CHECK POINT + ANOMALI

ACTIONABLE THREAT INTELLIGENCE

ACTIONABLE THREAT INTELLIGENCE

Solution Benefits

- Secure threat sharing across trusted communities to power secure collaboration
- STIX/TAXII compliant for bi-directional intelligence exchange
- Tightly integrated threat intel and security enforcement
- Augments Check Point threat prevention with curated threat intelligence
- Threat model analysis across intelligence from IoCs and malware to threat actors and campaigns

Security teams struggle to combat advanced attacks and protect their environments. That's because modern cyber threats are highly dynamic, with sophisticated adversaries constantly finding new ways to exploit outdated systems. Once they have a beachhead within an organization, it can be days and even months before their presence is detected.

To meet the challenge, security and incident response leaders must form a unified defense — one that brings together intelligence, action, and best-of-breed technologies.

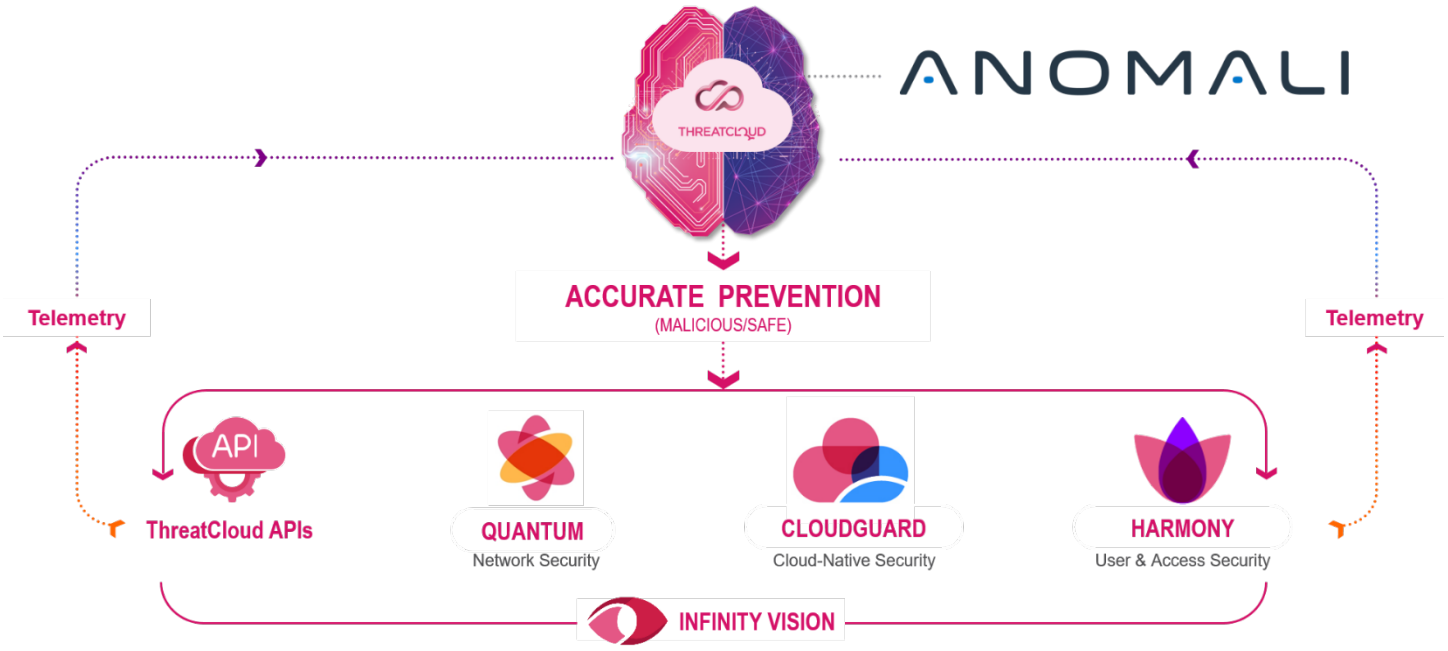
UNIFYING THREAT INTELLIGENCE WITH THREAT PREVENTION

Check Point and Anomali are partnering to integrate intelligence from Anomali's ThreatStream to identify and prevent malicious threats with the best-of-breed Check Point cyber security platform. ThreatStream automatically delivers high-fidelity threat intelligence to Check Point to surface relevant threats to help actively protect users and assets from dynamic and sophisticated attacks.

Firewalls and network security solutions are often regarded as the key to preventing malicious threats from penetrating a network. To protect users from unknown and zero-day threats, Check Point security products are dynamically updated via ThreatCloud, a cloud service that aggregates and analyzes big data telemetry and millions of Indicators of Compromise (IoCs) every day. This threat intelligence database is fed from Check Point sensors, Check Point Research, external feeds and now Anomali ThreatStream with an Anomali REST API and Check Point CloudGuard NDR integration.

CloudGuard Network Detection and Response (NDR) is the latest addition to the Check Point unified security architecture, providing non-signature threat detection, visibility and investigation capabilities with an additional security layer that uncovers hidden threats.

Anomali ThreatStream IoCs are automatically ingested into CloudGuard NDR where the IoC metadata and data set assignments may be further modified by security staff and then fed into ThreatCloud to protect Check Point customers from threats.



SECURITY INTELLIGENCE THAT YOU CAN USE

At most organizations, the problem isn't a shortage of threat data — it is information overload. To make this information truly useful, you need to quickly understand what's relevant to your environment, evaluate it in context, then put it to work. Anomali's ThreatStream threat intelligence platform aggregates data from multiple sources to deliver operationalized threat intelligence that helps you understand your risk, make informed and proportionate decisions, and improve your security posture. Together, Check Point and Anomali uncover hidden threats targeting your environment.

MAKES INTELLIGENCE ACTIONABLE	EMPOWERS INVESTIGATIONS
• Connect threat data to threat models and workflows • Supports collaboration and information sharing • Reduce duplicate, dated, and inaccurate data • Enrich info for full context and significance • Distribute threat intel to the security stack	• Network reconnaissance and lateral movement • Suspicious users and applications • Anomalous traffic patterns • Data exfiltration activities • Infected assets

ABOUT ANOMALI

Anomali is the leader in global intelligence-driven cybersecurity. Our customers rely on us to see and detect threats, stop breaches, and improve the productivity of security operations. Our solutions serve customers around the world in every major industry vertical, including many of the Global 1000. Anomali is a SaaS company that offers native cloud, multi-cloud, on-premises, and hybrid technologies.

ABOUT CHECK POINT SOFTWARE

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.