents, in real-time
- Preventing data loss and misuse



**Get your free ITM trial**

[proofpoint.com/  
us/learn-more/itm-free-trial](https://proofpoint.com/us/learn-more/itm-free-trial)

**proofpoint.**

# Top 10 data breaches of 2021

---

WHILST ORGANIZATIONS ARE MOVING TO A NEW 'WORK-FROM-ANYWHERE' REALITY, IT'S CLEAR THAT CYBER-CRIMINALS ARE BECOMING MORE SOPHISTICATED AND ACTIVE IN THEIR ATTACKS TO TAKE ADVANTAGE OF THIS SHIFT. THIS MEANS THAT MORE DATA AND INFORMATION THAN EVER IS BEING ACCESSED AND EXPOSED BY UNAUTHORIZED INDIVIDUALS.

---

Data doesn't lose itself—it's either stolen by an external criminal, lost due to a careless user, or exposed by a malicious or disgruntled employee. We uncover the top 10 data breaches in 2021 to highlight why context is key in protecting your data.



**Victim:**

# Robinhood

**Summary:**

Robinhood disclosed a data breach impacting roughly 5 million users of the trading app. Email addresses, names, phone numbers, and more were accessed via a customer support system.

**Date:**

November 2021

**What do we know?**

- An unauthorized party socially engineered a customer support employee by phone and obtained access to certain customer support systems.
- The unauthorized party obtained a list of email addresses for approximately 5 million people and full names of 2 million people.
- After the intrusion was contained, the unauthorized party demanded an extortion payment.

**'Robinhood blog, 2021'**

[blog.robinhood.com/news/2021/11/8/data-security-incident](https://blog.robinhood.com/news/2021/11/8/data-security-incident)

## 2

**Victim:****Panasonic****Summary:**

The Japanese tech giant revealed a cyberattack had taken place – a data breach occurring from June 22 to November 3, with discovery on November 11 – and admitted that information had been accessed on a file server.

**Date:**

November 2021

**What do we know?**

- The attack could have happened as early as June 2021 but was only discovered in November 2021.
- The attacked servers stored information about Panasonic business partners and the company's technology.
- The ransomware incident involved a subsidiary of the company that also leaked business information.

**'ZDNet, 2021'**

[zdnet.com/article/panasonic-confirms-cyberattack-and-data-breach/#:~:text=ZDNet%20Recommends&text=In%20a%20statement%20released%20on,been%20accessed%20during%20the%20intrusion.%22](https://www.zdnet.com/article/panasonic-confirms-cyberattack-and-data-breach/#:~:text=ZDNet%20Recommends&text=In%20a%20statement%20released%20on,been%20accessed%20during%20the%20intrusion.%22)

## 3

**Victim:****Neiman Marcus****Summary:**

In October, Neiman Marcus made a data breach that occurred in May 2020 public. The intrusion was only detected in September 2021 and included the exposure and potential theft of over 3.1 million payment cards belonging to customers, although most are believed to be invalid or expired.

**Date:**

September 2021

**What do we know?**

- The breach occurred in May 2020, but was only discovered in September 2021.
- It included personal customer information such as names, contact information, payment card information, usernames, and online security passwords.
- Almost 5 million online customers were notified, and 3 million payment cards were affected, although 85% were expired or invalid.

**'ZDNet, 2021'**

[zdnet.com/article/neiman-marcus-breach-includes-payment-card-numbers-and-expiration-dates/](https://www.zdnet.com/article/neiman-marcus-breach-includes-payment-card-numbers-and-expiration-dates/)

4

**Victim:**  
**Coinbase****Summary:**

Coinbase sent out a letter to roughly 6,000 users after detecting a “3rd party campaign to gain unauthorized access to the accounts of Coinbase customers and move customer funds off the Coinbase platform.” Cryptocurrency was taken without permission from some user accounts.

**Date:**

October 2021

**What do we know?**

- Cryptocurrency was stolen from approximately 6,000 users after a 3rd party gained unauthorized access to customer accounts.
- Cybercriminals who accessed these accounts saw personal information like names, email addresses, home addresses, dates of birth, IP addresses for account activity, transaction history, account holdings and balances.
- Some accounts may have had information changed when they were accessed.

**‘ZDNet, 2021’**

[zdnet.com/article/coinbase-sends-out-breach-notification-letters-after-6000-accounts-had-funds-stolen/](https://www.zdnet.com/article/coinbase-sends-out-breach-notification-letters-after-6000-accounts-had-funds-stolen/)

5

**Victim:**  
**T-Mobile****Summary:**

T-Mobile experienced yet-another a data breach in August 2021. According to reports, the names, addresses, Social Security numbers, drivers' licenses, IMEI and IMSI numbers, and ID information of customers were compromised. It is possible that approximately 50 million existing and prospective customers were impacted.

**Date:**

August 2021

**What do we know?**

- A 21-year-old took responsibility for the hack and claimed to have stolen roughly 106GB of data from the telecoms giant.
- The hacker claimed T-Mobile already kicked them out of the breached servers but noted that copies of the data had already been made.
- The hacker can sell samples of this data with 30 million Social Security numbers and drivers' licenses on an underground forum.

**‘ZDNet, 2021’**

[zdnet.com/article/t-mobile-says-hackers-accessed-user-data-but-wont-confirm-ssn-breach-of-100-million-customers/](https://www.zdnet.com/article/t-mobile-says-hackers-accessed-user-data-but-wont-confirm-ssn-breach-of-100-million-customers/)

6

**Victim:****Volkswagen, Audi****Summary:**

The automakers disclosed a data breach impacting over 3.3 million customers and some prospective buyers, the majority of which were based in the United States. An associated vendor could have been the cause of the breach.

**Date:**

June 2021

**What do we know?**

- Compilation of data used for sales and marketing was left unsecured and exposed online between August 2019 and May 2021.
- Approximately 90,000 Audi customers in the US may have had purchase and lease eligibility data compromised.
- An unauthorized 3rd party could have accessed this information, including full names, mailing addresses, email addresses, phone numbers, tax ID numbers, account numbers and vehicle information.

**‘ZDNet, 2021’**

[zdnet.com/article/volkswagen-audi-disclose-data-breach-impacting-over-3-3-million-customers-interested-buyers/](https://zdnet.com/article/volkswagen-audi-disclose-data-breach-impacting-over-3-3-million-customers-interested-buyers/)

7

**Victim:****CNA Financial****Summary:**

CNA Financial employees were left unable to access corporate resources and were locked out following a ransomware attack which also involved the theft of company data. The company reportedly paid a \$40 million ransom.

**Date:**

March 2021

**What do we know?**

- \$40 million payment paid out after a ransomware attack crippled CNA Financial's networks.
- A sophisticated cybersecurity attack was detected in March 2021 that caused disruption to the network and systems.
- Employees were locked out of the company's systems and confidential data was stolen.

**‘ZDNet, 2021’**

[zdnet.com/article/us-insurance-giant-cna-financial-paid-40-million-ransom-to-wrestle-back-control-of-systems/](https://zdnet.com/article/us-insurance-giant-cna-financial-paid-40-million-ransom-to-wrestle-back-control-of-systems/)



8



9

**Victim:**

## Twitch

**Summary:**

Game-streaming platform Twitch has been the victim of a leak, reportedly divulging confidential company information and streamers' earnings.

