Check Point Infinity SOC

Achieving SOC Certainty

A cloud-based platform that enables SOC analysts to expose, investigate, and shut down attacks faster, and with 99.9% precision.

KEY BENEFITS

99.9 precision: Automatically exposes and shut down only real attacks

Rapid Investigation: Accelerates and deepens threat investigations with the industry's most powerful threat intelligence

Zero friction: No deployment, integration, and privacy issues.

ADDITIONAL BENEFITS

Increase SOC efficiency by automating manual and tedious security tasks.

Enable every SOC to easily perform the most complex tasks.

Increase security ROI with advanced detection engines that use existing gateways.

SOC Challenges

For many Security Operations Center (SOC) teams, finding malicious activity inside the network is like finding a needle in a haystack. They are often forced to piece together information from multiple monitoring solutions and navigate through tens of thousands of daily alerts.

The results: critical attacks are missed until it's too late.

Check Point Infinity SOC

Designed to address these common SOC challenges, Check Point Infinity SOC helps enterprises protect their networks by delivering:

- **99.9 precision to quickly detect and shut down real attacks:** Infinity SOC automatically exposes even the stealthiest attacks from millions of daily logs and alerts with unrivalled accuracy, powered by AI-based incident analysis.

- **Rapid incident investigations:** powered by ThreatCloud, the world's most powerful threat intelligence database, Infinity SOC enables teams to 'google search' any indicator of compromise (IOC) from a centrelized portal, and quickly get highly processed threat intelligence including global spread, attack timelines and patterns, malware DNA and more.

- **Zero-friction deployment:** Infinity SOC is a single, centrally-managed cloud platform, improving teams' operational efficiency and reducing TCO. It deploys in minutes and avoids costly log storage and privacy concerns with unique cloud-based event analysis that does not export and store event logs.

99.9% PRECISION

Expose and Shutdown Only Real Attacks

Automatically pinpoints only real security incidents

Infinity SOC utilizes AI-based incident analysis to pinpoint real security incidents across your entire IT infrastructure: networks, cloud, endpoints, mobile devices, and IoT. The overview dashboard enables the SOC team to clearly see their organization's security posture through a single pane of glass. In the example in Figure 1, Infinity SOC has detected **3,000 malicious activities** (e.g., lateral movement and data exfiltration attempts) targeting **40 different hosts**. However, it narrows this down by pinpointing only the **11 hosts that have been actually infected. These are the 11 most critical security incidents which** require the SOC immediate attention.

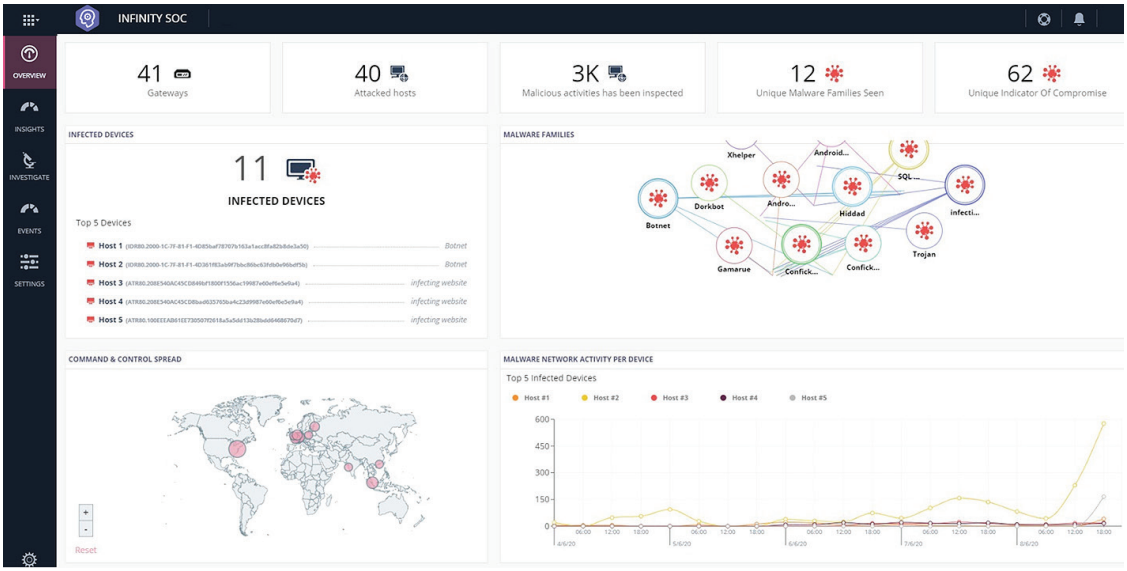

Figure 1: The Infinity SOC overview dashboard enables the SOC team to see their organization's entire security posture through a single pane of glass.

