Check Point
SOFTWARE TECHNOLOGIES LTD.

SECURE YOUR EVERYTHING™

SandBlast Now

CYBER DEFENSE PLATFORM

DEPLOY - HUNT - PREVENT

Product Benefits

- Web-based Cyber Defense Center (CDC) portal for cyber situational awareness
- Highly scalable multi-tenant, multi-tier cloud backend, as a service - and as a product
- Service platform for MSSPs, IR teams, enterprise SOCs, and network auditors
- Advanced analytics and threat visualization supports threat hunting and forensics
- Fully automated sentry deployment - on traditional networks and cloud fabrics
- Implements Check Point's high catch-rate threat prevention engines:
  - SandBlast Zero-Day Threat Emulation, Extraction
  - IPS, Anti-Bot, Anti-Virus
  - Application and Identity Awareness
- Integrated Threat Intelligence Platform (TIP) feeding both SandBlast Now sentries and other Check Point gateways
- Patent-pending Cooperative HTTPS Inspection

HOW DO YOU PROTECT AGAINST TOMORROW'S ATTACKS?

As the world becomes more connected and networks continue to evolve, securing IT environments is becoming more complex than ever. We are now facing Gen V (5th Generation) of cyberattacks, large scale attacks that quickly spread and move across attack vectors and industries. Gen V attacks are more sophisticated than ever, crossing mobile, cloud, and network, bypassing conventional defenses.

Walls, deceptions, and other types of cyber fortifications may encumber the adversary, but no technological defense is forever perfect. A persistent attacker will always find ways to establish footholds on a target network, and will leverage them to achieve his or her objectives. This is especially true in today's borderless cyberspace, where network and cloud dissolve into each other.

Cyber defenders need a new concept of operations for detecting, disrupting, and repelling these ever more prevalent attacks.

Check Point Infinity is a fully consolidated cyber security architecture that protects against Gen V cyber-attacks across all vectors. The Infinity architecture supports automatic, immediate threat intelligence sharing across all security environments, and enables efficient security operation.

SandBlast Now extends Check Point Infinity to empower a new cyber defense paradigm. SandBlast Now tenets are DEPLOY – HUNT – PREVENT. **Deploy** operationalizes Infinity components anywhere that visibility and control are needed – literally in minutes! **Hunt** combines an advanced set of analytical tools, combining artificial intelligence with advanced visualization techniques to allow cyber analysts to identify and investigate attacks that got through or past the other lines of defense. **Prevent** is the ability to convert analytical insights into action, via a Threat Intelligence Platform (TIP) that manages threat indicators and delivers them to the Infinity enforcement points. Together, these SandBlast Now functions provide cyber defenders with the agility needed to address any attack, anywhere.

DEPLOY

SandBlast Now sentries go beyond mere detection, providing the cyber defender with the ability to selectively disrupt attacks. Sentries are augmented versions of Check Point's Security Gateway appliances for on-premises deployment, and of CloudGuard IaaS instances for private and public cloud environments.

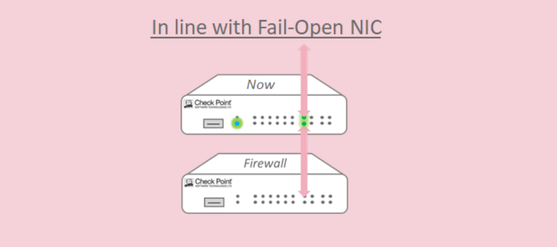
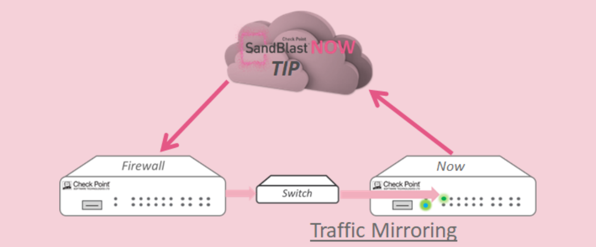
Physical appliances are attached either passively (Monitor Mode), processing mirrored traffic, and/or inline bump-in-the-wire (Bridge Mode). Both modes provide plug and play operation, with no need to modify network routing.