**Date:**

October 2021

**What do we know?**

- More than 100GB of data was posted online.
- The documents appear to show Twitch's top streamers each made millions of dollars from the Amazon-owned company in the past 2 years.
- Full source code breach of the streaming gaming site revealed a trove of internal data & documents including core config packages, devtools, and payments to top streamers.

**'BBC News, 2021'**

[bbc.co.uk/news/technology-58817658](https://www.bbc.co.uk/news/technology-58817658)

**Victim:**

## Health Service Executive

**Summary:**

Health Service Executive (HSE) confirmed confidential medical information for 520 patients, as well as corporate documents were published online as a result of a data breach.

**Date:**

May 2021

**What do we know?**

- Originally, 12 private health records were published online after a data breach. However, 2 weeks later it was discovered that in fact 520 patient records were affected.
- The increase of the breach may have been due to HSE not using usual channels to report breaches due to the disruption of IT systems.
- The gang behind the attack threatened to publish or sell 700GB of data unless HSE paid 16.4 million Euros.
- There was a significant increase in reports of people receiving phone calls from fraudsters attempting to extract money while claiming to be from HSE.

**'Irish Times, 2021'**

[irishtimes.com/news/crime-and-law/hse-confirms-data-of-520-patients-published-online-1.4578136](https://www.irishtimes.com/news/crime-and-law/hse-confirms-data-of-520-patients-published-online-1.4578136)

# 10

**Victim:**

## Star Alliance

**Summary:**

Airline data hack: hundreds of thousands of Star Alliance passengers' details stolen. The Geneva-based company runs passenger processing systems for airlines such as ticketing and baggage control.

**Date:**

February 2021

**What do we know?**

- The company was the victim of a cyber-attack leading to a breach of passenger data held on its passenger service system (PSS) servers.
- The breach was linked to frequent flyer data, but limited to information such as their name, tier status and membership number.
- The company acted swiftly and initiated targeted containment measures alongside leading cyber-security experts.

**'The Guardian, 2021'**

[theguardian.com/world/2021/mar/05/airline-data-hack-hundreds-of-thousands-of-star-alliance-passengers-details-stolen](https://theguardian.com/world/2021/mar/05/airline-data-hack-hundreds-of-thousands-of-star-alliance-passengers-details-stolen)



# THE THREE PILLARS OF DATA LOSS PREVENTION

As distributed workforces become more common, the shift in working patterns has caused a rise in cloud-first IT that's redefined the modern security perimeter. Data doesn't lose itself; people's actions—whether negligent, compromised, or malicious—are the primary cause of security breaches that result in data loss. Now it's more important than ever to maintain visibility across the workforce and ensure a safe environment.

**S**ecurity teams need a truly proactive approach to protecting their organizations from data loss. Proofpoint Information Protection provides organizations with a modern, people-centric approach to protecting against insider risk and data loss by bridging all data loss prevention (DLP) channels.

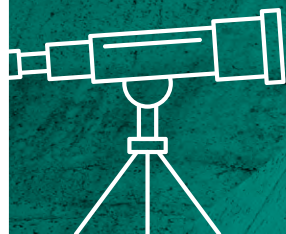
Let's take a look at the three primary pillars of a modern approach to DLP to understand why legacy DLP solutions just won't cut it in today's work-from-anywhere world.





## Pillar

1

**Gain greater visibility**

Creating an excellent hybrid work environment necessitates a high-quality end-user experience for everyone. This includes employees, customers, and third-party vendors and partners. Often, this means juggling a growing number of devices (including personal devices) and facilitating an always-on working style that allows employees to access the organization's resources whenever they want (and from any location).

Enabling this accessibility presents a unique set of challenges, specifically because data movement is harder to monitor. Truthfully, it's never been harder to balance tech needs while maintaining the right level of security and privacy.

With legacy DLP tools, organizations lacked visibility and context around data movement unless the action triggered an alert. But with a people-centric strategy found with a modern approach to DLP, organizations can identify sensitive data in motion and at rest across email, web, cloud and file shares by leveraging automated classifiers.

After all, data doesn't move itself; people move—and lose—data. Gaining real-time visibility into data movement is an effective way to mitigate some of the IT-related challenges of today's work environment.

## Pillar

2

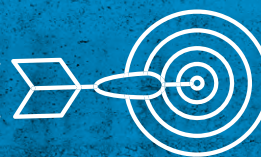
**Gain context to understand intent**

Visibility goes hand-in-hand with context. In fact, visibility and context are critical pieces to the insider threat management puzzle. Context allows security teams to correlate user activity with data movement, so security teams can more effectively identify risky behavior. With context, you gain knowledge of 'who, what, when, why and where,' enabling security teams to prioritize the multitude of alerts that can easily overwhelm security teams.

Context is of particular importance in today's world because previous red flags of potentially risky behavior, like logging on late at night, or over the weekend no longer apply. The freedoms associated with remote and hybrid workforces mean organizations are seeing their employees log in to get work done when—and where—it's most convenient for them. Because of this, security teams need to not only have visibility into data movement, but they must also understand the context of data movement. Leveraging a people-centric approach to DLP enables security teams to understand intent more effectively, so they can identify risky behavior, protect against data loss and address insider threats.

## Pillar

3

**Streamline incident management**

Responding to security incidents can be tedious, high risk, and require a lot of employee resources. Frequently, the security team tasked with understanding what actually happened, and deeper investigations require collaboration across a number of business units, including HR, legal and compliance teams. Being equipped with the 'who, what, when, why and where' of an incident can streamline these collaborative efforts to work toward faster containment more effectively.

In fact, reducing response time is one of the most significant ways organizations can lessen the impact of security breaches caused by insiders. Data from the 2022 Cost of Insider Threats: Global Report shows incidents that took more than 85 days to contain cost organizations an average of \$17.19 million per year.

This is why a modern approach to DLP is critical in today's work-from-anywhere world. With the right DLP tools in place, security teams can more easily detect compromised accounts, and more effectively monitor third party app risk and cloud threat detection. This, in turn, enables the security team to have greater clarity on next steps.





## Proofpoint Information Protection provides fast time to value

The three pillars of an effective approach to DLP in today's world requires a modern architecture, one that is lightweight and fast to deploy. As we previously mentioned, the longer an incident goes without containment, the greater the costs. Implementing a modern DLP solution enables organizations to reduce the mean time to detect (MTTD) and the mean time to respond (MTTR) by identifying, responding and managing data loss incidents and mitigating insider risk faster and more effectively than with legacy DLP tools.

Proofpoint Information Protection is your solution to address today's need for a modern approach to DLP. Proofpoint consolidates email DLP, CASB, Endpoint DLP, and Insider Threat Management (ITM) using a single unified console. This increases your visibility across channels by removing the challenges associated with sharing data across disparate tech solutions. Additionally, Proofpoint Information Protection is built on a modern, cloud-native platform, optimized for scale, security, analytics, privacy, extensibility, and end-user experience.



