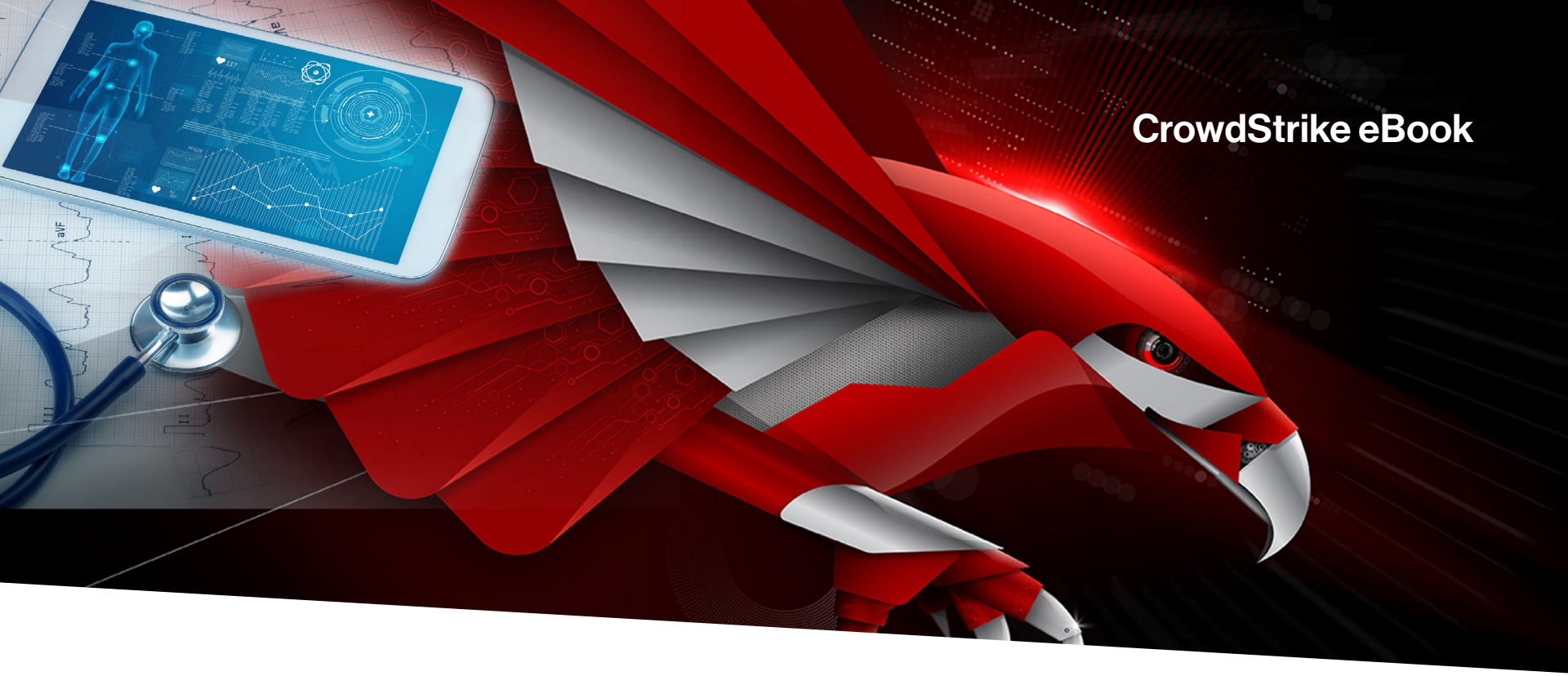


CrowdStrike eBook

PROTECTING HEALTHCARE SYSTEMS AGAINST RANSOMWARE AND BEYOND

CYBERCRIMINALS ARE UPPING THEIR GAME IN HEALTHCARE

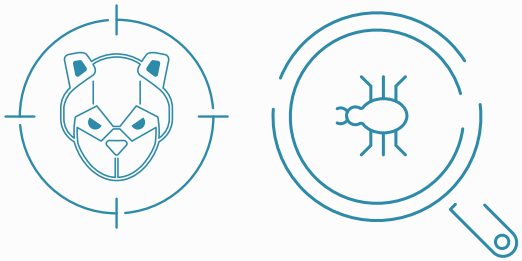
FIN12, a ransomware group targeting healthcare, uses a network of other threat actors to deploy common but powerful malware tools.

