SOLUTION BRIEF

Protecting Healthcare Information With Proofpoint

Protect patient data against insider threats, data loss and cloud risks with the Information Protection platform

Products

- Enterprise Data Loss Prevention
- Insider Threat Management
- Intelligent Classification and Protection
- Email Encryption
- Isolation
- Cloud App Security Broker
- Web Security
- Managed Information Protection (Premium Services)

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, the cloud and endpoints

This solution set is part of Proofpoint's integrated Human-Centric Security platform, mitigating the four key areas of people-based risks.

Healthcare organizations have long been prime targets for cyber criminals. Because these organizations handle many types of data—intellectual property (IP), clinical trial data, protected health information (PHI) and personal financial details—attackers have many options to cash in from even a single attack on just one of them. For their part, healthcare institutions are only expanding their attack surface as they embrace the cloud, remote work and telehealth. And as employees in the industry continue to operate in increasingly high-stress jobs, organizations also face increased risk from both malicious and well-intentioned insiders.

Proofpoint provides a human-centric approach to safeguard sensitive data in widely distributed healthcare networks. Our Information Protection platform delivers unmatched visibility and control over sensitive data. This allows organizations like yours to better manage data risk while also saving you time and operational costs. 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.

Hospitals, clinics, health insurance providers and biotech firms should treat information protection as a top priority. They must protect their own research data and IP. But they must also safeguard patient PHI, personal identifiable information and payment card data.

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 cyber criminals.

At the same time, their digital footprints 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 more sensitive data travels outside the network perimeter. And as the economy settles into a “new normal,” hybrid work rules mean that employees now often work remotely.

Unfortunately, attackers have followed their targets outside the perimeter. The healthcare industry was hit with an astounding 25% of all ransomware attacks[1] and nearly 35% of overall cyber attacks in the span of one year.[2] And data breaches are far more costly in this industry than in any other. In 2022, a data breach cost an average of $10.93 million.[3] These costs can include ransoms paid out, 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.

Information Protection Challenges

Hospitals, clinics, health insurance providers and biotech firms should treat information protection as a top priority. They must, of course, protect their own research data and IP. But they must also safeguard 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 insiders00

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

Looking for a break, for instance, curious employees might be tempted to sneak a peek at, say, the medical records of a famous patient. This is called electronic health record (EHR) snooping. And it can pose a big risk for an institution if the information of a deep-pocketed patient were to be exposed to the public.

Well-meaning workers could click on phishing emails that they might have been able to recognize were the workers not so overwhelmed. Emotional stress could even lead to malicious insider threats against an employer. And if a trusted user’s account is compromised due to credential theft, then it can lead to dire consequences before anyone even realizes what has happened. You must take a proactive approach to prevent all of these threats.

[1] Giles Bruce (*Becker’s Hospital Review*). “25% of Ransomware Attacks Aimed at Healthcare Industry, FBI Says.” October 2022..

[2] Richard Payerchin (*Medical Economics*). “Health Care Leads Cybersecurity Breaches for 2022.” February 2023.

[3] Ponemon Institute and IBM. “Cost of a Data Breach Report 2023.”

Cover a growing attack surface as healthcare embraces the cloud

Many healthcare organizations were slow to embrace the cloud. But they have since jumped in with both feet. 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 them 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 inevitably accessed, shared and stored elsewhere. And as healthcare data travels across larger geographies, protecting that data becomes much more of a challenge.*

Even when EHRs are housed on premises, details from these records are inevitably 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. But these services are vulnerable to cyber threats. Even more, cyber criminals increasingly use these recognized file shares to deliver their exploits.

Unify information protection 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 many devices in the course of a 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 is even more critical that security protection be integrated. In the case of information protection, this means having integrated data loss prevention (DLP) tools across endpoint, email and cloud.

A Human-Centric Approach

Legacy approaches to information protection 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 the key. So 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 that data.

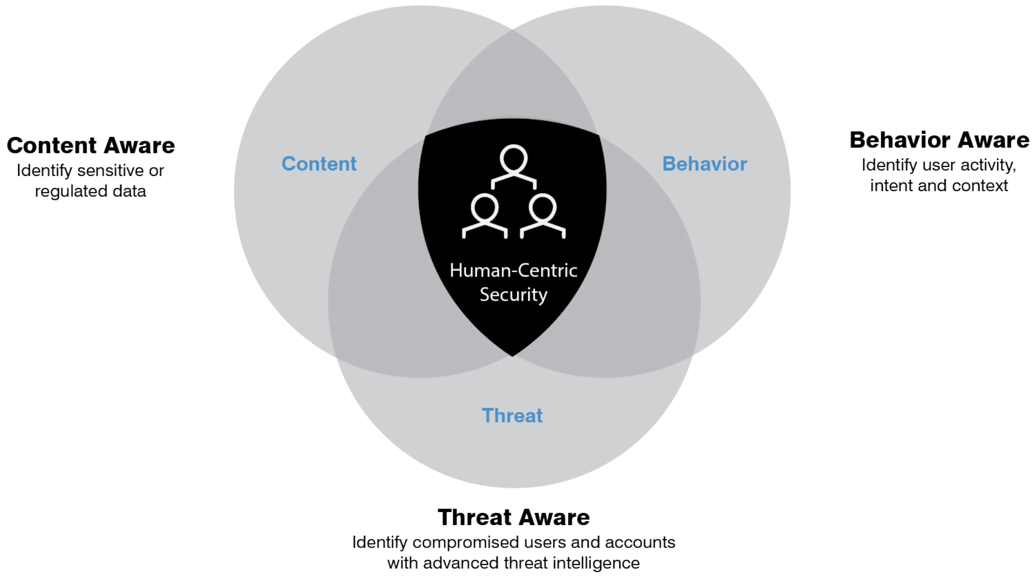
Content Aware
Identify sensitive or regulated data
Content
Behavior
Behavior Aware
Identify user activity, intent and context
Human-Centric Security
Threat
Threat Aware
Identify compromised users and accounts with advanced threat intelligence

