Analyze User Behavior and Content Across All Channels to Defend Data

Behavioral AI and a fully integrated toolset are critical elements for information protection

Healthcare organizations face a surge of cybersecurity risks driven by increasing digitization of patient records, cloud utilization and data sharing across systems. Cybercriminals are targeting sensitive health data, financial records and user credentials in highly distributed healthcare networks. In 2024, healthcare experienced the most expensive cyberattacks, with an average breach costing nearly $10 million.[1] And with the expansion of ransomware and extortion exploits, healthcare organizations will likely be targeted by more such attacks in the future.

"Healthcare CISOs are talking very openly about the motivations of threat actors today, and that's mainly extortion," said Ryan Witt, Proofpoint's Vice President of Industry Solutions and chair of the company's Healthcare Customer Advisory Board. "They are trying to extort payment from that organization. 'You give me money, and I'll give you your system back.' That's a trend we're seeing."

It's not just the documented increase in ransomware and phishing attempts that keep healthcare CISOs awake at night. They are also concerned about data loss, including protected health information (PHI), attributable to malicious insiders, compromised accounts and careless users who rely on insecure email, remote work apps, cloud computing and productivity platforms.[2]

The arrival of AI-enhanced ransomware, phishing and insider threats creates a need for advanced security measures to protect patient information and ensure the integrity of healthcare operations. Understanding the current landscape of cyber threats in healthcare and the strategies needed to mitigate these risks and defend data represents the first step toward adopting a human-centric, proactive approach to data protection.

Safeguarding your data: start with people

Today, attackers target people, not technology. And that's where cybersecurity leaders should focus their attention and their resources.

"Think of the pure economics of taking over somebody's account," said Brian Reed, Proofpoint's Senior Director of Cybersecurity Strategy. "The headlines tend to glorify zero-day exploits; however, the cybercrime economy is largely based on how exploited humans interact digitally. It's a far lower barrier of entry to socially engineer a victim or craft a phishing lure than to spend time and energy building, testing, and releasing zero-day exploits."

Reed estimates that in healthcare, as in most other industries, about 80 percent of all attacks focus on human elements rather than on technical vulnerabilities. He breaks those people-focused attacks into three areas:

- Ransomware attacks, in which bad actors use credential phishing to infiltrate a network. It usually involves an inducement to install a browser extension, click a link or download an app.
- Business email compromise, in which there is no link, attachment or payload, just a disguised attempt to get the user to take an action outside of the usual workflow.
- Data loss due to insiders, whether they are malicious, compromised or merely careless users.

"The vast majority of those cases of data loss are just good people making bad decisions," said Reed. "And a lot of times it's just misconfigurations around access control or it's oversharing."

This recognition has prompted some to label human targets "the weakest link," but Reed contends that the opposite is true. "If you think about trying to disrupt an attack, humans are your opportunity — to have them be suspicious, raise a question, phone a friend," he said. "That's not a weakness."

Preventing accidental and intentional data loss

Traditionally, cyber defense has meant stopping exploits at the network perimeter: patching vulnerabilities, stopping inbound phishing attempts and identifying social engineering efforts before they reach vulnerable end users. But in today's healthcare ecosystem, with a constantly fluctuating workforce that can include temporary employees and traveling clinicians, an exponential increase in endpoints and widespread cloud adoption has increased the demand for data loss protection (DLP) solutions.

"Healthcare CISOs are talking very openly about the motivations of threat actors today, and that's mainly extortion."

RYAN WITT | Vice President of Industry Solutions | Proofpoint

"It makes sense to begin with firewalls and endpoint protection. But the problem is that's not how human attacks happen."

BRIAN REED | Senior Director of Cybersecurity Strategy | Proofpoint

According to Proofpoint's *2024 Data Loss Landscape* report, 70% of respondents now report careless users as a leading cause of data loss and regulatory violations.[3] Verizon's *2024 Data Breach Investigation Report* found that 68% of breaches involved a "non-malicious human element, like a person falling victim to a social engineering attack or making an error."[4]

Looking at just one vector, a 2023 report from Tessian (now a Proofpoint company) found that about one third of employees sent about two emails to the wrong recipient annually.[5] The ease and insecure access controls of productivity platforms and cloud storage also increases the potential for data disaster.

"It makes sense to begin with firewalls and endpoint protection," Reed said. "But the problem is that's not how human attacks happen. If you think about mis-delivered email, or accidentally oversharing via OneDrive and SharePoint, how much will firewalls and endpoint prevention software help you there? Zero."

