Protecting K-12 Schools from Ransomware Attacks

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

K-12 security challenges

- Protect district infrastructure, apps and data from vulnerabilities and known and emerging threats—despite disruptive moves to virtual classrooms
- 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 school districts

Ransomware attackers are notoriously opportunistic. According to the VMware Carbon Black 2021 Cybersecurity Outlook survey, 66% 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. And just in the past year, cyberattacks against U.S. schools have increased by 18% over 2019.[1]

The VMware Security has observed that with the rise of remote classes and the digital campus, ransomware attackers have new territory to target and easy payouts. After all, faculty, staff, and students are navigating new online systems, and attackers are poised to take advantage in every way. Lack of cybersecurity awareness and training, limited funding, and scarce resources (no dedicated individual for cybersecurity) make for a perfect cybersecurity storm. Plus, many legacy security tools that districts adopt 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. The K-12 Cybersecurity Resource Center, The State of K-12 Cybersecurity: 2020 Year in Review, 2021..

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 K-12 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 district-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

Lack of security visibility increases ransomware risks for school districts

Until school districts 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 school districts lack the funding and resources to fully invest in ransomware prevention or detection. Despite cybersecurity concerns being top of mind for superintendents, school board members, and parents, a school district's primary charter is teaching and learning initiatives rather than implementing and managing cyber security technologies.

Proactive security with VMware Carbon Black

VMware Carbon Black Cloud protects K-12 districts 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, resource-strapped IT teams at school districts 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, school districts 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. School district 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.

"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

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 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, K-12 districts can consolidate ransomware protection while also benefitting 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

"Time is money, and VMware Carbon Black saves us time, which saves us money."

William Stein,
Director of Information Systems
MSD of Mt Vernon

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

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/security.html

CONSOLIDATED CYBERSECURITY FOR K-12	
VMware Security Solution	Benefits for K-12
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 K-12 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 state and local government 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.

Item No: 80646 K-12 Ransomware Solution Brief 8/22