Figure 1: Understanding and mitigating user risk.

How Proofpoint Can Help

The Proofpoint Information Protection platform gives you unmatched visibility. It provides a unified, cloud-native interface that can help you protect your sensitive information by focusing on the people who manage it. The platform is content-, behavior- and threat-aware (see Figure 1). It combines on-premises information protection with cloud security. This ensures that your staff, clinical workers and patients are protected, no matter where their data travels.

Proofpoint Enterprise Data Loss Prevention

Proofpoint Enterprise DLP is our most comprehensive and market-leading DLP offering. It brings together our solutions for email, cloud and endpoint and protects your organization against all data loss that originates with insiders. Our human-centric approach combines content, behavior and threat telemetry from all of these channels. The elements are merged into one modern timeline view to give you a more comprehensive and nuanced understanding of specific events. This allows you to address the full spectrum of data loss scenarios—compromised, malicious and negligent.

Proofpoint Enterprise DLP can be deployed on-premises or with a software as a service (SaaS) model. It includes customary data classifiers. It also lets you apply common DLP policies and extend them to a new channel. It has a unified alert and investigations interface, which enables quick response. And since visibility is anchored to the person, it allows you to quickly shut down compromised accounts.

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 like EHR snooping within timeline-based visualizations and analytics.

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

Proofpoint Intelligent Classification and Protection

Proofpoint Intelligent Classification and Protection takes an AI-powered approach to identify and classify your business-critical data. Misclassified data can result in data breaches and noncompliance fines. With this solution, you can reduce false positives, gain visibility at scale, prioritize action for risk reduction and extend the efficiency of your DLP program.

Proofpoint Email 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. Our solution features simplified policy management, no-touch key management and integrated information protection with your existing email and information protection solutions.

Proofpoint Isolation

Proofpoint Isolation keeps users' personal activity and harmful content out of your environment. It works by insulating webmail and any URLs they contain within a protected container. Users can access their personal accounts freely and privately through their usual web browser. But potentially harmful content and actions are disabled, so your environment can stay safe.

Proofpoint Cloud App Security Broker

Proofpoint Cloud App Security Broker (CASB) protects users from cloud threats. It safeguards sensitive data and governs cloud and oAuth apps within Microsoft Office 365, Google Workspace and more than 900 apps that IT may approve or tolerate. It extends Proofpoint's visibility of Very Attacked People™ (VAPs) to your cloud-based services. This lets you better protect cloud accounts and data. Proofpoint CASB provides a granular view of cloud access, user behavior and the handling of sensitive data like PHI. It helps you stay compliant with privacy and data security regulations.

You can deploy Proofpoint CASB in multiple modes. The one you choose depends on the use case. For near real-time visibility with fast time to value, CASB will integrate with your cloud app APIs and infrastructure logs. For real-time access and data controls, you can use risk-based SAML authentication, isolation and in-line forward proxy capabilities. And in true SSE fashion, you can integrate Proofpoint CASB with Proofpoint Web Security to connect and secure remote workers across web and cloud apps.

Proofpoint Web Security

Many of your workers still log in from outside of the network perimeter. Proofpoint Web Security can protect your distributed workforce against advanced threats when they browse the web. By inspecting all SSL traffic, our solution uncovers and blocks threats such as ransomware and zero-day phishing attacks. It also prevents users from browsing dangerous and noncompliant content.

Proofpoint Managed Information Protection

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 our Proofpoint Managed Information Protection premium service, you can use our global team of data security experts augment your team. We have decades of experience. Over 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 CASB to ITM, we use advanced machine learning and engaged human analysis to protect your healthcare information. 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 can get back to focus on other issues.

Conclusion

Healthcare institutions like yours have faced unprecedented challenges over the past few years. The turmoil continues to this day as you try to return to stability in the face of expiring federal pandemic support, workforce shortages and more. On the infrastructure side, attack surfaces have grown. The need for information protection 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 the Proofpoint Information Protection platform, 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.

LEARN MORE

For more information, visit **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 75 percent of the Fortune 100, 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**.