Inline appliances are equipped with fail-open 1Gbps copper or 10Gbps fiber network interfaces[1], ensuring that the sentries do not disrupt business traffic, even

[1] Fail-open NICs available on select appliance models. See Check Point Product Catalog for details.

if powered down or faulty. Bypass mode can also be explicitly controlled from the Cyber Defense Center (CDC) portal.

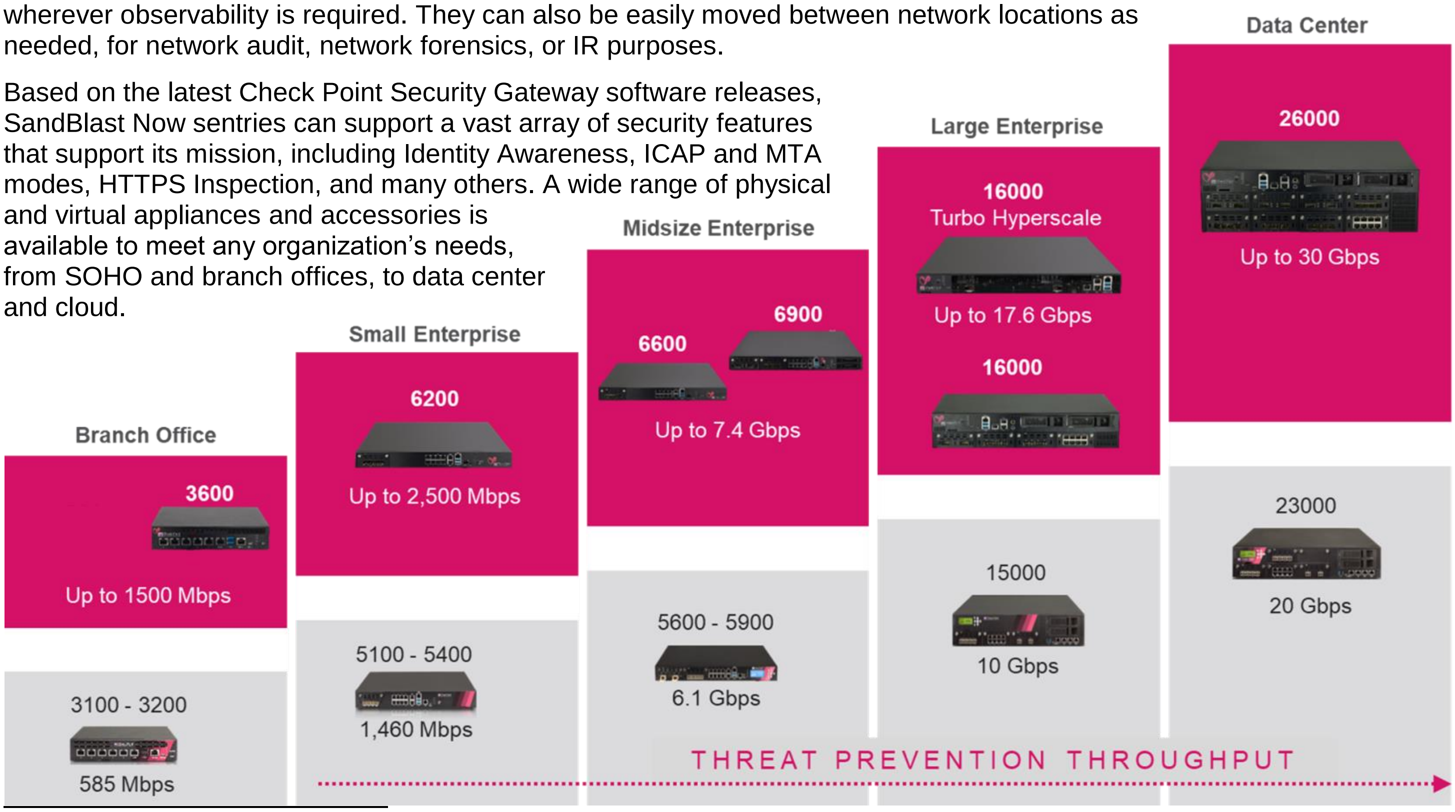
Traffic mirroring is also supported[2] on public cloud platforms. Cloud-native APIs are used to achieve fully automated sentry deployment, with no modifications required to customers’ VPCs.

