Protecting Higher Education Systems from Ransomware

66%

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

Higher education security challenges

- Protect campus infrastructure, apps, portals and data from vulnerabilities and known and emerging threats – despite disruptive moves to remote teaching or hybrid learning environments
- 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 higher education

Ransomware attackers are notoriously opportunistic. In a June 2021 EDUCAUSE article, a West Coast university was the victim of a ransomware attack involving data within their school of medicine's research department. After the university realized hackers had encrypted valuable research data, the school chose to pay the hackers $1.14 million in cryptocurrency in hopes they would provide a decryption key. Fortunately, the school reported that it received a key to restore access to the files and copies of the stolen documents.[1] Tragically, data breaches of this scale have become an all-too-common occurrence.

The VMware Security has observed that with the rise of remote learning and the digital campus, ransomware criminals have targeted higher education as a prime attack surface with easy payouts. A lack of cybersecurity awareness and training, limited funding, and resources stretched thin to stay on top of cyberattacks create the ideal environment for criminals to gain access to substantial amounts of personal student data or medical research data. Plus, many legacy security tools that colleges and universities use are built for old requirements. This gap in functionality and scale has put student data privacy and security at risk. In today's environment, it is critical to protect against sophisticated attacks such as ransomware that use your existing software against you for villainous purposes.

> "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, "Disrupting Ransomware and Dismantling the Cybercrime Ecosystem"

1. Educause, The Increasing Threat of Ransomware in Higher Education, June 2021. For more information, please see: https://er.educause.edu/articles/2021/6/the-increasing-threat-of-ransomware-in-higher-education

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

Benefits for higher education customers

- Access comprehensive threat intelligence, and global industry knowledge
- Experience a flat learning curve for rapid campus-wide deployment
- 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
- Extend your security staff with dedicated Customer Success Manager (CSM) and Technical Account Manager (TAM)

Lack of security visibility increases ransomware risks for higher education

Until higher learning institutions gain a better understanding of their overall attack surface – endpoints, network access, servers, and virtual machines – they will not have the ability to quickly pinpoint the initial stages of a ransomware attack or isolate any compromised hosts in time. At the same time, most colleges and universities lack the funding and resources to fully invest in ransomware prevention or detection. And despite data breaches being a huge concern for most institutions, their primary focus is on teaching and learning initiatives, and some struggle with implementing and managing best of class cyber security technologies.

How can institutions of higher learning begin to protect themselves in such an unpredictable environment? EDUCAUSE identified three potential scenarios: restore, evolve, or transform. Each scenario was designed to help guide colleges and universities to start proactively thinking about how to prepare and fight against cyberattacks.

Proactive security with VMware Carbon Black

VMware Carbon Black Cloud protects higher learning institutions against ransomware scenarios even for systems disconnected from the campus network. 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 faculty, staff, and students for attacks underway. Second, VMware Carbon Black Cloud can block all unapproved USB mass storage devices or only enable the USB drive on certain devices (e.g., faculty and staff devices). 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.

Ransomware prevention, detection, and response - without the complexity

Whether large or small campuses, resource-strapped IT teams require security controls that can reduce the attack surface, while also being able to quickly detect a ransomware incident 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, higher learning institutions 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. Campus 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.

"AppDefense, like Carbon Black, allows us to improve our security footprint and stay ahead of the curve so that we don't end up in the news and we don't have a tragic story of being breached or losing customer data."

Jamie Andrews, Director of Network Operations at Columbia Southern University

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

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 over 1 trillion 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, educational institutions 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.

Return on your cybersecurity investment

Endpoints are now one of the most targeted assets for higher education institutions. 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

Industry recognition

- Named a **'Visionary' in Gartner Magic Quadrant™ 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 SLED Security Specialist team for a personalized demo or more information, including how to take advantage of VMware Security Assessments and/or Proof of Value engagements.

Email ploughlin@vmware.com or visit vmware.com

CONSOLIDATED CYBERSECURITY FOR HIGER EDUCATION	
VMware Security Solution	Benefits for Higher Education
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 college and university 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 college and university IT teams a much-needed view into attacks with recommendations for the actions needed to remediate the threat.

2. VMware Carbon Black, The State of Cybersecurity: Best Practices for Securing Critical Infrastructure for State and Local Government, January 2020. For more information, please see: https://www.carbonblack.com/wp-content/uploads/VMWCB-Whitepaper-Best-Practices-Securing-Critical-Infrastructure-State-Local-Governments.pdf

Item No: 80693 Higher Ed and SLG Ransomware Solution Brief 8/22