proofpoint.

E-BOOK

Top Three User-Focused Information Protection Use Cases in the Cloud Era

proofpoint.com

Insider-related incidents cost companies on average $11.45M[1]

77 days on average to contain each insider threat[2]

Introduction

Not every data breach is caused by external attackers. In fact, most data breaches stem from insider threats. Our research found that in the last two years, insider threats have risen 47%.[1] This trend reveals a real and often under-addressed cybersecurity threat. No matter what form it takes, all data loss has something in common—it always involves people.

Now is a critical time to rethink information protection. Organizations often relegate data loss prevention (DLP) products of old to a checkbox on a compliance list. But the middleman approach—intercepting data between the user and the network—hasn't stopped sensitive data from getting into the wrong hands. The lack of telemetry and actionable alerts bred dangerous blind spots. That's because the focus stayed firmly on traditional data leakage prevention, authentication and perimeter controls.

[1] Proofpoint. "2020 Cost of Insider Threats Global Report." April 2020
[2] Ibid.

Now that the security community knows better, protecting data requires a new strategy. Today's organizations need a people-centric approach that addresses the entire spectrum of data loss. Most people do not go to work with the intention of leaking data. But they are often targeted by others with less noble intentions. And besides, humans make mistakes—the simple act of working generates risk.

In this e-book we take a closer look at the people-centric nature of data loss incidents. Through three use cases, we'll explore data loss scenarios and the risk they pose to your organization.

