proofpoint.

SOLUTION BRIEF

Securing Healthcare Data with Proofpoint

Protect patient data against insider threats, data loss and cloud risks

Key benefits

- Identify and mitigate risk from negligent, compromised and malicious insider threats
- Ensure scalable protection across all elements of the attack surface as digital footprints grow
- Prevent data loss from email, cloud and endpoints

10%

of all ransomware attacks in the last two years hit the healthcare industry.

Source: SC Media

Healthcare organizations have long been prime targets for cybercriminals. These organizations handle many types of data, including intellectual property (IP), clinical trial data, protected health information (PHI) and personal financial details. Attackers have many options to cash in from an attack on any one of them. As healthcare institutions embrace the cloud, remote work and telehealth, they're also expanding their attack surface. And because employees in the industry operate under increasingly high stress, organizations face increased risk from both malicious and well-intentioned insiders.

Proofpoint provides a human-centric approach to protecting sensitive data in distributed healthcare networks. Our data security solutions deliver unmatched visibility and control of sensitive data. We help you defend your people and their sensitive data against accidental disclosure, malicious attacks and insider risk. Our protective shield extends across cloud services, email, endpoint and on-premises file shares.Your organization can better manage data risk while also saving time and operational costs.

A growing threat

Like many businesses, healthcare organizations store payment card and other financial information. But they also handle vast stores of patient PHI and clinical research data. They even keep data related to government grants. All of this makes them a lucrative target for cybercriminals.

At the same time, the digital footprints of healthcare institutions are getting more complex. The industry now hosts a growing array of services in the cloud. An increasing number of lifesaving internet of medical things (IoMT) devices is expanding their attack surface. Expanded telehealth options also mean that sensitive data increasingly travels outside the network perimeter. And hybrid work rules mean that employees now often work remotely.

Unfortunately, attackers have followed their targets outside the perimeter. In the last two years, the healthcare industry was hit with 10% of all ransomware attacks and cyberattacks targeting the medical sector grew by 32%.[1] These figures are far higher than for other sectors and industries. Data breaches are also more costly in healthcare than in any other industry.

1. Shaun Nichols (*SC Media*). "Cyberattacks targeting medial organizations up 32% in 2024." February 2025.

32%

Cyberattacks targeting the medical sector grew by 32% in the last two years.

Source: SC Media

$9.77M

In 2024, a healthcare data breach cost an average of $9.77 million.

Source: Ponemon Institute and IBM

In 2024, a healthcare data breach cost an average of $9.77 million.[2] This cost can include ransoms paid, systems remediation, noncompliance fines, litigation and brand degradation. System downtime or compromised data integrity can also result in negative health outcomes. They can even lead to loss of life.

Data security challenges

For hospitals, clinics, health insurance providers and biotech firms, data security should be a top priority. These institutions must protect their own research data and IP. But they must also secure patient PHI, personal identifiable information (PII) and payment card data. They face many challenges. This section describes just a few of them.

Prevent EHR snooping and other threats from insiders

Healthcare organizations are some of the most stressful places to work. This means they are at increased risk of insider threats.

Looking for a break, for instance, a curious employee might look at the medical records of a famous patient. This is called electronic health record (EHR) snooping. And it's a serious risk for an institution if the information of a deep-pocketed patient is exposed to the public. Well-meaning, but overwhelmed workers might open phishing emails or accidentally send emails with sensitive data to the wrong recipients. Emotional stress might lead to malicious insider threats against an employer. If a trusted user's account is compromised by credential theft, it can lead to dire consequences before anyone realizes what has happened. Preventing these types of threats requires a proactive approach.

Address the security risks of generative AI

Healthcare organizations are finding a growing list of uses for generative AI (GenAI). These include enhancing clinician productivity, improving patient and member engagement, and streamlining administrative efficiency. They also include optimizing quality of care and delivery, as well as expanding beyond clinical applications to improve overall patient care interactions. But AI use comes with risks. Aside from the dangers of inaccurate or biased output, healthcare providers must ensure that AI models do not inadvertently expose or misuse PHI. This might occur, for example, when AI handles unstructured data such as clinical notes. In addition, integrating GenAI into clinical practice often faces complex regulatory hurdles.

Cover a growing attack surface as healthcare embraces the cloud

Many healthcare organizations were slow to embrace the cloud. But now, almost all of them have multiple services in public, private and hybrid clouds. This has improved patient care by making information available to providers in real time. It has helped organizations streamline operations and reduce the need for capital funding for IT. But it has also expanded the attack surface.

Even when EHRs are housed on premises, details from these records are often accessed, shared and stored elsewhere. Think mobile devices, remote endpoints, IoMT devices and cloud-based email systems. And as healthcare data travels across larger geographies, protecting that data becomes much more of a challenge.

With a growing cloud footprint comes an increased risk of credential theft. More and more office software and collaboration functions are delivered through cloud services such as Microsoft 365 and Google Workspace. As a result, cyber criminals increasingly exploit these services.

2. Ponemon Institute and IBM. "Cost of a Data Breach Report 2024."

Products

- Adaptive Email DLP
- Proofpoint Enterprise DLP
- Email DLP
- Encryption
- Insider Threat Management
- Data Security Posture Management
- Applied Services for Data Security

Unify data security across all channels and platforms

Today's healthcare institutions use many modes to communicate and transfer data. These can include EHR systems such as Epic, cloud-based and on-premises email systems, other messaging systems and file-sharing services. They also have a large array of endpoints. These include PCs at the point of care, hundreds of types of medical devices, desktop computers, laptops and mobile devices. Many workers use multiple devices in a single day. Your sensitive data is housed across servers in both the data center and the cloud. And it regularly travels between the two.