# The benefits of leveraging a modern approach to DLP





















From the ability to prioritize alerts based on greater context and actionable intelligence, to making faster, more accurate decisions, a modern approach to DLP not only prevents data exfiltration but also mitigates insider risk. Here are some of the benefits:

- **Greater visibility and context.** Gaining visibility and context into data movement helps organizations create a proactive strategy to protect against data loss and address insider risk.
- **Make faster, more accurate decisions.** By giving your entire team easy access to all the information, they can make better, more informed decisions faster. Reducing your mean time to respond (MTTR) can save your organization money.
- **Save time and administrative hassle.** By leveraging pre-built rules and templates, and common detection technology, security teams can minimize reduce alert fatigue, and the need for manual scans for restricted content. This frees up IT and security teams to focus on more complex challenges, and helps your organization maximize resources.
- **Reduce organizational risk.** A streamlined approach to incident management can help reduce the cost of incidents and limit legal risk when challenges arise.
- **Improve risk management.** Gaining context into the threat landscape can help your team identify the best way to manage high-risk assets.

# THE CASE FOR MODERNIZING YOUR DLP APPROACH

Here’s a closer look at how modern DLP compares to legacy DLP in common use cases.

- None 
- Partial 
- Complete 

MONITOR		
LEGACY DLP CAPABILITIES	MODERN DLP CAPABILITIES	USE CASES
		Data discovery
		Insider risks (malicious users, privileged users, departing employees, server and workstation usage)
		Third-party application usage
		Threat hunting and DLP analytics (including data and file history)
DETECT		
LEGACY DLP CAPABILITIES	MODERN DLP CAPABILITIES	USE CASES
		Intellectual property and regulated data loss across cloud, email and endpoint (accidental data leakage or malicious data exfiltration)
		Abnormal user behavior (compromised logins, malicious content or malicious user behavior)
PREVENT		
LEGACY DLP CAPABILITIES	MODERN DLP CAPABILITIES	USE CASES
		Data loss across channels (email, cloud and endpoint)
		Abnormal user behavior (compromised or malicious users)
RESPOND		
LEGACY DLP CAPABILITIES	MODERN DLP CAPABILITIES	USE CASES
		Data loss, insider threat and account compromise investigations
		Integrations across SIEM, SOAR, business communication and ticket management tools



# Envisioning the future of information protection; assessing your current capabilities

Building a strategic roadmap to your envisioned data loss prevention (DLP) future state requires you to recognize where you're starting from.

You need to assess any DLP technology currently deployed in your environment and consider the following questions:

- What capabilities and limitations exist?
- Are there specific pain points or coverage gaps that need to be addressed?
- How can your existing investments be used as part of a more comprehensive information protection solution for your organization?
- What additional capabilities do you need to protect your hybrid workforce today and in the future?



# Envisioning the future of information protection; assessing your current capabilities



Many organizations use a capability maturity model to help determine their current state and identify key areas where improvements are needed. In the case of modern information protection, there are five key capabilities that most organizations have already deployed, but with varying levels of success and functionality:

## Level 1: Email

Email remains the most common attack vector for data breaches today. Increasingly sophisticated phishing campaigns lure unsuspecting users into exposing sensitive information (such as account credentials) or to click on malicious links and attachments. At its most basic level, email security should provide some level of protection against spam, phishing, malware and data loss for all your users. More advanced capabilities should include business email compromise (BEC) protection and seamless yet robust email encryption for partners and others you need to share sensitive data with.

## Level 2: Cloud

A cloud access security broker (CASB) service provides organizations with visibility and control of the software-as-a-service (SaaS) based applications and file-sharing services used by your workforce—no matter where they're accessing the cloud from. Advanced CASB capabilities include application programming interfaces (APIs) for cloud apps, traffic log auditing, application risk scoring, adaptive access controls, browser isolation, forward proxies, and cloud security posture management.

## Level 3: Endpoint

Modern endpoint protection should extend beyond basic malware protection to include data activity monitoring for all users and insider threat management (ITM) for specific business purposes. Some examples of users and business purposes include newcomers, leavers, and business activity groups like mergers and acquisitions, finance, research and development (R&D), and so on.



A GLOBAL AND HIGHLY-ELASTIC CLOUD FRAMEWORK IS CRITICAL TO ENSURE USERS STAY SAFE WHILE BROWSING THE WEB—AND THAT ATTACKERS DON'T COMPROMISE AN ORGANIZATION'S CRITICAL DATA AND ASSETS.

## Level 4: Web

In the age of work from anywhere and data everywhere, having a web gateway appliance in centralized data centers doesn't work. A global and highly-elastic cloud framework is critical to ensure users stay safe while browsing the web—and that attackers don't compromise an organization's critical data and assets. Modern web security capabilities include the ability to inspect all traffic (including encrypted traffic) for threat protection and DLP as well as the ability to apply granular controls through integration with browser isolation. While in isolation, the user can access the site in read-only mode without risking exposure to threats or data loss.



## Level 5: Integrations

A modern information protection platform should provide seamless integration to enable complete end-to-end coverage of third-party and custom systems, applications, and services across your entire digital estate. This includes on-premises, cloud, and remote/mobile. Advanced analytics should enable deep business and security insights into threats across email and cloud, user behavior, and data usage. Integration with interactive security awareness training modules ensures that the right users get the right training to maximize effectiveness while reducing user friction.

A unified admin and response console simplifies day-to-day security operations and accelerates response by combining advanced tools including:

- Policy management
- Incident and investigative workflow
- Threat hunting and explorations
- Reporting and analytics
- Attribute-based administration and data privacy controls

# PROOFPOINT ACQUIRES DATHENA; STRENGTHENS ENTERPRISE INFORMATION PROTECTION OFFERING

The combined solution will solve legacy endpoint data loss prevention challenges and deliver real security value through detection, response, and compliance.

**P**roofpoint acquires Dathena, an innovator in artificial intelligence-powered data protection. With this acquisition, Proofpoint strengthens its cloud-based people-centric security solutions by adding AI-based data classification to its Information & Cloud Security platform, helping organizations to better understand information risk and help to eliminate data loss in today's hybrid world.



**dathena**  
a Proofpoint Company



“Data doesn’t lose itself. People lose data, and organizations are increasingly adopting data loss prevention strategies to manage that risk. Unfortunately, legacy products fall far short in actually preventing, detecting, and investigating data loss incidents in real time or immediately after they occur. Integrating Dathena’s multi-patented, next-gen AI engine into our people-centric DLP solutions will provide our customers with unparalleled data protection and help them meet their challenging internal and regulatory compliance requirements. We’re thrilled to welcome the talented Dathena team that built this cutting-edge technology to Proofpoint, and we look forward to working together to help our customers protect their data.” – Gary Steele, CEO, Proofpoint.

Proofpoint’s unique people-centric approach to data loss prevention (DLP) is trusted by organizations worldwide – whether due to unintentional mistakes or malicious intent. With an automated common content classification that has been honed for nearly 15 years, Proofpoint’s cloud-based solution provides data visibility and context across multiple channels from a single console. In today’s hybrid world with increased digital file sharing, regulation, and privacy requirements, data discovery and classification is key to an effective DLP strategy.

Dathena’s cutting-edge AI and cloud technologies will complement Proofpoint’s Information & Cloud Security platform, enabling organizations to automatically discover and classify data in real-time and better understand information risk with industry specific out-of-the-box and custom AI and Machine Learning (ML)-driven data classification models.

“Proofpoint has firmly established itself as a DLP leader, and joining them provides us with the perfect opportunity to fulfill our mission of protecting the data and privacy of organizations around the world. I’m incredibly proud of what we have achieved as a team through our unique technology and many innovations enabling better data protection. Working together with Proofpoint we will reach thousands of new customers, while further building trust in a digital world.” – Christopher Muffat, Founder & CEO, Dathena.

