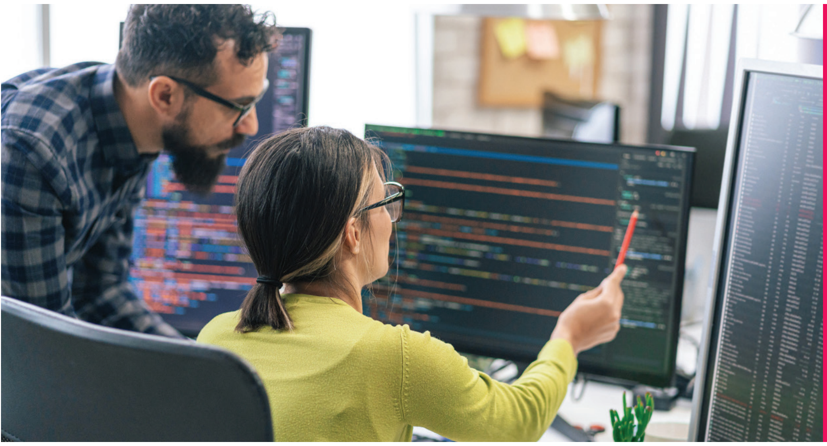
CHECK POINT™

Infinity
Playblocks



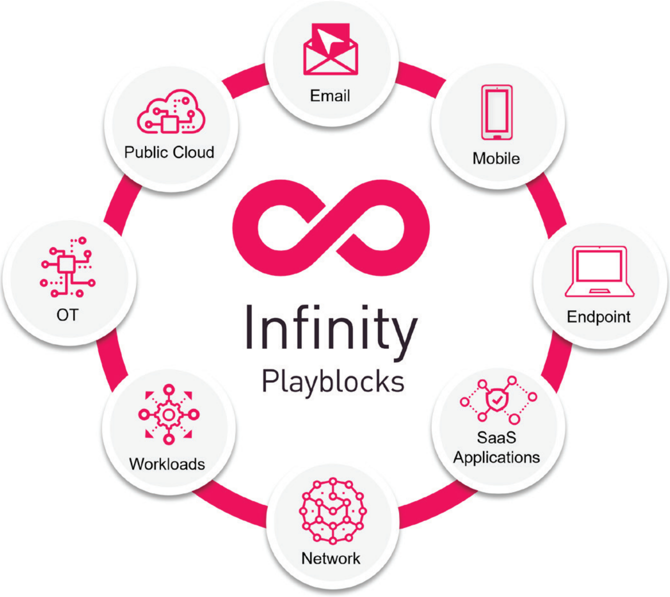
Security Automation & Collaboration Platform

The Need for Collaboration in Security

The traditional security approach is siloed. Each deployed security tool is designed to provide a specific type of protection across different areas like the network, endpoints, email, and cloud environments; but prevention on one enforcement point does not improve prevention on any other points, leaving them vulnerable.

As a result, persistent attackers are eventually able to find an entry point, attacks then spread quickly, and SOC teams using manual processes struggle to keep up. A traditionally siloed approach to security means that security teams are still left with critical challenges:

- **Attacks spread quickly** across the organization
- **Attackers are persistent** and attack from different vectors
- **Security teams struggle** with skills shortage & error prone manual work



Infinity Playblocks introduces a collaborative approach to security - when a single enforcement point identifies a potential security threat, it triggers Playblocks to activate automated preventions across the entire security infrastructure.

