Protecting Healthcare from Ransomware Attacks

66%

percent of security teams and IT professionals reported being targeted by ransomware during the past year – much of it likely sold by e-crime groups on the dark web as Ransomware as a Service.

VMWARE CARBON BLACK 2021 CYBERSECURITY OUTLOOK SURVEY

Healthcare Security Challenges

- Protect IT infrastructure, telehealth apps (and others), EMR data from vulnerabilities and known and emerging threats – without adding significant complexity or costs
- Detect, respond to and remediate exposures and attacks quickly without adding complexity (e.g., more tools and agents)
- Contain costs while effectively preparing for ransomware and other attacks

The rise and cost of ransomware attacks against the healthcare industry

Ransomware attackers are notoriously opportunistic. According to the VMware Carbon Black 2021 Cybersecurity Outlook survey, 66 percent of security teams and IT professionals reported being targeted by ransomware in the past year – much of which likely sold by e-crime groups on the dark web as Ransomware as a Service. In 2020 alone, VMware Security found that there were more than 239 million attacks targeting healthcare customers with an astonishing 816 attempted attacks per endpoint[1].

With the rise of telehealth services and remote work at scale, ransomware attackers have new territory to target with lucrative and easy payouts. After all, electronic medical records (EMRs) are exponentially more valuable to sell on the dark web than credit card or social security numbers. Even before the move to remote work, healthcare firms have historically struggled with gaining the necessary technology, people, and process to defend against escalating cyberthreats. The rapid shift to delivering telehealth has added even more challenges:

- **Process breakdowns** – increase in sensitive patient data requests through unsecured methods like email
- **Supply chain challenges** – rapid, reactive procurement impedes the supplier vetting process and increases a reliance on third parties who may have their own supply chain issues
- **BYOD complexities** – unmanaged systems can increase the overall attack surface area

[1] VMware, "The State of Healthcare Cybersecurity: VMware Carbon Black Explores the Surge in Cyber Threats", February 2021. https://blogs.vmware.com/security/2021/02/the-state-of-healthcare-cybersecurity.html

VMware Security

- Embraces NIST and CISA frameworks for ransomware protection
- Participates in MS-ISAC and other information sharing organizations
- Serves over 30,000 customers worldwide

> "VMware solutions are the central nervous system of our IT infrastructure, enhancing our digital parameters and enabling us to deliver quality care. They have allowed us to run business-critical applications, and seamlessly transition from a siloed IT setup to a virtualized one."
>
> DR. SANDEEP GANNI
> CHAIRMAN, GSL GENERAL HOSPITAL AND MEDICAL COLLEGE
> (SOURCE: GSL GENERAL HOSPITAL & MEDICAL COLLEGE CASE STUDY)

> "Collateral damage in the cyber sense is very real. We're seeing critical infrastructure increasingly become a top target for cybercriminals who are using ransomware to ensure profitability and cause mass disruption. It's time for organizations to fight back."
>
> Rick McElroy, Principal Cybersecurity Strategist at VMware
> (Source: "Disrupting Ransomware and Dismantling the Cybercrime Ecosystem")

Lack of security visibility increases ransomware risks for the healthcare sector

With a distributed workforce, IT security teams in healthcare firms lack the visibility they need to spot unusual and unauthorized activity that could signal ransomware in the environment. The ability to quickly pinpoint the initial stages of a ransomware attack or isolate any compromised hosts is essential. After all, disrupting the attack **before** an attacker can establish a foothold and start the encryption process, is optimal. Despite cybersecurity concerns being top of mind for hospital administrators and board members, a healthcare firm's primary charter is providing quality care to patients rather than implementing and managing complex cybersecurity technologies. The challenge is finding the right partner, one who can work to deliver granular security visibility and control without complexity.

Proactive security with VMware Carbon Black

VMware Carbon Black Cloud protects healthcare organizations against ransomware scenarios even for systems accessing and processing sensitive patient data. It integrates across your existing controls as well as tools within the VMware technology portfolio. First, VMware Carbon Black Cloud detects and alerts on known malicious IP addresses to prepare IT teams that their hospitals or clinical systems may be being targeted by a ransomware attacker. Second, VMware Carbon Black Cloud can block all unapproved USB mass storage devices or only enable the USB drive on certain devices (e.g., in-house clinician PCs). Finally, VMware Carbon Black Cloud will identify malicious IP addresses, and if the attacker copies their tools and ransomware to the endpoint they are connected to, then VMware Carbon Black Cloud will stop destructive actions early in the kill chain.

