Protecting K-12 Schools from Ransomware 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.

The VMware Security Business Unit 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”

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 cybersecurity 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 Cloud’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.

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, 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 K-12 districts. 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

### CYBERSECURITY FOR K-12

<table>
<thead>
<tr>
<th>VMware Security Solution</th>
<th>Benefits for K-12</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Carbon Black Cloud Endpoint</td>
<td>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.</td>
</tr>
<tr>
<td>VMware Carbon Black Cloud Workload</td>
<td>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.</td>
</tr>
<tr>
<td>VMware Carbon Black Cloud Managed Detection</td>
<td>Offered as a managed service, VMware Carbon Black Cloud Managed Detection provides K-12 IT teams a much-needed view into attacks with recommendations for the actions needed to remediate the threat.</td>
</tr>
</tbody>
</table>


---

**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.

---

**VMware**, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Copyright © 2021 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of **VMware**, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: 80646 K-12 Ransomware Solution Brief 01 8/21

---

"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 Proof of Value engagements.

Email ploughlin@vmware.com or visit vmware.com/security.html

---

“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