1
The Compromised User

2
The Malicious User

3
The Negligent User

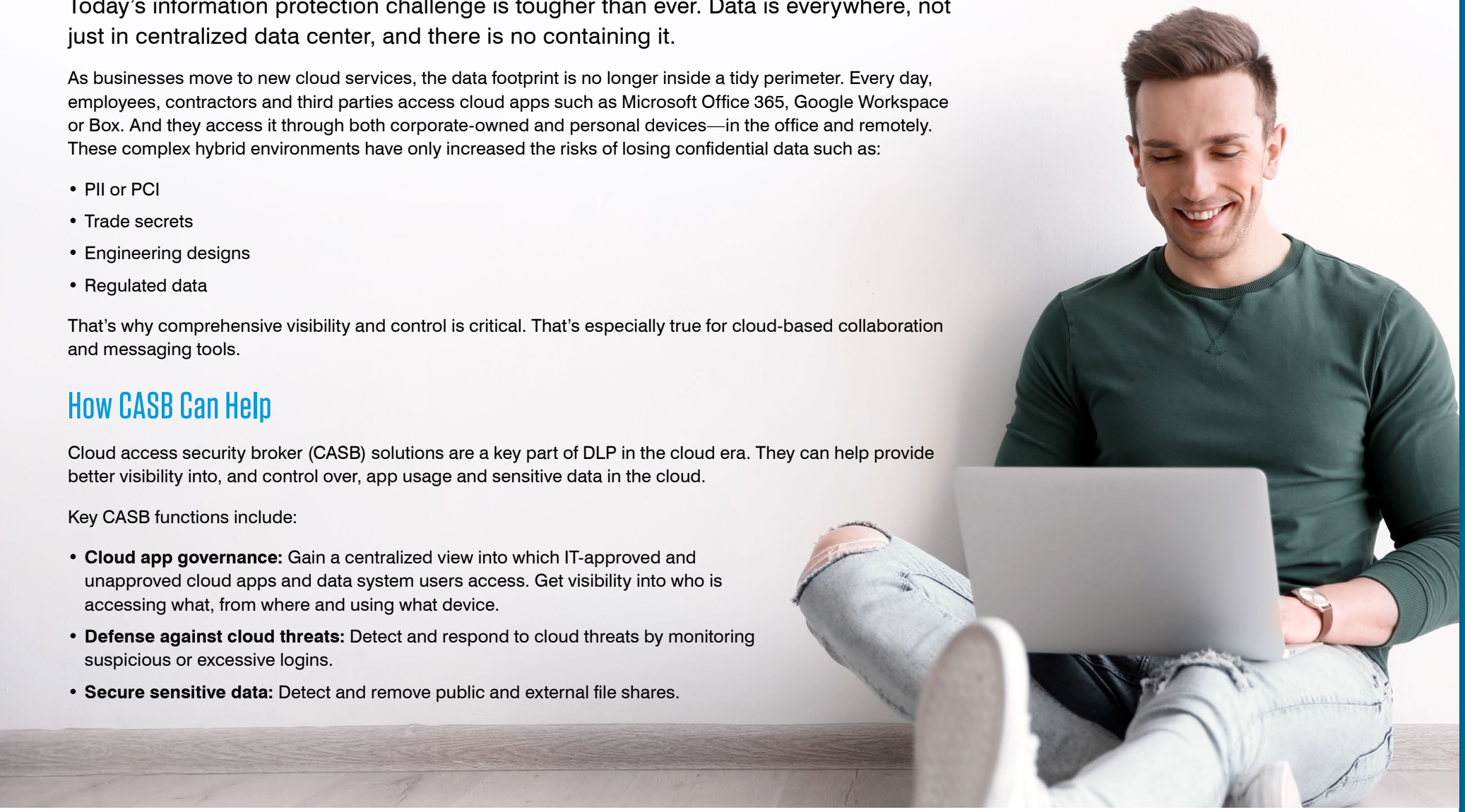
Information Protection in the Cloud Era

Today's information protection challenge is tougher than ever. Data is everywhere, not just in centralized data center, and there is no containing it.

As businesses move to new cloud services, the data footprint is no longer inside a tidy perimeter. Every day, employees, contractors and third parties access cloud apps such as Microsoft Office 365, Google Workspace or Box. And they access it through both corporate-owned and personal devices—in the office and remotely. These complex hybrid environments have only increased the risks of losing confidential data such as:

- PII or PCI
- Trade secrets
- Engineering designs
- Regulated data

That's why comprehensive visibility and control is critical. That's especially true for cloud-based collaboration and messaging tools.



How CASB Can Help

Cloud access security broker (CASB) solutions are a key part of DLP in the cloud era. They can help provide better visibility into, and control over, app usage and sensitive data in the cloud.

Key CASB functions include:

- **Cloud app governance:** Gain a centralized view into which IT-approved and unapproved cloud apps and data system users access. Get visibility into who is accessing what, from where and using what device.
- **Defense against cloud threats:** Detect and respond to cloud threats by monitoring suspicious or excessive logins.
- **Secure sensitive data:** Detect and remove public and external file shares.

Where to Focus Your DLP Efforts

Data doesn't lose itself.

It's the people within the organization that utilize the data. It's the people that lose the data. And it's people that should be the focus of your information protection efforts.

The cloud has expanded the threat surface, but it is only part of the protection equation. Data has mushroomed. People are working from anywhere. And they are using more devices and cloud apps. Still, users are always the central security issue.

Most users cause no problems. But organizations should always plan for the worst. Understanding user risk personas and how each causes data loss can help you manage the potential risks. While some security controls span personas, they are applied in different ways based on each persona's unique traits and other risk factors.

Use Case #1:

The Compromised User

The Compromised User

ABOUT:

As someone with privileged access to data, the compromised user is a prime target for exploitation. This user is often unaware of their appeal to attackers and will unknowingly fall victim to credential compromise or malware that compromises their devices.

Very Attacked People

Proofpoint coined the term Very Attacked People (VAPs) to describe this category of users. Attackers used to favor high-volume opportunities or "spray and pray" tactics. Now they use a more targeted approach.

They may start with diligent research on the target. This may include gaining access to organizational charts and collecting information from social media and other sources. These attackers often know how organizations work better than security teams do. Armed with this information, attackers then narrowly target key users, usually with higher rates of success.