"From 2020 to 2021, FIN12 managed to halve its time-to-ransom (TTR), or the amount of time from when they access an environment to when they deploy ransomware. Mandiant discovered that the group can complete a cyberattack lifecycle in just 2.5 days."

Source:
FIN12 Ransomware: Why It's a Healthcare Threat, How to Prevent an Attack

Healthcare organizations are uniquely vulnerable to cyberattacks, and at the same time, they're in a tough spot, as they're increasingly dependent on new, interconnected technologies to deliver quality care to more patients. These organizations are being called upon to:

1. Integrate new medical and personal devices, while continuing to rely on legacy cybersecurity systems that are increasingly vulnerable to attack
2. Provide better patient engagement and customer service via self-service options and increased transparency (via web portals and mobile apps)
3. Incorporate more third-party connections, including clinical partners and software and other service providers that are often deeply integrated into the healthcare delivery organization's network
4. Perform third-party risk assessments and proactively monitor their risk posture over time
5. Manage a growing number of critical or zero-day vulnerabilities on equipment managed by third parties and vendors that are too slow to patch



Lapses in security in any part of this complex environment create opportunities for adversaries, increasingly drawn by the high value of protected health information (PHI) that resides in and passes through healthcare systems, as Health IT Security reported in 2021:

> "... as the pandemic continues to overwhelm providers and threat actors get savvier, healthcare data breaches are not slowing down. [The HHS's Office for Civil Rights] named over 550 covered entities that have experienced a data breach in 2021, at the time of publication. Over 40 million individuals faced PHI exposure as a result of these breaches."[1]

Healthcare delivery organizations will continue to face increasing regulatory pressures (e.g., HIPAA reporting requirements and state-specific privacy initiatives) and penalties when their cybersecurity efforts fall short. They will need to control risk when sharing information in evolving electronic health information (EHI) exchanges like the Trusted Exchange Framework and Common Agreement (TEFCA) initiatives.[2]

---

1. "This Year's Largest Healthcare Data Breaches," Health IT Security, November 30, 2021

2. https://rce.sequoiaproject.org/tefca/

In addition, financially motivated organized criminal groups will continue to target the healthcare sector, with the deployment of ransomware being a favored tactic given the urgency of delivering healthcare.[3] A 2021 report found 34% of healthcare delivery organizations worldwide were hit by ransomware.[4]

In this eBook, you'll learn three key strategies that enable you to deliver the highest quality care and stay competitive while keeping patient and employee data safe:

- **Reduce your attack surface and risk** by enforcing Zero Trust in managing the identities of the people, devices and applications requesting access to your valuable assets
- **Replace the complexity of your legacy infrastructure and security tools** with a simpler, more powerful, cloud-based solution and services that deliver value immediately
- **Offload the burden your staff faces from cyber threats by automating** many defenses and, during attacks, applying expertise in a cost-effective way for your organization

3 . https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf

4 . https://news.sophos.com/en-us/2021/05/17/the-state-of-ransomware-in-healthcare-2021/

CYBERCRIMINALS ARE UPPING THEIR GAME IN HEALTHCARE

In 2021,

59%

of attacks against the healthcare sector took aim at credential theft;
across all sectors, about

45%

of credential phishing attacks targeted Microsoft Office users, highlighting the need for Active Directory hardening.

Source:
Cofense 2021 Annual State of Phishing Report.

