Transforming DLP

Why insider threat management should be a critical part of your data loss prevention program

proofpoint.

Preventing Data Loss in an Era of Transformative Change

An employee of a well-known technology company steals gigabytes of its confidential data and then holds that data for ransom.[1] A massive breach exposes the information of 22.5 million Malaysian citizens, including the country's home minister.[2] An employee of a global electronics firm pastes confidential source code into ChatGPT to check for errors.[3] The wrong file is emailed to people outside a healthcare organization and exposes the personal data of 14,000 employees.[4]

Each of these real-world cases is unique. But they all resulted in data loss—along with public relations issues, remediation costs and the brand damage that comes with it.

Data loss, which can result from both external compromise and insider threats, has always been a serious security issue. But in modern business settings, the challenge has become even more complicated and acute. That's because today's organizations have embraced cloud-based infrastructure, remote work and a varied mix of employees, contractors and outside vendors.

1   Bleeping Computer. "Former Ubiquity Dev Pleads Guilty to Trying to Extort His Employer." February 2023.
2   The Straits Times. "Data from 22.5 Million Malaysians Born 1940 – 2004 Allegedly Being Sold for US$10k." May 2022.
3   Mashable. "Whoops, Samsung Workers Accidentally Leaked Trade Secrets via ChatGPT." April 2023.
4   Infosecurity Magazine. "Data Leak Hits Thousands of NHS Workers." February 2023.
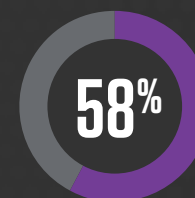
While every organization is unique, one thing is always true: data doesn't move itself. People move, misuse and leak data.
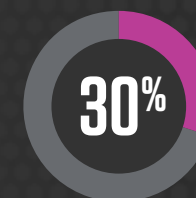
71%
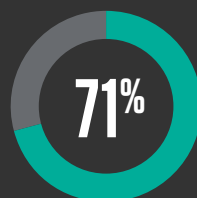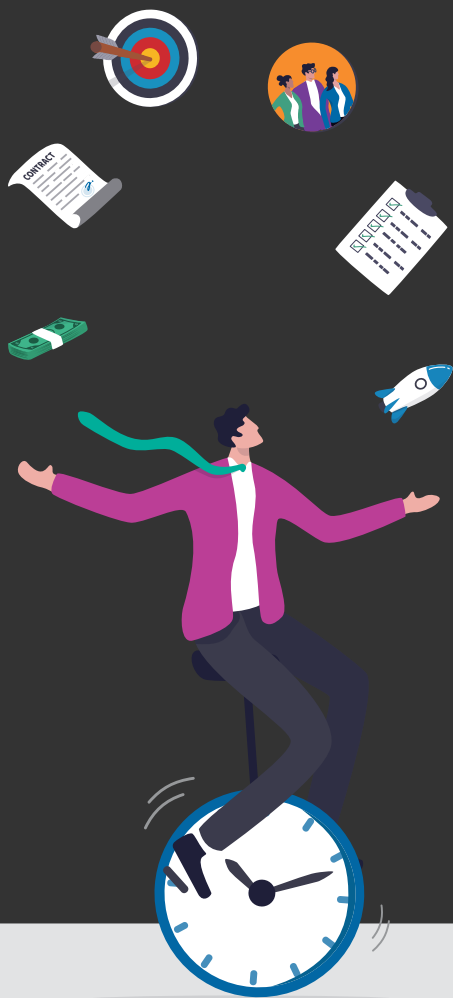
of respondents stated that a careless user was the cause of data loss.[5]

20%
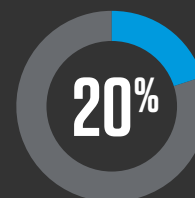
of respondents stated that a malicious employee or contractor was the cause of data loss.[6]

58%

of organizations had compromised cloud accounts.[7]

30%

of tenants experienced post-compromise data exfiltration or manipulation.[8]

Compounding the data loss challenge, compliance regulations are more complicated. And the penalties for noncompliance are more severe than ever before.

Solving it requires a new approach.

This e-book explores the growing challenges of today's fast-evolving workplace and IT environments. It explains why traditional data loss prevention (DLP) approaches aren't up to the task. And it provides a roadmap for DLP built for the way modern organizations work.

5   Proofpoint. *Data Loss Landscape Report*. 2024.
6   Ibid.
7   Ibid.
8   Ibid.

| Introduction | Section 1:
Data Loss and the Modern Organization | Section 2:
Why Insider-Led Data Loss Must Be Part of Your DLP Strategy | Section 3:
The Modern DLP Difference | Conclusion |

SECTION 1

Data Loss and the Modern Organization

For most organizations, the last few years have been a whirlwind of change. 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 and data security more challenging, especially for teams using security tools and processes built for an earlier era of work.

Careless users may make an honest mistake or try to take a shortcut to do their jobs.

Compromised users may have their accounts taken over and misused by an outside cyberattacker.

Malicious users can intentionally exfiltrate data for personal gain.

More remote and hybrid workers

In the past few years, the nature of work has been completely transformed. Today, terms such as "work from home" and "work from anywhere" are now a part of our regular lexicon. Remote work and hybrid work schedules, once considered a job perk, are now routine. No longer are knowledge workers bound to their cubicles, 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.