As your attack surface grows and your infrastructure gets more complex, it's even more critical that your security protection is integrated. In the case of data security, this means having integrated data loss prevention (DLP) tools across endpoint, email and cloud.

A human-centric approach

Legacy approaches to data security look only at the data. But information does not lose itself. People allow data loss to happen. They can do so accidentally, or they can do so maliciously. Either way, with cybersecurity, visibility is key. You must understand the personas that are most likely to bring risk. A human-centric approach works to understand the dynamics of the individuals who interact with your data.

How Proofpoint can help

Proofpoint's unified human-centric data security solution gives you unmatched visibility. With a cloud-native interface, you can protect your sensitive information by focusing on the people who interact with it. Our solutions are content-, behavior- and threat-aware. They combine on-premises information protection with cloud security. This ensures that your staff, clinical workers and patients are protected, no matter where their data travels.

Core components of our unified data security solution are the following:

Proofpoint Adaptive Email DLP

Adaptive Email DLP uses behavioral AI to prevent both accidental and intentional data loss by email. 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. With this analysis, Adaptive Email DLP can identify anomalous email behavior when it occurs. When it suspects a misdirected email, misattached file or data exfiltration event is occurring, it shows the user a contextual warning message in the moment. This allows the user to remediate and prevent the data-loss incident in real time, with no administrator input.

Proofpoint Enterprise DLP

Proofpoint's market-leading DLP solutions drive an adaptive, human-centric approach to preventing data loss. They provide deep visibility into user behavior and content, enabling effective detection and prevention of significant data loss risks. Proofpoint updates traditional DLP strategies by integrating protection 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. Using powerful analytics, you can quickly assess data risk, reach high-fidelity verdicts and take appropriate actions.

Proofpoint Email DLP

Proofpoint Email DLP reduces your risks of losing sensitive data through email and ensures compliance by enforcing policy-based prevention and encryption. It's easy to deploy with email security or as part of a unified enterprise DLP approach. Email DLP automates regulatory compliance with out-of-the-box policies for PCI, PII, GDPR, SOX, HIPAA and more. You can also use custom dictionaries — including AI-powered classification — to identify and protect data unique to your organization.

Proofpoint Encryption

Proofpoint Email Encryption automatically protects messages and attachments with complete transparency. Unlike with traditional encrypted email services, this all happens in the background — users don't need to do anything manually. With Email Encryption, you can protect sensitive email messages while ensuring that your affiliates, business partners and users have seamless access to secured messages on computers or mobile devices.

Proofpoint Insider Threat Management

Proofpoint Insider Threat Management (ITM) correlates user activity and data movement. It allows your security teams to detect, investigate and respond to potential insider threats with human-centric behavior awareness. 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 EHR snooping within timeline-based visualizations and analytics.

When an insider threat is identified, Proofpoint ITM provides workflows and irrefutable evidence of wrongdoing to accelerate incident response. This intelligence is collected by lightweight endpoint sensors. It's then analyzed within a modern architecture for scalability, security and privacy. You can also deploy using on-premises or SaaS delivery models.

Proofpoint Data Security Posture Management

Proofpoint Data Security Posture Management (DSPM) addresses the root cause of many breaches — blind spots in data environments — while prioritizing the reduction of human-centric risks in data security. By identifying where sensitive and valuable data resides, who has access, and which risks pose the greatest threat, DSPM empowers healthcare organizations to close gaps, reduce the attack surface and automate compliance. DSPM also enables safe adoption of AI tools by identifying sensitive data, enforcing data protection policies and providing real-time sensitivity analysis for AI workflows.

Proofpoint Applied Services for Data Security

The healthcare industry has been facing a workforce shortage for many years. This has been a real challenge for providing quality care to patients. With fewer skilled workers to manage security, more healthcare organizations are turning to managed services to help them address their security needs. With Proofpoint Applied Services for Data Security, you can use our global team of data security experts to augment your team. We have decades of experience. In this time, we have built best practices and maturity modeling to optimize your program. We cover application management, scope and policy governance, event triage, incident management, reporting and analytics. This protects you against IP theft and patient data breaches. Our experts design, implement and operate a program tailored to your security and compliance needs. From DLP to ITM, we use advanced machine learning and engaged human analysis to secure your healthcare data. We inspect and act upon alerts. And we deliver rapid response to attempted breaches. Let us help you improve your security and leverage your team, so you focus on other issues.

Conclusion

Healthcare institutions like yours have faced unprecedented challenges over the past few years. This turmoil continues as you try to return to stability in the face of cost cutting, declining reimbursements, workforce shortages and more. On the infrastructure side, attack surfaces have grown. The need for data security has expanded from the data center into multiple clouds. Logins from remote locations by both employees and patients remain high. And the number of IoMT devices at the network edge continues to grow. For almost two decades, organizations have focused on securing the perimeter. But recent trends mean that the traditional perimeter is no more. These days, the individual worker is the perimeter—and the edge. With Proofpoint's data security solutions, you can gain real-time insights into data risk. You can also prioritize and respond to incidents and prevent data loss. The platform also offers a range of compliance and regulatory features, including data discovery, classification and encryption. These help you meet regulatory requirements and industry standards. You'll be protecting your institution by protecting the people that work with your sensitive information.

proofpoint.

DISCOVER THE PROOFPOINT PLATFORM →

0207-005-01-04 6/25