The acquisition of Dathena reinforces Proofpoint’s commitment to innovation and growth as a private company and increases its presence and investment in Asia. The integration allows Proofpoint to fully migrate customers of legacy DLP suites with data at rest requirements and extends the existing integration with Microsoft Information Protection.

**“DATHENA’S CUTTING-EDGE AI AND CLOUD TECHNOLOGIES WILL COMPLEMENT PROOFPPOINT’S INFORMATION & CLOUD SECURITY PLATFORM, ENABLING ORGANIZATIONS TO AUTOMATICALLY DISCOVER AND CLASSIFY DATA IN REAL-TIME AND BETTER UNDERSTAND INFORMATION RISK WITH INDUSTRY SPECIFIC OUT-OF-THE-BOX AND CUSTOM AI AND MACHINE LEARNING (ML)-DRIVEN DATA CLASSIFICATION MODELS.”**

**Christopher Muffat**  
Founder & CEO, Dathena.



## Proofpoint Information Protection solutions

Find out more about Proofpoint’s people-centric, cloud-based security solutions.

[proofpoint.com/us/products/information-protection](https://proofpoint.com/us/products/information-protection)



# Ransomware and data loss prevention; shifting from detection to prevention



**BRIAN REED**  
Product Evangelist,  
Proofpoint

---

**RANSOMWARE IS NOTHING NEW. IT HAS BEEN A SIGNIFICANT THREAT TO ORGANIZATIONS AROUND THE WORLD FOR SOME TIME NOW. HOWEVER, WHAT WAS ONCE A RELATIVELY STRAIGHTFORWARD THREAT IS FAST BECOMING INCREASINGLY COMPLEX.**

---

**T**raditionally, cybercriminals would force their way through perimeter defences, drop their malicious payload and demand a ransom to “fix” the situation. This brute force method of attack was usually remedied by detection, containment and recovery. Essentially, systems would be shut down and backups restored.

Today, however, ransomware is much more sophisticated, targeted and further reaching. Rather than forcing their way in, cybercriminals will target users looking to compromise their credentials, trick them into making a mistake or convince them to launch a malicious attack against their employer.

To defend against this, cyber teams must shift left—earlier in the attack chain. Moving away from detection and recovery and focusing on preparation, prevention—and people.

## Defending your data

The detection and response approach to ransomware was understandable when the issue was solely about information protection. However, with fewer organizations caving in to ransom demands, cybercriminals have changed tack to protect their revenue streams.

Modern ransomware now often carries an extra sting in the tail, be that corporate espionage or data theft, making it very much a data loss prevention (DLP) issue.

That’s why any effective defence against ransomware should place data at its heart. This starts with classification. You need to understand what data is at risk, who needs access to it, who has access to it and how prized it is likely to be by cybercriminals.

When making these classifications, go beyond geography and data location. The traditional data in use and data at rest model is no longer fit for purpose. A modern DLP strategy must follow the user wherever they go—for it is your people that put your data at risk.



## The people problem

With over 90% of cyber-attacks requiring some form of human interaction, your users are the biggest risk factor facing your organization.

These days, cybercriminals rarely break down the door. Instead, they are invited in by your people through either malice, carelessness or compromise. The more you know about your users, their activity and behavior, the better you can spot the early warning signs of an attack, whatever the driving factor.

**Malicious:** A malicious user is one who knowingly looks to cause harm to your organization. They may be disgruntled and looking for revenge or being paid by criminal gangs for access to your networks and data.

Vigilance is critical when detecting malicious users. Implement a solution that can spot suspicious behavior such as out of hours logins or unusual access requests, and limit access to sensitive information to only your most privileged employees.

**Careless:** Careless users let cybercriminals inside your perimeter defences by mistake. This may be because they do not log out of corporate systems correctly, use default passwords or fail to apply security patches.

When it comes to spotting carelessness among your teams, keep an eye out for poor security hygiene, such as

writing down passwords and installing unauthorized applications.

**Compromise:** A compromised user is one whose devices or credentials have been commandeered by cybercriminals. Accounts and devices can be compromised by malware, phishing or another form of targeted attack.

Unfortunately, account compromise is notoriously hard to spot. The best defence is to minimise compromise in the first place, through protections such as multi-factor authentication and cybersecurity training.

## Rooting out ransomware

The ultimate target of ransomware may be your data, networks and systems. But it can only reach that target via your people. Therefore, the most effective way to keep it at bay is to remove the human element entirely.

With a robust email protection and data loss prevention solution in place, you can analyse, filter and block malicious messaging before it reaches the inbox.

However, even the best perimeter defences can be breached.

Email protections should be coupled with deep insight into the telemetry of your access logs and network activity. You need to know who's accessing your data—how, when and why. The more you know, the faster you can spot anything out of the ordinary. And then there's the last line of your defence, your people. Every user must know exactly what to do when faced with a ransomware attack and the consequences of failing to stop one. Most importantly, they must understand how their behavior can put your organization at risk.

This is only possible through ongoing and adaptive security awareness training that goes beyond multiple-choice tests and standard best practices. The ultimate goal of any training program should be to create a security culture in which cybersecurity is everyone's responsibility.

The simple fact is, ransomware is growing ever more sophisticated, rendering traditional defences ineffective—and when the cure no longer works, prevention is the only remedy.

## A modern approach to information protection

Brian Reed, Product Evangelist at Proofpoint gives an overview to the modern approach to information protection.

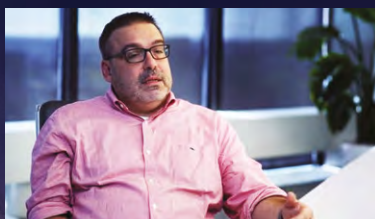
[share.vidyard.com/watch/hwBrm3eJWZau2xXcpyPzf6](https://share.vidyard.com/watch/hwBrm3eJWZau2xXcpyPzf6)



# GROUNDING INSIDER THREATS

WITH PROOFPOINT INSIDER  
THREAT MANAGEMENT





## Watch the customer story video



[proofpoint.com/us/customer-stories/aircastle-grounding-insider-threats](https://proofpoint.com/us/customer-stories/aircastle-grounding-insider-threats)



## The company

Aircastle is a publicly traded company that acquires, leases and sells commercial jet aircraft to airlines throughout the world. It has built a highly successful organization with a lean and dedicated team of employees.

As of 2019, Aircastle owns and manages 277 aircraft, leased to 87 lessees located in 48 countries. It has earned its reputation as a company with a unique and necessary position in the commercial aircraft leasing industry.



