proofpoint.

SOLUTION BRIEF

Securing Healthcare Provider Organizations with Proofpoint

Protect people, processes and patient data

Products

- Aegis Threat Protection platform
  - Email Protection
  - Secure Email Relay
  - Targeted Attack Protection
  - Threat Response
  - Isolation
  - Security Awareness
  - Email Fraud Defense
- Sigma Information Protection platform
  - Enterprise Data Loss Prevention
  - Email Encryption
  - Web Security
  - Cloud App Security Broker
  - Insider Threat Management
- Identity Threat Detection and Response
  - Spotlight
  - Shadow
- Intelligent Compliance Platform
  - Archive

Key Benefits

- Combating ransomware, impostor attacks, insider threats and attacks through medical devices
- Protecting cloud services like Office 365, DropBox and Salesforce from infiltration
- Protecting PHI and maintaining compliant data storage and sharing processes

The past several years have been tough for healthcare provider organizations. Workforce shortages, inflation, mergers, facility closures and a worsening cyber threat landscape have proven to be quite a challenge. Faced with increasingly sophisticated cyber attacks, however, many institutions still use security tools that focus on protecting the traditional perimeter. But this perimeter no longer exists, as most cyber attacks these days are now aimed at people—especially those who have access to sensitive data. Proofpoint can help your healthcare provider organization protect its employees, third parties and patients with people-centric solutions.

Confronting Converging Challenges

While challenges have hit all industries, healthcare has seen the most turmoil. The global pandemic was, of course, a seismic disruption for these organizations. But now, as the overall economy settles into a “new normal,” they face many barriers to a return to stability. These include the following:

- **Workforce shortages.** Organizations for years have had to deal with a deepening shortage in healthcare providers. The COVID-19 pandemic only accelerated the trend. The American Nurses Association found that more registered nurse jobs were vacant in 2022 than any other profession in the United States.[1] And projections envision a shortage of 275,000 nurses[2] and 124,000 physicians[3] in a decade. That is in the United States alone.
- **Budget constraints.** Healthcare provider organizations faced huge fluctuations in both income and costs over the past three years. Now, with most pandemic-related government support expired, they face higher labor costs due to the

[1] Lisa M. Haddad, et al. (*National Institutes of Health*). “Nursing Shortage.” Updated February 2023.
[2] American Association of Colleges of Nursing. “Nursing Shortage.” Accessed March 31, 2023.
[3] American Association of Medical Colleges. “The Complexities of Physician Supply and Demand: Projections from 2019 to 2034.” June 2021.

provider shortage.[4] At the same time, global inflation has increased the cost of medical supplies.[5] But in some cases reimbursement rates have not kept up with these cost increases. Some formulas have even reduced payouts to providers.[6]

- **Mergers and acquisitions.** The pace of consolidation in the healthcare industry quickened in 2021. And mergers and acquisitions remained historically high in 2022, with more than 2,850 deals globally. Many medical practices merged. Others were absorbed into hospital networks, which themselves often merged. While this may result in more stability in the long run, the short-term turmoil can be very disruptive.
- **Rural hospital closures.** At the same time, small-town hospitals in the United States continued to close. A record 19 of them shuttered in 2022,[8] which brought the total number of closures to 155 since 2001. These facilities often housed a community's only healthcare practices, and their closures forced providers to close or relocate. This has left their patients without local care—and it left staff without jobs.
- **Increased cyber attacks.** Healthcare organizations have experienced more cyber attacks than any other industry in recent years. In fact, they were the targets of 25% of all ransomware attacks[9] and nearly 35% of overall attacks over the past year.[10] Healthcare breaches also tend to get more publicity than most. This is thanks to a provision of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, which requires all breaches that involve 500 or more records to be posted on a website. The site is informally known as the "wall of shame."[11]

Moving Beyond the Perimeter

Your IT systems are critical. Digital networks support not only the business side of your operation, they also have a direct impact on patient care. Patients' medical records are digitized. A growing percentage of medical devices is also connected to the internet—and to patients. Clearly, cybersecurity is a patient-safety issue that is core to your overall mission.

Unfortunately, most healthcare provider organizations have invested mostly in traditional security tools that protect the perimeter. But organizations are quickly moving services outside of the data center and into cloud-based services. Perimeter-focused tools cannot see—let alone stop—many of the advanced threats that put healthcare data at risk.

