CHECK POINT + CYSIGHT
ULTIMATE NETWORK ANOMALY ANALYTICS AND FORENSICS

BENEFITS

- Provides an integrated security monitoring, performance management, and capacity planning environment for SOC and NOC teams
- Eliminate network blind spots
- Collects, tags, retains, and correlates network flows and application metadata to identify cyber-threats that would otherwise be undetectable using predictive AI
- Anomaly detection, security forensics and performance monitoring to highlight hidden anomalies
- Perpetual diagnostics detects spurious traffic from DDoS attacks, P2P abuse and insider threats
- End-Point threat intelligence identifies botnets, hackers, traders in illicit material, or other known bad actors
- Complete drilldown forensics into suspect communications
- Easy to deploy, easy to use
- Highly automated: requires a low labor effort to manage

INSIGHTS

The information security landscape has become so complex and diversified that companies need reliable and real-time diagnostics, network analysis and performance monitoring to leverage existing security strategies.

JOINT SOLUTION

Check Point and CySight have partnered to enable enterprises to have uncompromised protection against all types of threats and real-time qualification, granular historical visibility of all traffic flows recorded for enhanced security forensics, compliance, trending, alerting and automated traffic diagnostics.

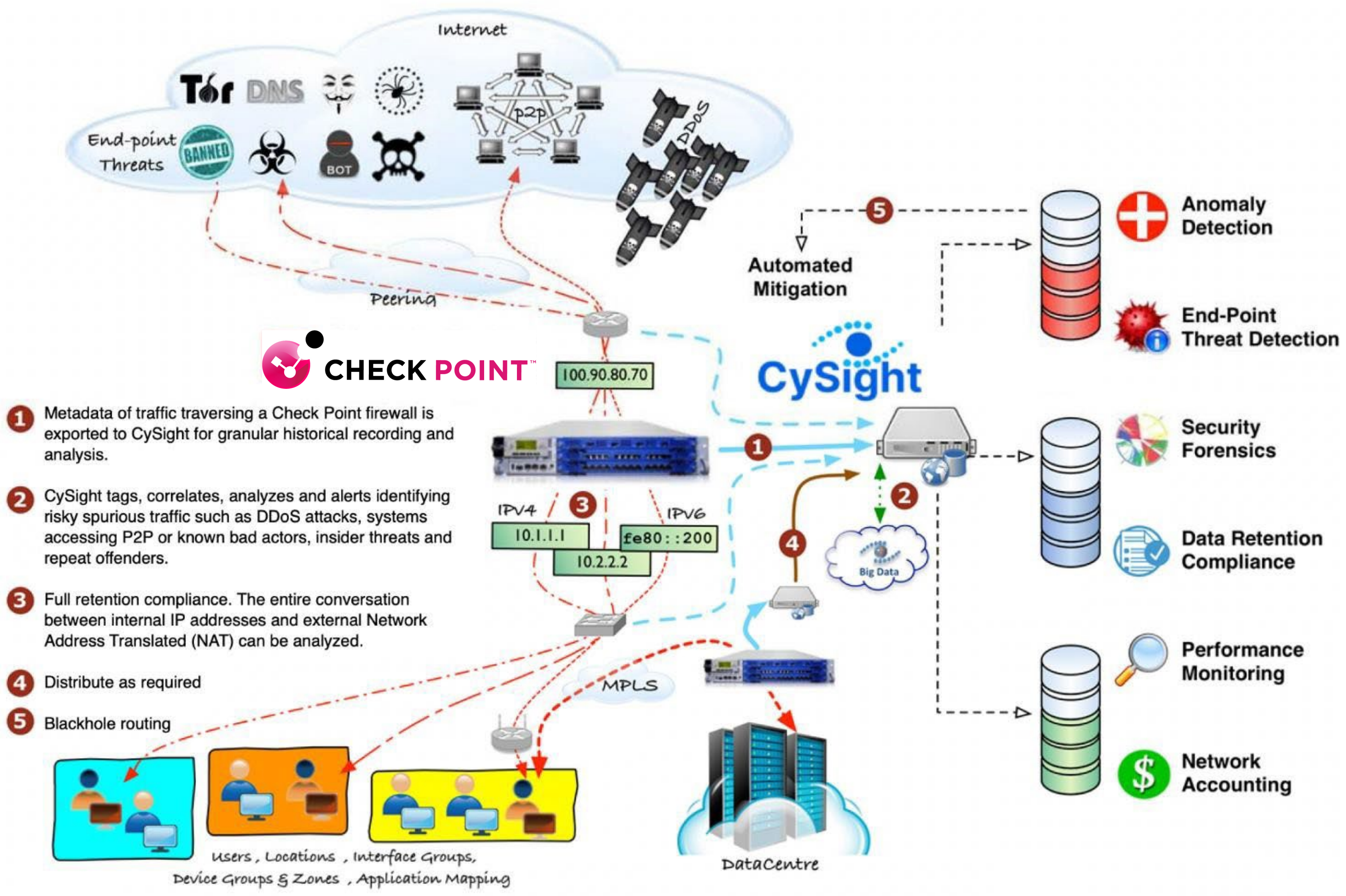
Check Point's fined-grained packet-based access control coupled with CySight's granular flow-based real-time detection and long-term security surveillance provides an enhanced security solution with complete visibility into suspect communications and connects the dots between internal IP addresses and external Network Address Translated (NAT) conversations substantially strengthening the ability to defend your digital assets.