# AIRCATTLE USES ITM TO SAFEGUARD SENSITIVE INFORMATION WHILE PROTECTING PRIVACY

## The challenge

- Safeguard key financial information (earnings, details of M&A and other information)
- Meet SOX compliance mandates by maintaining detailed records
- Uphold privacy regulations and culture of respect for employees and contractors

## The solution

- Proofpoint Insider Threat Management

## The results

- Gained full visibility into user activity
- Received rapid alerts on suspicious activity
- Developed the capacity to conduct investigations in a matter of minutes, not days
- Increased instances of employees reporting out-of-policy behavior to curb insider threats with the ability to investigate claims rapidly



**“WITH A SMALL IT TEAM, WE DO NOT HAVE TIME TO CONSTANTLY BABYSIT A PRODUCT LIKE DLP. WITH ITM, THERE IS NO BABYSITTING. I RECEIVE GOOD, SOLID ALERTS. THE INFORMATION IS RELEVANT AND DOESN'T WASTE MY TIME WITH SEARCHING.”**

Bill Duenges, SVP of Information Technology, Aircastle



## The challenge

As a public company, Aircastle must carefully safeguard key financial information. That includes everything from earnings to details of mergers and acquisitions to ensure it is not leaked prior to regulated disclosure dates. Leaks could endanger the business, exposing them to financial and legal headwinds.

Additionally, Aircastle is beholden to the Sarbanes-Oxley Act, another burden of being a publicly held company. This mandates the company to continually maintain detailed financial and IT records for regulatory bodies. Moreover, as a company with offices located internationally, they must uphold certain privacy regulations. Even outside these laws, Aircastle values its culture of privacy and respect for its employees and contractors.

The Aircastle team had been using a traditional endpoint DLP for data loss prevention. But they had run into significant issues with time-consuming set-up, constant monitoring requirements, and system crashes. They tried two different DLP solutions, but both were overly file-focused. And they required constant hands-on maintenance, straining its small IT team.

“I have a small IT team of six people,” said Bill Duenges, Senior Vice President of Information Technology, Aircastle. “So, it’s very difficult to have a product you have to constantly babysit like a DLP.” On top of that, users were far from thrilled with the DLP’s effect on its endpoints. “As soon as we started using a DLP, all our users knew it was there because of the instant slowdown.” Some figured out how to bypass the DLPs. And even when they didn’t, the tools created mountains of work for Duenges’ team while slowing down investigations.

## The solution

After an extensive search process, Duenges and his team conducted a proof of concept with ITM. They were pleased with the results and settled on ITM as a means to help Aircastle gain more context into user activity within the organization. This would let them receive immediate alerts if, for example, an employee attempted to exfiltrate confidential financial information via a cloud storage service.

Initially, Duenges admitted, “My team saw ITM as a ‘nice-to-have’ product. We thought it was just something we’d layer into our existing security stack.” However, two years into their engagement with ITM, Duenges now describes the platform as a “must-have” that will be part of their security stack “forever.”

## “INSIDER THREAT INVESTIGATIONS THAT USED TO TAKE DAYS NOW TAKE 15-20 MINUTES ON AVERAGE.”

ITM enables Aircastle's small IT and security team to receive rapid alerts on suspicious user activity and conduct investigations in a matter of minutes, rather than days.

They are now aware of any insider activity impacting sensitive financial data and other valuable business files in near real time. Additionally, team members sometimes report out-of-policy behavior they witness. And now, Duenges' team has a tool that can help him verify the claims.

“The first tool I go to for investigations is ITM,” says Duenges. “We get alerts from other tools, but ultimately use ITM for full context around various incidents. With ITM's easy-to-use, quick-to-set-up and lightweight solution, my team is more productive, users aren't impacted, and our valuable assets are better protected.”

Finally, ITM's fine-grained privacy settings enable the team to ensure that only the appropriate team members have access, and only after clearing access with their chief legal officer. This ensures that user privacy is protected without sacrificing security.

“On top of all that, ITM helps us meet SOX compliance,” says Duenges. “So that's one more thing off my plate.”

### The results

The Aircastle team now has full visibility into user activity across endpoints. When an alert fires, they are able to rapidly determine what happened. And they can now understand what took place before and after the incident to place it in context.

When actual insider-caused data exfiltration incidents take place, the team can rapidly investigate and respond to them with complete context around user and data activity from ITM. ITM enables the Aircastle security team to clearly understand not just what happened but why. In several cases, this has enabled them to exonerate employees who were acting in good faith but may have exceeded the boundaries of security policy.

As a side benefit, Aircastle has dramatically improved its NIST benchmark security score by demonstrating the features that ITM has added to its security stack.



### LEADING PEOPLE- CENTRIC INSIDER THREAT MANAGEMENT (ITM)

Proofpoint's ITM protects against data loss and brand damage involving insiders acting maliciously, negligently, or unknowingly. We correlate activity and data movement, empowering security teams to identify user risk, detect insider-led data breaches, and accelerate security incident response.

**Find out more about  
Proofpoint ITM**



[proofpoint.com/us/products/information-protection/insider-threat-management](https://proofpoint.com/us/products/information-protection/insider-threat-management)



# THE WAY WE ACCESS DATA HAS CHANGED; IT'S TIME TO CHANGE THE WAY WE PROTECT IT TOO

**IAN PUGH**

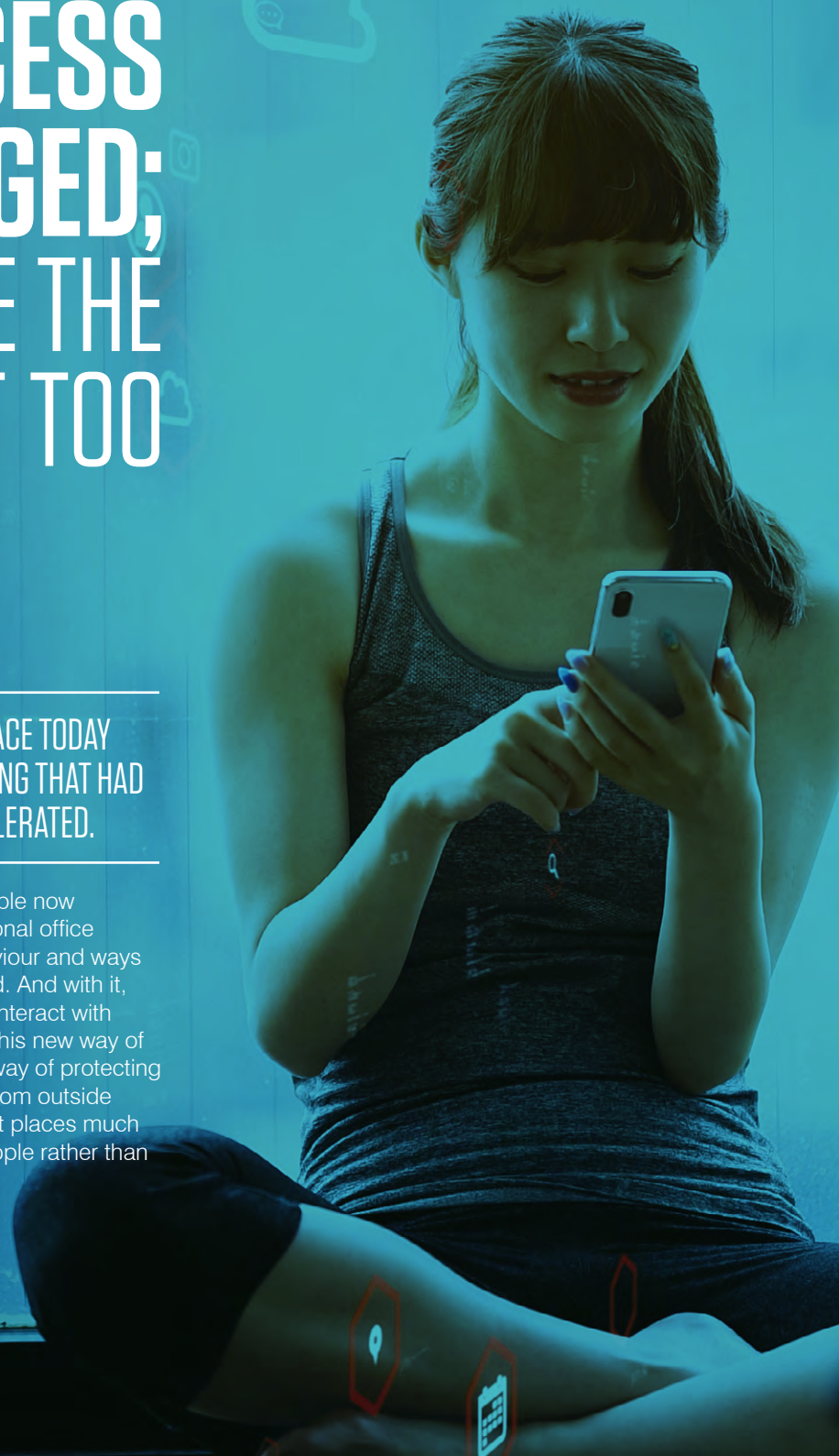
Senior Director, Information Protection at Proofpoint