Incurring New Kinds of Attacks

Attackers have followed healthcare organizations outside the perimeter. But their threats do not just move to a new location—they also take on new forms and targets. Every person in a healthcare organization is a different kind of security or compliance risk. These risks are based on the data that each user has access to as well as how they use technology to do their job. For example:

- Nurses have direct access and exposure to patient information. This makes them a primary cyber target.
- Clinical researchers have access to prized intellectual property. This significantly raises their vulnerability level.
- Staff members who order medical supplies regularly interact with a variety of third-party systems. This raises their threat level.

Different risks also come from different attack vectors. For example, login details that were stolen through credential phishing can unlock access to far more than just an email account. They give attackers access to a wealth of data stored in the cloud, which is beyond the reach of traditional security tools. Healthcare workers, patients, doctors and others are exposed to this new breed of people-focused attacks.

Facing Myriad Cybersecurity Challenges

Healthcare providers embrace innovative approaches to improve health outcomes and the quality of life for patients. But they must do this without putting clinicians, patients or the business at risk.

[4] Victoria Bailey (*Revcycle Intelligence*). "Inflation, Labor Costs Will Increase Healthcare Spending by $370B." September 26, 2022.

[5] American Hospital Association. "Massive Growth in Expenses & Rising Inflation Fuel Financial Challenges for America's Hospitals & Health Systems." April 2022.

[6] Medical Economics. "Medicare's 2023 Fee Schedule: Cuts in Reimbursement, Expanded Payments for Behavioral Health." November 2022.

[7] Dan Dufner (White & Case). "Global Healthcare M&A Delivers Strong Performance." January 2023.

[8] American Hospital Association. "AHA Report: Rural Hospital Closures Threaten Patient Access to Care," September 2022.

[9] Giles Bruce (Becker's Hospital Review). "25% of Ransomware Attacks Aimed at Healthcare Industry, FBI Says." October 2022.

[10] Richard Payerchin (Medical Economics). "Health Care Leads Cybersecurity Breaches for 2022." February 2023.

[11] The Fox Group. "HIPAA Wall of Shame: No Hiding from the Public Facts," March 2023.

Several challenges make this difficult. Some are as follows:

- **Big demand for PHI.** Healthcare organizations bear the brunt of global cyber attacks. There is a growing, high-value market for protected health information (PHI), which can be used for medical identity theft. Cyber criminals can then file fraudulent claims to get prescription drugs and expensive medical equipment so they can resell them. This is one reason that data breaches are far more costly in healthcare than in any other industry—$10.10 million on average in 2022.[12]
- **Email fraud on the rise.** Email fraud is one of today's greatest cyber threats. Also known as business email compromise (BEC), these attacks are socially engineered to target people, not technology. BEC impacts healthcare organizations of all sizes around the globe. Fraudsters prey on human nature to steal money and information from the staff, patients and business associates of an organization. The U.S. Department of Justice recently charged 10 defendants in BEC and money-laundering schemes that targeted Medicare, Medicaid and other victims and resulted in more than $11.1 million in total losses.[35]
- **An expanding attack surface.** The growing use of mobile health (mHealth) apps, telehealth, connected medical devices and home-based medical technology expands the attack surface of provider organizations. And emerging technologies that blur the lines between clinical and home settings only adds to the complexity. Clinicians often bring personal devices to work. They also take work devices home. In some cases, patients even connect personally owned wearable devices to medical networks to assist with monitoring. These trends have made the corporate perimeter a thing of the past. They are quickly moving your medical practice from a centralized architecture to a very distributed one. And this is much more difficult to protect.
- **The scourge of ransomware.** A recent spike in ransomware attacks is yet another factor in the high cost of healthcare breaches. The cost of maintaining business continuity—and patient safety—can be quite significant when ransomware shuts down systems, whether or not you pay the ransom. The most damaging cyber attacks are deployed against people who sit at strategic entry points in your organization. If these employees make one mistake when dealing with incoming communications, it can leave you open to a damaging attack.

Today's cyber attacks target people, not technology. That's why you must take a people-centered approach to secure your clinical workers and non-clinical employees as well as the sensitive data that they use and share.