Apply Zero Trust to Protect Access to Healthcare Systems

Four factors have presented additional opportunities for cybercriminals to exploit vulnerabilities in the security of healthcare delivery organizations:

- **Bad actors now have more targets for attacks, given the explosion of endpoints outside the protection of a "traditional" network.** Telehealth, mobile devices, home care, connected medical devices, facility and building-control systems, and the addition of Internet of Things (IoT) and Internet of Medical Things (IoMT) devices to the environment have expanded the potential attack surface.
- **Work-from-anywhere initiatives have pushed machines and staff outside the network boundary.** Security teams must find ways to deal with challenges like legacy routers, firewalls and other vulnerable devices on home and public networks used in work-from-anywhere environments.
- **Healthcare delivery organizations continue to migrate to the cloud.** Skills needed for cloud management differ significantly from those used in on-premises operations, creating opportunities for misconfiguration and security exposure.
- **Organizations face challenges in securing identities due to high staff turnover (e.g., contract nurses and the "Great Resignation"), coupled with the complex management of technology used to authenticate, authorize and validate all users of the network.** The high value of healthcare data and the dire consequences of it not being available make it a target for ransomware attackers like WIZARD SPIDER (aka FIN12), a ransomware group that targets healthcare organizations. (In a typical ransomware attack, bad actors look to gain access to a network, deploy malware and exfiltrate copies of data, forcing the healthcare delivery organization to revert to pre-established electronic health record downtime procedures as it attempts to recover.)

Endpoints with poor identity security give bad actors the access they need. From 2020 and 2021, the healthcare sector saw an 80% increase in credentials as the type of data compromised in data breaches, according to a comparison of the Verizon Data Breach Investigation Report for the respective years.[5] Adversaries have also become adept at expanding their footprint, developing sophisticated malware that exploits weaknesses in identity security to traverse networks looking to take advantage of additional extortion opportunities.

Enforcing a **Zero Trust** security framework tightens up security, requiring the identities of all users — whether in or outside the organization's network — to be authenticated, authorized and continuously validated for security configuration and posture before being granted or retaining access to applications and data.

Zero Trust enforces identity security across the board — for mobile devices, cloud workloads, servers and containers in modern hybrid, multi-cloud data centers, and traditional endpoints running Windows, macOS and Linux — including the people who manage and use these resources.

This may sound like a tall order for healthcare delivery organizations already strapped by too few security experts working with a disjointed collection of legacy security solutions.

Since visibility is key, a cloud-native solution, rather than one running on premises, is best positioned to enforce a Zero Trust framework when it enables real-time monitoring and controls to identify and halt malicious activity quickly. In addition, it is important that clinical workers not be encumbered by responding to false positives. Advanced artificial intelligence (AI) can help, focusing workers on actionable insights from comparing live authentication traffic against baseline behaviors and attack patterns to highlight actionable insights.

---

5 . https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdf, https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf

The ability to re-examine all default access controls automatically and continuously is another requirement because Zero Trust assumes would-be attackers can always be present, both inside and outside the network.

An endpoint protection and identity protection solution based on a Zero Trust framework employs a variety of preventative techniques:

- Visibility into user identity and type of credential, credential privileges on each device, and behavior patterns for credentials and devices compared to a norm — especially important in managing service accounts that are often misused by internal staff and targeted by attackers
- Multifactor authentication (MFA) that relies on two or more pieces of evidence to assess a user's credibility
- Least-privilege access, granting only the level of access required to each user or device (ideally revisiting permissions on a regular basis)
- Network segmentation that divides the network into multiple zones, allowing security professionals to better contain attacks

Zero Trust must also align with your broader security strategy by incorporating a variety of endpoint monitoring, detection and response capabilities.

REPLACE LEGACY INFRASTRUCTURE AND SECURITY TOOLS WITH A CLOUD-BASED SOLUTION

3

In the past, many cybersecurity teams fought adversaries by using technology and strategies focused on keeping the bad guys out of their system, building "higher castle walls and deeper moats" to protect the valuable data inside the network from external threats.