Benefits for healthcare customers

- Extend your security staff with dedicated Strategic Success Manager and Technical Assessment Methodology (TAM)
- Access comprehensive threat intelligence, and global industry knowledge
- Experience a flat learning curve for rapid, distributed deployments
- Gain a deep understanding of workload, cloud, network, and endpoint security
- Reduce the time required to complete compliance audits
- Securely store 30 days of data retention and 180 days of alert retention
- Reduce mean time to recovery (MTTR) and administrative overhead
- Increase security efficiency, while eliminating alert fatigue
- Ease manageability with agentless workload security

VMware Carbon Black use cases

- Implement Zero Trust with fewer tools and silos
- Consolidate vendors and tool consolidation
- Gain shared security visibility and context across security, IT, and development teams
- Integrate easily using robust APIs and third-party integrations
- Scale incident response with confidence, speed, and accuracy with threat intelligence from VMware Threat Analysis Unit (TAU) and context-aware security features

Ransomware prevention, detection, and response—without the complexity

Whether large or small, resource-strapped IT teams at healthcare organizations require security controls that can reduce the attack surface, while also being able to quickly detect a ransomware attack in progress, remediate, investigate, and recover. Unfortunately, many solutions are overly complex, difficult to implement and manage over time, or worse – they lack critical functionality.

Instead, healthcare companies can use VMware Carbon Black's NextGen AV to identify behavior consistent with a ransomware attack and prevent it from executing. Additionally, our Endpoint Detection and Response (EDR) capabilities enable teams to accurately discern between a false positive and a credible threat. IT teams who need additional support can extend their security staff with our Managed Detection service for alert triage and console management. As a testament to our EDR market leadership, many leading Incident Response (IR) firms choose VMware Carbon Black for our deep forensic analysis capabilities and ransomware detection and remediation.

The power of the cloud

The VMware Carbon Black Cloud is a cloud-native endpoint protection platform (EPP) that combines the intelligent system hardening and behavioral prevention needed to keep emerging threats at bay, using a single lightweight agent and an easy-to-use console. Leveraging the power of the cloud, we analyze more than 500B events per day across millions of global endpoints, helping you stay ahead of emerging attacks.

Simplicity and deep granularity are not mutually exclusive

Alternative EDR, NGAV, and workload security platforms lack the data breadth and policy granularity offered by VMware Carbon Black Cloud. With our solution, healthcare organizations can consolidate ransomware protection while also benefit from rich data retention policies and fast and flexible deployment – without being overly complex to manage over time.

Industry Recognition

- Named a **'Visionary' in Gartner Magic Quadrant**TM **for Endpoint Protection Platforms (EPP)**, May 2021
- Named a **'Leader' in The Forrester Wave™: Endpoint Security Software As A Service**, Q2 2021

> "Integrations between access controls, device management, device security, network security, and application allow for granular, risk-based security policies in support of a Zero Trust strategy."

THE FORRESTER WAVE™: ENDPOINT SECURITY SOFTWARE AS A SERVICE, Q2 2021 REPORT

Learn More

Set up a meeting with our sales team for a personalized demo or more information, including how to take advantage of VMware Security Assessments and/or Proof of Value engagements.

Email contact@carbonblack.com or visit https://www.carbonblack.com/schedule-a-demo

Return on your cybersecurity investment

Endpoints are now one of the most targeted assets for healthcare organizations. At VMware, we understand this risk, and are committed to providing the best possible endpoint protection. We recently commissioned Forrester Consulting to evaluate the potential return on investment (ROI) companies receive when they deploy their next-generation antivirus (NGAV) and endpoint detection and response (EDR) on the VMware Carbon Black Cloud. According to the study's top three findings[2], we helped our customers:

1. Avoid costs of a data breach
2. Reduce time and costs - faster investigation and remediation and less frequent reimaging
3. Achieve cost savings from simplified operations

Consolidated Cybersecurity for Healthcare

VMware Security Solution	Benefits for Healthcare
VMware Carbon Black Cloud Endpoint	As part of VMware's security approach, VMware Carbon Black Cloud consolidates multiple endpoint security capabilities using one agent and console, helping you operate faster and more effectively. As a simpler, faster, smarter path to Zero Trust, VMware Carbon Black Cloud spans the system hardening and threat prevention workflow to accelerate responses and defend against a variety of threats.
VMware Carbon Black Cloud Workload	Tightly integrated with VMware vSphere, VMware Carbon Black Cloud Workload helps healthcare IT security and infrastructure teams increase visibility, harden workloads against attack, and focus on the most high-risk vulnerabilities and common exploits across their environments to significantly reduce the attack surface.
VMware Carbon Black Cloud Managed Detection	Offered as a managed service, VMware Carbon Black Cloud Managed Detection provides healthcare IT teams a much-needed view into attacks with recommendations for the actions needed to remediate the threat.

[2] Forrester Consulting, The Total Economic Impact™ (TEI) of VMware Carbon Black Cloud, study commissioned by VMware, May 2020. For more information, please see: https://blogs.vmware.com/security/2020/05/forrester-study-vmware-carbon-black-cloud-provides-379-roi.html

Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER and MAGIC QUADRANT are registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

Item No: Protecting Healthcare from Ransomware Attacks Solution Brief 8/22