In line deployment modes	Passive inspection deployment modes
 In line with Fail-Open NIC Now Check Point Firewall Check Point	 SandBlast NOW TIP Firewall Check Point Switch Now Check Point Traffic Mirroring
Prevent: Inline Now blocks all attack traffic. Exceptions used to filter out false positives.	**Detect**: Now used for threat hunting and protection development and testing w. zero impact to network.
Detect: Blocks only identified attack patterns as directed by cyber analysts (exceptions or IOCs).	**Prevent**: Attack signatures are published via the SandBlast Now TIP, driving main line prevention.
Bypass: Fail-Open NIC ensures no network disruption during upgrades and maintenance.	**Bypass**: Continued observability when bypass engaged. Now is “ready for action” via ‘bypass off’.

SandBlast Now is fully plug and play. Sentries are preconfigured so that they become fully operational within minutes of deployment, whether on physical or virtual networks. Both DHCP and static network configuration are supported. The sentry automatically registers on the Sandblast Now Cloud, establishes an SSL VPN (TCP port 443) tunnel for all control plane traffic, and initiates network traffic inspection, with no further administration or configuration required.

Painless deployment allows Managed Security Service Providers (MSSPs) to use SandBlast Now sentries as Customer Premises Equipment (CPE) for delivery of value-add services, such as threat hunting, Managed Security Service (MSS), and Incident Response (IR)[3]. The CPE solution eliminates any dependency on customers’ existing security estate, thereby greatly reducing service Total Cost of Ownership (TCO) on training, maintenance, and integration. Enterprises can also enjoy the benefits of an independent cyber overlay approach that does not require them to change or upgrade their existing security management platforms in order to enjoy the latest Check Point Infinity cyber security engines. Appliances can be shipped to remote branches and installed by unskilled personnel. Sentries can be easily deployed wherever observability is required. They can also be easily moved between network locations as needed, for network audit, network forensics, or IR purposes.

Based on the latest Check Point Security Gateway software releases, SandBlast Now sentries can support a vast array of security features that support its mission, including Identity Awareness, ICAP and MTA modes, HTTPS Inspection, and many others. A wide range of physical and virtual appliances and accessories is available to meet any organization’s needs, from SOHO and branch offices, to data center and cloud.



[2] SandBlast Now sentries for public cloud are branded “Check Point CloudGuard IaaS TAP”.
[3] MSS and IR services can optionally be further supported by corresponding Check Point service offerings.

© 2020 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

SandBlast Now sentries' role is to perform Deep Packet Inspection (DPI) on both North/South and East/West network traffic. Sentries are not intended to replace existing lines of defense; rather they provide cyber defenders with network observability and a fulcrum for threat hunting. As such, they are typically installed for maximum visibility – off core switches, WAN cores, data center edge, OT networks, DMZs and honeypot networks, branch office networks, as well as within private and public cloud environments. Additionally, appliances fitted with fail-open NICs can be inserted inline at network choke points, for a 'shoot back' capability, or simply as plug and play dedicated threat prevention devices.

In both inline and passive deployments, TLS-encrypted network traffic can be transparently decrypted by SandBlast Now's patent-pending, revolutionary Cooperative Inspection capability. Cooperative Inspection provides true plug and play operation, with no need to pre-register protected servers nor import their certificates. Ultra-fast, highly secure, and with no interference with the traffic stream (no Man in the Middle necessary), Cooperative Inspection can even interoperate with client certificates and certificate pinning applications.

SandBlast Now can also inspect TLS traffic in its original encrypted form, analyzing envelope data, including SNI and certificate attributes, as well as peer endpoints and traffic volumes and periodicity.

