Securing Healthcare Provider Organizations with Proofpoint

Protecting People, Processes and Patient Data

Cyber attacks on the healthcare industry is constantly on the rise. Highly sensitive patient data can have high monetary value making attackers target such organizations. COVID-19 has made this industry even more vulnerable. Now, physicians and non-clinical staff deliver more patient care services remotely increasing the exposure of cyber threats. Proofpoint can help you. Our cybersecurity and compliance solutions protect you, your staff and your patients.

Telehealth and work from home options are powerful tools that have made it easy for healthcare staff to deliver patient care. But these new remote work options open doors to cyber threats that could expose medical data, disrupt patient care or negatively impact your patients’ safety.

Healthcare institutions now consider cybersecurity a patient safety issue core to healthcare’s overall mission. However, like many organizations across a variety of industries, healthcare has invested in traditional security tools that protect the perimeter. These tools can’t see—let alone stop—advanced threats that put healthcare data at risk.

Besides, threats are changing. As the healthcare industry moves beyond the network perimeter, so do attackers. But threats don’t just move, they take on new forms and targets. Every person in your healthcare organization represents a different level of security or compliance risk. It is based on the data they have access to and how they use technology to do their job.

Nurses have more access and exposure to patient information, making them a primary cyber target. Clinical researchers have access to prized intellectual property which significantly raise their vulnerability level. Hospital staff working in the supply chain regularly interact with a variety of third-party systems raising their threat level. Threats like credential phishing unlocks access to far more than an email account. It gives attackers access to a wealth of data stored in the cloud, beyond the reach of traditional security tools. Healthcare workers, patients, doctors and others are exposed to this new breed of people-focused attacks.
Healthcare Cybersecurity Challenges
Healthcare organizations face new challenges as they seek to embrace innovative approaches to the delivery of care without putting themselves, their clinicians or their patients at risk. The challenges facing healthcare IT and security leaders in 2020 and beyond are far more complex. This makes it harder for healthcare institutions to maintain a secure environment to enable digital health.

Shift to secure new care models
The use of mobile health, telemedicine and the internet of things has increased the attack surface. Healthcare consumers use a variety of mobile health (mHealth) applications, wearable medical devices and home-based medical technology. Clinicians bring personal devices to work and take work devices home. And emerging technologies and the blurring lines between clinical and home settings add to the complexity. They have contributed to a decentralized, perimeter-less IT infrastructure. This has made it much more difficult to protect.

Data storage and protection
Securing the doctor-patient relationship is an important part of healthcare. If data is not stored securely with third parties or if it is sent un-encrypted, they risk exposing patient information. While all healthcare organizations report that they collect, store, and share sensitive data, only 38% said they are encrypting the data.\(^1\)

Cloud security
Healthcare understands the many benefits of cloud computing: leveraging standardized applications, utilizing pay-per-use models, and reducing capital expenditures. Because there is perceived risk with cloud services, healthcare has been slow to adopt cloud offerings, but is now catching up. Recognizing the benefits of cloud solutions, healthcare security leaders are seeking out solutions that offer robust compliance, maintain privacy and transaction integrity and are adaptable to safeguard cloud applications from business associates and supply chain ecosystem partners.

Supply chain security
Healthcare providers depend on a variety of external suppliers, partners and business associates to support their business. These interdependent relationships form a complex third-party ecosystem vulnerable to theft and emerging cyber risks. New points of entry that threat actors can use to compromise the hospital supply chain. The old phrase “a chain is no stronger than its weakest link” is more relevant now in healthcare than ever. Devastating losses can happen when a single weak spot of a hospital supply chain is infiltrated and is then weaponized to extract sensitive data.

Evolving healthcare cyber threat landscape
The growing high-value market for medical information makes healthcare organizations an attractive target. You must take a defensive posture and assume the industry is under attack from threats like nation-state attacks and hacking. Simple viruses and malware belong in the past. The most damaging cyber attacks are both targeted at and operated by people with strategic entry points plotted over time and collectively posing serious damage. In fact, according to research, it takes healthcare organizations the longest to discover a data breach at an average of 329 days.\(^2\)

---

1. 2019 Thales Data Threat Report
2. 2020 Cost of a Data Breach Report from IBM Security, by the Ponemon Institute
Take a People-Centric Approach

Today’s cyber attacks target people, not technology. That’s why healthcare organizations must take a people-centered approach to securing their clinical workers, non-clinical employees, and the sensitive data they use and share. The nature of clinical work requires a focus on providing optimal patient care, often at a rapid pace, rather than considering the legitimacy of an email. It’s one reason the industry remains an easy target for malicious activity. And the potential payoff of successful attacks is high. Our 2020 report, “Healthcare Threat Landscape” explores what we call Very Attacked People™ (VAPs) in healthcare. We use the term to describe users within an organization who are the most heavily targeted by cyber threats. Figure 1 shows a real-life example.

Children’s Hospital

In this example, the “physician” was the most attacked title. Privacy concerns are heightened with children because they are a popular target for identity theft. A minor’s patient record is extremely valuable on the dark web or underground economy. Most children have not established a credit history and will not be applying for loans or credit cards at the time of breach. Cyber crime actors know most people are not monitoring if their data is being used for fraud. Notably, the volume of backdoor activity was highest in facilities management which often have weak security controls.

These environments often employ permissive assets, such as Internet of Things (IoT) devices and HVAC systems. They are often network pivot points for attack in corporate IT enterprise.

