CUSTOMER CASESTUDY

TROFI SECURITY DEFENDS CLIENTS' PRICELESS ASSETS WITH CHECK POINT INFINITY AND CLOUDGUARD

Customer Profile

Trofi Security provides comprehensive security services to leading organizations such as the U.S. Holocaust Memorial Museum.

Challenge

- Improve monitoring effectiveness in AWS environment
- Uncover previously unseen threats and accelerate response
- Increase security management efficiency

Solution

- Check Point Infinity Total Protection
- Check Point CloudGuard Network Security
- Check Point CloudGuard Cloud Security Posture Management (CSPM)
- Check Point Infinity Network Detection and Response (NDR)
- Check Point CloudGuard AppSec
- Check Point Infinity SOC
- Check Point R81.10 Security Management

Benefits

- Identify previously unseen threat vectors and quickly remediate vulnerabilities
- Automatically expose, investigate, and shut down real attacks quickly with 99.9% precision
- Saved hours, reduced errors and accelerated response with automated triage

> "Check Point makes life as a security professional much better. Integration and automation not only make security easier, they're a better long-term approach to managing security."
>
> - Michael Trofi, Founder and CEO, Trofi Security and acting CISO, United States Holocaust Memorial Museum

Overview

Founded in 1999, Trofi Security provides information security architecture, management, and testing services to world-leading public- and private-sector organizations. The firm delivers a comprehensive range of security planning, governance, control testing, risk assessment, and other services.

Business Challenge

Fortifying the Security Posture

With a long history as a trusted partner to its clients, Trofi Security stays on the leading edge of security protection. This is especially important for clients who maintain irreplaceable assets, such as the United States Holocaust Memorial Museum. Its website and internal assets represent the world's leading online authority on the Holocaust—available in 16 languages and visited by millions of people from around the world. Funded by the U.S. government and private donors, the Museum must protect physical, data, and donor information assets.

The Holocaust Memorial Museum faces daily cyber attacks from rogue and state-sponsored actors. Attack levels are comparable to those experienced by high-level United States government agencies. Monitoring, identifying, and responding to threats in this environment demand advanced security intelligence and capabilities.

"Digital threats have become more adaptive, pervasive and destructive," said Michael Trofi, Founder and CEO of Trofi Security and acting CISO for the United States Holocaust Memorial Museum. "We wanted to increase the Museum's protection in the cloud. At the same time we needed to accelerate our ability to assess threats and uncover those that might otherwise go undetected."

SOLUTION

A Powerful Security Architecture

Protection starts with the Check Point Infinity Architecture, which delivers real-time threat prevention, shared intelligence, and the most advanced security across networks, cloud, endpoint, and mobile environments. Within the Infinity architecture, Check Point ThreatCloud delivers intelligence sourced from millions of sensors worldwide, enriched with AI engines and exclusive research data.

To improve monitoring in the Museum's AWS cloud environment, Trofi chose Check Point Infinity Network Detection and Response (NDR). Infinity NDR deploys in minutes and integrates with AWS services and Check Point CloudGuard security gateways that are protecting the Museum's AWS deployment. It passively mirrors cloud traffic and uses ThreatCloud intelligence with behavioral AI to correlate events. Powerful threat discovery, visibility, and investigation capabilities prioritize events and present them visually so the team knows immediately where to focus their investigations each day. The Museum gains real-time traffic visibility and anomaly detection without affecting business traffic throughput.

Also part of the architecture, Check Point Infinity SOC enables the team to find malicious activity inside their network—exposing, investigating, and shutting down real attacks quickly with 99.9% precision. With Infinity SOC, the team immediately knows what to investigate. Visibility into internal endpoint browsing enables them to identify known command-and-control websites and malware distribution points. Automated triage accelerates response, saving hours of time. Infinity SOC is implemented in minutes with no impact to users and no need for additional endpoint agents.

"Check Point Infinity gives us access to Check Point's security portfolio under one umbrella," said Trofi. "As a subscription offering, it allows us to easily add new features and remain highly cost effective over time."

Industry-Leading Cloud Protection

The Museum also relies on Check Point CloudGuard Network Security, CloudGuard CSPM, and CloudGuard AppSec for the most advanced protection. CloudGuard Network Security integrates seamlessly with the Museum's AWS environment to deliver an industry-leading 100% block rate, 100% malware prevention, 100% exploit resistance, and 0% false positives. CloudGuard Posture Management enables continuous

> "Check Point CloudGuard paid for itself the first week by identifying threat vectors that we previously could not see, enabling us to quickly eliminate any vulnerabilities."
>
> - Michael Trofi, Founder and CEO,
> Trofi Security and acting CISO,
> United States Holocaust Memorial

compliance and automates governance, giving Trofi's team granular visibility into all cloud assets, networks, and security groups. Web-facing applications are secured by CloudGuard AppSec. A contextual AI engine learns how Museum applications are used and then profiles users and content to identify malicious requests.

"CloudGuard Network Security gives us advanced threat prevention, perimeter security and network segmentation. We rely on CloudGuard CSPM to protect our Amazon S3 buckets," said Trofi, "and CloudGuard AppSec secures our web interface continuously, even as our web application evolves. Its learning capability is extremely fast and is perfect for threat prevention in our environment where foreign threat actors typically go 'low and slow' to find vulnerabilities."

"We see everything instantly," said Trofi. "Check Point CloudGuard paid for itself the first week by identifying threat vectors that we previously could not see, enabling us to quickly eliminate any vulnerabilities."

Compared to other vendor implementations in the same environment, the Check Point solution requires far less hands-on interaction and fewer human resources. A consistent interface across Check Point products greatly simplifies the team's cross training and improves efficiency.

"Check Point's graphical interface is consistent across Check Point Infinity solutions" said Trofi. "For that alone, I would recommend Check Point over Palo Alto."

Benefits

Fast Identification and Resolution

Infinity NDR enables Trofi's team to quickly identify state-sponsored and rogue actors' activities targeting the Museum's cloud environment. They have proactively shut down scanning by foreign nations, attempts at website defacement, and command-and-control software injection.

"With Infinity SOC, we also monitor protocols and traffic volumes coming from specific websites," said Trofi. "We know who's communicating and the destination sites. That's a huge upside for our traffic analysis."

Efficient Teamwork

A unified security architecture and management addresses one of the biggest challenges facing any security organization—keeping pace with threats. People alone can't react fast enough.

"Security efficiency has become more important than ever," said Trofi. "Check Point makes life as a security professional much better. Integration and automation not only make security easier, they're a better long-term approach to managing security."

> "Check Point's graphical interface is consistent across Check Point Infinity solutions. For that alone, I would recommend Check Point over Palo Alto."
>
> - Michael Trofi, Founder and CEO, Trofi Security and acting CISO, United States Holocaust Memorial Museum