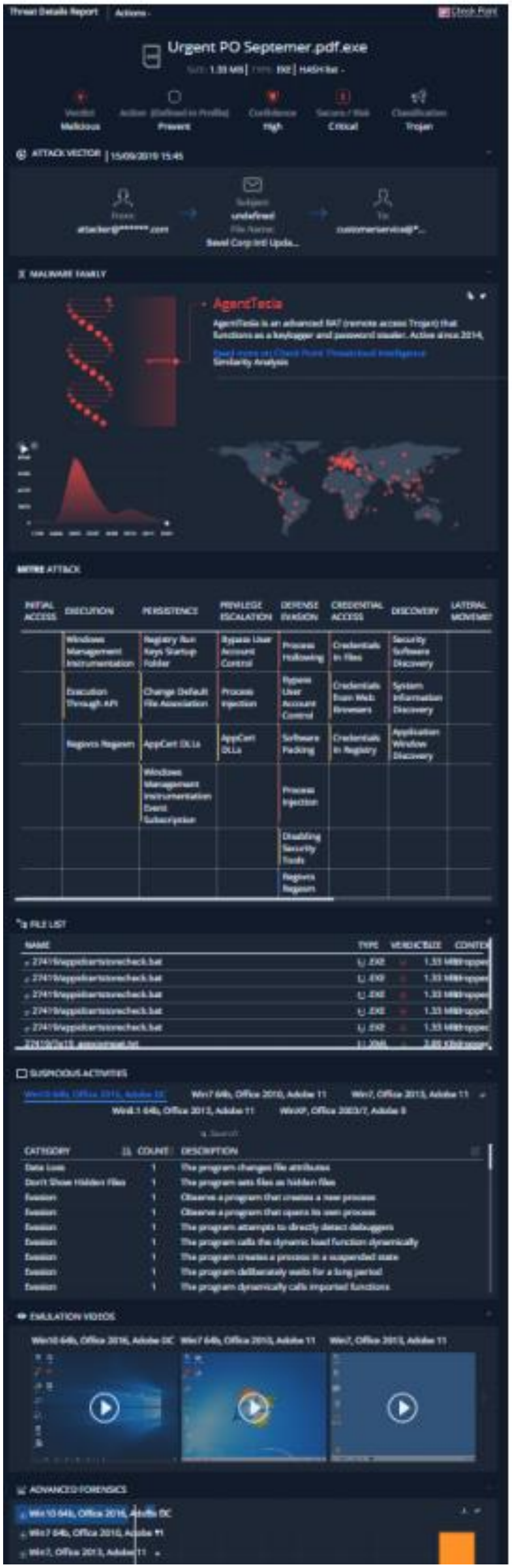
Each sentry applies a multitude of industry-leading analytics engines on the traffic in real time, including application fingerprinting, reputation-based and behavioral analysis, pre-infection and post-infection pattern matching, static and dynamic content inspection, as well as applying various AI models for anomaly detection and false positive reduction.

These engines leverage Check Point's ThreatCloud, a real-time collaborative big data repository delivering up to date threat intelligence that drives threat prevention. Utilized in four billion security decisions daily, ThreatCloud gleans cyber-attack data from hundreds of millions of protected assets worldwide across cloud, mobile, endpoint, and network, as well as top notch research by Check Point Research Labs and the industry's best threat intelligence feeds.

Analytical results are delivered to a Cyber Defense Center Web portal, in the form of logs for further analysis and visualization. Packet captures can also be extracted for further triage and network forensics. Threat Emulation reports (see example in sidebar) accessible from the CDC portal provide further deep insight into transmitted file payloads. Insightful reports can be generated and scheduled for tracking compliance posture and providing management visibility.

SandBlast Now's plug and play paradigm applies to threat prevention policy as well. Check Point's "Strict" profile is applied on all sentries. On sentries configured in Prevent mode, this profile will prevent all traffic that is flagged as malicious with Medium or High confidence. Even low-confidence matches will be logged. This approach provides a high catch rate with low false positive ratio. In cases where a false positive does occur, users can easily provision an exception via the CDC.

Customers who desire a tailored threat prevention profile may also purchase a dedicated SmartCloud management instance in the SandBlast Now Cloud. Check Point's Tailored Safe extension can then be used to automatically tune the profile to the customer's operational network traffic profile and application set.



Urgent PO Septemer.pdf.exe

Size: 1.33 MB | Type: EXE | HASH: [illegible]

Verdict	Action (Defined in Profile)	Confidence	Severity / Risk	Classification
Malicious	Prevent	High	Critical	Trojan

ATTACK VECTOR | 15/09/2019 15:45

From: attacker@*******.com → Subject: undefined File Name: Swed Corp Intl Upda... → To: customerservice@*...

MALWARE FAMILY

AgentTesla

AgentTesla is an advanced RAT (remote access Trojan) that functions as a keylogger and password stealer. Active since 2014.