59%

of employees whose jobs can be done remotely are working from home all or most of the time.[9]

$15 MILLION

is the total average cost of an insider data breach.[10]

71%
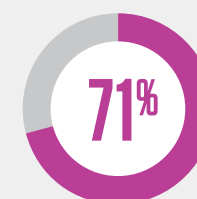
of privilege misuse incidents resulted in data loss.[11]

9 Kim Parker, Juliana Menasce Horowitz, et al. (Pew Research Center). "COVID-19 Pandemic Continues To Reshape Work in America." February 2022.
10 Ponemon. *2022 Cost of Insider Threats Global Report*. February 2022.
11 Verizon. *2023 Data Breach Investigations Report*. June 2023.

Employee turnover

Layoffs, employee churn and resignations can lead to indifferent or disgruntled employees. With little incentive to protect the organizations they're leaving, some of them may be tempted to disregard security policies, steal data—or even sabotage operations.

Users may not realize that the data they produced in the course of their work belongs to the employer. Others may try to take sensitive information to give themselves a leg up in their new job. And in some cases, former employees may simply fall through the cracks, retaining access to the organization's data and systems long after they've left.

So it's no wonder that in a recent Proofpoint study, 63% of surveyed security professionals rated users with access to critical business data as their organization's top cybersecurity risk.[12] The scope of this problem cannot be overstated. Just look at what happened in 2023. Technology companies ramped up layoffs that had begun in 2022 on a massive scale. By April, there were 18,000 employees laid off from Amazon, 10,000 from Microsoft, 26,000 from Meta and 6,650 from Dell—to name just a few. This has pushed insider threats even higher than they already were.[13]

12 Proofpoint. *2024 State of the Phish Report*. February 2024.
13 Claire Meyer (Security Management). "In the Wake of Mass Layoffs, Insider Threats Multiply." April 2023.

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.

Alongside remote work, organizations are embracing the cloud. Users rely on Software-as-a-Service (SaaS) platforms, cloud storage, collaboration tools, chat and videoconferencing.

More places for data to leak

Alongside remote work, organizations are embracing the cloud. Users rely on Software-as-a-Service (SaaS) platforms, cloud storage, collaboration tools, chat and videoconferencing. Even venerable industries such as government, healthcare and manufacturing are using 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 own information, systems and applications. 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 also malicious, careless and compromised users within their ranks.

Generative AI (GenAI) also introduces a new channel for data loss. Employees are embracing it as a new way to work and increase their productivity. But this can mean that they inadvertently leak confidential data. So it's no surprise that 59% of board members believe that GenAI is a security risk for their business.[14] And when security teams try to block sensitive data from leaking, they find that they simply don't have the DLP tools. In response, they often stop employees from using GenAI tools altogether.

14 Proofpoint. Cybersecurity: The 2023 Board Report. 2023.

More "outsiders" with insider-level access

Beyond their 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 key 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 applications and use shared accounts on servers.
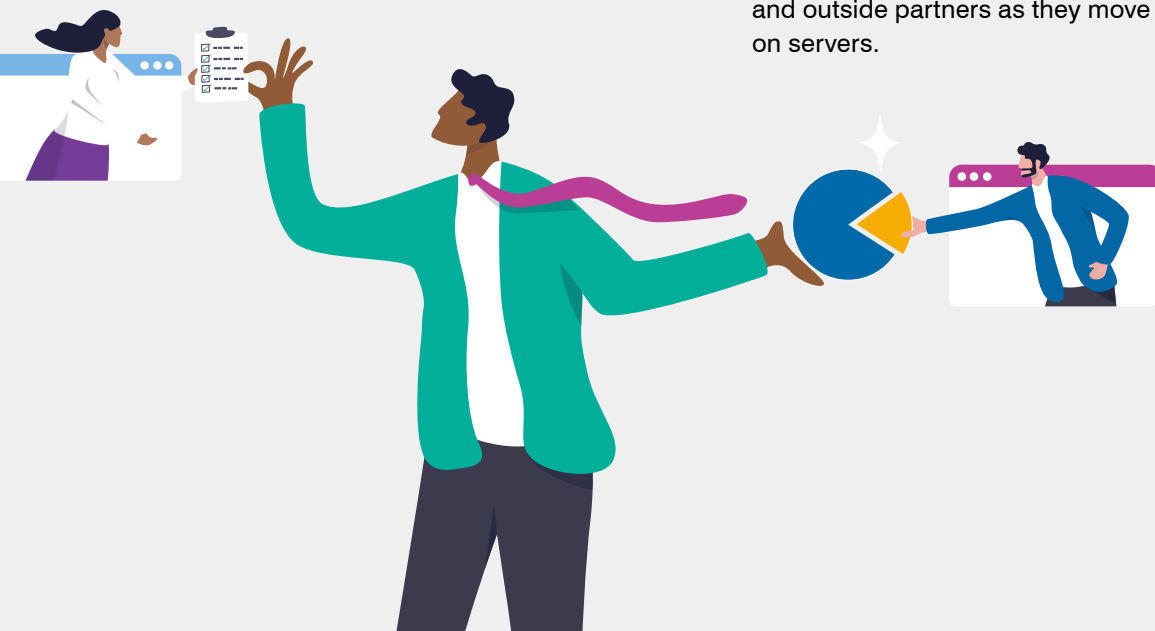
Introduction

Section 1:
Data Loss and the Modern Organization

Section 2:
Why Insider-Led Data Loss Must Be Part of Your DLP Strategy

Section 3:
The Modern DLP Difference

Conclusion

SECTION 2

Why Insider-Led Data Loss Must Be Part of Your DLP Strategy

The ways we create, store and use data have changed. The categories of users who are given access to that data have changed. The risks and potential impacts have changed.