- **Burgeoning volumes of data.** The total amount of data is growing faster in healthcare than in any other industry. While the global datasphere is expected to grow at a compound annual growth rate (CAGR) of 27% by 2025, healthcare data will grow by 36%.[14] Factors in this growth rate include the digitization of all patient records and the increase in continuous monitoring by a growing array of medical devices and healthcare-related mobile apps. If your data is not stored securely or if it is sent unencrypted, then you risk exposing patient information.
- **Vulnerabilities in the cloud.** Healthcare organizations were at first slow to adopt cloud-based services. But they have since jumped in with both feet.[15] As a provider organization, you understand benefits such as leveraging standardized apps with automatic updates, utilizing pay-per-use models and reducing capital expenditures. You must find solutions that ensure compliance, maintain data integrity and have robust segmentation features. The latter are needed to shield specific cloud apps and data from internal and external users who don't need them to do their jobs.

[12] Ponemon Institute and IBM. "Cost of a Data Breach Report 2022."

[13] The United States Depart of Justice. "10 Charged in Business Email Compromise and Money Laundering Schemes Targeting Medicare, Medicaid, and Other Victims." November 2022.

[14] RBC Capital Markets. "The Healthcare Data Explosion." Accessed March 2023.

[15] Vantage Market Research. "Healthcare Cloud Computing Market Global Industry Assessment & Forecast." January 2022.

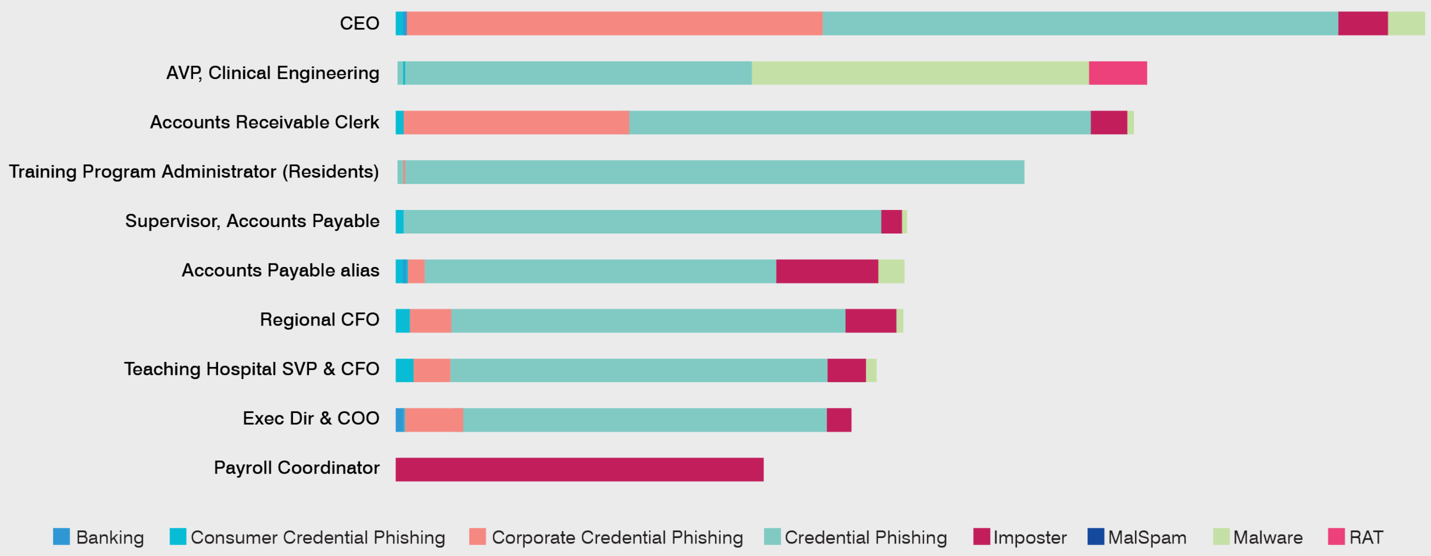

Figure 1: Top 10 Very Attacked People™ (VAPs) at a large nonprofit integrated health network