Read more on Check Point ThreatCloud Intelligence

Similarity Analysis

MITRE ATTACK

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT
	Windows Management Instrumentation	Registry Run Keys Startup Folder	Bypass User Account Control	Process Hollowing	Credentials in Files	Security Software Discovery	
	Execution Through API	Change Default File Association	Process Injection	Bypass User Account Control	Credentials from Web Browsers	System Information Discovery	
	Regsvcs Regasm	AppCert DLLs	AppCert DLLs	Software Packing	Credentials in Registry	Application Window Discovery	
		Windows Management Instrumentation Event Subscription		Process Injection			
				Disabling Security Tools			
				Regsvcs Regasm			

FILE LIST

NAME	TYPE	VERDICT	SIZE	CONTEXT
2741f6appdatartstorecheck.bat	EXE		1.33 MB	Dropped
2741f6appdatartstorecheck.bat	EXE		1.33 MB	Dropped
2741f6appdatartstorecheck.bat	EXE		1.33 MB	Dropped
2741f6appdatartstorecheck.bat	EXE		1.33 MB	Dropped
2741f6appdatartstorecheck.bat	EXE		1.33 MB	Dropped
[illegible]	XML		2.85 KB	Dropped

SUSPICIOUS ACTIVITIES

Win10 64b, Office 2016, Adobe DC | Win7 64b, Office 2010, Adobe 11 | Win7, Office 2013, Adobe 11 | Win8.1 64b, Office 2013, Adobe 11 | WinXP, Office 2003/7, Adobe 9

Search

CATEGORY	COUNT	DESCRIPTION
Data Loss	1	The program changes file attributes
Don't Show Hidden Files	1	The program sets files as hidden files
Evasion	1	Observe a program that creates a new process
Evasion	1	Observe a program that opens its own process
Evasion	1	The program attempts to directly detect debuggers
Evasion	1	The program calls the dynamic load function dynamically
Evasion	1	The program creates a process in a suspended state
Evasion	1	The program deliberately waits for a long period
Evasion	1	The program dynamically calls imported functions

EMULATION VIDEOS

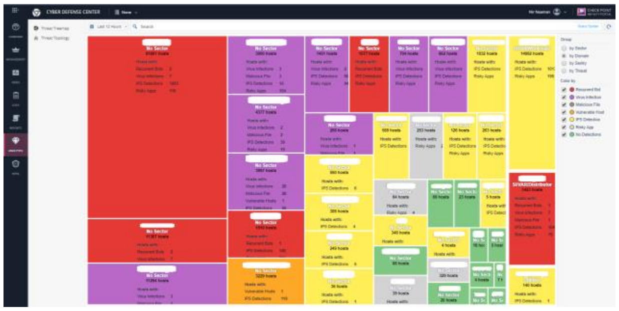
Win10 64b, Office 2016, Adobe DC | Win7 64b, Office 2010, Adobe 11 | Win7, Office 2013, Adobe 11

ADVANCED FORENSICS

- Win10 64b, Office 2016, Adobe DC
- Win7 64b, Office 2010, Adobe 11
- Win7, Office 2013, Adobe 11

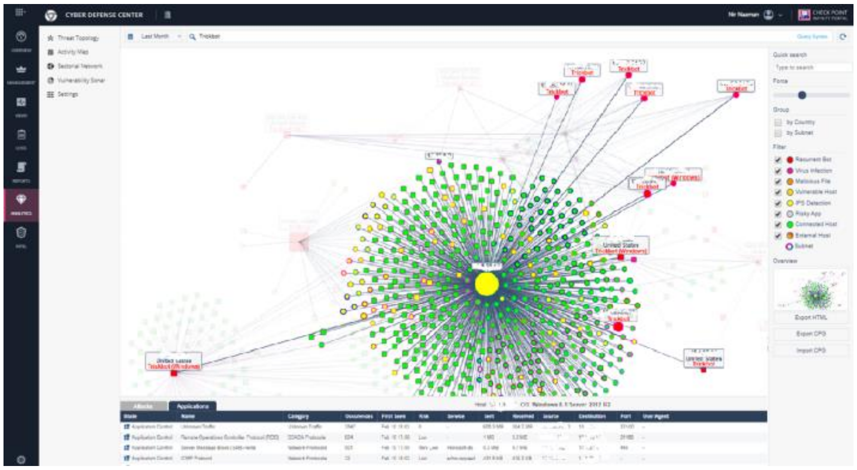
© 2020 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

