Protecting Government Agencies 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

State and local government security challenges

- Protect agency infrastructure, apps and data from vulnerabilities and known and emerging threats – despite disruptive incidents
- 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 state and local government agencies

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 is likely sold by e-crime groups on the dark web as Ransomware as a Service. Government agencies are no exception. From 2018 to 2020, 246 ransomware attacks were unleashed on government organizations, impacting an estimated 173 million people, and costing roughly $52.88 billion in damages.

Unlike many enterprise and retail businesses, government entities did not heed the warning from the widely publicized Target attack of 2013 and shore up their infrastructure. This oversight was in large part due to limited budgets and scarce resources (no dedicated individual for cybersecurity). Nevertheless, these deficiencies opened the door for the perfect cybersecurity storm. Now, government agencies are adding Internet-connected services and technology at a rapid rate, often without securing that new technology. This provides new attack surfaces for cyber criminals and nefarious nation-state actors. The risk of an increased attack surface is compounded by the reality that organized crime groups have adopted cybercrime as an emerging business model with help from the dark web.[1]

> "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. 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

VMware security business unit

- 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 state and local government customers

- Access comprehensive threat intelligence, and global industry knowledge
- Experience a flat learning curve for rapid 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 agency 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 government agencies

Until state and local government agencies gain a better understanding of their overall attack surface – endpoints, network access, and servers – 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 agencies lack the funding and resources to fully invest in ransomware prevention or detection. While these types of attacks are not new, what is "new" is the increased frequency as attackers are taking advantage of smaller, more vulnerable entities. We continue to see new attacks on state, city, county, and local governments, which sheds light on the need for more comprehensive cybersecurity protection and awareness. To shed light on areas government agencies need to be aware of to develop a stronger security posture, the National Association of State Chief Information Officers (NASCIO) offers its State CIO Top 10 Priorities 2021 lists with practical advice to get agencies thinking about next steps. .

Proactive security with VMware Carbon Black

VMware Carbon Black Cloud protects government agencies against ransomware scenarios even for systems disconnected from the main 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 state and local employees 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., government personnel 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 city, county or state government entities, 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, state and local government agencies 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. Government agency 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.

"One of the biggest benefits of adopting VMware is how all of the solutions integrate together so seamlessly. With just a click of a button, solutions start working together to give us the compliance and performance we need."

Daniel Caban
Director of Information Technology,
Osceola County Sheriff's Office

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, government entities 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

"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

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

CONSOLIDATED CYBERSECURITY FOR STATE AND LOCAL GOVERNMENT AGENCIES	
VMware Security Solution	Benefits for Government Agencies
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 state and local government 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. 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: 80694 State and Local Ransomware Solution Brief 10/21