How Attacks on Compromised Users Work

Here's how organizations lose data through compromised users:

1. The attacker gains access to the user's credentials through a social engineering attack such as phishing and malware-based compromise.
2. Armed with the same access and privileges as the compromised user, the attacker can now access everything the victim can.
3. From there, the threat actor steals data or moves further into the organization's network or cloud for more valuable data.

Over 61% of breaches within hacking involved credentials.[3]

[3] Verizon. "2021 Data Breach Investigations Report." 2021

Protecting From the Compromised User

Do you know who your VAPs are? If not, you should.

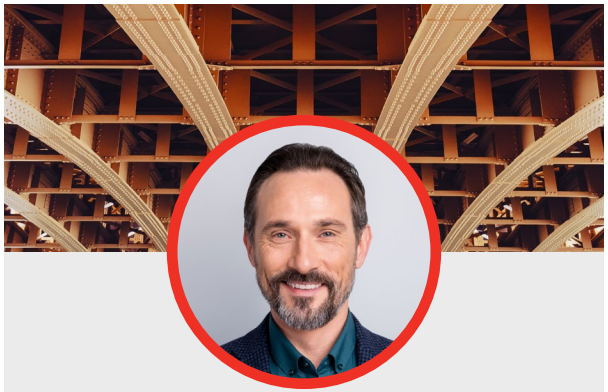
Compromised users are often unaware that they are the starting point for data loss scenarios. For that reason, organizations must deploy controls that actively look for suspicious behavior across channels that may trigger data leakage.

The Compromised User Protection Checklist:

- **Protect users from compromise.** Cutting off the source of risk is an important step in data loss prevention. For VAPs, adaptive security controls like Proofpoint Email Isolation can help. This defensive technique insulates VAPs from URL and web-based attacks by analyzing and isolating anything they click on within corporate email, based on a configured policy.
- **Train users on good cyber hygiene and to spot potential compromise.** A people-centric approach to cybersecurity always includes training. Users should know security best practices such as:
  - Keeping usernames and passwords a secret
  - Knowing who is sending an email before opening
  - Identifying suspicious-looking login screens to prevent compromise
- **Gain visibility post-data compromise.** When a user account is compromised, Email DLP and encryption becomes the next line of defense. These tools offer visibility into what type of data is being sent through email. It automatically enforces rules such as blocking or encrypting based on what data the email contains.
- **Stop risks from spreading into the cloud.** Organizations can use CASB to help mitigate risks that start with OAuth abuse by automatically revoking access tokens for Microsoft 365 and Google Workspace that pose potential risk.
- **Monitor and remediate compromised cloud accounts.** When cybercriminals compromise the credentials for Microsoft 365 or Google Workspace accounts, they can launch attacks inside and outside of your organization. Cloud Account Defense (CAD) correlates cloud and email threat activity to:
  - Identify users at risk
  - Detect compromised accounts
  - Automate security response with flexible policy controls

Use Case #2:

The Malicious User



The Malicious User

ABOUT:

Unlike the compromised user, the malicious user knowingly causes harm. This employee consciously undermines the sanctity of corporate data by leaking it out for personal gain. The malicious user is usually financially driven, often part of an industrial espionage scheme. In this scenario, the insider steals trade secrets, such as engineering designs or source code, and sells it to a competitor or on an illegal market.

The malicious user often understands the security controls in place and will work to bypass security hurdles in their way.

What Makes Malicious Users So Dangerous? Trust.

Malicious users can be the hardest to detect. They have gone through the organization's hiring process, including background checks, and knows the environment. The result: implicit levels of trust and access to confidential data.

And because they are doing something they know is wrong, these users often take steps to avoid being detected. They maneuver around DLP tools. They exploit blind spots to exfiltrate data. They cover their tracks.

Users' methods of stealing data vary from old-school USB drives that are still commonly used by field teams to more advanced techniques such as steganography (hiding a data file within another data file). Leaving no trace behind, malicious users often clear cookies and browser caches—or just wipe the endpoint clean.

