

Redefining 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 cybersecurity vendor sells data from 68,000 customers to a phone scammer.¹ A large Singaporean healthcare provider leaks the records of 1.5 million patients, including the country's prime minister, in a series of major security lapses.² An IT vendor's poor security hygiene causes France's oldest national daily newspaper to expose 7.4 billion records, including readers' personal information.³

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.

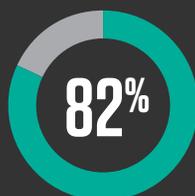
Data loss, which can result from both external compromise and insider threats, has always been a serious security issue. But in modern business settings, the challenge has become even more complicated and acute. That's because today's organizations have embraced cloud-based infrastructure, remote work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

1 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.

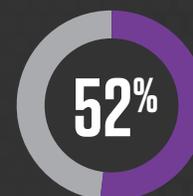
While every organization is unique, one thing is always true: data doesn't move itself. People move, misuse and leak data.



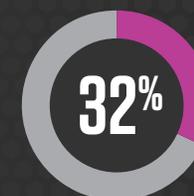
of breaches involved a human element⁴



of breaches involved malicious, negligent or compromised insiders⁵



of organizations had compromised cloud accounts⁶



of compromised organizations faced post-compromise activity in cloud accounts: manipulation, email forwarding and OAuth app activity⁷

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.

⁴ Verizon. "2022 Data Breach Investigations Report." June 2022.

⁵ Ibid.

⁶ Itir Clarke and Assaf Friedman (Proofpoint). "OAuth abuse: Think SolarWinds/Solorigate campaign with focus on cloud applications." March 2021.

⁷ Ibid.

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 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 cyber attacker.



Malicious users can intentionally exfiltrate data for personal gain.

More remote and hybrid workers

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. Remote work and hybrid work schedules, once considered a job perk, are now routine. No longer are knowledge 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.



of employees whose jobs can be done remotely are working from home all or most of the time⁸

\$15 MILLION

is the total average cost of an insider-caused data breach⁹



of misuse resulting from data breaches involved privilege abuse¹⁰

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

Employee turnover

Resignations, layoffs and employee churn 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 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.

According to business risk consultancy Kroll, today's fluid labor market and economic turbulence may push already-soaring insider threats even higher in the months ahead.¹¹



¹¹ Laurie Iacono, Keith Wojcieszek et al. (Kroll). "Q3 2022 Threat Landscape: Insider Threat, The Trojan Horse of 2022." November 2022.

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 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, negligent and compromised users within their ranks.

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 apps and use shared accounts on servers.

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 negligent, compromised and malicious users. The result: negligent 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.

Negligent 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.

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.

\$3.5B

total projected DLP spending by 2025¹⁴

77 DAYS

to resolve insider threats¹⁵

85%

of organizations are targeted by cloud attacks¹⁶

56%

of incidents relate to user negligence¹⁷

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.

It's no wonder that 81% of decision makers—even before the pandemic—said they need a better way to protect their sensitive data while keeping up with the pace of innovation.¹²

It's not for lack of trying. Organizations are spending more than ever before to combat insider threats. The average cost of managing insider threats has soared more than 85% since 2016. Investigation costs alone for these threats have jumped 18% in only two years.¹³



81%

of decision makers—even before the pandemic—said they need a better way to protect their sensitive data while keeping up with the pace of innovation.¹²



18%

is how much investigation costs alone have jumped in just two years.¹³

¹² Forrester. "It's Time For Next-Generation Data Loss Prevention." May 2019.

¹³ Ponemon. "2022 Cost of Insider Threats Global Report." February 2022.

¹⁴ The Radicati Group. "Data loss prevention (DLP) market revenue forecast worldwide from 2019 to 2025." May 2022.

¹⁵ Ponemon. "2022 Cost of Insider Threats Global Report." February 2022.

¹⁶ Assaf Friedman and Itir Clarke (Proofpoint). "How Attackers Use Compromised Accounts to Create and Distribute Malicious OAuth Apps." May 2021.

¹⁷ Ponemon. "2022 Cost of Insider Threats Global Report." February 2022.

