proofpoint.

SOLUTION BRIEF

Securing healthcare providers with Proofpoint

Protect people, AI agents, and patient data to ensure safe, resilient care delivery

This solution set is part of Proofpoint's integrated human-centric security platform, securing people and data in the agentic workspace.

Overview

As care delivery becomes more digital, distributed, and automated, healthcare providers are grappling with an attack surface that is expanding everywhere at once. Workforce shortages mean staff are often too busy to follow security protocols. Cloud services and connected medical devices add new attack entry points. And AI-enabled workflows introduce new vulnerabilities.

Threat actors have taken notice and are using all this change to their advantage. They understand that healthcare breaches often begin with humans or with the AI agents that act on their behalf. So, they're focusing on identity-driven attacks, social engineering, and abuse of trusted access.

Proofpoint helps hospitals, health systems, clinics, and integrated delivery networks protect their clinicians, staff, systems, and patients. It secures the full ecosystem of people, AI agents, and data. Our integrated cybersecurity and compliance solutions reduce breach risk, safeguard sensitive information, and support resilient, uninterrupted care delivery.

High-value targets in the healthcare industry

Healthcare providers are among today's most targeted organizations. Not only do they operate under intense pressure, but they manage large volumes of highly sensitive data, including:

- Protected health information (PHI) such as medical records, diagnostic results, and treatment data
- Personally identifiable information (PII)
- Financial, billing, and payroll data

This information is highly valuable to attackers and costly to lose. A breach can result in regulatory penalties, litigation, reputational damage, and disruption to patient care and safety.

Healthcare providers also face challenges that are unique to care delivery:

- Clinicians require fast, uninterrupted access to systems.
- Communications frequently contain sensitive, time-critical information.
- Care teams collaborate across hospitals, clinics, labs and third parties.
- Legal scrutiny, audits, and investigations are common.

Email and cloud collaboration tools are essential to coordinated care. However, they are also the primary entry points for cyberattackers.

Verizon's *2025 Data Breach Investigations Report* found that 60% of breaches involved the human element.

Healthcare provider cybersecurity challenges

As providers modernize their operations, they face several escalating risks.

Securing patient and clinical data

Healthcare providers must protect PHI, PII, and financial data. And they must do so across email, cloud platforms, and endpoints. Any breach can trigger HIPAA and HITECH violations, state privacy penalties, PCI DSS compliance issues, and costly litigation.

Managing insider risk in clinical environments

Elevated insider risk is everywhere. Not only is workforce turnover high, but there's a rotating list of staff, contractors, and residents. And there's broad access to EHRs. Accidental data exposure, credential sharing, and misuse of access can all result in reportable breaches.

Stopping impersonation and account takeover threats

Healthcare providers rely on a complex ecosystem of third parties. These can include labs, device vendors, suppliers, insurers, and government agencies. Attackers exploit these trusted relationships using business email compromise (BEC), vendor impersonation, and credential phishing. Shared mailboxes and service accounts are particularly attractive targets.

Responding quickly to advanced threats

Security teams face overwhelming alert volumes. And manual reviews do not easily scale. This is especially true when attacks reach hundreds of users or come from trusted identities that look legitimate.

Preparing for a cloud-first care environment

Clinicians increasingly access systems remotely, and they often use their personal devices. It's no longer practical to route all traffic through on-premises security controls. To have effective security, teams need to be able to see who is accessing sensitive data—as well as how and why.

A human and agent-centric approach to healthcare security

Together, humans and agents now form the operational surface of healthcare delivery. While clinicians and staff initiate care and business processes, they also have help. Many actions are now executed by non-human agents, including:

- Shared mailboxes and service accounts
- Cloud identities and APIs
- Automation workflows and AI-driven systems
- Connected medical devices
- Clinical and business applications such as Epic

That's why today's cyberattacks do not target technology alone. They exploit trusted humans and trusted agents.

Unfortunately, traditional perimeter-based security tools cannot identify the difference between legitimate actions and malicious behavior. This is especially true when attackers use compromised identities rather than malware for their fraudulent activities.

Proofpoint secures this environment by correlating identity, behavior, and data access across both people and agents. This closes the blind spots that attackers actively exploit.