Criminal or malicious insiders are to blame for 23% of attacks, costing organizations an average of $755,760 per incident.[4]

[4] Proofpoint. "2020 Cost of Insider Threats Global Report." April 2020

Protecting From the Malicious User

The only way to catch the malicious user is with tools that provide visibility into the full spectrum of user activity. That includes watching data movement. Armed with the knowledge of how all users are accessing data, organizations can then spot outliers that may represent a malicious user.

The Malicious User Protection Checklist:

Reduce the cloud attack surface. A workforce is likely to include employees, contractors, partners and consultants. And they need varying levels of access to cloud applications, data and other resources. This expanded attack surface makes it easier for the malicious user to hide.

A CASB can shine a light in the dark corners of the cloud by consolidating visibility on cloud usage at a global, application and user level. With this insight, organizations can identify software-as-a-service (SaaS) files at risk. That includes details such as ownership, activity and who they shared it with. Plus, it can reveal activity on orphaned and compromised accounts to stop any malicious activity.

Keep a watch on where malicious data exfiltration could happen. Deep visibility into how the malicious user tries to exfiltrate data, and whether the intent is malicious, are critical in protecting from DLP. By using behavioral analysis, organizations can ease investigations and determine what the user was attempting by having a full audit trail of activities such as:

- Installing unsanctioned tools (FTP, hacking and spoofing)
- Privileged use (password change)
- Backdoor access (shell scripts, network/OS changes)

Stop critical data from leaving. Cloud-based Enterprise DLP can be easily and quickly deployed to detect and keep sensitive data and confidential information from leaking outside the organization using custom dictionaries or custom identifiers. If the malicious user attempts to exfiltrate confidential data via their corporate email account, personal cloud storage or a USB, Enterprise DLP will provide visibility for investigations and stop the attempt to alleviate administrative headaches.

Use Case #3:

The Negligent User

The Negligent User

ABOUT:

Negligent users are well-meaning people who accidentally leak confidential or sensitive data. For example, while working at home on their personal device the negligent user may download PII data. They may then modify it and save it to their personal cloud storage, rather than the company-managed cloud storage.

Since 2018, the average number of incidents involving employee or contractor negligence has increased from 13.2 to 14.5 per organization.[5]

Anyone Can be a Negligent User

New employees acclimating to corporate systems and users with poor cyber hygiene are only a portion of an organization's negligent users. Seasoned employees are a culprit too. Especially as users are increasingly working remotely and often from multiple devices. Thus creating a greater chance of mishandling corporate sensitive data.

Four Common Forms of Human Error:

1. Falling for Phishing Attacks – As people work on the go on their mobile devices or are distracted by other priorities, they are more susceptible to clicking a link or attachment they might otherwise have questioned to be suspicious.
2. Poor Credential Management – Sharing passwords, reusing passwords across various online platforms, using obvious passwords and not using a password manager—the list of poor credential practices can go on forever—all leading to inadvertently exposing data.
3. Mis-sent Emails – As people send emails, oftentimes the email client begins auto filling the name. If users don't get the warning message of "Did you mean to send it to…" they may send PII or other sensitive data directly into the hands of an unintended recipient.
4. Unauthorized Users Accessing Corporate Devices – Especially with remote work, corporate-issued devices are outside of the office and available for unauthorized use by people not associated with the organization.