A Check Point firewall is positioned at key points in a network to control access. Traffic metadata traversing the Check Point firewall is exported to CySight for granular recording and analysis.

CySight's Predictive AI Multi-Dimensional Baselines and Threat Intelligence Correlation technology analyzes flow records in real-time and uses machine learning making use of historical data trends and threat intelligence to identify risky spurious traffic such as DDoS attacks, P2P abuse and insider threats and to mitigate security threats that would otherwise be hidden.

CySight's measurements provides engineers clear analytics to completely understand their traffic flows enabling access lists to be more clearly checked or monitor when access has been discontinued enabling unnecessary rules to be removed maintaining Check Point firewall efficiency. IPv4, IPv6, MAC, QoS, MPLS, VLAN, ASN and application grouping and real-world naming make it easy to identify traffic ownership.

CySight constantly monitors your network traffic and provides total visibility to quickly identify and alert on who did what, where, when, with whom and for how long. Led by a smart network predictive AI baselining solution, CySight continues to generate actionable insight by delivering the right monitoring information to the right teams at the right time.



1. Metadata of traffic traversing a Check Point firewall is exported to CySight for granular historical recording and analysis.
2. CySight tags, correlates, analyzes and alerts identifying risky spurious traffic such as DDoS attacks, systems accessing P2P or known bad actors, insider threats and repeat offenders.
3. Full retention compliance. The entire conversation between internal IP addresses and external Network Address Translated (NAT) can be analyzed.
4. Distribute as required
5. Blackhole routing

AUTHENTICATION FLOW DIAGRAM

ABOUT CHECK POINT

Check Point Software Technologies Ltd. is the largest pure-play security vendor globally, provides industry-leading solutions, and protects customers from cyberattacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks to mobile devices, in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes. At Check Point, we secure the future.

ABOUT CYSIGHT

CySight (CySight.ai), trusted by Fortune 500 companies worldwide, gives NetOps and SecOps unparalleled insight into on premises and cloud networks with contextual big-data, small footprint forensics. Every flow is analyzed by CySight's Predictive AI Baselining. Intuitive AI diagnostics and global threat intelligence classify and extract intelligence from the broadest metadata flow sources to rapidly evaluate usage and abuse, detecting threats and malicious traffic, providing the appropriate monitoring information to the right people at the right time.