- **Risks in the supply chain.** You depend on external suppliers, partners, insurers and other healthcare providers for patient care. The relationships you have with them are interdependent and they form a complex third-party ecosystem. Many of these players must have access to sensitive data like electronic medical records (EMRs). This means that the integrity of your data depends on the security practices at organizations that you do not control. What's more, the security of every connected entity is critical for compliance with the Health Insurance Portability and Accountability Act (HIPAA). A single weak link in your supply chain can be devastating if it is infiltrated and then weaponized to extract sensitive data.
- **A growing medical device footprint.** It is no surprise that medical devices have been called "the next disruptor in healthcare."[16] Hospitals today have 10 to 15 devices per bed on average. This translates to as many as 7,500 in a typical 500-bed hospital.[17] Even more overwhelming from a security standpoint is the growing number of unique device types that must be tracked, maintained and secured. The risk is real. One study found that 20% of ransomware attacks on healthcare organizations began through a medical device.[18]

A People-Centric Approach

Today's cyber attacks target people, not technology. That's why you must take a people-centered approach to secure your clinical workers and non-clinical employees as well as the sensitive data that they use and share. Patient care is top of mind for every clinician, and time is often of the essence. So when the human stakes are high, it can be easy to place less focus on whether a specific email is legitimate. This is yet another reason the industry remains an easy target for malicious activity.

Figure 1 depicts the Top 10 Very Attacked People™ (VAPs) at a real-life large nonprofit integrated health network in the United States. As you can see, two types of people receive the most attacks:

- Executives across the clinical, financial, educational and the operations part of the business
- Employees responsible for accounts receivable, accounts payable and resident training

[16] Modern Healthcare. "Life-Changing Medical Devices: The Next Disruptor in Healthcare." January 2019.
[17] Tamer Baker (*MedCity News*). "How Hospitals Can Address Medical Device Vulnerabilities." September 2022.
[18] Ponemon Institute and Censinet. "The Impact of Ransomware on Healthcare During COVID-19 and Beyond." Accessed March 2023.

Two of the top 10 work for teaching hospitals in the network. These include institutions that possess both student data and information about large grants from governments and foundations. We see a lot of impostor activity on individuals who manage incoming and outgoing financial payments, most notably the payroll coordinator.

How Proofpoint Can Help

Your people are the new perimeter. They are your greatest assets. But they are also the source of your greatest security risk.

Combat ransomware and other advanced threats

In healthcare, a wide variety of organizations and IT environments coordinate, collaborate and share information. Email is a popular method of exchanging confidential data. But it is also the most common attack vector for cyber criminals. Most high-profile healthcare ransomware attacks and other data breaches begin with a phishing email. These often target people who play specific functions in the organization.

The Aegis Threat Protection platform from Proofpoint has the right solutions for the healthcare industry by protecting users in the way they work. This platform includes the following:

- **Proofpoint Email Protection.** This delivers top-rated email security to stop malware and non-malware threats.
- **Proofpoint Targeted Attack Protection.** With sandboxing capabilities, this detects and stops advanced threats.
- **Proofpoint Threat Response.** This delivers security orchestration, automation and response (SOAR) to share intelligence on new threats.
- **Proofpoint Security Awareness.** This provides employee training to spot healthcare-themed social engineering attacks, such as sophisticated phishing ploys.

Keep sensitive data safe

PHI, personal identifiable information (PII) and payment card industry (PCI) are among the most sensitive kinds of data. Proofpoint offers the right data loss prevention (DLP) tools for email, cloud and endpoint, which ensures your sensitive and critical information is classified and accessed by the right people.

- **Proofpoint Enterprise DLP.** Part of the Proofpoint Sigma Information Protection platform, this helps you protect your data as well as identify and respond quickly to risks posed by negligent, compromised and malicious users. Our unified platform allows customers to define data that is of interest and leverage these definitions across the entire platform. It protects the confidentiality of individual email messages through Proofpoint Email Encryption. Users can trigger encrypted messages automatically by adding a keyword of choice to the subject line. They can also trigger message-level encryption on the basis of DLP rules.
- **Proofpoint Web Security.** This automatically blocks malicious threats whether your staff browses the web from inside your organization or from a remote location. This with our market-leading DLP capabilities isolates web traffic to prevent uploads and downloads as well as copying and pasting of PHI, PII, PCI or other sensitive data.

Protect against impostor attacks

Impostors use BEC to steal money or confidential data. These attacks can be hard to detect. For one, they are designed to look as if they're from someone who the recipient knows or can trust. For another, they don't exploit technical vulnerabilities. BEC attacks target specific job functions that have access to activity that can be monetized. Pharmacists, clinical researchers, accounting personnel and hospital foundation staff are often targets.