DLP solutions recognize that stopping data loss from the inside is just as important as preventing external exploits from getting through the perimeter. Most approaches use sophisticated pattern matching to try to identify sensitive data that might accidentally or intentionally be exfiltrated before it can leave the network.

But advanced DLP goes much further. First, large language models can look at billions of records and begin to classify sensitive data, not through brute patterns, but by understanding context and the relationships between and among files and directories.

Proofpoint's Enterprise Security Advisor, Joshua Linkenhoker, said these models can scan outbound email or file transfers to identify, for example, that an attachment looks like a financial earnings statement. Even more powerfully, AI can be trained on human behaviors to stop common, but hard to catch, mistakes such as accepting an incorrect autofill suggestion for an email recipient. Linkenhoker calls it "behavior-driven functionality."

"Instead of using a large language model, like we would on the data side, we're going to examine a year's worth of your sending habits," he explained. "AI technology can look at your subject lines, recipients and attachments. And it will generate preventative actions like prompting you to make sure you are sending your email to the right recipient."

Detect data exfiltration from email, the cloud and endpoints

Real-time AI interventions add a powerful component to automated compliance, which is a boon to heavily regulated industries such as healthcare. Every time an employee is guided to make the right choice when emailing potentially sensitive data, a potential HIPAA violation is avoided.

Beyond email, behavioral AI can coach users to think twice before moving data onto an insecure cloud storage folder or sharing a sensitive file via OneDrive or SharePoint. According to Witt, the growth in cloud-based productivity apps that default by design to sharing information has become a major vulnerability in healthcare.

Reed agreed that it's one thing to anticipate the moves of a determined cybercriminal, but much harder to anticipate the creative, if insecure, workarounds of an overburdened healthcare workforce that is under pressure to move quickly. It requires both human and organizational psychology to understand the plethora of human-driven use cases.

Of course, he added, behavioral AI can also stop anomalous behavior with more malicious intent. When a user who's already given notice starts renaming sensitive financial files "family pictures.zip," moving them to a USB drive and deleting them from a local drive, it's clear that this kind of exfiltration isn't innocent. And without the ability to use scalable AI to recognize suspicious behavior, it's hard to identify internal bad actors.

"Not every insider risk is a threat, but every single insider threat out there started as some form of insider risk," Reed said. "So it's important to understand who might be a potential risk at some point in the future."

With an increasing number of endpoints and channels to monitor, specialized information security solutions have multiplied. And while a "defense in depth" approach is valuable, a multiplicity of data feeds can make it more difficult for healthcare security analysts to review incidents in real time and understand human actions in context. "You need to try to knit all of these [data feeds] together to reduce human error and human computational time," Linkenhoker noted.

AI technology can look at your subject lines, recipients and attachments. And it will generate preventative actions."

JOSHUA LINKENHOKER | Enterprise Security Advisor | Proofpoint

Many IT teams would agree. Proofpoint research indicates that nearly 70% of surveyed IT professionals rank visibility into sensitive data, user behavior and external threats as the most important capability for their data loss prevention programs.[6] It's a complex problem because information security analysts need to see both deeper and wider simultaneously — visibility at scale.

"You want *defense in diversity* while understanding how your vendors interoperate," Reed pointed out. "What do they show you? What information are they providing? And most importantly, are you able to bring it all together for a picture of current situational awareness?"

When information that flows from different sources is integrated, healthcare organizations can move from protecting against known, commoditized attacks, which make up the bulk of current threats, to preventing the most advanced, tailored and unanticipated exploits. And it provides an opportunity to employ AI across information silos to achieve a truly contextual, 360-degree view of the threat environment.

"You now have to go find the needle in the haystack," Witt said. "You need that level of full visibility, that level of analytics, that level of AI that is detecting a small number of interactions.... You're capturing just a very small fraction of the totality of the traffic, but it's that little bit that really matters."

To learn more, visit proofpoint.com/healthcare.

References

1. IBM and Ponemon Institute. 2024. *Cost of a Data Breach Report 2024*. https://www.ibm.com/reports/data-breach.
2. Proofpoint and CyberEdge. 2024. *The 2024 Data Loss Landscape*. https://www.proofpoint.com/us/resources/threat-reports/data-loss-landscape.
3. Ibid.
4. Verizon. 2024. *Verizon 2024 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/.
5. Proofpoint. 2024. *Transforming DLP* [eBook]. https://www.proofpoint.com/sites/default/files/e-books/pfpt-us-eb-rethinking-dlp.pdf.
6. Proofpoint and CyberEdge, *The 2024 Data Loss Landscape*.

proofpoint.

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 85 percent of the Fortune 100, rely on Proofpoint for human-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.

Produced by HIMSS®