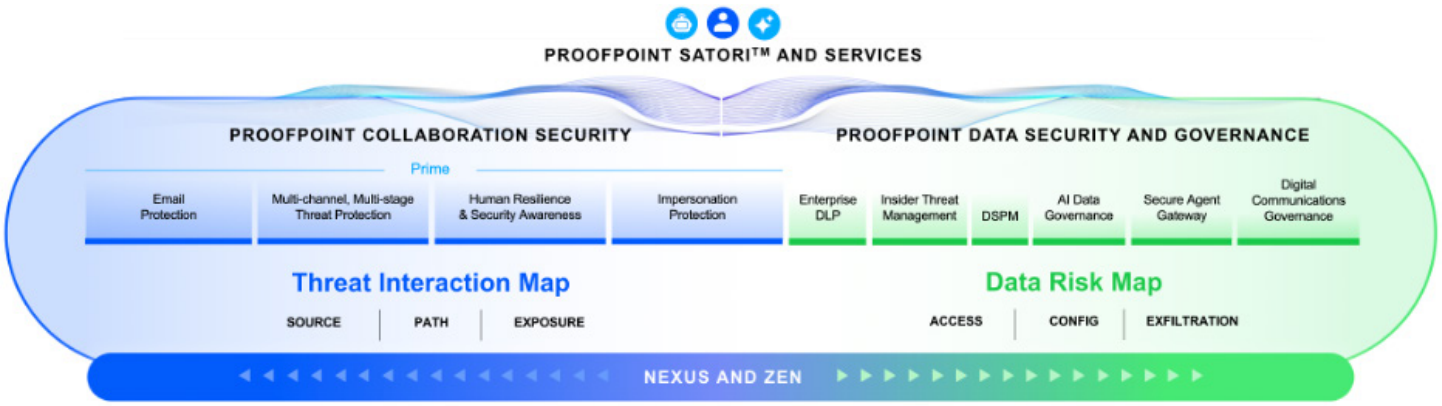


Figure 1. Proofpoint solutions secure the full ecosystem of people, AI agents, and data.

Products

- Proofpoint Collaboration Security Prime
- Proofpoint Secure Email Relay
- Proofpoint Data Loss Protection (DLP)
- Proofpoint Adaptive Email DLP
- Proofpoint Data Security Posture Management (DSPM)
- Proofpoint Satori
- Proofpoint Account Takeover Protection
- Proofpoint Insider Threat Management
- Proofpoint Communications Governance
- Proofpoint ZenGuide

How Proofpoint can help healthcare providers

Trusted by 67% of Fortune 500 healthcare companies, only Proofpoint delivers an integrated platform that secures humans, agents, and data together.

This section discusses the many ways we can help.

Protect against ransomware and other advanced threats

Proofpoint Collaboration Security Prime delivers an end-to-end approach to stopping human and agent-targeted attacks across email, collaboration tools, cloud applications, web channels, and social platforms. Powered by **Proofpoint Nexus®**, it uses advanced AI, behavioral analysis, and threat intelligence to block attacks across the full threat lifecycle from pre-delivery to time of click.

Secure critical email and application communications

Healthcare providers rely on system-generated email for essential clinical and operational workflows, including:

- Patient notifications and appointment reminders
- Care coordination and clinical alerts
- Billing statements and financial communications
- Compliance, reporting, and administrative messages

These communications are often sent at high volume by trusted applications and must be:

- Delivered reliably
- Authenticated and trusted by recipients
- Secure and compliant

Proofpoint Secure Email Relay enables healthcare providers to securely send large volumes of application-generated email while protecting patients, partners, and the organization from impersonation and fraud. Secure Email Relay:

- Enables DMARC-compliant email delivery from critical applications such as Epic, ServiceNow, and other clinical and business platforms
- Protects system-generated email from spoofing and lookalike domain abuse
- Ensures trust and integrity in patient-facing and operational communications
- Reduces risk from compromised or misconfigured application email

By securing non-human senders, Secure Email Relay extends Proofpoint's agent-centric cybersecurity model. It ensures that critical healthcare communications remain trusted, compliant, and resilient.

Keep patient data secure

Proofpoint Data Loss Prevention (DLP) solutions prevent accidental and malicious data loss across email, cloud, and endpoints by providing deep visibility into user behavior and content.

Proofpoint Adaptive Email DLP uses behavioral AI to analyze normal email-sending patterns and deliver real-time, contextual warnings to clinicians and staff. It prevents misdirected messages and data exposure without disrupting care delivery.

Proofpoint Data Security Posture Management (DSPM) identifies where sensitive data lives, which humans and agents can access it, and where excessive or risky permissions exist. This enables providers to reduce exposure and safely adopt AI and automation.

Proofpoint Satori™ extends DSPM with real-time data access governance for healthcare environments. Satori continuously monitors and controls access to sensitive patient data. It does this across cloud data stores, analytics platforms, and AI pipelines without disrupting clinical workflows.

With Satori, providers can:

- Discover and classify sensitive patient data and clinical data across cloud platforms
- Enforce least-privilege access for clinicians, staff, applications, and AI agents
- Detect and remediate risky or anomalous data access in real time
- Apply policy-based controls to protect PHI while enabling analytics, research, and AI innovation

Detect compromise and misuse at scale

Proofpoint Account Takeover Protection and **Insider Threat Management** detect suspicious behavior across both human and agent identities. They identify credential compromise, privilege abuse, lateral movement, and data exfiltration. By correlating identity, behavior, and data movement, Proofpoint enables a faster, more accurate response before patient care is disrupted.

