# Protecting Financial Services from Ransomware Attacks

## The rise and cost of ransomware attacks against financial services firms

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

### Financial institutions security challenges

- Protect IT infrastructure, apps and data from vulnerabilities and known and emerging threats
- 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

### 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

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 a similar VMware report, 89 percent of CISOs in the financial services sector indicated that they experienced an increase in the number of cyberattacks, and 67 percent said they fear a material breach.[1]

The VMware Security Business Unit has found that several factors have contributed to making it easier for ransomware attackers to target financial services firms for easy payouts. First, human error remains one of the top three major root causes of cyberattacks and the cybersecurity skills shortage adds to this risk. Additionally, many financial services firms may not have a rigorous business continuity plan in place, with regular backups and system recovery testing procedures. Without these processes, financial institutions remain vulnerable to ransomware attacks. Finally, supply chain risks as well as a reliance on legacy tools all contribute to escalating the risks of ransomware for financial services firms.

> "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")

1. VMware Carbon Black, VMware Carbon Black Global Security Insights Report, 2021.

"Introducing VMware Carbon Black has made life so much easier for our Technical Information Security Officer (TISO). Instead of spending a week working through all the latest security regulations, he now has time to devote to implementing innovative projects."

ROBERT SEIDEMANN
VICE PRESIDENT OS&IT - ENGINEERING & OPERATING SERVICES, DVB BANK SE

### Benefits for financial services 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 enterprise-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 financial services firms

Without a comprehensive understanding of their overall attack surface – endpoints, network access, servers, and virtual machines – IT teams will not have the ability to quickly pinpoint the initial stages of a ransomware attack or isolate any compromised hosts in time. Identifying the initial stages of a ransomware attack is critical to stop the attacker from gaining a foothold, moving laterally across the network, and encrypting important data. At the same time, most financial services firms are reluctant to invest in yet another security technology for ransomware prevention or detection. All this security visibility cannot come at the expense of increased complexity or administrative overhead.

## Proactive and pragmatic security with VMware Carbon Black

VMware Carbon Black Cloud protects financial services firms against ransomware scenarios no matter how large or geographically distributed the organization. Our platform 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 security teams 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., CEO's laptop). 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.

### 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 and Security teams at financial institutions 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, banks and financial services firms 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 SOC teams to accurately discern between a false positive and a credible threat. Organizations 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, financial 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.

## 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 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 www.carbonblack.com

## Return on your cybersecurity investment

Endpoints are now one of the most targeted assets for financial services firms. 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 through faster investigation** and remediation and less frequent reimaging
3. **Achieve cost savings** from simplified operations

| CONSOLIDATED CYBERSECURITY FOR FINANCIAL SERVICES | |
|---|---|
| VMWARE SECURITY SOLUTION | BENEFITS FOR FINANCIAL SERVICES |
| 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 financial industry 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 financial industry IT teams a much-needed view into attacks with recommendations for the actions needed to remediate the threat. |

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


Item No: 80740 Protecting Financial Services from Ransomware Attacks - Solution Brief R1 11/21