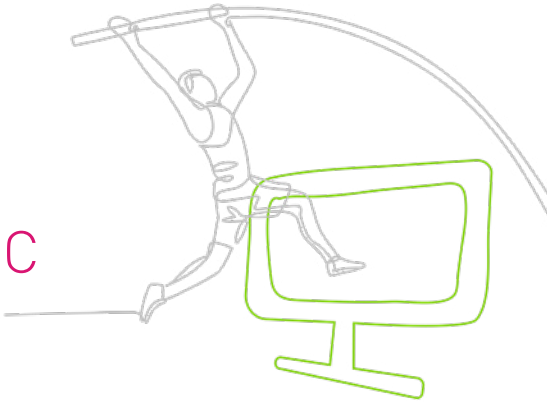
SE2 RELIES ON CLOUDGUARD TO AUTOMATE SECURITY FOR A DYNAMIC CLOUD ENVIRONMENT



Customer Profile

SE2 is a third-party administrator of life insurance contracts and annuities.

Challenge

- Secure a complex, multi-account AWS environment
- Gain visibility and enforce governance without inhibiting business-critical development
- Secure and manage on-premises and cloud environments with the same team

Solution

- Check Point CloudGuard Cloud Security Posture Management (CSPM)
- Check Point Infinity Network Detection and Response (NDR)
- Check Point R80 Security Management

Benefits

- Automated access and remediation to remove development roadblocks
- Simplified compliance and alignment with NIST standards
- Ensured cloud security while enabling innovation
- Improved visibility into anomalous traffic and hidden threats

"We want security to be an enabler—not a blocker. Check Point CloudGuard Security Posture Management allows us to define and enforce policies without compromising flexibility."

- Saul Schwartz, Technology Manager, SE2

Overview

SE2 is an insurance technology and services firm. Headquartered in Topeka, KS, the company enables insurers to quickly build and launch new products that support digital transformation. SE2 currently administers nearly 2 million active life insurance and annuity policies on behalf of its clients. It also has $100 billion in assets under administration with more than 200,000 new business applications annually.

Business Challenge

Securing Continuously Changing Targets

Delivering a best-in-class customer experience has become a priority for life and annuity insurance companies. As a result, many seek help with digital transformation initiatives. SE2 recognized this opportunity early—building a DevOps organization and business practice focused on rapid solution development and deployment for insurance clients.

Moving to the cloud gave the company agility and resilience. SE2 relies on a multi-account structure in AWS. Within those accounts, there are 500 EC2 instances with several hundred security groups and multiple users who are authorized to make configuration changes. The security team now had to secure more, faster, in a constantly changing cloud environment while ensuring the company's security posture stayed strong.

"Protecting our development intellectual property and client data is business-critical," said Saul Schwartz, Technology Manager for SE2. "We needed leading-edge protection for workloads and data in the public cloud—but in a flexible, manageable way."

"Protecting our development intellectual property and client data is business-critical. We needed leading-edge protection for workloads and data in the public cloud-but in a flexible, manageable way."

- Saul Schwartz,
  Technology Manager, SE2

SOLUTION

Set It and Forget It

SE2 chose Check Point CloudGuard Cloud Security Posture Management (CSPM) to simplify governance. CloudGuard CSPM automates governance across multi-cloud assets and services. It enables the SE2 team to easily visualize and assess security posture while providing misconfiguration detection and enforcing security best practices and compliance frameworks.

"Automated remediation really makes our lives easier," said Schwartz. "We assign alerts and automatic remediation to the items of our choice, and Check Point takes care of everything. When I set security policy, it applies to existing AWS accounts and new AWS accounts or workloads that spin up."

Visibility from Cloud to Ground

The SE2 team also uses Check Point Infinity Network Detection and Response (NDR) capabilities to augment cloud security with continual visibility and alerting. Infinity NDR provides non-signature-based threat detection, visibility, and investigation capabilities for cloud deployments without affecting business traffic. It alerts the team to hidden threats, network reconnaissance, lateral movement attempts, data exfiltration, and other tactics used by malicious actors.