Unfortunately, this model of cybersecurity can create a false sense of security. As healthcare organizations arm their IT teams with the ability to build technology stacks to advance patient care, there's an urgent need to accelerate cybersecurity transformation programs as a way to help secure massive digital health investments and dependencies.

Attackers are organized globally — they share and sell attack techniques and software via the web — and they are becoming more sophisticated. Legacy security solutions:

- Cannot detect fileless and zero-day malware, the exploitation of known vulnerabilities (such as a Golden Ticket attack that targets the authentication process in a Windows environment), encrypted malware and credential theft
- Focus only on individual devices (not users) and provide little attack information across multiple devices and the entire network
- Are designed in ways that result in "bloat" and the performance problems that go with scheduled scans
- Do not offer protection across the entire threat lifecycle and do not support Zero Trust — there is no inclusive growth path for increasing or broadening security

Simply replacing an existing on-premises legacy antivirus solution with another on-premises solution will not significantly advance the security posture of a healthcare delivery organization.

As described earlier, enforcing a Zero Trust security framework tightens up security, requiring the identities of all users — whether in or outside the organization's network — to be authenticated, authorized and continuously validated for security configuration and posture before being granted or retaining access to applications and data.

Providing more comprehensive endpoint protection from a cloud solution gives you flexibility, cost and productivity benefits similar to those gained when moving workloads to the cloud. A cloud-based endpoint protection platform:

- **Delivers immediate security benefits** on a subscription basis — you accelerate time-to-value by not incurring large upfront acquisition or deployment costs, and there are no on-premises controllers to be installed, configured, updated or maintained
- **Eliminates the bloat and performance issues** of the increasingly ineffective scheduled scans associated with legacy antivirus solutions
- **Consolidates endpoint agents** into a single, lightweight agent automatically maintained by the vendor, shifting the burden of updating and maintaining solutions to the service provider
- **Increases and expands visibility** — it sees endpoints everywhere, including virtual machines and data centers, providing protection even when endpoints are offline
- **Continues to improve efficiency** and frees up funds by phasing out multiple point solutions, consolidating capabilities while continuing to use the same familiar user interface
- **Scales to grow and adapt to your needs** without adding complexity or more monitoring, all while managing your environment with a web console

AUTOMATE DEFENSES AND APPLY HEALTHCARE SECURITY EXPERTISE MORE COST-EFFECTIVELY

4

Healthcare delivery organizations face three main challenges in staffing for security operations:

- They are typically burdened by a security workload that far outstrips the bandwidth and expertise of existing staff
- They have difficulty hiring and retaining experts that fit an organization's security requirements and budget
- The increase in zero-day and other high-risk vulnerabilities requires more resources for the operations staff to react to critical vulnerabilities on both equipment owned and managed by the health delivery organization (HDO) and on vendor-managed equipment

Rapid response to breaches is critical. Breakout time — the average one hour and 38 minutes[6] that it takes an intruder to jump from the machine that's initially compromised and move laterally through your network — is emerging as a critical window to stop a breach. However, it's not the only crucial metric you need to know. When an attack is in progress, you have, on average, one minute to detect it, 10 minutes to understand it and 60 minutes to contain it.[7]

The intelligent automation of security operations across all endpoints is key — it allows your staff to offload ordinary tasks and focus on where they add the most value in your mission to deliver high-quality patient care. Intelligent automation provides or enables:

- Automatic monitoring on every endpoint on premises and in the cloud, on or off the network
- Continuous collection of data and real-time analytics to correlate and give context to information and provide insight earlier in the attack cycle

---

6. https://www.crowdstrike.com/resources/reports/global-threat-report/

7. https://www.crowdstrike.com/resources/crowdcasts/the-1-10-60-minute-challenge-a-framework-for-stopping-breaches-faster/

