proofpoint.

SOLUTION BRIEF

Securing Healthcare Payers with Proofpoint

Defend against human-targeted attacks and regulatory exposure

The insurance companies and health plans, which pay for a large share of U.S. healthcare costs, face many of the same security challenges as other healthcare institutions. That's because threat actors consider financial information to be king. The rise in identity-driven threats, social engineering and supply chain compromise puts sensitive member, provider and financial data at constant risk. One fact remains: Bad actors breach healthcare networks primarily through people.

Proofpoint helps health insurers safeguard their people, defend their data and reduce business disruption. Our cybersecurity and compliance solutions protect you from the attacks that target your workforce, members and partner ecosystem.

Cybersecurity Challenges

These are just some of the challenges that healthcare organizations are up against.

Securing data

Healthcare payer companies collect and maintain the same kinds of personal information about their customers that hospitals and clinics do. You have to protect:

- Protected health information (PHI), such as medical records and lab test results
- Personally identifiable information (PII), such as birth dates and social security numbers
- Payment card information

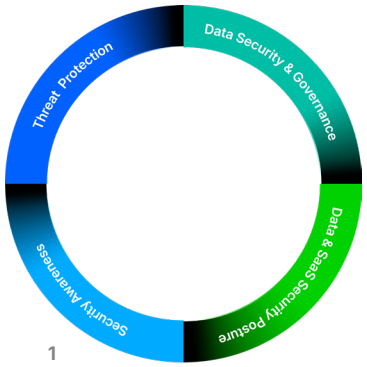
A data breach that compromises any of this information would be devastating. And your organization understandably wants to stay out of the headlines. Such an event could cause damage to your reputation, degrade client trust in you and harm your bottom line in the medium-to-long term. It could also result in compliance fines and financial losses through litigation by victims of the breach.

Dealing with insider risk

Health insurance companies face complex insider risk challenges due to the sensitive nature of member data, the scale of their operations, and the wide range of individuals with access to critical systems such as employees, contractors and third-party vendors. Risks such as unauthorized data access, improper sharing of PHI and PII and credential compromise are common, especially in high-turnover departments like claims and customer service.

One primary insider threat use case for health insurance companies is time fraud. This is when an employee gives someone else access to do their work while still being paid. Time fraud is considered an insider threat because of the harm that can arise from an insider misusing their authorized access to the organization's network, systems or data.

This solution set is part of Proofpoint's integrated human-centric security platform, mitigating the four key areas of people-based risks.



Stopping impersonation and account takeover threats

Healthcare payers are deeply interconnected with a vast ecosystem of third-party vendors, suppliers and service providers. Each represents a potential entry point for cyberattackers. Business email compromise (BEC) targeting these relationships is a growing threat. In one real-world example, a healthcare insurance company was targeted through a real estate development partner involved in building a new office. The attacker impersonated the vendor using a spoofed email domain and requested a change to payment instructions. This is an increasingly common BEC tactic.

In other cases, attackers gain access to legitimate accounts through credential phishing, taking over shared email aliases like help desk accounts to send internal requests or gain access to critical systems. These messages often appear completely legitimate, bypassing basic security filters. Because BEC relies on social engineering rather than malicious payloads, it can be difficult to detect without human-centric controls.

Addressing advanced threats quickly

Advanced threats move quickly. So you must be ready to act on them rapidly. You likely have a team in the security operations center (SOC) that responds to email- and cloud-based threats attacks. The volume of threats, however, can sometimes be overwhelming. Automating security processes can increase the efficiency of the SOC. You should automate the process of reviewing and quarantining suspicious emails, for example. Manual reviews can be extremely tedious, as suspect messages are often duplicated to hundreds of inboxes in an enterprise.

Cloud-based applications are also vulnerable. These applications can be hosted on cloud services or delivered through a software as a service (SaaS) model. To respond to incidents quickly, SOC teams need granular visibility into their entire cloud environment at a glance.

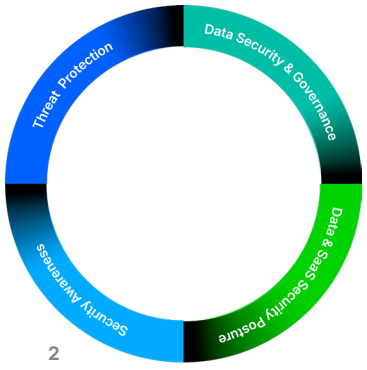
Protecting against legal risk

Your organization must protect against legal risk from healthcare patients and providers. Processing incorrect or delayed claims can damage relationships with both. Doing so often invites lawsuits. When litigation arises, you must have all communications documented and accessible on demand.

Preparing for a cloud-first architecture

Healthcare organizations were late in adopting cloud-based solutions. Some payer organizations, however, have begun to operate in multiple clouds. But they still keep core applications like claims processing on premises. Even so, there is little integration between these clouds. So different workflows are adjacent to one another but are not connected.

As you move applications and workflows to the cloud, you will need to rethink cybersecurity from a cloud-centric point of view. More of your employees will use cloud resources, often remotely. As a result, it will become increasingly impractical to route all network traffic through the data center for security checks. A key to managing a cloud-first architecture is visibility.



