proofpoint.

SOLUTION BRIEF

Protecting Healthcare Payers with Proofpoint

Mitigating cybersecurity and compliance risks for health plans and insurance companies

Products

- Proofpoint Email Protection
- Proofpoint Email Fraud Defense
- Proofpoint Threat Response Auto-Pull (TRAP)
- Proofpoint Threat Intelligence Services (PTIS)
- Proofpoint Security Awareness Training
- Proofpoint Email Data Loss Prevention
- Proofpoint Content Capture
- Proofpoint Enterprise Archive
- Proofpoint Cloud App Security Broker (CASB)

Key Benefits

- Ensure timely threat response
- Protect sensitive data and comply with regulations
- Bolster protection of growing cloud infrastructure
- Minimize supply chain risk

The insurance companies and health plans that 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. But healthcare payers face uniquely daunting pressures to ensure the security of their payment practices and sensitive data. One fact remains: Bad actors breach healthcare networks primarily through people. Proofpoint can help. Our cybersecurity and compliance solutions protect you, your staff and your customers from these kinds of attacks.

Healthcare organizations of all kinds are seeing a growing number of cyber attacks. The insurance companies and health plans that pay for a big chunk of medical care in the United States are no exception. Like hospitals and clinics, they have two valuable kinds of data: electronic medical records (EMRs) and personal identifiable information (PII), which includes patient financial information. Both types of data can bring big profits to cyber criminals if they got their hands on them.

When cyber criminals steal this kind of data, healthcare payers face incredible financial risk. Compliance fines can be assessed, litigation can lead to large settlement payouts to victims and reputational damage can impact the long-term bottom line. Healthcare payers like you face security challenges that are specific to your line of business. These challenges are unique even among other companies within the healthcare sector. With technological advances, for example, your consumers now demand near real-time service and a seamless, personalized experience. These demands can put added pressure on your already-overextended security and compliance teams. Your organization's decisions on the treatments to cover—and how much to pay for them—have a huge impact on individual lives. So companies like yours inevitably have unhappy providers and customers. Lawsuits are not uncommon, and the integrity of data such as email is critical to reduce legal exposure.

Email is a primary means of communication for your business. Communications with both providers and patients often contain sensitive information. But email also is the most common path that cyber criminals use to get into health insurance companies. The 2020 HIMSS Cybersecurity Survey found that 89% of respondents had a significant security incident in which email was the initial point of compromise.[1] The same report cited email phishing of all types as the primary means for compromising systems and networks.

So protecting your data is critical to the continued success of your business. When a data breach occurs, the financial impacts can be enormous. Everyone is responsible for protecting important data at your company.

Healthcare Payer Cybersecurity Challenges

After 18 months of COVID-19-related disruption and uncertainty, your company is likely looking at a transition back to "business as usual" in the second half of 2021. You'll face many challenges.

Compliance and maintaining client trust

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

- EMRs
- Personal health information (PHI)
- 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.

In the United States, the Health Insurance Portability and Accountability Act (HIPAA) and related federal statutes govern the use of PHI. For health-plan providers that do business in California, the California Consumer Protection Act (CCPA) places sweeping restrictions on how PII is used and stored. Other states have a patchwork of requirements for both PHI and PII. And payment systems must follow payment card industry (PCI) standards.

Rapid incident response

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. This allows them to see the entire cloud architecture at a glance.

Claims integrity and legal mitigation

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. Most have not yet taken a cloud-first approach. 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, like the noodles on a plate of spaghetti, 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. So 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.

Addressing supply-chain risk

Every business relationship runs the risk of supply-chain fraud. One recent intrusion at a healthcare payer company started with a real estate developer that was working with the

[1] HIMSS. "2020 HIMSS Cybersecurity Survey." November 2020.

company to build a new office. Hospitals and clinical providers can present similar but potentially larger risk.

Business email compromise (BEC) attacks are often disguised to look as if they come from trusted partners. A cyber attacker will request sensitive information in the name of a trusted contact. The attack succeeds if a victim responds with that information.

Taking a People-Centric Approach

Our 2020 Healthcare Threat Landscape report discusses Very Attacked People™ (VAPs). VAP is a term we use to define the most heavily targeted employees and email accounts in an organization. Figure 1 shows a real-life example from a healthcare payer, based on Proofpoint telemetry.

In this example, 19 of the top 20 VAPs are not individual people at all. They are email distribution lists. With these lists, email accounts are probably managed by more than one person. For an attacker, these addresses are easy to find on a target company's website. And bad actors know that they are harder to secure. When multiple people have access to an email account, multifactor authentication (MFA) does not work. This means that a username and password are the only layer of defense for the account. When using cloud-based email, the security team must have visibility into these accounts.

In this example, we also see a prevalence of imposter attacks. These attacks are also known as BEC. And as noted, BEC attacks are highly targeted and designed to look like they came from a trusted source. Imposter attacks use social engineering tactics to get staff to transfer money or share sensitive information. They also don't carry malicious payloads. And that makes them difficult to detect.

But identifying your VAPs is not enough. A true people-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 holistic risk and build a cybersecurity strategy that can address:

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

How Proofpoint Can Help

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

- Threat protection
- Information protection
- Compliance

This section discusses many ways we can help.