"I recommend Check Point Infinity NDR for organizations that are considering or moving to public cloud environments," said Schwartz. "It allows us to gain visibility and alerting functionality. We now have actionable visibility into overall security across both on-premises and AWS environments."

Benefits

Minimizing Risk Without Compromise

CloudGuard CSPM helps the SE2 team avoid unnecessary risk. For example, developers might need to change a security group temporarily as they test a new functionality or product. If a user spontaneously changes a security group, CloudGuard CloudBots remediation reverts it to the original state until the security team can review the request and evaluate risk.

"The CloudGuard CloudBots feature helps us keep our large number of

"Automated remediation really makes our lives easier. We assign alerts and automatic remediation to the items of our choice, and Check Point takes care of everything. When I set security policy, it applies to existing AWS accounts and new AWS accounts or workloads that spin up."

- Saul Schwartz,
Technology Manager, SE2

security groups secure and congruent," said Schwartz. "We keep those groups in full protection mode, and developers can request access to a security port for a period of time for testing workloads without putting the company at risk."

Security as an Enabler

Schwartz says that CloudGuard CSPM gives SE2 extra "guardrails." Application development is a competitive differentiator for the company, so it's crucial to ensure a strong security posture without limiting DevOps teams from doing their best work.

"We want security to be an enabler—not a blocker," said Schwartz. "CloudGuard CSPM allows us to define and enforce policies without compromising flexibility."

For example, developers need access to certain configuration items as they develop, run, and test solutions. The security team can define policies that allow access and enable automatic remediation so developers don't have to rely on the security team for point-in-time reviews or access. In addition, the CloudGuard CSPM logic feature enables the security team to dig into logs and quickly identify source destination protocols. If a developer is running into a security problem with a workload, the security team has immediate access to security context and details for resolution.

"With the ability to aggregate multiple accounts and cloud providers, CloudGuard CSPM future-proofs our cloud security," said Schwartz. "If different workloads run better on a different cloud provider, we can easily say 'yes' and still keep all of our security functionality in the same pane of glass."

Compliance...Simplified

Compliance modules within CloudGuard CSPM give the SE2 team options for choosing the best practices that are relevant to their business. For example, SE2 aligns with the U.S. National Institute of Standards and Technology (NIST) framework to craft a robust security posture. The CloudGuard CSPM NIST compliance check identifies anything that is not aligned with the standard and automatically remediates it or alerts the team. Alerts with context and automatic notification simplify troubleshooting and help eliminate any shadow IT activities that might occur. When a new workload is created, the team is automatically notified.

"With CloudGuard CSPM, I can use the same team to manage and secure on-premises and cloud workloads," said Schwartz. "Our team can continue to learn new technologies while enabling the company to innovate securely."

Schwartz doesn't stay awake at night worrying about security breaches caused by misconfigurations. Protection is always on. The team has complete visibility across the on-premises and cloud environments. Automatic alerting and remediation handle events transparently.

""I recommend Check Point Infinity NDR for organizations that are considering or moving to public cloud environments. It allows us to gain visibility and alerting functionality. We now have actionable visibility into overall security across both on-premises and AWS environments."

- Saul Schwartz,
Technology Manager, SE2

"CloudGuard CSPM aligns with the cloud shared security model and has made us much more secure," said Schwartz. "We have a really good solution in place to make our dynamic cloud environment as secure as possible."

Improved visibility into anomalous traffic and hidden threats

Infinity NDR provides powerful non-signature-based detection of unknown attacks, including Deep Packet Inspection and AI-based behavioral analysis of N-S and E-W traffic. It applies powerful analytical and behavioral engines on the traffic in real-time and uses various AI models for anomaly detection and false-positive reduction. An added benefit of these engines is the deep contextual visibility, including a threat topology map, activity mapping and instant observability of vulnerabilities.

Schwartz added, "We really enjoy the log aggregation and threat intelligence capabilities of Infinity NDR as well as the threat topology map."