HUNT



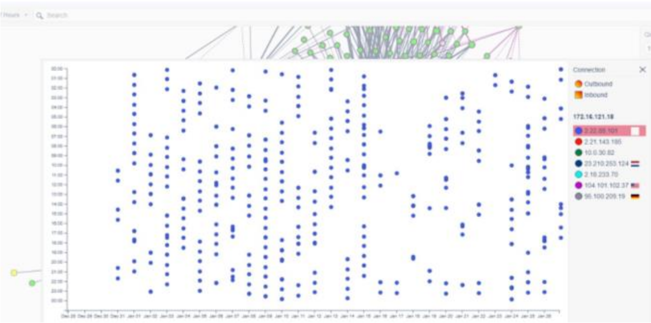
The Cyber Defense Center (CDC) is a Web-based portal whose purpose is to provide cyber defenders and SOC analysts with cyber situation awareness and the ability to intervene and disrupt undesired communication. This scalable, multi-tenant, multi-tier platform also allows customers to enjoy cyber defense as a service from Check Point and its service partners, as well as participate in collaborative defense with other industry sector colleagues.

Each customer ‘domain’ incorporates, consolidates, and correlates event logs from one or more physical and virtual sentries, combining on-premises and cloud visibility into a single picture. Tiering support also enables delegation of duties, so that complex environments can be divided into subdomains, while retaining a birds-eye view and reporting capability for the entire estate, on a single pane of glass.

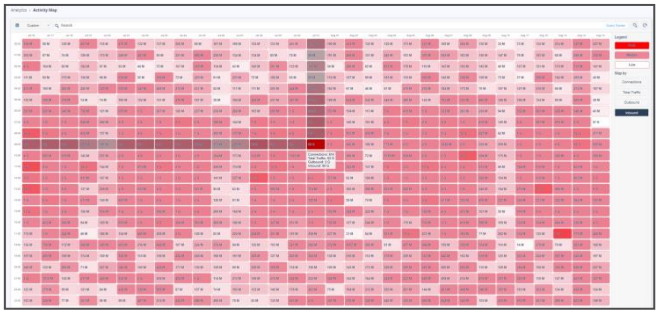


Application and threat visualization appears on the CDC portal within minutes of automated deployment. In contrast with competing solutions that rely only on baselining and behavioral analysis for anomaly detection, SandBlast Now harnesses the power of ThreatCloud threat intelligence and the industry’s largest application fingerprinting library, together with its integrated set of behavioral analytics in order to deliver immediate insights into the traffic patterns, as well as reducing the false-positive noise level that is characteristic of pure-behavioral analysis.

Triage of anomalous network traffic involves a combination of automated analysis and human analysts, working together to ensure timely, accurate and relevant information is delivered for effective response to cyber-attacks. While automated controls excel at sifting through huge amounts of big data and detecting anomalous behavior, human intelligence is still superior when it comes to identifying patterns of unauthorized behavior, weeding out false positives, categorizing events by motive and intent and identifying effective and safe Courses of Action (COAs). This methodology allows identification of initial attack vectors, as well as subsequently subverted hosts and compromised data.



The SandBlast Now threat hunting concept of operations starts with threat indications from the sentry threat prevention engines, driven by real-time ThreatCloud threat intelligence. These are each categorized by confidence and severity. Typically high-confidence detections would also be blocked by the customer’s primary lines of defense (assuming these are up to par). A high-confidence true positive match therefore implies that an attack might have bypassed or penetrated defenses. For example, in the Trickbot example depicted above, the detected beacons serve to incriminate compromised entities on the network. The analyst then pivots on this data set, performing a data flow analysis using CDC tools in order to identify covert communication paths and lateral movement mechanisms. Logs and packet captures can be further analyzed to pinpoint attacker Tactics, Techniques and Procedures (TTPs).



Lower-confidence threat indications are also highly valuable as they can sometimes serve to identify an anomaly that is the “tip of the iceberg” for an otherwise stealthy attack. Analysts triage these detections, correlating them with evidence of anomalous application traffic as well as behavioral transitions pre- and post-detected event. False positives are filtered out to reduce noise.