THE WORLD OF WORK AND BUSINESS IS A VERY DIFFERENT PLACE TODAY THAN JUST TWO YEARS AGO. TRENDS SUCH AS HYBRID WORKING THAT HAD BEEN GAINING TRACTION FOR SOME TIME HAVE RAPIDLY ACCELERATED.

But while most businesses are now well accustomed to the post-pandemic world, many policies and procedures are not yet up to speed. Controls in place to protect data, for example, were primarily built around traditional working practices.

In many cases, traditional data loss protection (DLP) solutions have been focused on tools and perimeters designed to keep sensitive information in and malicious actors out. This legacy approach to DLP focused on data in use, in motion and at rest, without much context outside of this.

However, with many people now operating beyond traditional office settings, attitudes, behaviour and ways of working have changed. And with it, the way we access and interact with data has changed too. This new way of working requires a new way of protecting our sensitive data both from outside and from within. One that places much greater emphasis on people rather than just tools and controls.



## It's time to rethink DLP

While policies and procedures may be lagging behind in the new hybrid work environment, the same cannot be said of cybercriminals. Threat actors have wasted no time, first capitalising on the disruption caused by the pandemic and now honing their lures to target users in new and potentially less secure environments.

That old foe phishing increased significantly last year, with 95% of organisations experiencing an attack. Over half of these organisations suffered at least one compromised account, and the consequences for those on the receiving end are severe. The cost of containing a compromised account has doubled in recent years, up from \$382,920 in 2015 to \$692,531 in 2021.

While legacy DLP solutions may detect and deter initial phishing attacks, they do not collect any threat context information. This leaves organisations blind to data movement involving compromised user accounts and identities.

A modern DLP solution, on the other hand, can help IT teams quickly spot and revoke malicious third-party apps and block known threat actors and malicious IP addresses that could lead to account compromise.

Traditional solutions can also present challenges preventing data loss in other areas too. Blanket data protection controls applied to entire departments or organisations can be cumbersome, hampering productivity and resulting in false positives. In fact, nearly 70% of survey respondents reported that three in every four incident alerts they investigate within their traditional DLP solution are false.

A modern DLP solution overcomes this issue by adapting its detection, prevention and response to a user's risk level and to the sensitivity of the data that's being accessed. This tailored approach is particularly important for insider threats, the cost of which has increased by 31% between 2018 and 2021, now standing at \$11.45 million.

Legacy DLP may spot suspicious activity but it provides no behavioural awareness before, during or after risky data movement—and offers little in the way of risky user behaviour analytics. In other words, legacy tools can't help you answer the context of “who, what, where, when and why” behind an alert. The result is overburdened security teams and minimal insight into network activity.

## Putting your people first

Your people are at the heart of any potential data loss. They are the ones with privileged access to your networks. They are the ones entering their credentials in your systems. And, with over 90% of cyber-attacks requiring human interaction, they are the ones most likely to expose your data to cybercriminals.

That's why a modern DLP solution must account for human behaviour, whether in the office, at home, or in between. Unfortunately, this is not the case with many legacy systems. Most will see any anomalous behaviour as an instant red flag, impacting user experience and costing security teams precious time.

At a time when “normal” working practices can mean different things from day to day, this approach is no longer fit for purpose.

## A MODERN DLP SOLUTION OVERCOMES THIS ISSUE BY ADAPTING ITS DETECTION, PREVENTION AND RESPONSE TO A USER'S RISK LEVEL AND TO THE SENSITIVITY OF THE DATA THAT'S BEING ACCESSED

Remote and disparate workplaces need solutions that can proactively monitor and prevent data loss across endpoints while accounting for user behaviour, cloud access, and third-party apps.

And such adaptable protections are just one part of effective data loss prevention. This people-centric approach must extend into your training programme too. All the tools and controls in the world are not enough alone. Total data loss protection requires ongoing, targeted and adaptive security awareness training. Training that leaves users in no doubt of the part they can potentially play in reducing the number and impact of cyber-attacks.

Today's cybercriminals are constantly evolving, targeting new and sophisticated threats squarely at your people. Our defences must evolve too. If not, this is an arms race we don't stand to win.



# How to implement people-centric data loss prevention for Microsoft Office 365

MICROSOFT OFFICE 365 IS A CLOUD PLATFORM THAT FEATURES POWERFUL TOOLS FOR OFFICE APPLICATIONS, ONLINE MESSAGING, FILE SHARING AND CLOUD STORAGE. SO, IT'S NOT SURPRISING THAT ALMOST 70% OF CLOUD SECURITY PROFESSIONALS HOUSE THEIR SENSITIVE DATA WITHIN MICROSOFT SHAREPOINT ONLINE OR MICROSOFT ONEDRIVE, ACCORDING TO RESEARCH FROM THE CLOUD SECURITY ALLIANCE.

But, organizations using this platform also have concerns around data security and compliance. There are three primary data loss scenarios that are unique to the cloud:

- Excessive or unauthorized sharing of regulated or sensitive data.
- Inappropriate uploads and downloads of regulated or sensitive data.
- Data exfiltration and/or manipulation following Office 365 account takeover.

We explore 5 best practice steps to take when addressing data security in Office 365 platform and implementing cloud DLP.



## Step 1 - Define Office 365 policies based on content, context and control

### Content

Consider the levels of sensitive data:

- Data security and privacy regulations, e.g. General Data Protection Regulation (GDPR).
- Personal Identifiable Information (PII), e.g. credentials and passwords.
- Intellectual property, e.g. formulas, source code and product designs.
- Other sensitive data, e.g. financial information, mergers or acquisitions.



### Context

Define how data can be accessed, by whom, based on sensitivity level:

- Who can have access to sensitive data and who should we watch closely? VIPs, admins with privileged access, your Very Attacked People™ (VAPs), previously compromised accounts.
- What networks and devices are allowed to connect to the platform? Isolate access for unmanaged devices, read-only viewing for sensitive data.
- What types of data should not reside in Microsoft Office 365? Data that should be segmented due to compliance restrictions.