Keeping the trust

Here are a few examples of sensitive or confidential data that DLP is designed to protect:

- Personally identifiable information (PII) for employees and customers

- Personal health information (PHI) for employees and customers

- Personal financial and banking information for employees and customers

- Trade secrets

- Intellectual property

- Customers lists

- Vendor information

- Material nonpublic information

- Other sensitive business information

It's time for our approach to DLP to change, too. Organizations are investing more and more into DLP protection tools and getting less and less from them. With traditional DLP tools, there's no viable way to stop outside threats or threats from within.

These tools attempt a one-size-fits-all security approach to careless, compromised and malicious users. The result: careless users are frustrated and blocked while malicious users and outside attackers simply sidestep the controls.

Organizations can no longer focus on simply securing the perimeter (which could never protect against insider threats anyway). Instead, they must adopt a modern approach to DLP centered around people: who has access to specific data, what they are doing with it and how they are sharing it.

Careless users need coaching. Malicious users need monitoring. And compromised users need fast intervention. In other words, your protection, detection and response methods should change depending on the type of misuse occurring.

That's why incremental improvements aren't enough. Solving the modern DLP challenge calls for a whole new mindset.

DLP: the goal

The main goal of DLP programs is to protect against people moving sensitive or critical data out of the organization in ways that are risky or violate policy.

Increasingly, DLP programs are critical to complying with industry and regional data privacy regulations around personal data.

DLP technologies have a dual challenge. On the one hand, they must ensure that people access and use sensitive or critical data appropriately. On the other hand, DLP solutions shouldn't accidentally block business transactions or hinder user productivity.

Introduction

Section 1:
Data Loss and the Modern Organization

Section 2:
Why Insider-Led Data Loss Must Be Part of Your DLP Strategy

Section 3:
The Modern DLP Difference

Conclusion

$3.5B total projected DLP spending by 2025.[17]

77 DAYS to resolve insider threats.[18]

85% of organizations are targeted by cloud attacks.[19]

56% of incidents relate to user carelessness.[20]

DLP: the reality

Most organizations have adopted traditional DLP technologies to stay compliant. But these tools are often expensive. They're cumbersome to maintain. They get in users' way. And, worst of all, they fail to deliver on their already limited promises.

Organizations need a better way to protect their sensitive data. Large organizations can't just use one DLP tool. Instead, 72% of them cobble together two or more DLP tools as a part of their DLP and data security strategy.[15]

And organizations aren't just using more tools to combat insider threats, they're also spending more than ever before. Since 2016, the average cost of managing insider threats has soared more than 85%. Investigation costs alone for these threats have jumped 18% in only two years.[16]

72% of organizations cobble together two or more DLP tools as a part of their DLP and data security strategy.[15]

18% is how much investigation costs alone have jumped in just two years.[16]

15 Cloud Security Alliance. *Data Loss Prevention and Data Security Survey Report*. 2023.
16 Ponemon. *2022 Cost of Insider Threats Global Report*. February 2022.
17 The Radicati Group. "Data loss prevention (DLP) market revenue forecast worldwide from 2019 to 2025." May 2022.
18 Ponemon. *2022 Cost of Insider Threats Global Report*. February 2022.
19 Assaf Friedman and Itir Clarke (Proofpoint). "How Attackers Use Compromised Accounts to Create and Distribute Malicious OAuth Apps." May 2021.
20 Ponemon. "2022 Cost of Insider Threats Global Report." February 2022.

Data doesn't move itself

People lose and misuse data. That's why protecting data requires knowing the context of what data your people have access to, what they're doing with it and how they're being targeted by cyberattackers seeking access.

Data-centric focus misses important context

Data doesn't move itself. People lose and misuse data. Protecting data requires knowing the context of what data your people have access to, what they're doing with it and how they're being targeted by cyberattackers seeking access. In other words, data-aware DLP is not enough—it must also be people-aware and threat-aware.

Traditional DLP typically overlooks context for these reasons:

- It has limited or no visibility into who is interacting with and moving sensitive data across the cloud, the web, email, print, USB devices and endpoints.

- It lacks insider threat detection and response.

- It cannot connect the dots between activities or view activities that don't rise to the level of an alert but are critical in context.

- It is not integrated with a threat protection platform or real-time threat intelligence.

Data loss detection policies are hard to write, easy to evade

Traditional DLP tools were built for regulated data that is easy for tools to detect and hard for users to alter. To avoid false positives, they require policies that are precise and granular. A typical policy might detail traits such as data identifiers, application name, data exfiltration channel and so on.

This level of policy detail was manageable when the data was stored in databases, on servers and at a few static locations.

Today, sensitive business information, regulated data and intellectual property can appear almost anywhere in all kinds of files and documents. This shift has made DLP policies much harder to write and far easier to evade.