60%

Verizon's *2025 Data Breach Investigation Report* found that 60% of breaches involved a human element.

A human-centric approach

Today's cyberattacks target people, not technology. Verizon's *2025 Data Breach Investigation Report* found that 60% of breaches involved a human element. That's why you must take a human-centric approach to secure your members and employees as well as the sensitive data that they use and share.

Figure 1 depicts the top Very Attacked People™ (VAPs) at a real-life large health insurer in the United States. In this VAP analysis, the most targeted roles were contract managers, claims processing staff and accounts payable with a shared alias in the No. 1 spot: the service desk.

These findings show how attackers are focusing on the people and teams that manage sensitive data and financial transactions at scale:

- Accounts payable is a common target for BEC, particularly involving fraudulent invoices or payment redirection schemes.
- Contract managers are often involved in high-value negotiations and vendor relationships, making them attractive targets for credential phishing.
- Claims processors have access to large volumes of PHI and PII that can be monetized or used for identity fraud.
- The inclusion of a service desk shared mailbox is becoming one of the top threat vectors in healthcare. These mailboxes handle password resets, access requests and system support. So gaining access can potentially provide a foothold into broader systems or privileged accounts.

But identifying your VAPs is not enough. A true human-centric approach also recognizes that people inherently pose a cyber risk to organizations. People make mistakes and access critical information that healthcare organizations rely on to operate. Therefore, you must understand risk holistically and build a cybersecurity strategy that can address:

- External attacks
- Human behavioral vulnerabilities
- Appropriate data access privileges

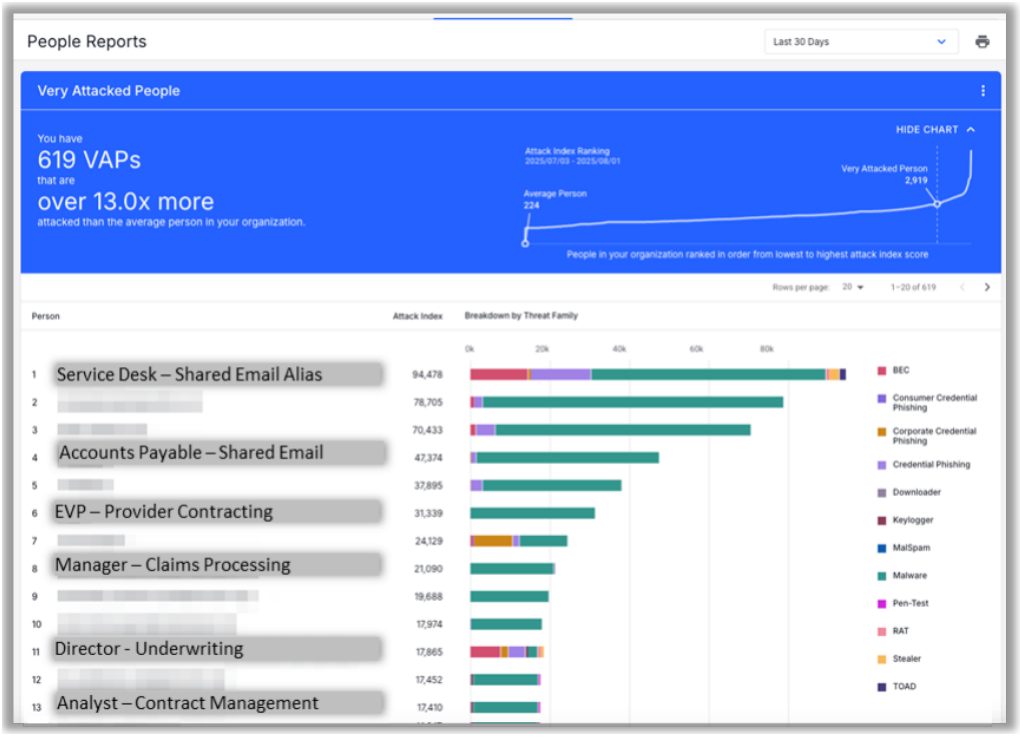
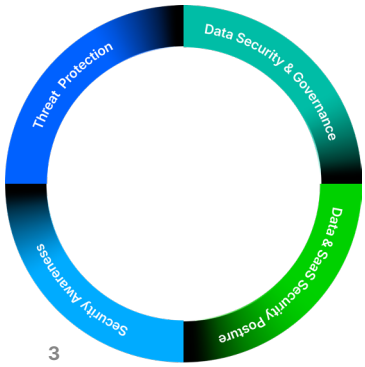
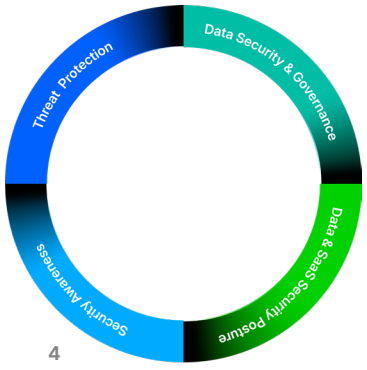


Figure 1: Breakdown of Very Attacked People at a managed health and insurance organization.