Stay compliant and litigation-ready

Proofpoint Digital Communications Governance solutions streamline compliance with HIPAA, HITECH, and retention requirements. They ensure clinical and business communications are captured, searchable, and available for audits, investigations, and e-discovery.

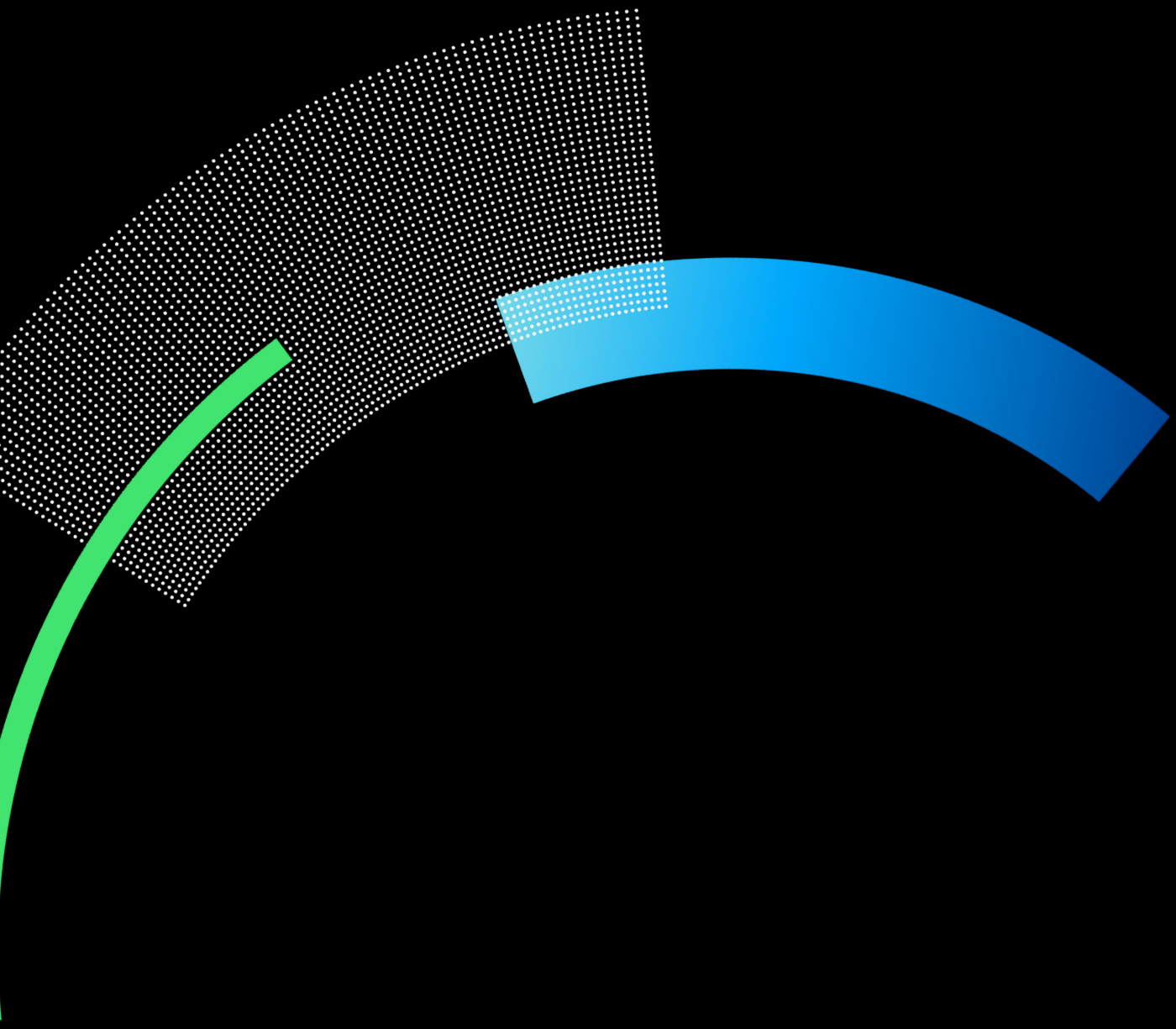
Reduce risk through behavior change

Proofpoint ZenGuide™ delivers role-based, risk-driven security awareness training that's tailored to clinicians and staff. It reinforces secure behavior using real-world healthcare threat scenarios without slowing care delivery.

Conclusion

Proofpoint has always protected people. Now our human and agent-centric security platform extends that protection to every interaction across people, data, and AI agents. It delivers control, compliance, and the freedom to embrace innovation.

With Proofpoint, healthcare providers can reduce the risk of a breach, protect patient data, maintain compliance, and deliver resilient, uninterrupted care in a complex threat landscape.



proofpoint.

About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organizations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at www.proofpoint.com.

Connect with Proofpoint: LinkedIn

DISCOVER THE PROOFPOINT PLATFORM →