Protecting Healthcare Information with Proofpoint

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

Products

- Proofpoint Cloud App Security Broker
- Proofpoint Email Data Loss Prevention
- Proofpoint Endpoint Data Loss Prevention
- Proofpoint Insider Threat Management
- Proofpoint Web Security
- Proofpoint Zero Trust Network Access
- Proofpoint Managed Services for Information Protection

Key Benefits

- Identify and mitigate risk from negligent users, compromised users and malicious insiders
- Prevent data loss from email, the cloud and endpoints
- Extend scalable protection to a growing number of widely distributed cloud services

The healthcare industry has long been a favorite target for cyber criminals. And the COVID-19 pandemic has only made it worse. Attackers have intensified their efforts to gain valuable data like vaccine trial information, protected health information (PHI) and financial data. And for their part, healthcare institutions are expanding their attack surface by moving to the cloud and letting more employees and patients log in remotely. These institutions also face increased risk from both malicious and well-intentioned insiders.

Proofpoint provides a people-centric approach to safeguard sensitive data in widely distributed healthcare networks. Our information protection solutions are easy to deploy and maintain. You can use them to build a robust secure access service edge (SASE) or security service edge (SSE). We help you defend your people and their sensitive data against accidental mistakes, attacks and insider risk. Our protective shield extends across cloud services, email, endpoint and on-premises file shares.

A Growing Threat

A breach can result in compliance fines, litigation and brand degradation for healthcare institutions—even loss of life. Unfortunately, the US Department of Health and Human Services reported an increase of 50% in healthcare-related security breaches in the first half of 2020. And in 2021, overall ransomware attacks more than doubled. That year, healthcare became one of the two most targeted sectors.

Growing numbers of life-saving medical Internet-of-Things (IoT) devices may be saving lives, but they also are increasing complexity. And COVID-19 has led more providers to use telehealth services. Some even provide these services from their homes rather than a clinic or hospital.

It's no wonder that Moody's Investors Service finds that cyber risk will remain high in healthcare for the foreseeable future. After managing nearly two years of an existential crisis, healthcare organisations must remain on guard.

Information Protection Challenges

Hospitals, clinics, health insurance providers and biotech firms should see information protection as a top priority in this dire threat landscape. They must safeguard patients' PHI, personal identifiable information (PII) and payment card data. They face a number of challenges.

Prevent EHR snooping and other threats from insiders

Healthcare employees are the heroes of the pandemic. As the crisis unfolded, they worked their intensely stressful jobs day after day, even when no end was in sight. Such stress can increase the risk of insider threat. Looking for a break, curious employees might, for example, be tempted to sneak a peek at, say, the medical records of a famous patient. This so-called electronic health record (EHR) snooping can pose a big risk for an institution if the information of a deep-pocketed patient were to be exposed publicly.

Well-meaning but overwhelmed workers might also click on a phishing email when they otherwise might recognise it. Emotional stress could even lead to malicious insider threats against an employer. You must take a proactive approach to prevent all of these kinds of threats.

Cover a growing attack surface as healthcare embraces the cloud

Many healthcare organisations were slow to embrace the cloud. But now almost all of them have multiple services in public and private clouds. This has improved operational efficiency. It has also eliminated the need to secure capital funding to build IT infrastructure. But it has also expanded the attack surface of healthcare institutions.

Even if EHRs are housed in on-premises infrastructure, details from these records are inevitably accessed, shared and stored elsewhere. Think mobile devices, remote endpoints, medical IoT devices and cloud-based email systems. As the places that healthcare information travels expands, protecting it becomes more of a challenge.

And with a growing cloud footprint comes an increased risk of credential theft. Office software and collaboration functions are increasingly delivered through cloud services like Microsoft 365 and Google Workspace. These services are vulnerable to cyber threats. Complicating matters even more, cybercriminals increasingly use these recognised file shares to deliver their exploits.

Protect healthcare staff and remote patients as delivery models evolve

Some of the sudden changes that the pandemic forced upon the workplace in early 2020 turned out to be temporary. But many will have an impact for years to come. In healthcare, one continuing trend is the increase in care delivered via telehealth. One study found that as late as February 2021, telehealth usage was still 38 times its 2019 baseline. This has resulted in a massive increase in the number of patients accessing corporate resources remotely.

On top of that, a large number of employees still work from home at least part time. Many of them manage electronic medical records (EMRs), patient financial information and research data. The growing volume of remote logins increases risk of attacks against people playing specific roles within an organisation.

Taking a People-Centric Approach

Legacy approaches to information protection look at the data only. Information, however, does not lose itself. People allow data loss to happen. They can do so accidentally or maliciously. With cybersecurity, visibility is the key, so you must understand the personas that are most likely to bring risk. A people-centric approach works to understand the dynamics of the individuals who interact with that data.

