CUSTOMER CASESTUDY

PROMINENT MUSEUM IN D.C. SAFEGUARDS ITS MISSION WITH CHECK POINT

Check Point's Consolidated Architecture Protects Irreplaceable Artifacts by Securing a Multi-Vendor Hybrid Cloud Environment

Customer Profile

Prominent Museum in D.C. documents, studies, and interprets history.

Challenge

- Preserve and protect irreplaceable documentation, photographs, videos, and recordings
- Protect user identities and credentials against account hijackings
- Secure SaaS and hosted applications across a multi-vendor hybrid cloud environment

Solution

- Check PointHarmony Email & Office
- Check Point CloudGuard Network Security
- Check Point Quantum Network
- Check Point R80 Security Management

Benefits

- Prevented multiple SaaS account breach attempts
- Reduced security team overhead by 50% through automation and management consolidation
- Ensured consistent policy and security across multiple vendors, cloud, and on-premises environments

> "Check Point CloudGuard™ Network Security automates protection across our dynamic cloud environments while Check Point R80 unifies visibility into threats across the network, enabling us to efficiently address security incidents with less effort."
>
> - Michael Trofi,
> Founder of Trofi Security & Acting CISO, Prominent Museum in D.C.

Overview

Prominent Museum in D.C.

This prominent museum in D.C. documents history and preserves artifacts. Since its dedication, the Museum has welcomed more than 40 million visitors, including 99 heads of state and more than ten million school-age children. To protect its irreplaceable documents, photos, videos, and recordings from today's fifth generation cyber-threats, the museum turned to Check Point.

Business Challenge

Preserving and Protecting

This museum keeps one of the world's largest archives of significant historical events, focused on their digital preservation and storage. More than 16.5 million people from over 200 countries visit the site annually, which is available in 16 languages.

The museum's systems are barraged by hate emails, vicious social media posts, and increasingly sophisticated 5th generation cyber-attacks from around the world.

September, 2018

"We needed a way to detect account hijacking attempts and prevent unauthorized access to petabytes of priceless data. In addition to our Check Point Firewalls, Check Point CloudGuard™ SaaS was the right solution."

-Michael Trofi,
Founder of Trofi Security
and Acting CISO,
Prominent Museum in D.C

"We're moving our applications to the cloud to eliminate our data center and maximize our resources," said Michael Trofi, founder of Trofi Security and Acting CISO. "With the risks we face, we needed strong, effective protection for users and applications across our existing on-premises and multi-vendor hybrid cloud infrastructure."

Solution

Securing All Applications Equally

Securing SaaS and hosted applications across a hybrid cloud environment is not as easy. One of the security team's first challenges was to manage and protect user identities across the entire infrastructure.

Employees and partners are located around the world with varying levels of online access to our institutional assets. The museum chose software-as-a-service (SaaS) applications, including Microsoft Office 365, Google Suite, file-sharing, and operations solutions to meet users' needs. Each is hosted in its respective vendor's cloud and protected by Check Point Harmony Email & Office. Check Point Harmony Email & Office delivers zero-day threat, identity, and data protection while preventing employee account breaches.

"Employees' Google email accounts and credentials were especially vulnerable to spoofing through the Chrome browser," said Trofi.
"We needed a way to detect account hijacking attempts and prevent unauthorized access to petabytes of priceless data. In addition to our Check Point Firewalls, Check Point CloudGuard™ SaaS was the right solution."

The museum also utilizes Check Point CloudGuard Network Security to protect its
applications that have been moved to public clouds. Financials, human resources, PCI-compliant payment systems, and data archives are being deployed on AWS, Google, Oracle, and Azure public clouds. By hosting various applications within their specific vendor's cloud, the museum is assured that application performance, upgrades, and maintenance are optimized by the cloud providers themselves, with a reduced effort by museum staff. Check Point CloudGuard Network Security extends the same protection as the Check Point firewalls to the museum's applications in these public cloud environments.

Harmony Email & Office and IaaS both benefit from Check Point Quantum™ Zero Day protection software which runs across all Check Point physical and virtual appliances at the heart of the Museum's security infrastructure. It provides multi-layered protection from known threats and zero-day attacks using Threat Emulation technology, as well as identity awareness, content awareness, antivirus, anti-bot, intrusion prevention, application control, and URL filtering capabilities. With Check Point Quantum, advanced protections are extended across all environments, regardless of the physical network construct or cloud environment used.

"We now have actual metrics about the volumes of phishing and malware targeting us, as opposed to what we thought was occurring."

- Michael Trofi,
  Founder of Trofi Security
  and Acting CISO,
  Prominent Museum in D.C

Benefits

Cloud Diversity, Security Management Uniformity

Michael Trofi's team now manages all security policies, threat prevention, and operations in a single pane of glass through Check Point's R80 Security Management. The team is also able to leverage automation of routine tasks to increase efficiency. Check Point R80 eliminates the need for monitoring multiple systems and ensures consistent policy across cloud and premises environments.

"Check Point CloudGuard Network Security automates protection across multiple dynamic clouds," said Trofi, "while Check Point R80 unifies visibility into threats across the network, enabling us to efficiently address security incidents with less effort."

Unified Security Architecture

Since deploying Check Point Harmony Email & Office, the museum has defeated multiple Gmail hijacking attempts. In one case, Harmony Email & Office detected an attempt by someone in New York to access a Gmail account in Argentina. Check Point R80 enables the team to view and correlate events across multiple clouds and physical firewalls with real-time visibility into the barrage of threats targeting the Museum.

"We now have actual metrics about the volumes of phishing and malware targeting us, as opposed to what we thought was occurring," said Trofi. "Visibility also uncovered configuration issues in partners' email systems that prevented donation requests from getting through. Check Point enabled us to address another issue that we weren't aware of previously."

Looking Forward

"We're defending our assets against advanced large scale, multi-vector mega attacks," said Trofi. "Check Point will be a next step, enabling us to proactively deploy new protections as the threat landscape changes."

Check Point is an all-inclusive subscription offering. With it, the Museum can instantly access new Check Point solutions as new threats emerge, instead of having to initiate procurement of individual components.

"Check Point operates invisibly to our users, partners, and outsiders," said Trofi. "That's the way it should be. Transparency goes a long way in augmenting our mission."

For more information, visit: https://www.checkpoint.com/products/ cloud-security/

September, 2018