Healthcare Use Cases—How Proofpoint Can Help

Distributed health security

Healthcare encompasses a wide range of organizations and IT environments coordinating, collaborating and sharing information between patients and clinicians for patient-centered or connected care. Email is a popular method of disseminating confidential information, and a large majority of high-profile healthcare data breaches begin with targeted phishing attacks.

Proofpoint has the right solutions for the healthcare industry by protecting users in the way they work today:

- Email Protection delivers top-rated email security to stop malware and non-malware threats.
- Data Loss Prevention (DLP) mitigates the risk of email data loss and protects against email fraud.
- Targeted Attack Protection (TAP) with sandboxing capabilities detects and stops advanced threats.
- Proofpoint Threat Response share intelligence on new threats.
- Proofpoint Security Awareness Training provides employees training to spot healthcare-themed social engineering attacks, such as sophisticated phishing ploys.
Protection against impostor attacks

Impostor emails are fraudulent messages designed to look like they’re from someone the recipient knows or can trust. These attacks can be hard to detect because they don’t exploit technical vulnerabilities. They target specific job functions that have access to monetizable activity—such as pharmacists, clinical researchers, supply chain workers or hospital foundation staff.

Proofpoint offers an integrated, people-centric, end-to-end solution that stops all forms of email fraud, no matter the tactic used or the person being targeted:

- **Advanced Email Security** blocks phishing and impostor emails that use spoofed and use lookalike domain names. It uses advanced machine learning and multiple detection engines to detect these targeted attacks. And it stops them before they reach users’ inboxes.

- **Domain-based Message Authentication Reporting and Conformance (DMARC)** is deployed to help email authentication. It stops spoofed email before defrauding employees, clinical staff and business associates.

Securing O365 and other cloud environments

A cloud access security broker (CASB) is a critical element of cloud security architecture. Now more healthcare organizations move data and applications to the cloud and are accessing more sensitive data over internet connections. They need to see cloud activity as it unfolds across the healthcare ecosystem and supply chain.

Proofpoint CASB helps organizations scan and act quickly on potential cloud-based email policy violations across the continuum of care. It reduces the risk of a cyber-attack or data breach. And it uses an organization’s email flow to identify confidential data within cloud file services including Office365, DropBox, Box and Salesforce.

Telehealth

The demand for telehealth services has escalated during the coronavirus crisis. Even before the pandemic, the idea of seeing a doctor from home appealed to many. Especially to those with chronic conditions requiring frequent doctor visits. With this shift to remote care services emerged new honeypots for cybercriminals. Healthcare organizations now store and process more data. They have expanded their digital infrastructures and people are more distributed. **Proofpoint Meta** is a zero-trust solution that quickly and securely connects employees, business associates and patients to your datacenter and cloud. You get tighter security, a far better user experience and reduced IT hassle.

Secure care collaboration

Healthcare staff need effective collaboration and communication at the point of care. They have mobile solutions that connect clinicians and patients. But they are built for function and convenience rather than security. They are often used outside the confines of the protected enterprise network.

Physicians may access clinical applications from personal devices. At the same time, they may use personal email accounts on corporate-issued hardware. **Proofpoint Browser 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 stays safe.

Insider threat protection

An insider leaking patient information at a doctor’s office or hospital may seem like a scene from a TV medical drama. But insider threats are all too real. In fact, nearly half of all breaches in healthcare involve internal threat actors.3

Three of the most common insider threat risks and data loss for healthcare organizations include:

1. Theft or misuse of protected health information (PHI)
2. Theft or misuse of electronic health records (EHR)
3. Insurance and other financial fraud

**Proofpoint Insider Threat Management (ITM)** protects against data loss, malicious acts and brand damage involving insiders acting maliciously, negligently or unknowingly. Our ITM solution correlates activity and data movement, empowering security teams to identify user risk, detect and respond to insider-led data breaches, and accelerate security incident response.

3 2020 Verizon Data Breach Investigations Report (VBIR)
PHI Protection: Keeping patients’ data safe

The number one threat vector in healthcare is people being attacked on email. Having the right email data loss prevention (DLP) ensures sensitive and critical information is classified and accessed by the right people.

With Proofpoint People-Centric DLP, healthcare institutions can identify and respond quickly to data risks posed by negligent, compromised and malicious users. Our unified platform allows customers to define data of interest and leverage these definitions across the entire platform. It protects the confidentiality of individual email messages through Email Encryption. The user community can trigger encrypted messages automatically by adding a keyword of choice to the subject line, or trigger message-level encryption on the basis of DLP rules.

Manage regulatory compliance standards while reducing complexity

Many regulated companies struggle to:

• Identify where their business communications are taking place
• Ensure that this content is captured and securely archived
• Search and retrieve content for audits quickly and cost-effectively
• Monitor and supervise workers who use these channels

Proofpoint Archiving and Compliance solution provides all-in-one people-centric compliance.

That means:

• You are covered from the moment content is disseminated to when it is indexed, archived and retrieved.
• It applies your regulatory policies automatically, such as the Department of Health and Human Services, and HIPAA.
• You can be sure your digital engagement efforts comply with any communication and retention rules.
• You can supervise, remediate (revise or remove), and archive content easily, faster and inexpensively.

Conclusion

Proofpoint gives health institutions protection and visibility for their greatest cybersecurity risk: their people. We provide the most effective cybersecurity to protect healthcare workers whether they are targeted through email, the web, social media, or cloud apps. We help stop threats before they reach clinical and support staff, safeguard data, and ultimately help healthcare protect patients from cyber-attacks. Leading healthcare organizations of all sizes rely on Proofpoint to prevent, detect and respond to their most critical security before they cause lasting harm.

LEARN MORE

For more information, visit proofpoint.com/us/solutions/healthcare-information-security.