How Proofpoint Can Help

The Proofpoint Information and Cloud Security platform can help you protect your sensitive information by focusing on the people who manage it.

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 365, Google Workspace and more than 900 IT-approved and -tolerated cloud apps. 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 behaviour and the handling of sensitive data like PHI to help you stay compliant with privacy and data security regulations.

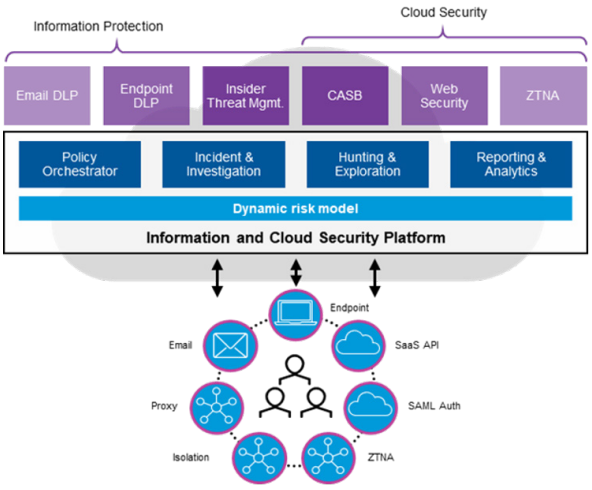

Figure 1: Proofpoint Information and Cloud Security Platform.

Proofpoint CASB can be deployed in multiple modes, depending on the use cases. For near real-time visibility with fast time to value, CASB will integrate with your cloud app APIs and your infrastructure logs. For real-time access and data controls, you can use risk-based SAML authentication, isolation and in-line forward proxy capabilities. In true SSE fashion, you can integrate CASB with Proofpoint Web Security and Zero Trust Network Access (ZTNA) to connect and secure remote workers across web and cloud applications.

Proofpoint Data Loss Prevention

Proofpoint Data Loss Prevention takes a people-central approach to data loss prevention (DLP). It brings together content, behaviour and threats, and provides context across all three. It presents its insights in a modern timeline view, which can give you a more comprehensive and nuanced understanding of specific events. The information can help you understand whether a flagged user is compromised, malicious or negligent.

Proofpoint Insider Threat Management

Proofpoint Insider Threat Management (ITM) correlates user activity and data movement. It allows security teams to detect, investigate and respond to potential insider threats. It delivers people-centric behaviour awareness. And it provides real-time detection and response to data exfiltration, privilege abuse, application misuse, unauthorised access, risky accidental actions and anomalous behaviour. This helps you detect, prevent and respond to threats like EHR snooping within timeline-based visualisations 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 analysed within a modern architecture for scalability, security and privacy. It also brings the flexibility to deploy using on-premises or Software-as-a-Service (SaaS) delivery models.

Proofpoint Web Security

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

Proofpoint Zero Trust Network Access

As applications move to the cloud, healthcare workers become much more mobile. This trend requires a better VPN alternative for secure access. Proofpoint ZTNA leverages a software-defined perimeter for each user. This provides them with cloud-delivered secure remote access to resources in the data centre and the cloud.

Each user is granted access to specific applications. The rest of the network is hidden from their view. Proofpoint ZTNA vets users before they enter the network. It increases security and visibility.

Proofpoint Managed Services for Information Protection

Managed Services for Information Protection (MSIP) augments your team with our global team of data security experts. With decades of experience, we have built best practices and maturity modeling to optimise your programme. We cover application management, scope and policy governance, event triage, incident management, reporting and analytics. This protects you against intellectual property theft and patient data breaches. Our experts design, implement and operate a programme tailored to your security and compliance needs. From DLP to cloud access security broker to ITM, we use advanced machine learning and engaged human analysis to protect your healthcare information. Alerts are inspected and acted upon with rapid response to attempted breaches. Let us help improve your security and leverage your team so you can get back to focus on other issues.

Conclusion

Healthcare institutions like yours have had to navigate huge changes in the world of work that COVID-19 brought about. Attack surfaces have grown. Information protection has expanded into multiple clouds. Logins from remote locations by both employees and patients are on the rise. And the number of medical IoT devices at the network edge continues to grow.

Going on almost two decades, organisations have sought to secure the perimeter. The recent explosion in cloud service usage and the expansion of remote work now means that the individual worker is the perimeter—and the edge.

These rapid changes require an emerging security architecture. The new approach is often called SSE. SSE is the security portion of a SASE. It provides users the secure access they need to all cloud services via cloud data centres. It is here that zero-trust network access and identity and access management are performed, and administrators monitor access using centralised controls.

You can leverage Proofpoint's Information and Cloud Security platform to build a robust SSE or SASE architecture. This will allow you to apply secure access and threat protection as people access applications and data—regardless of their locations or device types. 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 organisations' 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 organisations 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**.