Data doesn't move itself

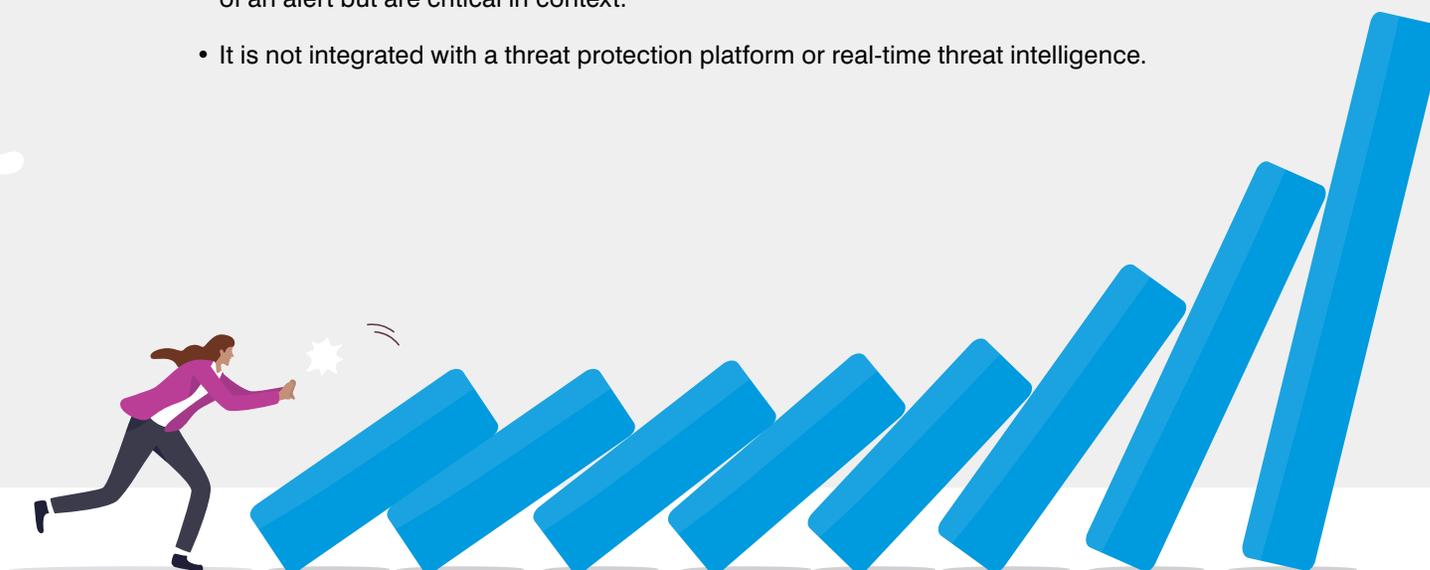
People lose and misuse data. That's why protecting data requires knowing the context of what data your people have access to, what they're doing with it and how they're being targeted by cyber attackers seeking access.

Data-centric focus misses important context

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 cyber attackers 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 because

- 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 within 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.