Automated, Collaborative Security Across the Enterprise

Overcome Limitations of Silos

to prevent attacks across
the entire security estate

Make Security Collaborative

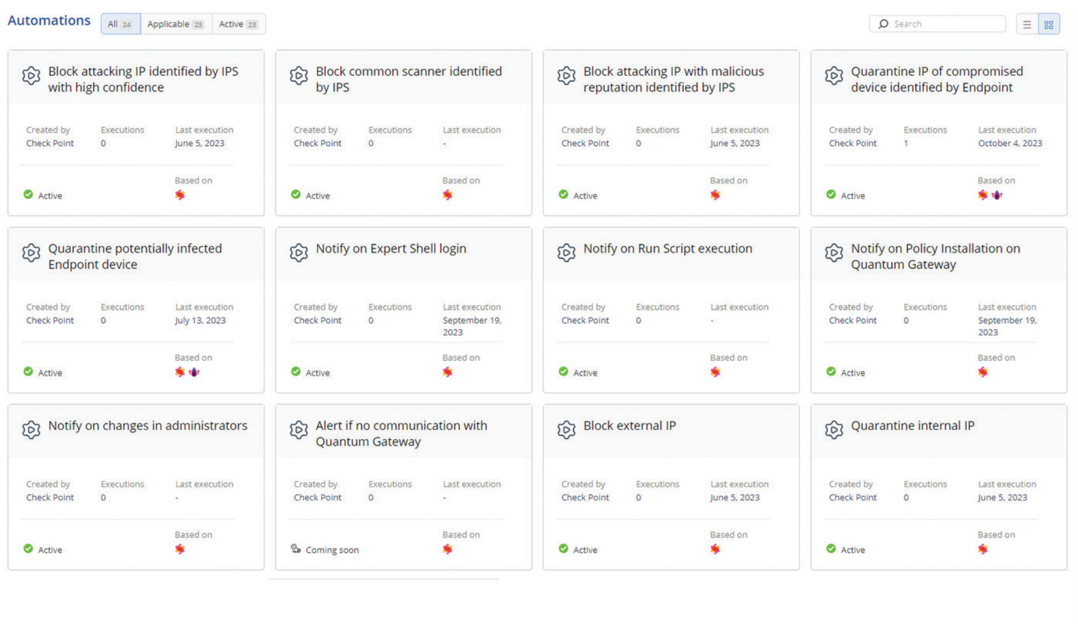
make products, people &
processes work together

The moment a single enforcement point identifies an attack, Playblocks triggers automatic preventative actions across the entire security infrastructure and immediately alerts security teams. Playblocks acts fast and eliminates the risk of human error, to keep your organization ahead of threats, reduce burden on SOC teams, and streamline security operations.

Playblocks helps security teams get their siloed security products to work together, to power automated, collaborative security across the entire enterprise. This allows organizations to quickly contain attacks and prevent them from spreading and reoccurring.

Collaborative Threat Prevention

Automatically contains and prevents attacks from spreading across the entire security environment by carrying out preventative actions, including isolating hosts, initiating kill processes, and notifying admins.



Block attacking IP identified by IPS with high confidence
Created by Check Point | Executions 0 | Last execution June 5, 2023
Active | Based on

Block common scanner identified by IPS
Created by Check Point | Executions 0 | Last execution -
Active | Based on

Block attacking IP with malicious reputation identified by IPS
Created by Check Point | Executions 0 | Last execution June 5, 2023
Active | Based on

Quarantine IP of compromised device identified by Endpoint
Created by Check Point | Executions 1 | Last execution October 4, 2023
Active | Based on

Quarantine potentially infected Endpoint device
Created by Check Point | Executions 0 | Last execution July 13, 2023
Active | Based on

Notify on Expert Shell login
Created by Check Point | Executions 0 | Last execution September 19, 2023
Active | Based on

Notify on Run Script execution
Created by Check Point | Executions 0 | Last execution -
Active | Based on

Notify on Policy Installation on Quantum Gateway
Created by Check Point | Executions 0 | Last execution September 19, 2023
Active | Based on

Notify on changes in administrators
Created by Check Point | Executions 0 | Last execution -
Active | Based on