Sensitive data and files are much harder to recognize and label with simple data identifiers. And users can easily change them—whether for a legitimate business reason, by accident or as part of a malicious action.

Countering such actions requires writing and maintaining a complex list of overlapping DLP policies. Any telemetry on data movement outside of a detected alert is stored in log files that are, at best, hard to access and analyze. And no user behavior or threat telemetry is recorded at all. If security analysts want to piece together these events into a narrative sequence for context, they have to do it manually or by using several disparate tools.

It's no wonder most security teams have such little visibility into data movement across their organization.

What are the top priorities for your organization's IT security department over the next two years? *(pick up to three)*

Improving information protection and data classification, enabling business innovation (DevSecOps, product development)	39%
Consolidating and/or simplifying security solutions and controls	37%
Outsourcing security controls	35%
Addressing insider threats	34%
Improving employee cybersecurity awareness	34%
Addressing supplier risk	33%

Source: *2023 Voice of the CISO*

| Introduction | Section 1:
Data Loss and the Modern Organization | Section 2:
Why Insider-Led Data Loss Must Be Part of Your DLP Strategy | Section 3:
The Modern DLP Difference | Conclusion |
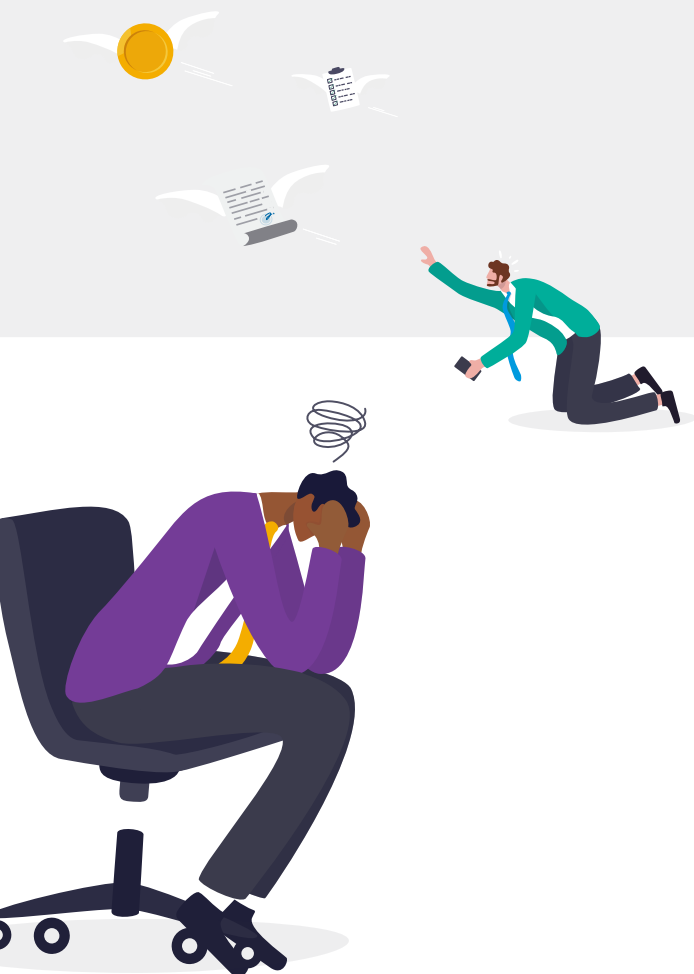
Limited prevention of careless users' mistakes

Clearly, these narrowly defined policies limit the degree to which traditional DLP tools can protect data. They also fail to address accidental or careless user behavior that leaves sensitive data exposed. To understand why this is such a problem, consider an all-too-common example of user carelessness: misdirected email.

It's easy for users who are in a hurry to make mistakes when they're adding recipients to their emails because most webmail and native email clients now offer address autofill. Unfortunately, small mistakes can quickly add up. According to 2023 data from Tessian (now a Proofpoint company), about one-third of users sent about two emails to the wrong person annually. That means a business of 5,000 employees can expect to deal with around 3,400 misdirected emails per year.

Or consider the issue of hard-to-decipher controls. These can lead users to inadvertently put their data at risk by sharing it publicly or with GenAI tools rather than just within the organization. Data can be compromised simply because traditional DLP tools weren't built for malicous or risky user actions.

Controls burden users, strain systems

Beyond resource-heavy endpoint agents, other aspects of traditional DLP tools can strain system resources and saddle users with onerous controls that get in the way of real work.

The more organizations need from their DLP tools, the less they get. They may try to set up complex and overlapping detection and prevention policies that require deeper content inspection only to see slower performance as a result.

Introduction

Section 1:
Data Loss and the Modern Organization

Section 2:
Why Insider-Led Data Loss Must Be Part of Your DLP Strategy

Section 3:
The Modern DLP Difference

Conclusion

96%

of users know when they are taking a risky action but do it anyway.[21]

Why users hate legacy DLP tools

Traditional DLP tools can also be overzealous in their blocking polices. With remote and hybrid work styles becoming the norm, security teams can hardly predict all the ways people may choose to work. When organizations rely on blocking policies, they prevent their people from using the public internet, accessing personal email at work or working with new cloud-based tools. Take GenAI tools as an example. Legacy DLP tools can't prevent data loss via prompt submissions. Blunt security practices such as web filtering GenAI sites will only drive employees underground, preventing security teams from understanding how the technology is used and increasing risks.