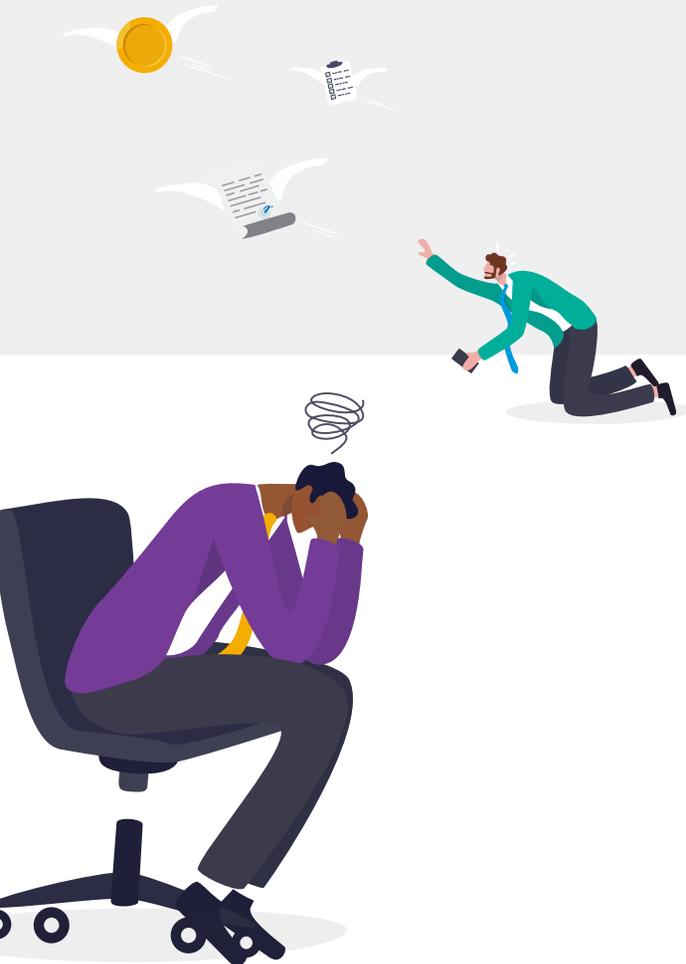
Countering such actions requires writing and maintaining a complex list of overlapping DLP policies. Any telemetry on data movement outside of a detected alert is stored in log files that are, at best, hard to access and analyze. And no user behavior or threat telemetry is recorded at all. If security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



Source: 2022 Voice of the CISO



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. (Leaving databases unprotected and storing passwords in unsecured files are just two all-too-common common examples.)

In some cases, hard-to-decipher controls can lead users to inadvertently put their data at risk by sharing it publicly rather than just within the organization. Data may be compromised simply because traditional DLP tools weren't built for malware 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. (Talk about perverse incentives!)

Why users hate legacy DLP tools

Traditional DLP solutions can also be overzealous in their blocking policies. 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.



Employees in 73% of all organizations that deploy DLP complain about it.¹⁸



66% of companies say their DLP solutions often prevent employees from accessing data even when they follow policy.¹⁹

In a Forrester survey, employees in 73% of all organizations that deploy DLP complain about it.¹⁸ It's easy to see why. It gets in the way of productivity. Often, it mistakenly blocks users from accessing or sharing data even if they are following policy.

In the same survey, 66% of companies say their DLP solutions often prevent employees from accessing data even when they follow policy.¹⁹ The unintended result: users abscond to shadow IT (unsanctioned apps and services) to get their work done.

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' (justified) 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.

¹⁸ Forrester. "It's Time For Next-Generation Data Loss Prevention." May 2019.

¹⁹ Ibid.

Some 75% of IT leaders surveyed by Forrester said deploying their DLP solutions took at least a month. A full 24% said it took six months or longer.²⁰

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.

Some 75% of IT leaders surveyed by Forrester said deploying their DLP solutions took at least a month. A full 24% said it took six months or longer.²¹



²⁰ Forrester. "It's Time For Next-Generation Data Loss Prevention." May 2019.

²¹ Help Net Security. "Alert overload still plagues cybersecurity industry." March 2021.



About 70% of respondents say that up to 3 out of every 4 alerts they investigate each day are false positives.²²

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 apps 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 a setting up and maintaining of 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 a recent survey, about 70% of respondents say that up to 3 out of every 4 alerts they investigate each day are false positives.²² What's more alarming, close to half of those polled said they turn off high-volume alerting features when they get overwhelmed—which means serious alerts may be missed completely.²³