[5] Proofpoint. "2020 Cost of Insider Threats Global Report." April 2020

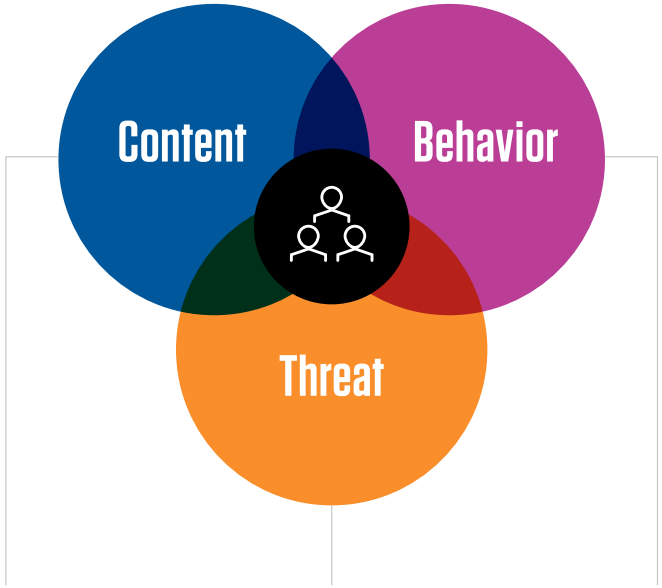
Protecting From the Negligent User

We cannot change humanness, instead organizations need security guardrails to predict and thwart our mistakes and negligent actions.

The Negligent User Protection Checklist:

- **Improve cyber hygiene:** Training should be as relevant as possible to the negligent user's day-to-day work to make it more impactful. While we encouraged VAPs to receive "defensive training," the negligent user benefits from offensive techniques to make them more mindful of security when working.
- **Keep cloud apps secure:** Beyond strong passwords, training and authentication, CASB adds an extra layer of protection against negligence. It can proactively:
  - Prevent sharing of confidential content with too broad an audience
  - Stop downloads from corporate apps to personal devices
  - Stop uploads of sensitive data to personal instances of cloud storage
  - CASB also provides granular visibility in situations when employees lose their devices, use shadow IT or if they share their password with someone which leads to compromised accounts, regardless of if the devices are managed or unmanaged.
- **Stop accidental data loss with robust DLP and encryption:** To protect against the negligent user accidentally sending confidential data to places it shouldn't go, Email DLP classifies all data sent through the email channel and can then either be blocked, quarantined or encrypted automatically.
- **Get visibility into how users work with data on their endpoint devices:** An insider threat solution allows you to see when users complete actions such as copying files to removable storage, printing or even copying to their cloud storage. In the case of the negligent user, this is often done unintentionally, but leads to a teachable moment for users to be re-trained on data security best practices.
- **Allow personal email, but isolate traffic:** Many organizations provide access to personal email even though it creates risk. To balance employee happiness and security, email isolation allows access, but locks the ability to attach files. This limits the risk of accidentally sending confidential company information through personal channels.

Key Telemetry to Understand and Mitigate All User Risk



Content Aware

Identify **sensitive** or **regulated** data.

Data classification, labeling/tagging, exact data matching, and more.

Threat Aware

Identify **compromised** accounts, **phished** users.

Advanced threat intel/ insights across cloud and email telemetry.

Behavior Aware

Identify user **activity**, **intent**, and **access** context.

User activity across channels, file source and destination, device, network, role, watchlist, and more.

Across the three personas, we recommended several of the same security controls, including Proofpoint CASB and Proofpoint Email DLP. But how each of these works depends on the type of user, which is identified with key telemetry.

How do you differentiate and defend against each user?

Understanding content—what is within an outgoing email or file—used to be the standard in DLP. But it did not include insight into compromised and malicious users. Today we have advanced to address the risks posed by all three personas with telemetry across email, endpoint and cloud.

Threat awareness gives insight into the compromised user to determine whether an account was compromised, how it was compromised, and to discover the data exfiltration.

Threat awareness would help you discover that an Microsoft 365 account was compromised through a state-sponsored actor resulting in data exfiltration.

Behavioral awareness uncovers insider threats by tracking behavior and isolating outliers. By weaving together user actions across different channels of data loss, a pattern of behavior can emerge pointing to a malicious user.

Behavioral awareness would help you understand that an employee is downloading a more-than-normal number of files from OneDrive and then doing another anomalous activity by installing a Dropbox client on the same machine.

Content awareness, while the oldest approach, provides insight on users. It identifies sensitive data to ensure that people aren't making any human errors with it.