4

- Smart filtering technology leveraging AI and machine learning (ML) to automatically detect and intelligently prioritize malicious activity in the "noise" of voluminous alert data to provide truly actionable intelligence that inform more timely, more effective remediation
- Intelligence to proactively hunt for threats and investigate them for triage and response
- Timely patching of critical vulnerabilities and zero days across the entire network

With regard to threat intelligence, your staff needs access to the most comprehensive, up-to-date collection of security data available: global in scope, gleaned from both private industry and the public sector. For applying the right kind of expertise, you need options that fit your unique circumstances:

- You may choose to add expertise in specific areas in which you feel you are weak or more vulnerable — for example, identity security, vulnerability management or cloud workload protection
- Or, due to an overwhelmed security staff or a widely distributed environment, you may opt to increase your security maturity and ensure 24/7 coverage by augmenting your team with experts to configure and operate your endpoint security and remediate incidents

HOW CROWDSTRIKE HELPS HEALTHCARE ORGANIZATIONS

5

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform provides 100+ healthcare delivery organizations around the globe with real-time protection and visibility across their entire technology network infrastructure, preventing attacks on endpoints on or off the network. In the United States, CrowdStrike safeguards over 1 million healthcare endpoints.

The Falcon platform is purpose-built in the cloud with a single lightweight-agent architecture that delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

The CrowdStrike Security Cloud correlates trillions of security events per day with indicators of attack and the industry's leading threat intelligence and enterprise telemetry from across customer endpoints, workloads, identities, DevOps, IT assets and configurations.

Using world-class AI, the CrowdStrike Security Cloud creates actionable data, identifies shifts in adversarial tactics, and maps tradecraft in the patented CrowdStrike Threat Graph® to automatically prevent threats in real time across CrowdStrike's global customer base.

CrowdStrike Intelligence gathers data on the more than 28 sophisticated threat actors who regularly set their sights on the healthcare industry and the tactics they use to conduct attacks.

For organizations with greater security maturity and staffing, the Falcon platform is flexible and extensible with components designed to protect endpoints, identity and cloud workloads against today's sophisticated threats.

For institutions that need more, **Falcon Complete for Healthcare**, CrowdStrike's managed detection and response (MDR) service, handles all aspects of endpoint and identity protection, freeing your staff to focus on your main mission.

Regulatory compliance is critical to healthcare delivery organizations, and CrowdStrike can assist with a broad range of compliance requirements, including:

- HITRUST and **HIPAA** requirements
- Affordable Care Act
- Distribution of medication regulations
- HHS fraud regulations
- Regulations that are state-specific regarding security — e.g., California (CCPA) and New York (SHIELD)
- Rapidly demonstrating adherence to non-healthcare specific requirements like:
  - Gramm-Leach-Bliley Act (GLBA)
  - PCI-DSS
  - GDPR
  - Freedom of Information Act (FOIA)
- Achieving a new standard in healthcare cybersecurity through adoption of a 1-10-60 security posture. This framework provides guidance for stopping breaches faster by overcoming common hurdles to establishing an effective incident response (IR) process.

CrowdStrike healthcare customers associated with state agencies may be able to access CrowdStrike solutions through a variety of Cooperative Purchasing Agreements, Blanket Purchase Agreements (BPAs) and Federal Supply Schedules (FSS), including:

- California: Software Licensing Program (SLP) Plus
- New York: Office of General Services (OGS)
- Texas: Texas Department of Information Resources (DIR) and The Interlocal Purchasing System (TIPS)

WANT TO LEARN MORE?

1 VISIT:

https://www.crowdstrike.com/healthcare/

2 CONTACT US:

https://www.crowdstrike.com/public-sector/request-information/

3 RESOURCES:

Read the report:
Healthcare IoT Security Operations Maturity

Download the article:
Navigating Today's Healthcare Threat Landscape

Access the eBook:
Digital Health Innovation Requires Cybersecurity Transformation

ABOUT CROWDSTRIKE

ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: **https://www.crowdstrike.com/**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**