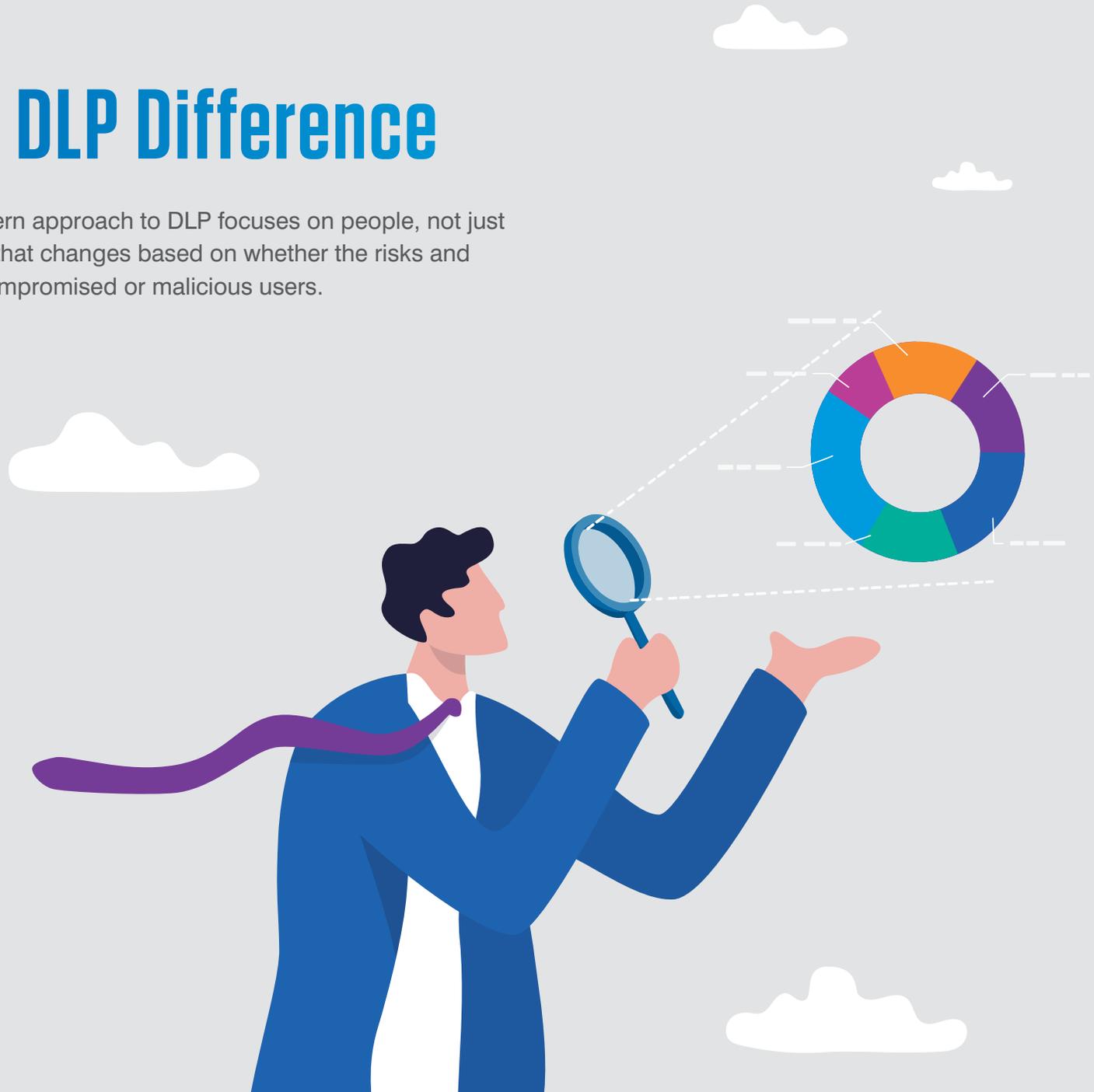
²² Help Net Security. "Alert overload still plagues cybersecurity industry." March 2021.

²³ Ibid.

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 negligent, 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 negligent, 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:

- 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 negligent users
- Better protection for sensitive data and intellectual property
- Consistent policies across multiple channels
- Extensibility to work in concert with the broader security ecosystem—without the need for significant engineering effort



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 cyber attacker.

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 people-centric

A modern DLP solution connects malicious, compromised and negligent users to any data movement or risky behavior across files, apps 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-centricity 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 negligent user based on context. This insight enables teams to optimize and automate their security approaches more effectively.

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 multitasking) 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 apps. 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, network 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 app 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, app-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.