Ultimately, security teams can't block employees from taking risky actions and putting themselves and the organization at risk. Even the best technical defenses can be undermined if users don't follow basic best cybersecurity practices. In a recent Proofpoint survey, 71% of users said that they took a risky action, and almost all of them—96%—were aware of the dangers but did it anyway.[21]

When blocking policies become stumbling blocks

Some DLP systems may even block legitimate processes simply because they aren't listed within DLP policies and approved lists. This is a major issue for modern businesses, which rely on friction-free digital transactions and communication. When DLP policies mistakenly block a legitimate transaction or message, security teams are left dealing with users' complaints.

In the worst cases, the endpoint DLP clashes with another endpoint security tool or causes system crashes. The result isn't just more security-related support tickets and emails. These have real bottom-line impacts on employees, customers and partners.

21 Proofpoint. *2023 State of the Phish Report*. February 2023.

Introduction

Section 1:
Data Loss and the Modern Organization

Section 2:
Why Insider-Led Data Loss Must Be Part of Your DLP Strategy

Section 3:
The Modern DLP Difference

Conclusion

Data discovery and classification take too long

With traditional DLP solutions, discovering and classifying data can take months. Instead of focusing on how users are moving data in real time, in potentially risky ways, traditional DLP focuses on what happened to data in the past.

The data discovery process is slow. Searches usually run only outside business hours to avoid the heavy toll they take on system performance and productivity.

Another problem is that most DLP tools cannot ingest prior data classification efforts, including Microsoft Information Protection, without high-priced professional services. With each new program, organizations have to reclassify their data within the new tool.

Deployment and maintenance are complex and expensive

Deploying traditional DLP tools—especially on premises—is often complex and expensive. Installing and integrating servers, applications, databases and other infrastructure can take months. Time-to-value can be even longer.

Endpoint DLP products can be just as problematic. Many use kernel-mode endpoint agents. These agents intercept every OS-level transaction and thus are heavy on the endpoint. They can bog down users' work, interfere with applications and even crash the device. (In many cases, these issues are so severe that they crop up in early testing stages.)

Once installed, many DLP products require setting up and maintaining complex rules and policies—a major investment of time and money.

False positives lead to alert fatigue

DLP incident responders are also frustrated by the lack of accuracy of traditional DLP solutions. To halt a potential breach in progress, they need to act fast. But they often have a difficult time dealing with the sheer volume of DLP alerts, many of them false positives.

According to one survey, 80% of respondents say that one-fifth of their cybersecurity alerts are false positives. What's more alarming, more than half (55%) say that their team has missed critical alerts because they don't prioritize alerts effectively.[22]

80%

About 80% of respondents say that one-fifth of their cybersecurity alerts are false positives.[22]

22 Orca Security. *2022 Cloud Security Alert Fatigue Report*. March 2022.

SECTION 3

The Modern DLP Difference

Unlike legacy DLP tools, a modern approach to DLP focuses on people, not just data. It's an adaptive approach that changes based on whether the risks and threats come from careless, compromised or malicious users.
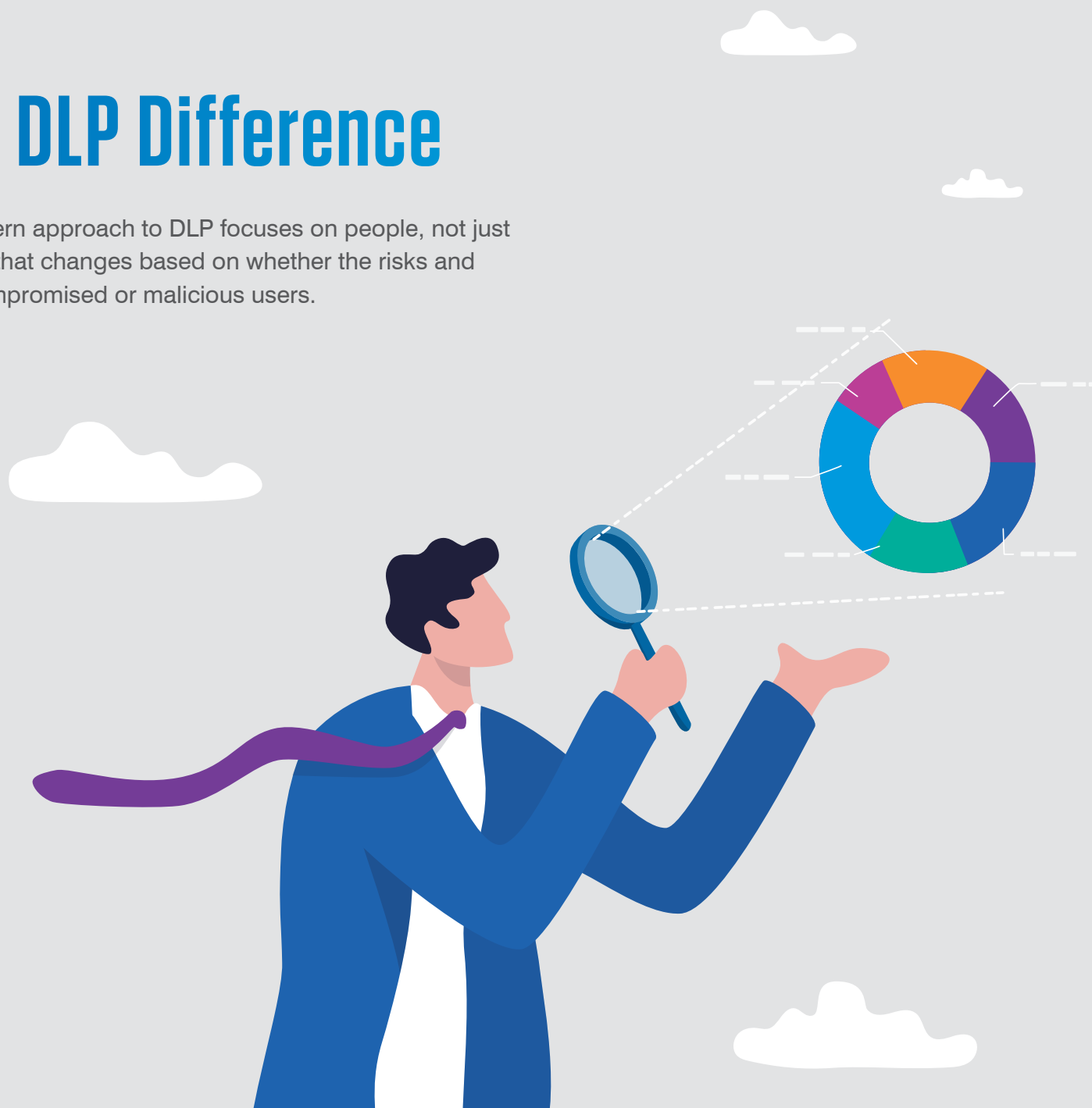
Focus on people, not just data