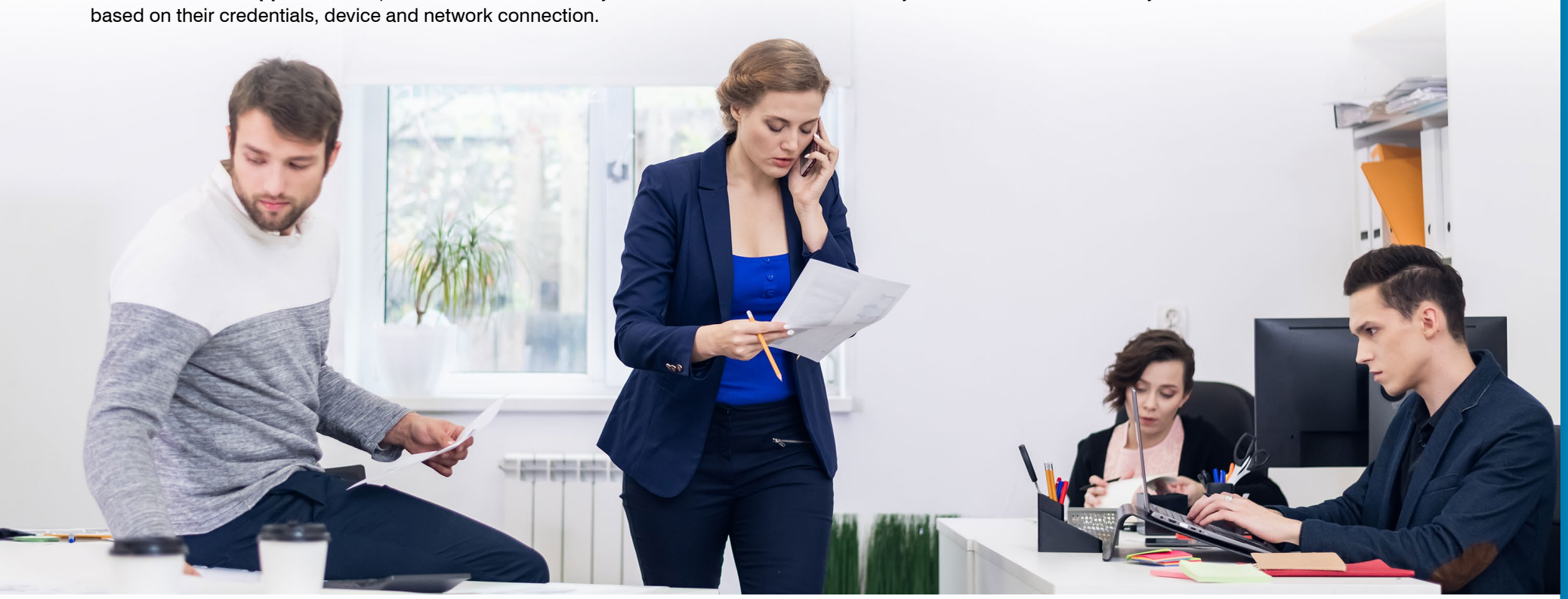
Content awareness would reveal if a user tried to send a healthcare record containing PHI to the wrong patient.

Key Benefits of Protecting Against the User Trifecta with People-Centric DLP

Even if your organization has a DLP strategy in place, the cloud era calls for change to address its unique challenges. Using a people-centric approach to information protection, you can ensure that you are securing where the real risk starts—your people—across email, cloud and endpoint.

When you adopt a people-centric approach to DLP, you can expect to:

- **Save time and administrative hassle:** Common DLP classifications can be applied across channels, resulting in less work and more security.
- **Experience faster investigation time and response:** With both threat and behavior telemetry added to content, you have all the information you need to determine intent and risk. Combining insights into a modern timeline, you can understand whether the user who triggered the DLP alert is compromised, malicious or negligent. And with a unified incident and investigations interface, you can quickly respond. Response actions might include shutting down a compromised cloud account or applying encryption to the email that triggered the policy.
- **Take a zero-trust approach:** People-centric DLP continually ensures users have access to only the data and resources they need based on what is known about them based on their credentials, device and network connection.