Proofpoint offers an integrated, people-centric, end-to-end solution that stops all forms of email fraud. The following solutions defend against these attacks no matter the tactic or target:

- **Proofpoint Email Fraud Defense.** This blocks phishing and impostor emails that use spoofed and lookalike domain names. It uses advanced machine learning and multiple detection engines to detect these targeted attacks. And it mitigates risk of impostor threats by verifying and enforcing DMARC on your inbound traffic. Email Fraud Defense also goes beyond DMARC implementation by providing visibility into your supplier risk. The Nexus Supplier Risk Explorer feature automatically identifies your suppliers and business associates, validates their DMARC records and uncovers the risk they pose.
- **Proofpoint Secure Email Relay.** This enables DMARC-compliant system-generated emails from third-party core applications like Epic, Salesforce and ServiceNow.

Shield O365 and other cloud services

Healthcare institutions are moving data and apps to the cloud. So more users will access more sensitive information over the internet. A cloud access security broker helps your organization see cloud activity as it unfolds across the internal ecosystem and in the supply chain.

- **Proofpoint Cloud App Security Broker.** This is part of the Proofpoint Sigma Information Protection platform. It 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 such as Microsoft Office 365, DropBox, Box and Salesforce.

Prevent attacks through medical devices

Connected medical devices create multiple security risks. Dozens or even hundreds of distinct device types run on unique software on a variety of operating systems. Some older devices have known vulnerabilities that cannot be patched. And devices based at hospitals and clinics can be used by multiple patients in the same day. These devices may be an attractive attack vector for cyber criminals, but they are not the end goal for the attacker. They are just a way to get into the network.

- **Proofpoint Spotlight.** This actively engages attackers in your environment to detect their presence and track their lateral movement. It continuously scans directory structures, privileged access management solutions and the devices themselves to reveal gaps in your organization's identity security.
- **Proofpoint Shadow.** This engages attackers with data that looks real but are in fact deceptions. This approach lures the attackers into revealing themselves. And once the adversaries are identified, the security team can take informed actions to stop the attack.

Securing coordinated care

Healthcare team members need effective collaboration at the point of care. They have mobile solutions that connect clinicians with each other and with patients. But they are built for function and convenience, not security. They are often used outside the confines of the protected enterprise network. On top of that, physicians might access clinical apps from personal devices. They might also use personal email accounts on corporate-issued hardware.

- **Proofpoint Isolation.** This 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. This way your environment stays safe.

Protecting against insider threats

An employee leaking patient data at a doctor's office might seem like a scene from a TV medical drama. But insider threats are all too real. In fact, 35% of all breaches in healthcare involve internal threat actors.[19] Three of the most common insider threat risks and data loss for healthcare organizations include theft or misuse of PHI, theft or misuse of electronic health records (EHR), and insurance and other financial fraud.

- **Proofpoint Insider Threat Management.** This part of the Proofpoint Sigma platform helps stop insider threats. It protects against data loss, malicious acts and brand damage that involves insiders acting maliciously, negligently or unknowingly. Our solution correlates activity

[19] Verizon. "Data Breach Investigations Report 2023."

and data movement. This empowers security teams to identify user risk, detect and respond to insider-led data breaches. It also helps accelerate security incident response.

Manage legal and content compliance

Like companies in other highly regulated industries, healthcare organizations struggle with the following:

- Identifying where their business communications are taking place
- Ensuring that this content is captured and securely archived
- Searching and retrieving content for audits quickly and cost-effectively
- Monitoring and supervising workers who use these channels

Proofpoint Archive. This provides all-in-one, people-centric compliance. This means you are covered from the moment content is disseminated to when it is indexed, archived and retrieved. Policies can be tailored to regulations like HIPAA or standards like those of the Department of Health and Human Services (HHS). You can supervise, revise, remove and archive content easily, quickly and inexpensively. With Archive, you can be sure your digital engagement efforts comply with all communication and retention rules.

Protect Your Providers and Patients

Proofpoint gives your healthcare provider organization protection and visibility for your greatest cybersecurity risk: your 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, protect patients from cyber attacks, and safeguard your sensitive data. Leading healthcare organizations of all sizes, including more than 75% of the Fortune 500 healthcare organizations, rely on Proofpoint for people-centric security and compliance solutions to mitigate their most critical security risks before they cause lasting harm.

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.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. Proofpoint.com

proofpoint.