It's an adaptive approach that changes based on whether the risks and threats come from careless, compromised or malicious users.

A modern approach to DLP offers a consolidated, easy-to-manage solution that works across all the tools people use—email, the cloud, endpoints, the web and file shares. And it uses a cloud-based architecture that is easy to deploy, offers privacy and security by design, easily scales up and integrates with a broader security ecosystem.

Modern DLP is more effective and requires less administrative overhead than traditional DLP. It also enables faster investigations, response and remediation, which makes severe data breaches less likely. And it makes security teams more efficient and productive.

Here are just a few of the benefits of modern DLP over traditional DLP:

- A unified console, simplifying management
- Data controls for managed and unmanaged devices
- Fast and easy deployment, accelerating time to value
- Scalability as organizations grow and change
- Privacy by design to keep pace with increasing data privacy regulations all over the world
- Context to discern malicious, compromised and careless users
- Better protection for sensitive data and intellectual property, including acceptable use policies for GenAI tools
- Consistent policies across multiple channels
- Extensibility to work in concert with the broader security ecosystem—without the need for significant engineering effort

Introduction

Section 1:
Data Loss and the Modern Organization

Section 2:
Why Insider-Led Data Loss Must Be Part of Your DLP Strategy

Section 3:
The Modern DLP Difference

Conclusion

Careless users may make an honest mistake or try to take a shortcut to do their jobs.

Beyond blocking risky activity, modern DLP provides coaching to help them understand and change their behavior while keeping them productive.

Compromised users may have their accounts taken over and misused by an outside cyberattacker.

Modern DLP uses risk-aware controls to look for signs of compromise and apply additional security controls, blocking risky activity where needed.

Malicious users can intentionally exfiltrate data for personal gain.

Based on risk factors such as resignations or unusual activity around sensitive files, modern DLP can monitor some users more closely, apply stronger access controls and proactively block malicious actions.

Modern DLP is human-centric

A modern DLP solution connects malicious, compromised and careless users to any data movement or risky behavior across files, applications and endpoints. It shows the sequence of events so that cybersecurity, IT, human resources and legal teams can quickly and easily understand the context. That means anyone, not just the IT team, knows the "who, what, where and when" around security alerts and incidents—and just as important, what the user intended.

The main building blocks of people-centric DLP are:

- **Content awareness** to identify sensitive or regulated data across multiple digital channels, leveraging such capabilities as data classification, labeling/tagging, multi-column exact data matching, dictionaries, proximity matching and more.

- **User behavior** awareness to recognize user activity and determine intent across digital channels, access activity, file sources and destinations, drives, networks, roles, watch lists and more.

- **External threat awareness** coupled with threat intelligence to pinpoint compromised accounts and users who were victims of phishing campaigns across the cloud and email.

With people-centric DLP, security teams can differentiate between a malicious, compromised or careless user based on context. This insight enables teams to optimize and automate their security approaches more effectively.

This is why industry experts like Gartner say that DLP and insider threat management (ITM) platforms are converging. A siloed approach to tracking data movement and user behavior doesn't cut it anymore. You need to be able to connect all the dots. With the convergence of DLP and ITM, you can do just that.[23]

23 Gartner. *Market Guide for Data Loss Prevention*. 2023.

Introduction

Section 1:
Data Loss and the Modern Organization

Section 2:
Why Insider-Led Data Loss Must Be Part of Your DLP Strategy

Section 3:
The Modern DLP Difference

Conclusion

Modern DLP is consolidated and unified

Switching context and screens in any technology role is challenging and inefficient. Studies show that frequent context switching (also known as multi-tasking) can be stressful and distracting. According to one study, people take nine and a half minutes to get back into a productive workflow after switching applications. It's no wonder that 45% of people said it makes them less productive, and 43% called it very tiring.[24]

Modern DLP solutions offer a better experience for security and IT teams. Beyond the productivity benefits of a single console, a modern approach gives IT and security experts a more complete picture of data loss.