Rapid threat response: Contain problems before they grow

Real-time response to attacks is critical in today's fast-moving threat landscape. And cyber criminals use email more than any other vector to attack people in healthcare. We offer the

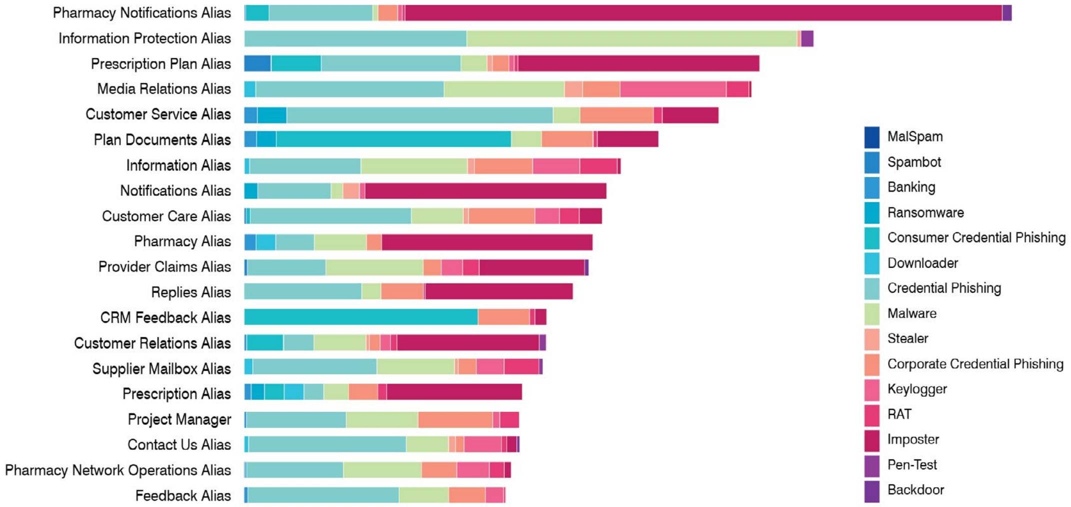

Figure 1: Breakdown of Very Attacked People at a managed health and insurance organization.

following solutions to protect against these threats:

- Proofpoint Email Protection — Helps identify and block malicious email using machine learning and multilayered detection techniques.
- Proofpoint Email Fraud Defense — Augments protection with tools and services to authorize legitimate email. Also provides comprehensive visibility into imposter attacks across your organization and supply chain.
- Proofpoint Threat Response Auto-Pull (TRAP) — Brings automation to the process of analyzing suspicious emails that have gotten through filters.
- Proofpoint Premium Threat Information Service (PTIS) — Provides deeper insight into the threat landscape and your organization's place in it. This kind of information enables you to prioritize security decisions.
- Proofpoint Security Awareness Training — Provides employees with training to spot healthcare-themed social engineering attacks, such as sophisticated phishing ploys.
- Proofpoint Email Data Loss Prevention (DLP) — Prevents data exfiltration. Threat protection may be the best defense, but it is not invincible. This feature protects information even if an exploit slips past your filters and highly trained staff.

Legal and compliance protection: Minimize risk and avoid cost

Healthcare payers are highly regulated. They also face litigation on a regular basis. To comply with regulations, corporate governance standards and court requirements, you must retain all content from all tools that your employees use to communicate. Proofpoint offers the following solutions to help you comply with regulations:

- Proofpoint Content Capture — Delivers this content to your data store or downstream services while maintaining the chain of custody.
- Proofpoint Enterprise Archive — Provides built-in high-performance search, litigation hold and export to address all of your e-discovery needs.

Cloud security: Manage a sprawling infrastructure

Healthcare payers are gearing up for a move to a cloud-first strategy. In the meantime, they struggle with visibility and coordination of security for their sprawling cloud infrastructure. Proofpoint Cloud App Security Broker (CASB) gives people-centric visibility and control over cloud apps, including monitoring suspicious logins and questionable activity.

Conclusion

In the United States, healthcare payers help make the whole healthcare system financially viable. Proofpoint can help your organization protect its confidential data by protecting its most important asset — its people.

With Proofpoint you get:

- Protection against email- and cloud-borne threats
- Visibility into your multicloud infrastructure
- Confidence that your business email is preserved for legal protection
- The most effective cybersecurity protection, whether you are targeted through email, the web, social media or cloud apps

Leading healthcare organizations rely on Proofpoint to prevent, detect and respond to cyber attacks before they cause lasting harm. According to Becker's Healthcare, 9 of the top 10 largest health insurers trust Proofpoint to protect their staff and customers.[2] We help stop threats before they reach clinical and support staff. We safeguard your valuable data and we protect your vulnerable patients from cyber attacks. See our Healthcare Solutions page at **proofpoint.com/us/solutions/healthcare-information-security** to learn more about how Proofpoint can protect your data, operations and care mission.

[2] Morgan Haefner (*Becker's Payer Issues*). "10 largest health insurers." February 2020.

LEARN MORE

For more information, visit **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.