Exposes even the stealthiest attacks with 99.9% precision

Existing detection tools do not provide SOC teams with the certainty they need to detect critical attacks quickly enough. Methods like 'rule-based' or behavior analysis (anomaly detection) either miss critical incidents too often or create too many false positives.

Infinity SOC exposes even the stealthiest attacks with 99.9% precision by leveraging a multi-layered approach to XDR:

1. **Enterprise-wide visibility:** analyzing network, cloud, endpoint, mobile, and IoT events over an extended period of time.

2. **External threat visibility:** leveraging ThreatCloud's global visibility into real-time internet traffic to detect external threats outside the organization.

3. **Threat Intelligence:** enriching every alert with threat intelligence and connecting the dots with big data analysis to uncover the most sophisticated attacks like APTs. Powered by ThreatCloud, the world's most powerful threat intelligence database.

4. **AI-generated verdict:** analyzing the aggregated information (from the three layers mentioned above) to accurately detect malicious activity using AI-based engines. Engines that have been trained and validated by some of the world's largest SOCs.

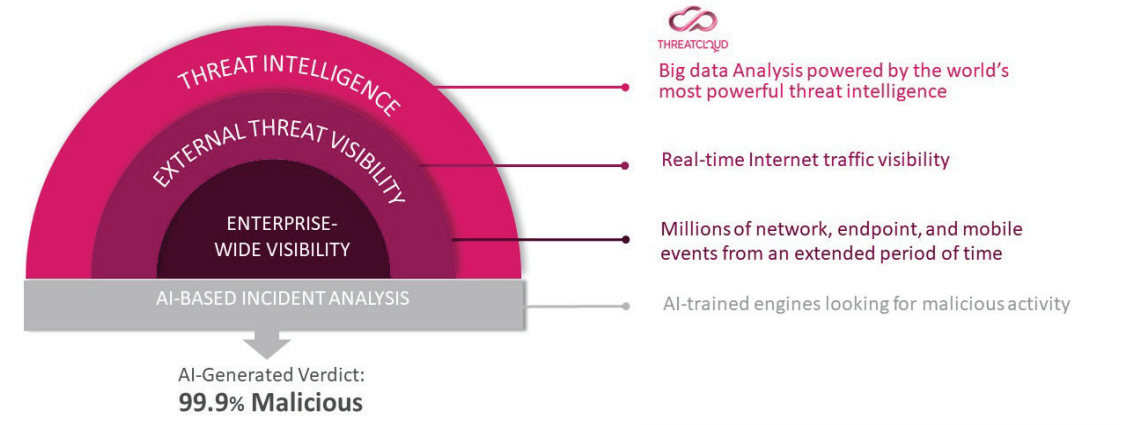

Figure 2: Infinity SOC goes beyond XDR by delivering 99.9% AI-generated verdict

Quickly respond to the most severe attacks with automated triage and single-click remediation using a lightweight client

Infinity SOC automatically triages security incidents based on their severity and probability so you can respond quickly to the most critical attacks. The faster an incident is detected and prioritized as critical, the lower the risk that your compromise will turn into a breach.

Figure 3: Automated triage provides prioritization so you can respond intelligently based on severity and probability

If an infected host is detected, Infinity SOC provides a lightweight agent that can be simply installed on the infected host to perform complete remediation. The agent automatically identifies and kills all malicious processes, blocks C&C communications, and deletes all connected malicious files. It then auto-generates a detailed forensic report that provides granular visibility into infected assets, the attack flow and its correlation with the MITRE ATT&CK framework, along with contextualized insights and a mitigation guide.