It brings all three primary digital channels—endpoint, email and cloud—into a cohesive whole. All alerts are accessed in one console so that technical teams have the complete picture right in front of them. They can follow along as a user moves data between channels. And they can prevent exfiltration even when the data originates in one channel and leaves in another.

24 Qatalog and Cornell University's Ellis Idea Lab. "Workgeist Report '21." June 2021.

Modern DLP is cloud-native and scalable

A modern DLP solution is a cloud-based one. That's because it has to be.

Most organizations have embraced cloud-based IT. But traditional DLP tools are architected to be on-premises. That means they don't scale. They don't offer the security modern organizations need. They're hard to manage and aren't extensible, so they can't evolve to keep up as your infrastructure and needs change.

A modern cloud-based architecture is the only way to scale up the scope of your DLP solution without a major performance hit—and sizable financial outlay. It's also the only way to get visibility into all of the digital channels that matter.

Cloud-based DLP architectures sit on top of lightweight but comprehensive telemetry collectors. They use a combination of cloud application API connectors, user-mode endpoint agents and email gateways to give you a full picture of data movement, use behavior and outside threats.

In short, you get powerful, application-agnostic visibility into what the user does in email, cloud and endpoint without hindering their work. A cloud-based approach also offers security controls that prevent users and compromised user accounts from accidentally or maliciously sharing data.

Modern DLP is adaptive and risk-based

People and data all come with varying degrees of risk. Some people may be constantly targeted by attackers. Others may have access to highly privileged data. And a few are more likely to fall for scams. Likewise, all data isn't equally at risk. Activities around sensitive data may peak and then plunge. And new—and unprotected—content and data types are created every day.

Security teams are faced with the seemingly impossible task of keeping data safe in an environment that's constantly in flux. That's why modern DLP solutions dynamically adapt to people risks and data risks.

Modern DLP solutions are converged with ITM, so they can protect against people risks. Because they understand who is most at risk from attacks, they can better protect the data that these users interact with. But that's not all. They can also see user behavior in context so that only risky actions are flagged. And they can adapt security rules and policies according to each user's changing roles and permissions.

Modern DLP solutions also have a much better grasp of which data needs to be protected thanks to AI-powered classifiers. This gives them the ability to automatically analyze and monitor a much broader range of content. Plus, it applies labels and tags, which means you can control who can access or edit that content and whether it must be encrypted when transmitted.

This gives them the ability to automatically analyze and monitor a much broader range of content. Plus, it applies labels and tags, which means you can control who can access or edit that content and whether it must be encrypted when transmitted.

Emerging technologies, like GenAI, have the potential to significantly change the way we work. When companies are able to identify a broader range of content, they can implement more flexible acceptable use policies for GenAI tools.

Introduction

Section 1:
Data Loss and the Modern Organization

Section 2:
Why Insider-Led Data Loss Must Be Part of Your DLP Strategy

Section 3:
The Modern DLP Difference

Conclusion
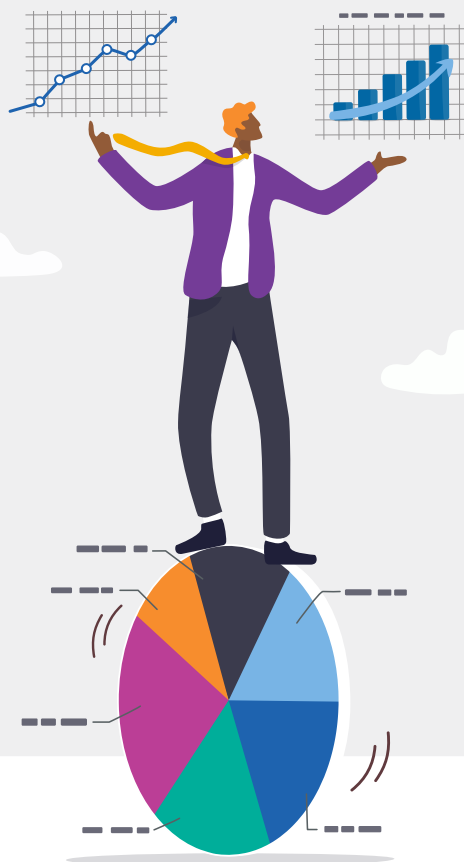
The case for modernizing your DLP approach

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

Monitor

Legacy DLP Capabilities	Modern DLP Capabilities	Use Cases
Partial	Complete	Data classification
None	Complete	Insider risks (malicious users, privileged users, departing employees, server and workstation usage)
None	Complete	Third-party application usage
None	Complete	Threat hunting and DLP analytics (including data and file history)
Partial	Complete	GenAI tool usage (application of acceptable use policies)

○ None   ◑ Partial   ● Complete

Detect

Legacy DLP Capabilities	Modern DLP Capabilities	Use Cases
Complete	Complete	Intellectual property and regulated data loss across cloud, email and endpoint (accidental data leakage or malicious data exfiltration)
None	Complete	Abnormal user behavior (compromised logins, malicious content or malicious user behavior)