Proofpoint: Your Single Source for People-Centric Security

When every second counts, you need a DLP solution that provides the full picture of user-caused incidents through visibility, detection and context. Proofpoint Enterprise Data Loss Prevention is the only people-centric solution that ensures you are alerted to the critical signs of data exfiltration and other policy violations. It gives you the "who, what, where, when, and why" of every event to help you protect your data.

Today's cloud-based platforms need cloud-based protection
Proofpoint brings together features and benefits to protect you end to end quickly and easily. The company's unified cloud architecture speeds up deployment so that you derive value right away.

Instead of protecting hundreds of thousands of users in weeks or months, Proofpoint protects your users in days. And it's not just about immediate protection and value. Each day it uses the cloud to update our software to ensure your protection stays ahead of attackers for continuous protection in a changing threat landscape.

You get access to all the tools you need:

Proofpoint Enterprise Data Loss Prevention

Address the full range of risk with comprehensive telemetry.

Proofpoint Email DLP

Leverage pre-built policies and deep content scanning to detect and manage sensitive data in email.

Proofpoint Email Encryption

Define encryption policies to meet the demands of your business while business communications flow securely.

Proofpoint CASB

Grant the right levels of system and data access to users and third-party add-on apps based on your business' risk factors.

Proofpoint Insider Threat Management

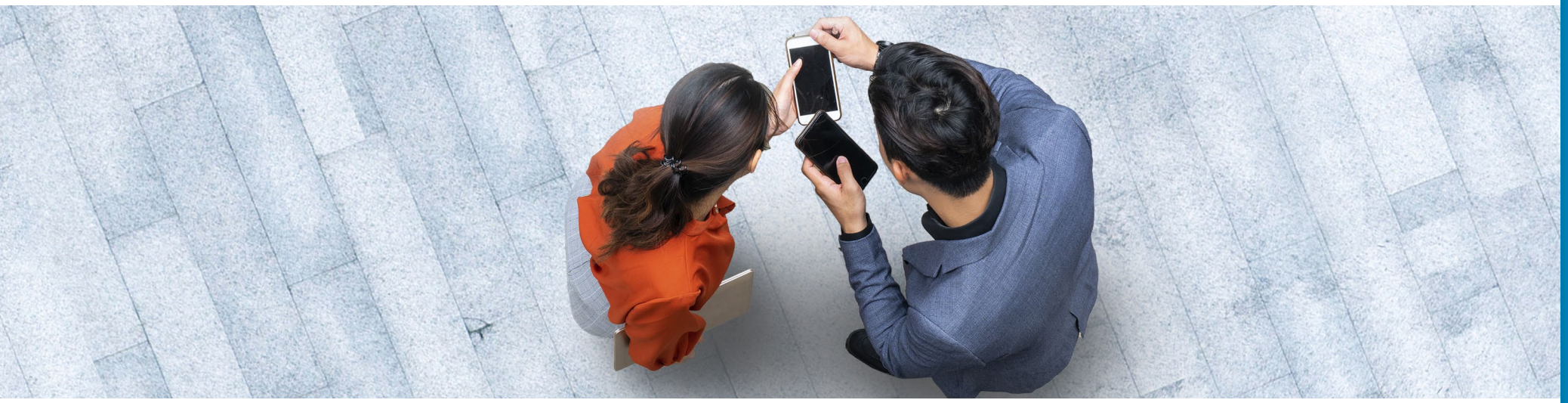
Protect against data loss, malicious acts and brand damage involving insiders acting maliciously, negligently or unknowingly on the endpoint.

Proofpoint Data Discover

Quickly discover, visualize and automate remediation of sensitive and confidential data in on-premises file shares and SharePoint sites.

Endpoint DLP

Prevent, detect, and respond to data loss incidents with granular visibility into how users are interacting with data on the endpoint.



Take the next step in moving to people-centric DLP for greater protection in the cloud era.

Learn more at **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) 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.

07/21