CHECK POINT + LOGZ.IO

WHERE SECURITY AND DATA MEET

Where Security and Data Meet

A Tightly Integrated Threat Prevention Ecosystem

Solution Benefits

- Prevent threats across network, cloud, mobile and endpoint
- Unifying operations and security data makes analytics and compliance easy
- Understand your security posture within 5 minutes with pre-built rules
- Scalability, availability, and security are assured when you use familiar open-source tools like ELK, Grafana and Jaeger, bundled as a fully managed solution

INSIGHTS

Time is of the essence when it comes to threat detection. In 2019 over 50% of breaches took months or longer to discover (Verizon DIBR, 2019). It's encouraging that more organizations are discovering breaches sooner, when compared with earlier years. How can more organizations lower the time it takes to discover a breach and when a breach is discovered, lower the time to remediation?

Visibility is key to securing any organization. Security technologies protecting networks, cloud, mobile and endpoint devices are a rich source of data and work best when a threat is known. When identified, threat analysis enables remediation and prevention when data from that analysis becomes IoCs (Indicators of Compromise) and enriches your security defenses. When security and SIEM (Security Information and Event Management) technologies are tightly integrated, organizations detect threats earlier, minimizing the impact of the breach on business processes and reputation.

CHECK POINT AND LOGZ.IO SOLUTION

Together, Check Point and Logz.io deliver a unique integration that leverages the rich offering of the Check Point security product portfolio and Logz.io's powerful security event visualization and investigation capabilities. Stated simply, Check Point Next Generation Threat Prevention technologies and Logz.io Cloud SIEM provide a simple, DevOps-native threat prevention and investigation solution to shorten the time it takes to respond to threats.

When a Check Point device detects a security threat, event logs are sent to Logz.io, where they can be parsed, enriched, analyzed and prioritized in order to provide the modern DevSecOps or SOC engineer clear insight into the organization's security posture at any given time. In addition, the Logz.io Cloud SIEM product uses built-in threat intelligence feeds to flag events that contain malicious IPs, domains and URLs.

INTEGRATED THREAT PREVENTION ECOSYSTEM

Check Point offers a fully consolidated cyber security architecture to protect your business and IT infrastructure against sophisticated cyber-attacks across networks, endpoint, cloud and mobile. Our prevention technologies stop both known and unknown zero-day attacks across all areas of the IT infrastructure, including cloud, endpoint and mobile. And if an attacker does penetrate the perimeter, we terminate command and control channels and break the cyber-attack kill chain before they can extract data. Check Point network, endpoint, cloud and mobile device events enrich the data that Logz.io then analyzes for threats.

LOGZ.IO CLOUD SIEM DEVOPS-NATIVE THREAT DETECTION AND SECURITY ANALYTICS

Logz.io is fast, easy to use, and built on ELK, a familiar open source log analytics solution. Security events are analyzed using custom rules and monitoring dashboards developed by Logz.io specifically for Check Point logs. These rules and dashboards are updated periodically, both by leveraging built-in Machine Learning capabilities and by a dedicated team of security researchers. As you onboard, you'll leverage Check Point rules provided out-of-the-box that will strengthen your security posture by surfacing events such as:

- SSL enforcement violation detection
- Malware activity detection on the network
- Malicious file received via email
- Port Scanning activity detected
- Failed login attempts
- And many more!

This collaboration enables you to collect and ingest data from multiple sources and services, whether on-premises or on cloud, and have all the data reside in a unified data lake. This makes it easier to correlate events from any source and gain a tighter control in all of your environments and a better protection for your workloads.

MUTUAL SOLUTION ECOSYSTEM BENEFITS

- **Correlated Threat Detection:** Use Logz.io data-driven out of the box rules created by security analysts, based on the prevention insights provided by Check Point. An IoC layer of threat intelligence is in place to enable proactive flagging of malicious indicators for the users, designed to reduce alert fatigue and help analysts stay focused on what's most important.
- **Ready to Use Dashboards:** The joint solution offers pre-built dashboards from which you can pick and choose the most relevant to your SOC demands including dashboards created especially for environments protected by Check Point security products.
- **See Most Important Events First:** Most Important Add a layer of visibility to surface up potential high-severity attacks that evaded prevention due to configuration. These are actionable events that need your attention and can result in a configuration change to strengthen your organization's security posture.
- **Timely Alerts in an App of your Choice:** Leverage Logz.io alerts capabilities to get your alerts where you want them to land, in your email, a Slack channel or another designated tool like ITSM or SOAR.
- **Monitor Check Point Systems:** Get notified in real-time upon a detection of operability issues such as an IPS engine issue or SmartConsole login failure, lowering the risk and saving time to remediation.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

ABOUT LOGZ.IO

Logz.io is a cloud observability platform for modern engineering teams. The Logz.io platform consists of three products — Log Management, Infrastructure Monitoring, and Cloud SIEM — that work together to unify the jobs of monitoring, troubleshooting, and security. We empower engineers to deliver better software by offering the world's most popular open source observability tools — the ELK Stack, Grafana, and Jaeger — in a single, easy to use, and powerful platform purpose-built for monitoring distributed cloud environments.

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-628-2117 | www.checkpoint.com