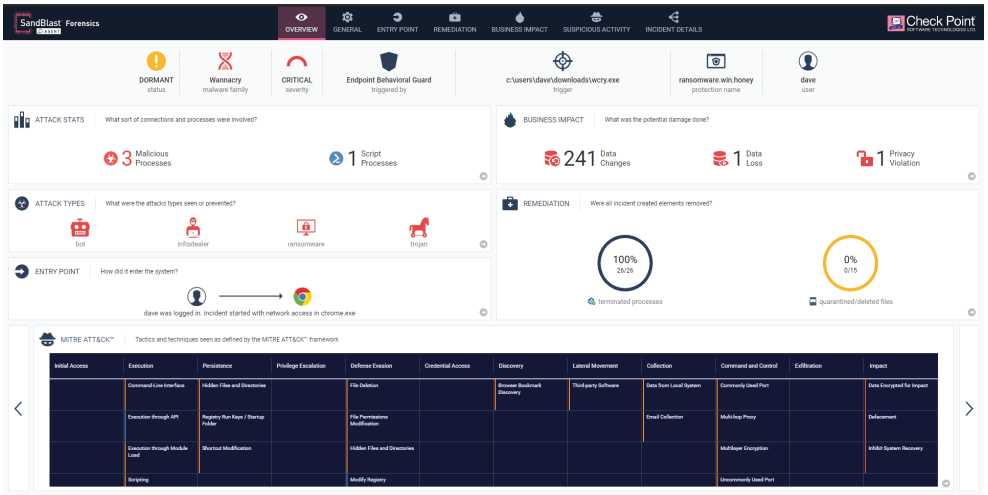

Figure 4: Detailed forensic report with actionable insights

Prevent hackers from launching phishing campaigns against your customers

Infinity SOC is the only solution that detects threats inside and outside the organization, providing you with a complete view of the entire threat landscape. Hackers often impersonate your brand to interact with your customers and steal their data. Infinity SOC alerts you when it detects a lookalike domain used to impersonate your corporate website and email domains and provides a takedown option to prevent any brand hijacking attempts.

Infinity SOC detects three times more threats than competing solutions because of its visibility into real-time internet traffic. Unlike other solutions, Infinity SOC does not detect based on new domain registration feeds. Instead, it analyzes the domain portion of the Fully Qualified Domain Name (FQDN). Additionally, Infinity SOC intelligently analyzes characteristics of the website such as the textual similarity, visuals, domain attributes and SSL certificates.

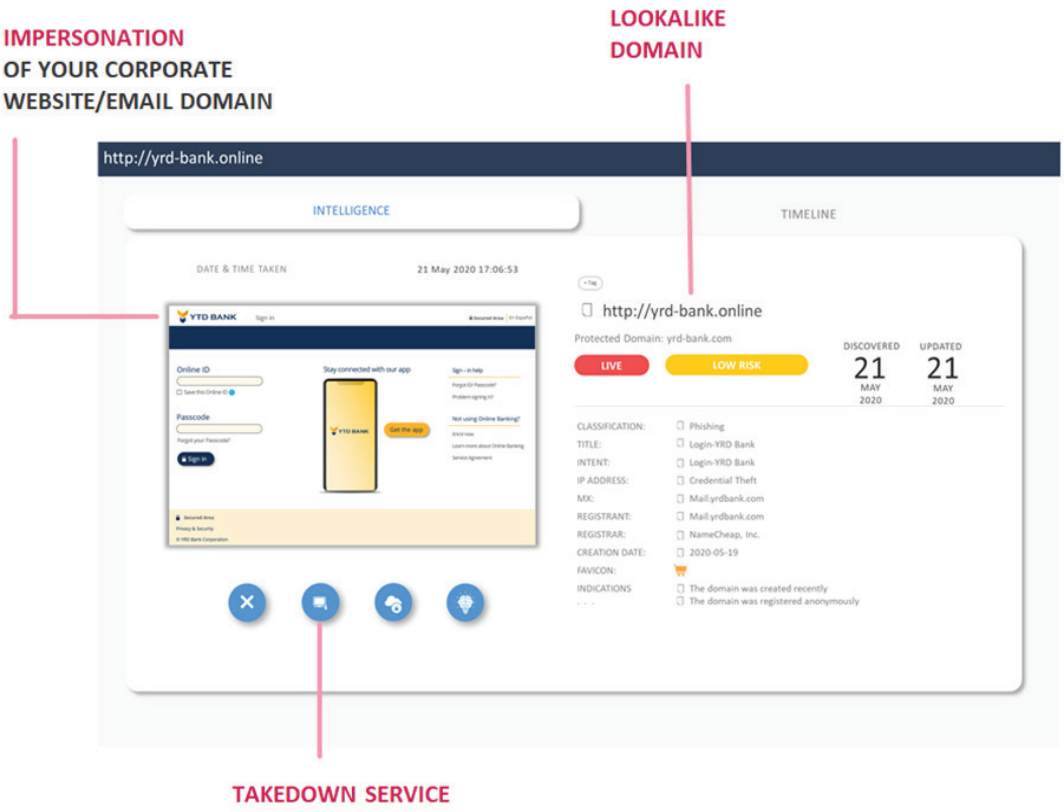

Figure 5: Infinity SOC provides alerts and options to takedown lookalike domains used to impersonate your corporate website and email domains

RAPID INVESTIGATION

Accelerate and deepen investigation with the Industry's Most Powerful Threat Intelligence

'Google search' any IoCs to obtain contextualized useful threat intelligence

Infinity SOC provides you with the tools and threat intelligence that enable you to conduct in-depth and faster investigations. With Infinity SOC, you can perform a search on any IOCs to obtain rich, contextualized threat intelligence that includes geographical spread, targeted industries, attack timeline, and methods.

