proofpoint.

SOLUTION BRIEF

Protecting healthcare against ransomware with Proofpoint

Prevent human-targeted attacks, defend against AI-driven deception and protect data from extortion

Overview

Ransomware is one of the most disruptive threats facing healthcare organisations today. These attacks are no longer confined to encrypting systems. They now combine credential theft, data exfiltration and extortion to maximise operational and financial impact. For hospitals and healthcare providers, the consequences go far beyond downtime to directly affect patient care, safety and trust.

Most ransomware attacks begin with a targeted email, a compromised account or a deceptive message that tricks a user into taking action. Email, cloud applications and collaboration platforms remain the primary entry points, with attackers exploiting human behaviour to gain initial access.

AI is now accelerating this threat. Adversaries use AI to craft highly convincing phishing messages, impersonate trusted individuals and scale attacks across healthcare organisations. At the same time, healthcare providers are adopting AI-driven workflows and automation, introducing new machine identities and automated interactions that attackers can also exploit.

Proofpoint helps healthcare organisations stop ransomware by preventing human compromise, detecting AI-driven deception and protecting sensitive data from exfiltration and extortion.

Impact of ransomware on patient care

Ransomware attacks are not just IT incidents; they're patient safety events.

When systems become unavailable or data is compromised, the impact is immediate and far-reaching.

- Delayed or disrupted access to electronic health records (EHRs)
- Diversion of emergency patients to other facilities
- Interruptions to critical care delivery and clinical workflows
- Inability to access diagnostic systems, lab results or imaging
- Exposure of sensitive patient data (PHI), leading to loss of trust

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

$1.2M

Average ransom payment in healthcare.[1]

Healthcare ransomware challenges

Ransomware in healthcare is uniquely damaging because it targets both operations and patient outcomes. Attackers deliberately focus on environments where downtime isn't an option.

These attacks follow a predictable pattern. Threat actors use phishing or social engineering to steal credentials, gain access to systems and move laterally across the organisation.

Once inside, they identify high-value systems and data, exfiltrate sensitive information and then deploy ransomware to maximise leverage and potentially stop operations.

What has changed is how these attacks are executed. Ransomware campaigns are now:

- Highly targeted, focusing on specific roles such as clinicians, finance teams and executives
- AI-enhanced, enabling more convincing impersonation and faster attack development
- Data-driven, prioritising theft of patient data and operational information before encryption
- Extended across ecosystems, exploiting suppliers, partners and shared platforms

At the same time, healthcare organisations must secure not only users, but also AI agents, automated workflows and non-human identities that interact with sensitive systems and data.

This convergence of human risk, AI-driven threats and data exposure is what makes modern ransomware so effective and so hard to stop with traditional controls.

A human- and agent-centric approach to healthcare security

Today's cyberattacks target more than technology. They exploit trusted humans and trusted agents. To stop ransomware, you need to shift your security approach from the final stage of encryption to the earliest stages of the attack chain.

Because ransomware is typically delivered through human interaction (clicking a link, opening a file or responding to a message), the most effective defence is to prevent compromise before attackers gain access.

This requires a security approach that:

- Understands who is being targeted
- Detects deception across email and cloud channels
- Secures AI-driven interactions and automated processes
- Protects sensitive data from exfiltration

Proofpoint delivers this through a unified, human- and agent-centric platform that correlates behaviour, identity and data access to stop ransomware across the full attack lifecycle.

1. Ponemon. *Study on Cyber Insecurity in Healthcare.* 2025.

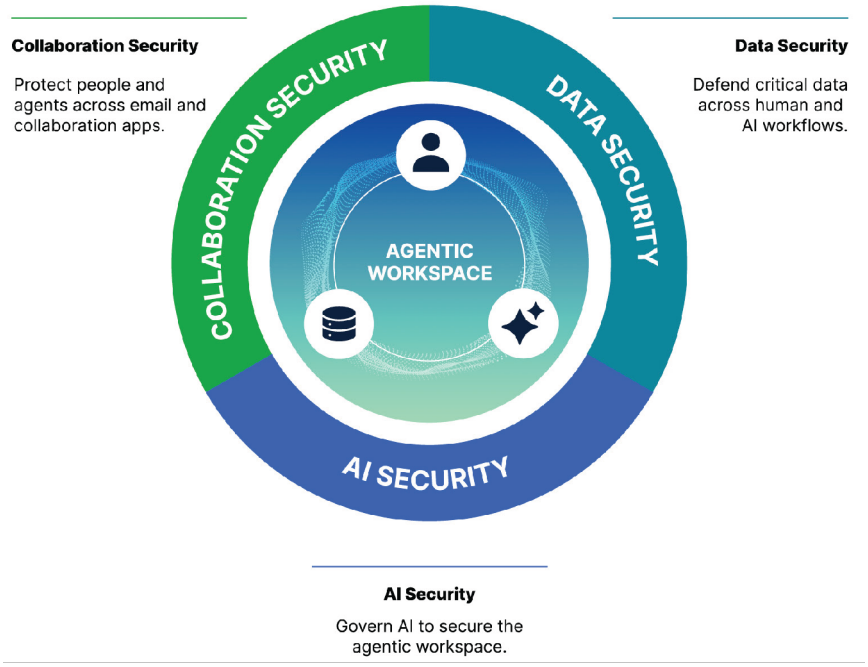

Figure 1. A platform approach that stops ransomware across the full attack lifecycle.

Products

- Proofpoint Collaboration Security Prime
- Proofpoint Nexus
- Proofpoint Data Loss Prevention (DLP)
- Proofpoint Adaptive Email DLP
- Proofpoint Data Security Posture Management (DSPM)
- Proofpoint Satori
- Proofpoint Account Takeover Protection
- Proofpoint Insider Threat Management
- Proofpoint ZenGuide

How Proofpoint can help

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

Prevent initial compromise

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, behavioural analysis and threat intelligence to block attacks across the full threat lifecycle from predelivery to post-click.

Defend against AI-driven deception and account takeover

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

Keep patient data secure

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

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

Proofpoint Data Security Posture Management (DSPM) identifies where sensitive data resides, 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 across cloud data stores, analytics platforms and AI pipelines without disrupting clinical workflows.

With Satori, healthcare providers can:
Discover and classify sensitive patient and clinical data across cloud data 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

Reduce human risk through behaviour change

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

Conclusion

Ransomware attacks in healthcare are inevitable, but their success is not. By focusing on the earliest stages of the attack chain and addressing the root causes, healthcare organisations can stop ransomware before it disrupts care delivery.

Proofpoint enables healthcare organisations to prevent attacks, protect patient data and maintain operational resilience with a modern, human- and agent-centric approach to ransomware defence.

proofpoint.

DISCOVER THE PROOFPOINT PLATFORM →