Navigating Today's Healthcare Threat Landscape:

A Three-Step Approach to Stay Ahead of Cyberattackers

Since the introduction of electronic medical record systems, healthcare organizations have been a favorite target of cybercriminals seeking personal health information — which generally yields the most lucrative return for those selling data on the "dark web."

"Health systems and payers have always faced unique threats due to the amount of sensitive data that these organizations hold and the operational value of that data," notes Josh Burgess, Lead Global Technical Threat Advisor for CrowdStrike, a leading cybersecurity technology company. "Add to that the amount of legacy systems — devices, legacy software that can't be updated, an MRI machine that runs on Windows XP that will never run anything else — and it creates an environment that's ripe for targeting."

But today's threat topography is expanding exponentially as nation-state actors and independent hackers take advantage of healthcare's unprecedented transformations: rapid consolidation, new reimbursement models, digital disruptors and, most recently, the COVID-19 pandemic.

Meanwhile, the attack surface of healthcare organizations has also grown, as an increasing number of endpoints — personal computing devices, medical devices, smart furniture and even facility systems like HVAC — leverage network connections.

Finally, the nature of the attacks themselves are more sophisticated. Given the criticality of their data, healthcare organizations are prime targets for ransomware attacks of the WannaCry or NotPetya variety. But rogue actors aren't just locking down data — once they get into your network, they are exfiltrating data, looking for extortion opportunities and stealing intellectual property.

Unfortunately, traditional, on-premises network defenses are no longer sufficient to stop bad actors. According to *Healthcare Finance News*, 132 successful breaches were reported to HHS between February and May 2020 — a nearly 50% increase over the same time last year.[1]

Separating the wheat from the chaff

Why can't traditional cybersecurity software stay ahead of today's rapidly evolving healthcare threat landscape? According to Jason Rivera, Director of the CrowdStrike Strategic Threat Advisory Group, it's the result of a one-size-fits-all approach to identifying attacks.

"Legacy systems can't collect the data needed to support advanced defenses that use behavioral models or machine learning to understand what the threat is, who's behind it and what they're targeting," he explains. "They just compare hashes on endpoints: Is it a good hash or a bad hash?"

"You need to be able to separate the wheat from the chaff," adds Burgess. "Without context, without the telemetry, you can't respond effectively. An alert that says 'malicious' or 'trojan.generic' isn't enough. If you don't know who's attacking, you don't know how they're attacking, you don't know what you're dealing with. There's no way to respond to an incident and do it effectively, do it quickly and make sure that you can do it thoroughly."

Frustrated by the limits of traditional security software, many forward-thinking healthcare organizations are moving their security to

"A successful cloud-based deployment works from the inside out, beginning with endpoint protection using next-generation antivirus technology to automatically block the majority of attacks."

JASON RIVERA | DIRECTOR OF STRATEGIC THREAT ADVISORY GROUP | CROWDSTRIKE

cloud-based vendors. In the process, they've benefited from three cloud-enabled advantages:

1. **Lightweight endpoint agents**: Cloud-based solutions move processing into the cloud, making security easier to administer and speeding up local devices for end users.

2. **'Big data' applications**: Aggregating worldwide threat data in the cloud enables artificial intelligence (AI), machine learning and other advanced technologies to perform advanced threat analysis, quickly identifying an attack's perpetrator, method and target.

3. **Flexibility**: A cloud approach enables IT and security teams to rapidly onboard and provision devices at scale — and with virtually no downtime.

"We've seen these advantages play out during COVID-19," Rivera says. "Suddenly, everybody has to work from home. But how do you rapidly adapt to that? A lot of organizations without a cloud-native approach really struggled to extend their remote workforce or stand up secure platforms for virtual health."

Three steps to cloud-based security

Deploying cloud-based security should follow a logical sequence to avoid the old one-size-fits-all approach.

"Historically, the industry has spent money first and taken all sorts of actions without actually understanding the adversaries that it is trying to combat," Rivera says. "So the place to start is to really understand the unique problems that you are trying to solve."

After that, Rivera says, a successful cloud-based deployment works from the inside out, beginning with endpoint protection using next-generation antivirus technology to automatically block the majority of attacks. Once that's achieved, then move to real-time attack visibility via endpoint detection and response (EDR), followed by more advanced solutions like threat hunting and threat intelligence that, according to Rivera, "allow you to see what's happening in the rest of the world and apply it to your own situation."

The key: Start at the center and deploy defenses outward in successive steps.

"Everybody is a target," Burgess emphasizes. "Cybersecurity isn't easy, and it takes resources. But given today's threat landscape, the consequences of not doing it right and hoping for the best could potentially close your doors forever."

"Cybersecurity isn't easy, and it takes resources. But given today's threat landscape, the consequences of not doing it right and hoping for the best could potentially close your doors forever."

JOSH BURGESS | LEAD GLOBAL TECHNICAL THREAT ADVISOR | CROWDSTRIKE

Reference

1. Hackett M. 2020. Number of cybersecurity attacks increases during COVID-19 crisis. HealthcareFinanceNews.com. June 4. https://www.healthcarefinancenews.com/news/number-cybersecurity-attacks-increase-during-covid-19-crisis.

CROWDSTRIKE

About CrowdStrike

CrowdStrike® Inc., a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security. With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform. There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.