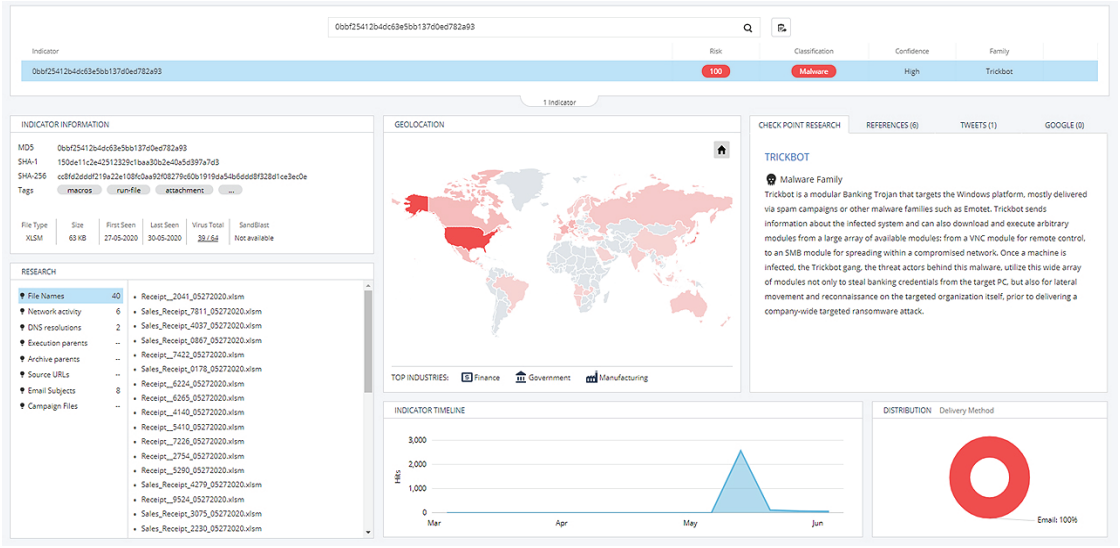

Figure 6: Infinity SOC allows you to investigate any IOCs to learn more about its geographical spread, targeted industries, attack timeline and more

Infinity SOC provides the ability to research and obtain unique threat intelligence data for every indicator of compromise (IoC). Obtain exclusive information on the threat and additional related IoCs, for example- campaign files, communication files, typical file names used, and network activity commonly associated with the IOCs.

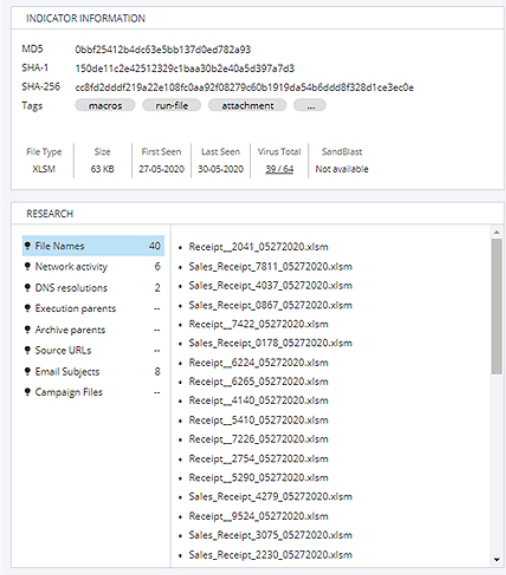

Figure 7: Infinity SOC provides unique and comprehensive information on the searched IOC

Infinity SOC leverages Check Point ThreatCloud, the most powerful threat intelligence database. ThreatCloud is continuously enriched by advanced predictive intelligence engines, data from hundreds of millions of sensors, cutting-edge research from Check Point Research and external intelligence feed. On a daily basis, ThreatCloud analyzes 10 trillion logs, 86 billion IOCs, 2.6 billion attacks and 3 billion website and files.