### Control

Ensure historical data is compliant with new data policies - remove or reduce sharing permissions for sensitive files. Apply preventive measures when data is in motion or in use by:

- Blocking the uploading of PCI data to SharePoint Online.
- Allowing read-only views to files from unmanaged devices.
- Quarantining files shared with anonymous (public) links.
- Coach users on DLP violations and add tombstones to inform the recipients.

## Step 2 - Use out-of-box tools to audit and fine-tune DLP policies

Improve your ability to detect DLP violations with these tools:

- Pattern matching (Social Security numbers, credit card numbers).
- Keyword matching ("highly confidential", "passwords").
- Predefined dictionaries (credit card terms, date-of-birth terms).

- Document fingerprinting (tax forms, medical forms, patent forms).
- Exact data matching (to match against a database of patient PII, for example).
- Optical character recognition (sensitive information in images).

Out-of-box tools in your Cloud Access Security Broker (CASB) solution refines detectors and the process for discovery, monitoring and reporting. Create rule sets to detect sensitive file activity in Office 365 and identify false negatives – increasing operational efficiency.



W

## Step 3 - Discover sensitive data in Office 365

Create a 'heat map' of your data to prevent data exposure and ensure compliance by:

- Scanning historical files to see if they contain sensitive data or sharing permissions (public, external and tenant-wide sharing).
- Applying sensitivity labels, such as Microsoft Information Protection labels, to sensitive files so you can track them more easily.
- Gaining a deeper understanding of how your data is handled and used for collaboration.
- Keeping a close eye on high-risk users (VIPs, VAPs and employees with high privileges) and personal cloud accounts.
- Making sure that your data is in the best location, has appropriate sharing permissions and is only accessed by people with privileges.

## Step 4 - Remediate automatically when prevention isn't feasible

Once you know where sensitive data is and how it should be handled, remediate DLP violations to return your data to a safe state. And prevent sensitive data from being migrated by:

- Reducing public sharing permissions for sensitive files at rest to internal only.
- Quarantining and moving the data back to approved applications.
- Restricting sensitive data downloads to managed devices and approved domains.
- Removing sensitive files after a user's account had been compromised.

P



## Step 5 - Reassess business processes and educate end users

With the new 'work from anywhere' reality, more data left the corporate perimeter and the visibility into that data has been significantly reduced. When there are changes to business conditions or processes, continue to reassess your data loss prevention (DLP) solution to ensure it remains effective by:

- Making sure that DLP classification and policy enforcement remains consistent across cloud services and the rest of the enterprise.
- Ensuring admins are notified of DLP incidents timely so they can investigate them.
- Re-prioritizing security incidents based on risk factors such as compromised accounts and VAPs.
- Notifying end users of DLP violations and coach them, so they don't repeat the same mistakes.
- Enrolling negligent users in security awareness training that focuses on data privacy or DLP so they can learn how to protect your organization's data.

## 5 STEPS TO BUILDING A SUCCESSFUL CLOUD DATA LOSS PREVENTION SOLUTION

Take a deep dive into best practices for cloud DLP - check out this webinar.

Watch the webinar

[proofpoint.com/us/resources/webinars/building-successful-cloud-dlp-solution](https://proofpoint.com/us/resources/webinars/building-successful-cloud-dlp-solution)

## How can Proofpoint help you improve cloud data loss prevention?

Get started on your cloud DLP journey with our Proofpoint Information and Cloud Security Platform - Cloud Access Security Broker (CASB) also enables you to implement consistent data loss prevention policies across email, cloud, web and endpoints.

Get started with CASB

[proofpoint.com/us/resources/white-papers/getting-started-with-casb](https://proofpoint.com/us/resources/white-papers/getting-started-with-casb)



# Taking a modern approach to data loss prevention





Proofpoint's **Karen Letain**, VP, Product Management, and **Andrew Rose**, Resident CISO, EMEA, recently sat down to discuss the changing face of data loss prevention (DLP) – and how it fits in the modern workplace. We cover the key takeaways from their discussion.

How do we incorporate information protection into a security awareness program?

#### Karen Letain

This is something we've been talking about a lot with our DLP team. We have been leaning towards leveraging 'in the moment' nano or microlearning and embedding it within the DLP solution. So, instead of a separate solution, it is fully integrated into the DLP.

It's important to think about it this way because while you absolutely should have a separate awareness program around information protection, you also need to be able to reinforce those behaviors in the moment when somebody is doing something incorrectly.

#### Andrew Rose

I agree – 'in the moment' training for information protection and DLP is so essential. It's about teaching users right there and then.

It's no use sending an email and then receiving a message ten minutes later telling you why you should not have sent it. By that point the data is long gone.

Plus, if you're approaching the problem retrospectively the individual is not learning the same lessons they would 'in the moment'.



Should 'in the moment' training be used in conjunction with retrospective learning?

**Karen Letain**

Absolutely. In the moment training has many advantages but it's also got its drawbacks. For example, some people are not in the zone to receive corrective information at the time they make a mistake.

Say you click on a link during a phishing simulation. You've made an error and may be embarrassed. So, you are likely to close any pop up as quickly as possible – in the hope that the incorrect response won't count perhaps.

But if you are moving a file from the network to your laptop that's when you want a pop up to say, "hey, that's something you probably shouldn't be doing". It's about delivering the right message at the right time, in context with the situation.

**Andrew Rose**

Yes, the opportunity to deliver 'in the moment' training is really very short because people are likely to close a pop up as soon as they can, out of frustration for making a mistake. They maybe also don't want to admit that they've made an error and certainly don't want everyone else around them to see it.

The immediate message should just be a few words, with a simple headline. We can then follow it up with a more detailed explanation of the error.

How important is it to teach users about the consequences of data loss?

**Andrew Rose**

It is very important to highlight the consequences around information protection. People become numb to the data they work with. We need to bring people's attention back to the potential value of data, because to them it may just be everyday information, but in the wrong hands it could be devastating for their employer.

**Karen Letain**

Yes, that's why specific role based training is so important. Because one size fits all just doesn't work.

We have moved to a more adaptive type of learning. We figure out what the key security domains are that we want to map the content to, and then apply a learning path.

You also need to be able to tailor learning to knowledge levels so that users don't tune out. It is no good giving IT staff an annual generic security training program because their knowledge level is far beyond what you're giving them and they won't learn anything from it.

Instead, you want to deliver a learning path that's progressive and tailored to their role and fundamental knowledge.



What is the best way to deliver ongoing security awareness training?

**Andrew Rose**

E-learning is great and that gets through to people. But you should also create content that can be delivered through other channels such as digital signage and team meetings. That way you're addressing all the people who learn in different ways.

The more varied the ways you deliver your security message, the more likely people are to pick up and retain information.

**Karen Letain**

This is also part of the tailoring process. So, as well as aligning training to job roles and knowledge, we align communication materials to those categories too.

Some workplaces react differently to different kinds of messaging too. Some prefer a more corporate sensibility, others like humor. Then there is animation versus live action. It is heavily dependent on the organization, their policies and their culture.



## How can organizations adjust the content strategy and communication structure for remote workers?

### Karen Letain

We find that remote workers tend to work longer hours and struggle to fit 12-15 minute training modules into their day. So now we're moving towards microlearning.

Of course, this isn't the case for everyone. That's why it's important to deliver training in multiple formats, so people can choose the way they want to learn. That could be one long module, many smaller ones back to back or a bitesize module whenever they have the time.

