

Industry

Financial Data Services

Environment

Approximately 40,000 endpoints and servers

Security Challenges

- Servers breached by attack undetected by antivirus software
- Remediate infected servers with lowest impact on business
- Protect all servers and endpoints from future advanced threats and malware

Solution

Carbon Black Enterprise Protection

Key Benefits

- Hundreds of infected servers locked down in less than a day by Carbon Black services team
- Fast detection, remediation and ongoing protection of infected servers by Carbon Black
- Real-time monitoring and recording of all activity on endpoints and servers

Top-10 Financial Technology Provider Stops Large-scale Server Attack with Carbon Black Enterprise Protection

Traditional solutions fail to stop advanced threat; Carbon Black remediates the problem quickly and effectively

Summary

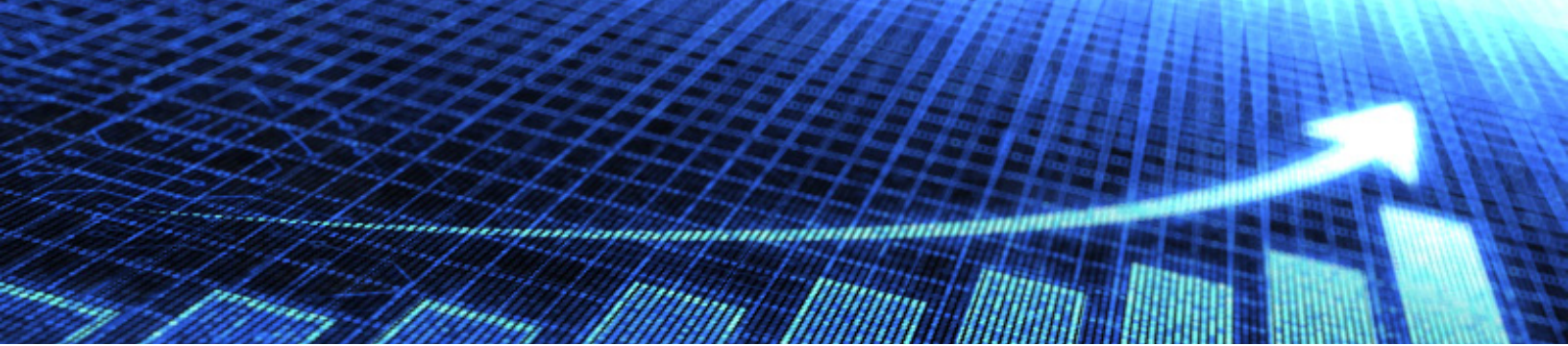
This top-10 financial data services company provides a variety of technology products and services to banks and other institutions. The firm's large data center, which supports thousands of customers around the world, suffered a massive breach. Network and security teams raced to stop the attack from spreading, but when other vendors' solutions proved incapable of remediating servers that had already been infected, the company turned to Carbon Black. Carbon Black Enterprise Protection was able to lock down the environment, identify and remediate infected machines, and prevent further damage. Carbon Black addressed the problem holistically, leading to faster resolution and ongoing visibility, detection, protection and forensics capabilities.

The Challenge

With offices worldwide, this Fortune 500 company delivers a comprehensive range of solutions for the financial services sector, including credit card processing, software, hardware, consulting and information technology outsourcing.

A constant barrage of malware and other cyber threats was hammering the company's IT infrastructure, an increasingly common occurrence for businesses that operate in financial services because of the sensitive and highly valuable financial data for which they are responsible. When the company suffered a major data center breach, the problem swiftly turned critical.

Almost a thousand servers were under attack; security and network teams were at a loss about how to stop it. The servers all were running McAfee anti-virus, but that was not enough to detect or prevent the spread of powerful malware. With thousands more servers and critical company and customer data at risk, the IT and security team needed a new approach to the crisis.



Carbon Black Commitment to Customer Privacy

At Carbon Black, we protect the identities of our customers as effectively as we protect them from advanced threats.

That's why this case study is presented without naming our customer. If your business becomes a Carbon Black customer, we'll protect your identity—and your endpoints and servers—just as effectively.

The Solution

The company deployed Carbon Black Enterprise Protection across the affected machines. Within minutes, they had visibility into the nature of the breach and how to stop it from spreading and remediate the damage.

The Carbon Black solution enabled the team to download, deploy and lock down the environment in less than a day. Other solutions would have taken half a day just to load agents on servers, according to the company's IT director.

Once the servers were in lockdown, security teams were able to identify the malware and how it had executed and morphed on every affected machine. Then, using the Carbon Black Software Reputation Service, the company was able to perform "background checks" on all its software and allow only trusted applications to run on its servers from that point forward.

Other products the company used to fight this attack forced the team to fly blind, not knowing if they truly had placed any of the infected machines in lockdown mode. These solutions also required multiple reboots during installation and changes—an unacceptable burden on production servers during business hours. The company took advantage of Carbon Black's support for image comparison, which helped uncover hidden malware and known bans on unauthorized software. Such insight helped ensure clean images were in place in the shortest time possible.

The Result

Carbon Black Enterprise Protection saved this Fortune 500 company from what was quickly turning into a catastrophe and enabled them to mitigate the situation as quickly as possible. The malware did not spread to other servers in the environment and the company's security team was able to prevent subsequent attacks. All this was done with the least possible disruption to business.

After seeing how effectively the Carbon Black solution performed, the company quickly became a customer and deployed Carbon Black on 2,500 of its Windows servers, integrating with McAfee antivirus, software distribution tools such as SCCM and Windows Active Directory.

The company's IT and security leaders were so pleased with the responsiveness and knowledge of Carbon Black's support team and the unmatched performance of the solution that they now have deployed Carbon Black across the environment, providing visibility, detection, protection and forensics for approximately 40,000 servers and endpoints.

About Carbon Black

Carbon Black leads a new era of endpoint security by enabling organizations to disrupt advanced attacks, deploy the best prevention strategies for their business, and leverage the expertise of 10,000 professionals to shift the balance of power back to security teams. Only Carbon Black continuously records and centrally retains all endpoint activity, making it easy to track an attacker's every action, instantly scope every incident, unravel entire attacks and determine root causes. Carbon Black also offers a range of prevention options so organizations can match their endpoint defense to their business needs. Carbon Black has been named #1 in endpoint protection, incident response, and market share. Forward-thinking companies choose Carbon Black to arm their endpoints, enabling security teams to: Disrupt. Defend. Unite.

**CARBON
BLACK**
ARM YOUR ENDPOINTS

1100 Winter Street
Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499
www.carbonblack.com