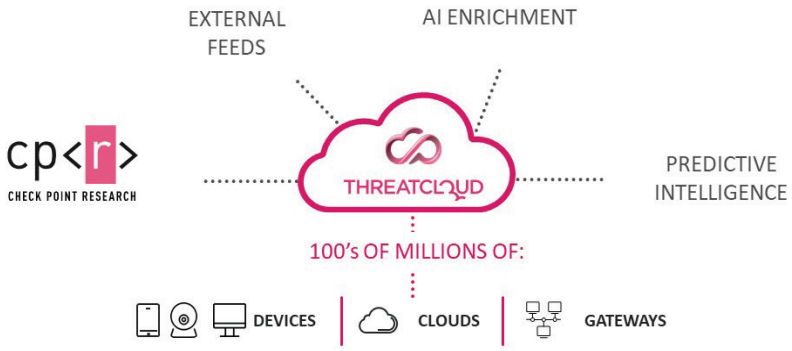

Figure 8: Check Point ThreatCloud is continuously enriched by advanced predictive intelligence engines, data from hundreds of millions of sensors, cutting-edge research from Check Point Research, and external intelligence feed.

Deepen investigations with unique research data and the industry's first deep-link IoC search on social media feeds and OSINT

Infinity SOC performs deep-link searches on social media and OSINT to find and surface relevant and useful information from web pages and documents for a more in-depth investigation.

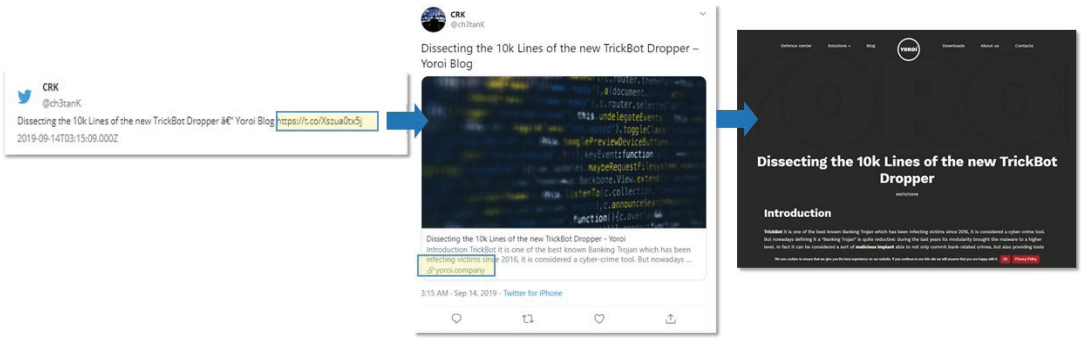

Figure 9: Infinity SOC analyzes links on social media feeds and OSINT to find and surface relevant and useful information from the linked pages and documents

Quickly determine whether a suspicious file is malicious using SandBlast's threat emulation service, which has the industry's best catch rate

Upload suspicious files at any time for analysis by SandBlast emulation service. Check Point's threat emulation sandboxing technology automatically analyzes the file and delivers the results in a detailed report that includes a wealth of forensic information such as malware family, targeted geography, MITRE ATT&CK techniques, emulation videos and dropped files.

Figure 10: SandBlast threat emulation service analyzes the uploaded file and delivers the results in a detailed report

Developed by the Check Point Research Team and used daily to expose and investigate the world's most dangerous and sophisticated cyber-attacks

Check Point Research Team consists of over 150 elite cyber security analysts and researchers that collaborate with other security researchers, law enforcement and Computer Emergency Response Teams (CERTs). Check Point Research Team's recently uncovered the following:

- Ongoing cyber espionage operation against several government entities in the Asia Pacific (APAC) region by the Naikon APT group
- Analysis of the Phorpiex botnet which acts like both a computer worm and a file virus
- Business Email Compromise (BEC) attacks by the group called Florentine Banker

Zero Friction

No deployment, integration and privacy issues

Reduce TCO with a single, centrally managed SOC platform.
Infinity SOC unifies threat prevention, detection, investigation and remediation in a single, centrally managed platform to give you unrivalled security and operational efficiency.

A non-intrusive implementation that takes minutes, without the need to deploy additional endpoint agents.
Infinity SOC utilizes an innovative network-based detection that does not require the deployment of additional endpoint agents or time to generate ground-truths for your models. Onboarding takes only minutes and you can start detecting threats immediately.

Avoid costly log storage and privacy concerns with a revolutionary cloud-based event analysis that does not export and store your logs.
With Infinity SOC, there is no need to send or store logs.

Summary

Today's SOC teams face a lot of challenges. However, Check Point Infinity SOC can help address these challenges. Check Point Infinity SOC is a cloud-based platform that enables security teams to expose, investigate, and shut down attacks faster, and with 99.9% precision. Infinity SOC unifies threat prevention, detection, investigation and remediation in a single platform to give unrivalled security and operational efficiency.

Learn more at: **https://www.checkpoint.com/products/infinity-soc/**

Worldwide Headquarters
5 Ha'Solelim 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: 650-654-4233

www.checkpoint.com