### Andrew Rose

It certainly changes the model because of course you can't have digital signage and posters around the home with security reminders.

Shareable content like graphics and memes with security reminders can be an interesting way to help to reinforce messages, but they should not be overly relied upon. This also requires careful management as something that connects with a millennial may mean nothing to an older employee.

## How can organizations position DLP and information protection so that it doesn't become a privacy issue?

### Karen Letain

This is a big concern. Employees do not want to feel like their every move is being watched and critiqued. Particularly if they are using their own device for work. So, how do you monitor and control what happens on a personal device?

Employers need to layer control to protect business information but without invading privacy. I don't think there is a 100% correct answer on how to do this yet, but communication is certainly key.

The C-suite need to communicate with users about the importance of protecting information and how data protection and privacy may overlap as a necessity.

Usage policies and technology such as browser isolation can also be used to draw those distinctions between allowing privacy and protecting information.

### Andrew Rose

I hope that is not too much of an issue anymore. It certainly was when people just had the one computer to work on.

But today, people can access personal services, such as Facebook and webmail, via their personal laptops and phones. People are working from home surrounded by their personal devices, so they are used to switching between the two. There shouldn't be too much of a privacy issue blocking or monitoring webmail for instance, as anything sensitive can just be done from their personal device.

Also, employers can sell a DLP solution as a positive for their employees. It's ultimately there to protect employees from making a mistake and exposing themselves and the organisation to the consequences of a cyber-attack.



# FROM MANUAL TO MANAGED

The changing face of data loss prevention



JEREMY WITTKOP

Senior Director, Technology  
Services, Proofpoint



**L**ike most cybersecurity tasks, managing data loss was once a human endeavour. IT and security teams would monitor activity with basic sensor technology, blocking anything suspicious or malicious.

Fast forward a few decades, and data loss prevention (DLP) is a very different beast. Where once analysts would focus solely on protecting information, today, the process encompasses a broad range of skills and disciplines across cloud security and all manner of data loss scenarios.

Then there is the issue of increasingly prevalent insider threats—defending from the outside in is an entirely different discipline to defending from inside out, after all. Most crucially, these varying solutions must integrate and communicate cohesively.

This presents a problem for the modern organisation. Managing DLP is difficult to resource due to the skilled roles which need to be involved. It's a multi-disciplinary program requiring several resources (some full-time and others part-time), as such, employing someone with expertise across all areas is almost impossible. With the skill gap widening by the day, this is something the cybersecurity industry can ill-afford to do.

That's where managed DLP comes in. Managed DLP helps organisations protect what matters—without the need for highly skilled but underused teams. When implemented correctly, managed DLP brings better outcomes with lower costs and fewer internal resources.

But, as with all technology implementations, there is much to consider. Not all DLP solutions are created equal. Before deciding to outsource, you need a firm understanding of your business requirements, your data risk and your metrics for success.

## Decisions, decisions and DLP

Outsourcing any essential function takes careful consideration. When that function is as potentially complex as DLP, the process of choosing a partner must be meticulous.

The first thing to keep in mind is that generalists struggle with DLP. If a provider offers 100 services of varying levels, the odds of a comprehensive and effective DLP solution being one of them are very slim.

DLP is a specialised field. It is not something to be tacked on to another product or offered in tiers. It is all or nothing. Otherwise, you may as well struggle on with it in house. That's not to say your provider should only offer DLP. Far from it. But it must be a specialism, with a dedicated solution, team and tried and tested process.

Next, you need to understand precisely what you need from your managed DLP service provider. Some “solutions” keep your systems up and running and do little else. To truly see the benefit of outsourcing this function, you need a much more comprehensive service.

## MANAGED DLP HELPS ORGANISATIONS PROTECT WHAT MATTERS—WITHOUT THE NEED FOR HIGHLY SKILLED BUT UNDERUSED TEAMS

Of course, managing your system configuration is important, but this is just the starting point. On top of this, your provider should develop and manage your DLP policies on your behalf and conduct security event triage. This gives the provider a vested interest in developing effective policies—as poor policies mean more time and money spent triaging events.

Your DLP provider should also understand the role that people play in data loss. Data doesn't lose itself. People lose data, through negligence, malice and compromise. And technological controls alone are not enough to keep that from happening.

Finally, your provider should have a clear framework for measuring the success of the solution. If it can't be measured, it cannot be accurately assessed—and, most importantly, it cannot be improved.

## Measuring the success of managed DLP

Some providers will tell you that measuring the success of a DLP solution is a complicated undertaking. But the reality is, with clearly defined metrics, it is anything but.

Work with your provider to determine how you will quantify the effectiveness of your solution. This should start with the basics, such as the number of false positives generated over a given time or the mean time to respond to an alert. These metrics and more can then be used to determine the overall level of risk facing your organisation.

But be sure to focus on data classification at this stage, too. Ideally, your provider should take several approaches to this process, combining automated classification to determine specific data labels and user-driven classification to decide when labels should be applied or removed.

You can also set more macro targets. Within a relatively short time, you should be able to determine whether outsourcing your DLP has reduced staffing levels, costs, and more.

## Managed DLP from Proofpoint

The way we access and process data has changed drastically in recent years. It's only reasonable that the way we protect that data must change too.

Legacy systems are not built to support modern working environments. They may spot and flag suspicious activity, but most fail to provide behavioural awareness before, during or after risky data movement—and offer very little in the way of user behaviour analytics.

At Proofpoint, we understand that all data loss is inherently people-centric. So, a modern managed DLP solution must account for human behaviour, whether in the office, at home, or in between.

By bringing together telemetry across email, cloud and endpoint, our Proofpoint Enterprise DLP solution allows your security and compliance teams to address the complete range of data loss scenarios in a single, bespoke solution.

This time-tested approach gives you a faster response and investigation time, clear metrics for success and total visibility across your systems, networks and data.



### Talk to us about Managed Data Loss Prevention (DLP)



Get the most from your Proofpoint investment and explore what Managed DLP could do for your organization with a regular Customer Business review.

**Book a Customer Business Review**

[go.proofpoint.com/customer-business-reviews.html](https://go.proofpoint.com/customer-business-reviews.html)



# DATA DOESN'T LOSE ITSELF

People lose data—through negligence, malice or compromise. Proofpoint Enterprise Data Loss Prevention (DLP) focuses on people-centric insight in the prevention of data loss.



**Learn more about  
Proofpoint Enterprise  
Data Loss Prevention**

[proofpoint.com/us/products/  
information-protection/enterprise-dlp](https://proofpoint.com/us/products/information-protection/enterprise-dlp)

**proofpoint.**



## USEFUL CONTACT DETAILS

If you would like to contribute to a future issue of New Perimeters, or to give feedback, contact: [info-EMEA-Customer@proofpoint.com](mailto:info-EMEA-Customer@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](http://www.proofpoint.com/us/support/technical-training)  
[training@proofpoint.com](mailto:training@proofpoint.com)

### Proofpoint University:

[www.proofpointlevelup.com](http://www.proofpointlevelup.com)

### Proofpoint Community Support:

[www.proofpoint.com/community](http://www.proofpoint.com/community)

### Professional Services:

[services@proofpoint.com](mailto: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 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](http://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.

**proofpoint.**