Products

- Proofpoint Prime Threat Protection
- Proofpoint Data Loss Protection (DLP)
- Proofpoint Adaptive Email DLP
- Proofpoint Insider Threat Management
- Proofpoint Account Takeover Protection
- Proofpoint Data Security Posture Management (DSPM)
- Proofpoint Digital Communications Governance
- Proofpoint ZenGuide



How Proofpoint Can Help

We give you the tools to protect all your people, from claims processing to sales and marketing. Only Proofpoint offers integrated solutions with a human-centric approach for:

- Threat defense
- Data and SaaS security posture
- Data security and governance
- Security awareness

Protect against advanced threats

Protect against ransomware, general phishing, credential-phishing attacks, email and other forms of digital fraud.

Proofpoint Prime Threat Protection delivers an end-to-end approach to stop all human-targeted cyberattacks—from email to collaboration tools to web applications and social media platforms. Powered by Proofpoint Nexus®, an ensemble of advanced AI, machine learning, behavioral analysis, threat intelligence and visual threat detection, Proofpoint delivers multilayered security that covers the whole threat attack chain—from predelivery to postdelivery and to click-time.

Keep data secure

Keep patient data private and safe from attacks, mistakes and insider risk.

Proofpoint Data Loss Protection (DLP) solutions take an adaptive, human-centric approach to preventing data loss by providing deep visibility into user behavior and content. Protection extends across email, cloud and both managed and unmanaged endpoints. Our DLP solutions are built on a cloud-native architecture with modern privacy controls and a highly stable agent. They scale automatically and are easy to deploy and maintain. A single, unified console helps you manage alerts and investigate incidents across all channels. And powerful analytics enable you to quickly assess data risk, reach a verdict and take action.

Proofpoint Adaptive Email DLP uses behavioral AI to prevent both accidental and intentional data loss by email. To get started, it analyzes more than 12 months of email data to learn the normal email-sending behaviors of employees, their trusted relationships and how they handle sensitive healthcare data. It can then identify anomalous email behavior. When it suspects a misdirected email, misattached file or data exfiltration event is occurring, the user gets a contextual warning message in the moment. This allows them to prevent the data-loss incident in real time, with no administrator input.

Proofpoint Insider Threat Management correlates user activity and data movement. It allows your security teams to detect, investigate and respond to potential insider threats. And it provides real-time detection and response to data exfiltration, privilege abuse, application misuse, unauthorized access, risky accidental actions and anomalous behavior. This helps you detect, prevent and respond to threats such as time fraud within timeline-based visualizations and analytics.

Manage security for the cloud

Keep your people and their cloud apps secure.

Proofpoint Account Takeover Protection detects compromised cloud accounts, protects your cloud environments and secures compromised cloud accounts. It uses AI, threat intelligence and behavioral analytics to detect suspicious activity across the whole attack chain. It detects post-compromise changes made by attackers, removes their access, and reverts malicious updates to mailbox rules and multifactor authentication (MFA) settings. It also removes suspicious third-party applications and quarantines and removes suspicious files. Detailed reporting shows suspicious logins, attacked users and impacted systems and settings.

Proofpoint Data Security Posture Management (DSPM) addresses the root cause of many breaches—blind spots in data environments—while making it a priority to reduce human-centric risks in data security. DSPM identifies where sensitive and valuable data resides, who has access, and which risks pose the greatest threat. As a result, it empowers healthcare organizations to close security gaps, reduce the attack surface and automate compliance. DSPM also ensures that AI tools can be safely adopted.

Stay compliant

Make better, informed compliance decisions, manage risk, and improve litigation readiness.

Proofpoint Digital Communications Governance solutions streamline regulatory compliance, enhance e-discovery processes and mitigate risks. Our comprehensive suite of solutions includes Proofpoint Archive, Automate, Capture, Discover, Patrol, Supervision and Track. Together, they provide a robust framework for capturing, storing, analyzing and supervising various forms of digital communication. These solutions use advanced technologies such as machine learning and intelligent classifiers to automate workflows, reduce false positives and make compliance review processes more efficient.

Change risky user behaviors

Help your employees identify, resist and report attacks.

Proofpoint ZenGuide enables security teams to automate and scale personalized learning paths based on each employee's unique risk profile, behaviors and role. It uses people-risk insights across the Proofpoint ecosystem to understand human risk. And it delivers relevant interventions that build security champions and reduce risky behaviors. Training modules use current, real-world threat examples, so employees are continuously equipped for new dangers. And with ZenGuide reporting, you can measure real-world behavior changes and benchmark them against your industry peers.

Conclusion

By focusing on the individuals most at risk, Proofpoint helps health plans and insurance companies detect, prevent and respond to targeted attacks, data loss and compliance exposure. With unmatched visibility into threat actor tactics and deep insight into user behavior, Proofpoint enables healthcare payers to better protect sensitive member data, ensure regulatory compliance, and build a more resilient workforce in an increasingly complex threat landscape.

proofpoint.

DISCOVER THE PROOFPOINT PLATFORM →

08/25