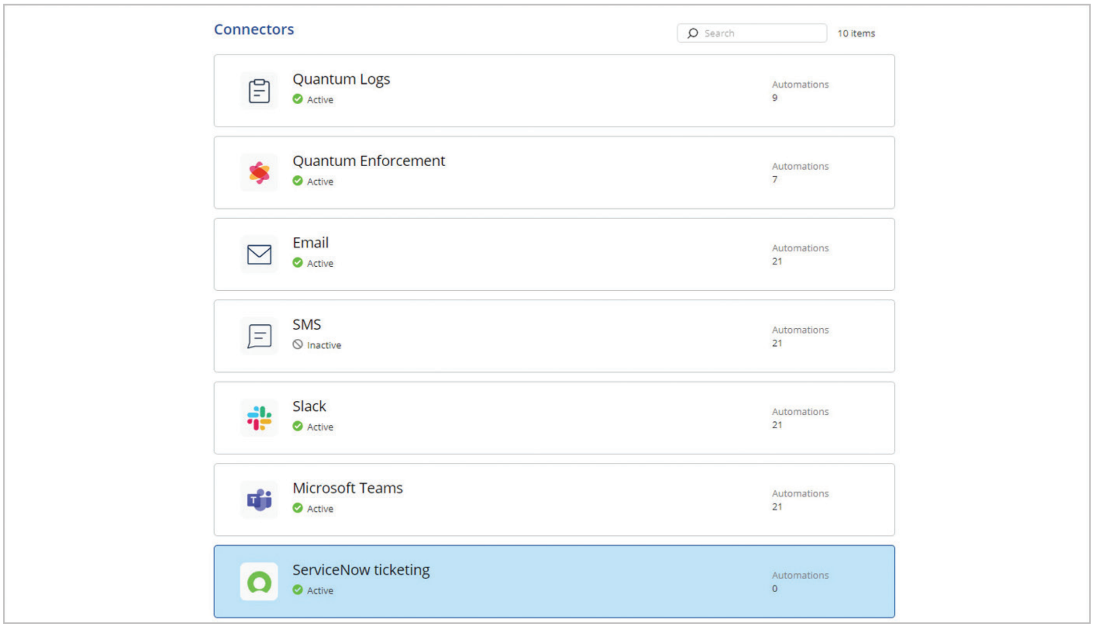
Alert if no communication with Quantum Gateway
Created by Check Point | Executions 0 | Last execution -
Coming soon | Based on

Block external IP
Created by Check Point | Executions 0 | Last execution June 5, 2023
Active | Based on

Quarantine internal IP
Created by Check Point | Executions 0 | Last execution June 5, 2023
Active | Based on

Consolidated

Triggered by security solutions across the enterprise to ensure the highest level of security at every enforcement point. Integrated with Check Point Quantum, Harmony Endpoint, Harmony Mobile, and third-party security vendors.



Connectors

Quantum Logs	✓ Active	Automations 9
Quantum Enforcement	✓ Active	Automations 7
Email	✓ Active	Automations 21
SMS	⦸ Inactive	Automations 21
Slack	✓ Active	Automations 21
Microsoft Teams	✓ Active	Automations 21
ServiceNow ticketing	✓ Active	Automations 0

Fast Time-To-Prevention

Activation takes just two minutes. Out-of-the-box playbooks are automatically set in motion; including the ability to automatically block a device or IP across all enforcement points, notify admins of policy installations on gateways, quarantining internal IPs, quarantining files, etc.

Prevention Powered by Collaboration

The Playblocks Security Automation & Collaboration Platforms offers dozens of automated playbooks off-the-shelf, and more are added on a regular basis. It is already included with Horizon XDR/XPR Extended Prevention and Response Platform or can be integrated with existing workflow management systems, such as ServiceNow, Jira, Microsoft Teams, etc.

Infinity
Playblocks

Automated Security Playbooks

- Platform that connects all your operational & security tools
- Attacks trigger automated threat prevention and operational action across the estate

Infinity
XDR/XPR

Intelligent, AI-Powered Correlation

- AI powered correlation between seemingly benign events ("clues")
- Indicators of compromise are correlated across tools to discover more threats and make smart decisions
- Wisdom of the global threat landscape with indicators of compromises from Check Point's 150,000 gateways and millions of endpoints (ThreatCloud)

Infinity Playblocks and XDR/XPR work together to prevent more advanced threats faster.

Learn more about Infinity Playblocks and sign up for a free demo.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

www.checkpoint.com