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
		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)

None Partial Complete

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		
		Data loss across channels (email, cloud and endpoint)
		Abnormal user behavior (compromised or malicious users)
Respond		
		Data loss, insider threat and account compromise investigations
		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.

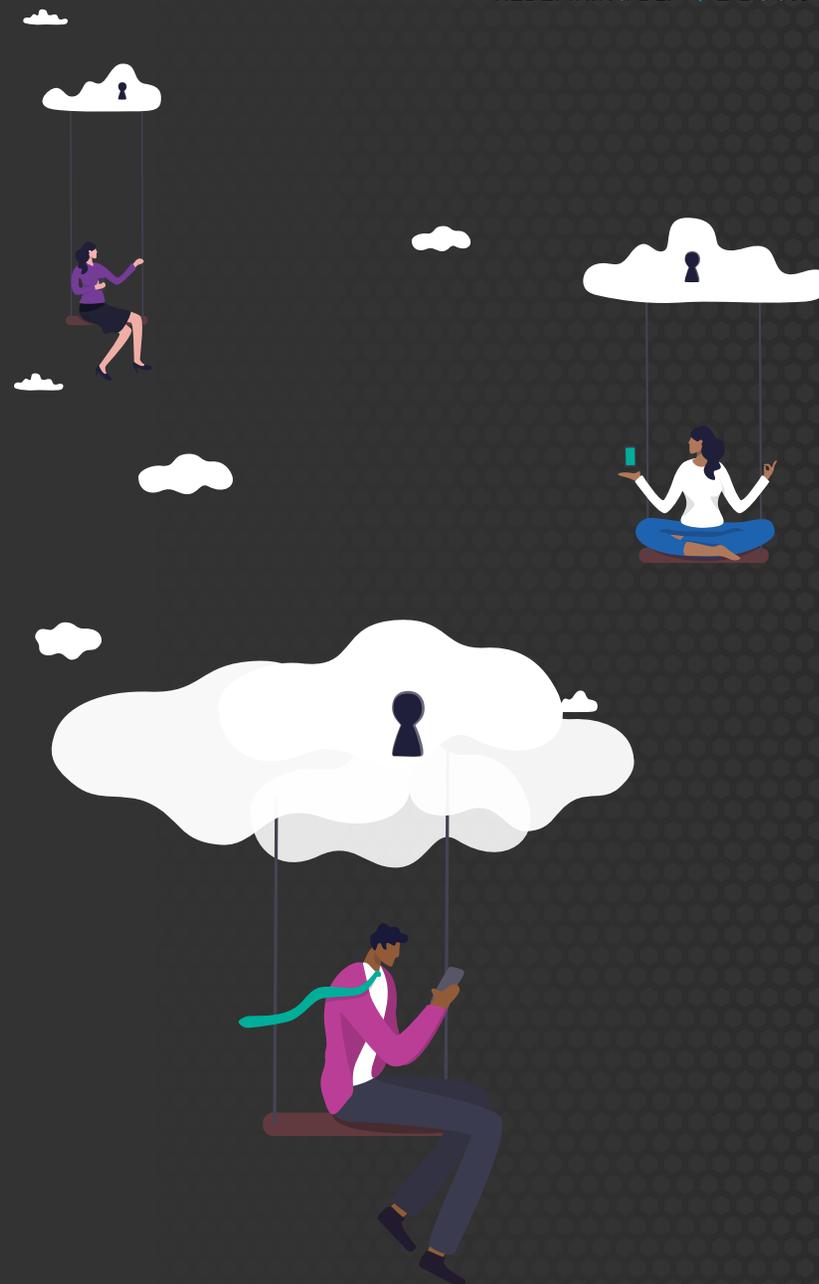
Built on a cloud-based architecture, modern DLP reduces data loss from insider risks and external threats, streamlines your team's workflow and speeds up incident detection and response.

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 apps in a way that adapts to the people misusing information, whether they are negligent, 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 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



LEARN MORE

For more information, visit [proofpoint.com](https://www.proofpoint.com).

ABOUT PROOFPOINT

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

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. [Proofpoint.com](https://www.proofpoint.com)