Grupo Financiero Multiva Safeguards Clients' Financial Assets from Malicious Attacks

Check Point SandBlast Provides Comprehensive Prevention Against Ransomware and The Most Evasive Advanced Threats

"We've had a really good experience with Check Point Next Generation appliances and SandBlast technology. We are now confident we are well protected against both known and unknown attacks."

— Juan Muñoz, Assistant Director of Infrastructure, Grupo Financiero Multiva

Customer Profile

Grupo Financiero Multiva is a Mexican provider of financial products and services.

Challenge

- Protect network against unknown malware and Zero-Day attacks
- Detect and prevent Denial-of-Service attacks
- Consolidate and simplify security solution

Solution

- Check Point SandBlast Zero-Day Protection with Threat Extraction and Threat Emulation
- DDoS Protector Appliance

Benefits

- Blocked DDOS attacks, advanced threats and ransomware
- Reduced time and resources expended on remediation
- Enabled business operation with no disruption

Overview

Grupo Financiero Multiva

Based in Mexico, Grupo Financiero Multiva is a financial group comprised of Banco Multiva, Casa de Bolsa, and Fondos de Inversión. It provides various personal and commercial financial products and services throughout 25 branches in Mexico.

Business Challenge

Securing Customers' Assets

As a financial institution, Multiva experienced growing security concerns regarding the protection of its customers' assets, such as customer transactions, account information and personal identification information.

Although the bank could deal with known malware via traditional tools, it remained defenseless against Zero-Day attacks because legacy solutions simply aren't sufficient any longer for detection and prevention. In addition, Multiva noticed a rise in the frequency of Distributed Denial-of-Service (DDoS) attacks. Facing targeted threats such as these as well as ransomware, APT, and email-borne attacks, Multiva knew it needed a central and manageable security solution with comprehensive protections.

"We realized we needed to enhance our security posture when we had a ransomware attack," said Juan Muñoz, Assistant Director of Infrastructure at Grupo Financiero Multiva. "While the attack did minimal damage, we needed to get the strongest protection out there to avoid being a victim again."

> "The Anti-DDoS solution is doing great on preventing DDoS attacks. We feel safe because we get alerts and reports in a timely manner. We actually know when we're being attacked, thanks to the box."
>
> — Juan Muñoz, Assistant Director of Infrastructure, Grupo Financiero Multiva

Solutions

Next Generation Threat Extraction

To find the best solution, Multiva tested Micro Solutions, FireEye, and Check Point SandBlast. Although Micro Solutions and FireEye could detect threats, they were not able to stop them as effectively as SandBlast. Neither were they able to deal with the complex task of remediating encrypted files in cases of ransomware which were a tremendous threat to the bank. FireEye's solution was too complex and expensive.

"We decided to look for a sandbox solution. We looked at Micro Solutions, FireEye and Check Point," said Muñoz. "Micro Solutions was out because it could only detect and not prevent. While FireEye could provide the same level of security, it required a separate appliance for each security protocol, making sandbox protection cost prohibitive and difficult to manage."

Multiva needed a large enterprise solution, and chose Check Point Next Generation appliances for threat prevention with greater performance, uptime, and scalability. NGTX stood out with comprehensive protections including Firewall IPS, Application Control, Anti-Bot, Anti-Virus, Anti-Spam & Email Security, URL Filtering, and the award-winning sandboxing technology in Check Point SandBlast. SandBlast did all that without interfering with the daily business flow of the organization.

With the appliance, Multiva received SandBlast Zero-Day Protection with Threat Extraction and Threat Emulation, ensuring the most advanced protections against unknown malware, vulnerabilities, and Zero-Day attacks. Integrating SandBlast with their email solution allows Multiva to stop email-borne ransomware and APT attacks.

For Multiva, the performance of the equipment and the integration with its Security Information and Event Management services truly stood out.

"We've had a really good experience with Check Point Next Generation Appliances and SandBlast technology," said Muñoz." We are now confident we are well protected against both known and unknown attacks."

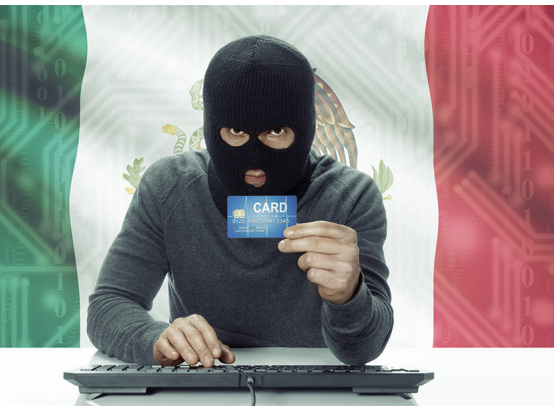
Fortifying The Perimeter

Since Multiva had experienced a rise in Denial-of-Service attacks, it sought to fortify its perimeter defense with the Check Point DDoS Protector Appliance, an add-on to Multiva's security architecture. The appliance responds to DDoS attacks quickly using multi-layer protection against volumetric, specific server, and application attacks.

Nowadays, DDoS attacks use new techniques that can circumvent traditional security solutions and cause serious network downtime and negatively impact businesses. The DDoS Protector is built to extend security perimeters to block DDoS attacks before any damage is done, and integrates seamlessly with Check Point Security Management.

When Multiva was recently targeted by a DDoS attack, the DDoS Protector was able to alert the Information Security team and prevent the threat.

"The Anti-DDoS solution is doing great on preventing DDoS attacks. We feel safe because we get alerts and reports in a timely manner," said Muñoz." We actually know when we're being attacked, thanks to the box."



> "Our team can do more now that they're not focused on mitigating. Thanks to Check Point's advanced threat prevention, the company can feel safe while expending fewer resources on remediation."
>
> — Juan Muñoz, Assistant Director of Infrastructure, Grupo Financiero Multiva

Benefits

Preventing Advanced Threats

Having SandBlast Threat Emulation and Threat Extraction has enhanced Multiva's security posture in the face of both known malware and Zero-Day attacks. The Threat Emulation capability, a sophisticated sandboxing technology, prevents infections from undiscovered Zero-Day threats and targeted attacks. Threat Extraction allows users to quickly get a clean, safe document while the file is in emulation, promoting efficiency without compromising security standards.

"Check Point Next Generation appliances have proven to be excellent at preventing attacks against our assets," said Muñoz.

Consolidated Enterprise Solution

One of the main appeals of the Check Point Next Generation solution to Multiva was the comprehensive yet simpler appliances. The NGTX package available to Multiva through Check Point 15000 Appliances offers a complete and consolidated security solution that is centralized and requires fewer appliances than competitors' solutions. The appliance-based Check Point solution is a more manageable security solution.

Improving Visibility with Actionable Forensics

The Check Point Next Generation appliances have meant significant cost-savings for Multiva. Single-pane-of-glass management and superb visibility into threats simplify the Information Security team's workload with threat alerts and granular reports.

Multiva's Check Point solution has positively impacted the bank's day-to-day operational efficiency.

"Our team can do more now that they're not focused on mitigating," says Muñoz. "Thanks to Check Point's advanced threat prevention, the company can feel safe while expending fewer resources on remediation."

For more information, visit: www.checkpoint.com/products/sandblast-network-security/