Prevent

Legacy DLP Capabilities	Modern DLP Capabilities	Use Cases
Complete	Complete	Data loss across channels (email, cloud and endpoint)
None	Complete	Abnormal user behavior (compromised or malicious users)

Respond

Legacy DLP Capabilities	Modern DLP Capabilities	Use Cases
None	Complete	Data loss, insider threat and account compromise investigations
Partial	Complete	Integrations across SIEM, SOAR, business communication and ticket management tools

Conclusion

Organizations are embracing the cloud, a work-from-anywhere culture and innovation as a core value. It's time that your DLP solution did, too.
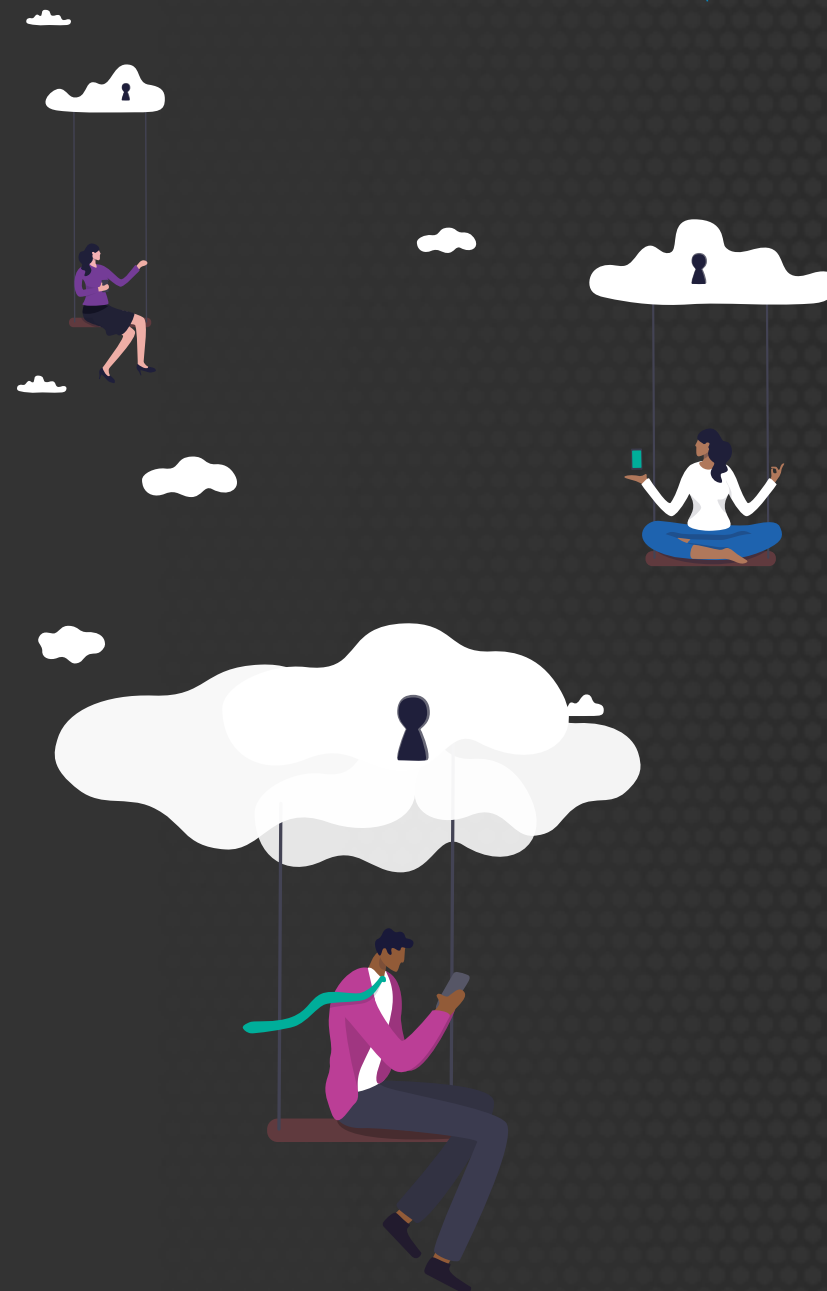
Built on a cloud-based architecture, modern DLP reduces data loss from insider risks and external threats, streamlines your team's workflow and speeds up incident detection and response.

As you embark on your own modern DLP journey, look for a solution that takes a holistic approach to data loss and includes these essential elements:

- **Scalable information protection.** Protect all data types, email and cloud applications in a way that adapts to the people misusing information, whether they are careless, malicious or compromised.

- **Cloud-native, flexible architecture.** Enable seamless integrations with other security solutions.

- **Fast deployment with a lightweight footprint.** See what's going on across the endpoint, cloud and email with deployments completing in just days or weeks.

- **Security and privacy by design.** 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.

Learn more about how Proofpoint can help you deploy a modern DLP architecture.
Visit www.proofpoint.com/us/products/information-protection

Introduction

Section 1:
Data Loss and the Modern Organization

Section 2:
Why Insider-Led Data Loss Must Be Part of Your DLP Strategy

Section 3:
The Modern DLP Difference

Conclusion

LEARN MORE

For more information, visit **proofpoint.com**.

proofpoint.