© 2020 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

CDC Threat Hunting Tools

- **SmartView** – traffic breakdowns by applications, attacks, data flow
- **Logs** - individual logs, as well as associated packet captures and Threat Emulation reports
- **Reports** – batch and scheduled report generation, including Check Point Security Checkup reports
- **Threat Topology** – a heuristics-based flexible graphical mapping of network traffic, supporting rapid identification of anomalous behavior
- **Threat Treemap** – event prioritization across sector, domain, sentry and threat patterns
- **Activity Mapping** – data flow analytics for identifying traffic anomalies such as data exfiltration
- **Vulnerability Sonar** – patent-pending fully-passive detection of exposed, vulnerable and potentially-compromised servers and endpoints
- **Recurrent Connections** – integrated AI-based bot detection
- **InfinitySOC Insights** – add-on AI Machine Learning-based identification of top-priority threats
- **InfinitySOC Investigate** – add-on threat enrichment research tool over ThreatCloud and 3rd party sources
- **ThreatCloud Managed Security Services**, **Incident Response Service** - add-on services, providing the SOC with proactive and reactive support by the industry's cyber experts.
- **Log Export** – to 3rd party SIEM

Beyond threat-based defense, analysts have at their disposal the powerful application and URL fingerprinting and risk categorization capabilities of Check Point Application Control, providing a deep understanding of business flows and anomalous behavior. Application Control incorporates over 8,000 application signatures and over 250,000 social network widgets, covering a diverse range of network traffic categories, from Web browsing, through business applications, and to SCADA and IOT protocols. Identity Awareness can be layered in for a complete User and Endpoint Behavioral Analysis capability.

Network accounting completes the depiction of inter- and intra-network segment and host-level traffic patterns, and mapping anomalous out of hours activities, potential data exfiltration, and undesirable downloads.

PREVENT

Cyber observability's objective is not solely situation awareness – the end goal is incident response, damage assessment, and recovery. In contrast with competing solutions that focus on detection, Check Point espouses prevention across the entire threat kill chain, both pre- and post-infection.

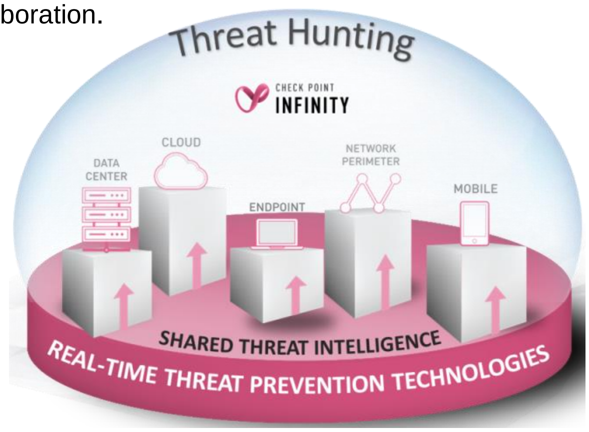
SandBlast Now sentries provide cyber defenders with security control points on monitored networks. When deployed inline, the sentries can be instructed to block malicious traffic, containing the threat, disrupting attacks, and buying precious time for cleanup and remediation.

Threat intelligence in the form of indicators and signatures is at the core of the Infinity architecture's threat prevention engines. The CDC provides a Threat Intelligence Platform (TIP) that allows customer SOCs and service providers to manage large scale repositories of threat indicators that augment Check Point's ThreatCloud intelligence.

Supported indicator types include reputation data on IP addresses, domain and URLs; file and application hashes (MD5 and SHA); and mail fields. Indicators can be fed into the TIP manually, in bulk, as well as using automated input feeds supporting industry standard STIX/TAXII and CSV-based intelligence sharing formats and protocols.

Analysts use the CDC threat hunting tools to identify previously unknown threat indicators. The analytics platform suggests candidates for inclusion in the data set; human analysts review, validate, qualify and commit these additional data points into the repository.

This process creates a feedback loop, delivering a Detect – Analyze – Prevent cycle. Data sets are delivered automatically to SandBlast Now sentries, and can also be published for ingestion by managed Check Point Infinity Security Gateways, as well as supporting inter-domain threat intelligence collaboration.



© 2020 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content