Check Point NOW onboarding page

Product Overview

Check Point CloudGuard IaaS TAP for AWS delivers unparalleled, seamless cyber observability into your AWS environment. The offering includes a CloudGuard IaaS gateway that is automatically deployed via Terraform in the customer's VPC, for performing Deep Packet Inspection (DPI) on inter-VPC ("North-South") and intra-VPC ("East-West") network traffic. AWS Traffic Mirroring is provisioned as part of the Terraform template to selectively mirror network traffic to the CloudGuard IaaS instance for inspection. CloudGuard IaaS TAP's passive operation means that there is zero impact to the business traffic: no added latency, no potential packet loss, nor any need for routing changes within the VPC.

CloudGuard IaaS TAP 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. The analytical results are delivered to a Cyber Defense Center SaaS 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 accessible from the portal provide further deep insight into transmitted file payloads. Insightful reports can be generated and scheduled for tracking compliance posture and providing management visibility.

CloudGuard IaaS TAP is delivered as a plug and play system. Application and threat visualization appears on the Cyber Defense Center portal within minutes of automated deployment. In contrast with competing solutions that rely only on baselining and behavioral analysis for anomaly detection, CloudGuard IaaS TAP combines the power of ThreatCloud threat intelligence and the industry's largest application fingerprinting library 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.

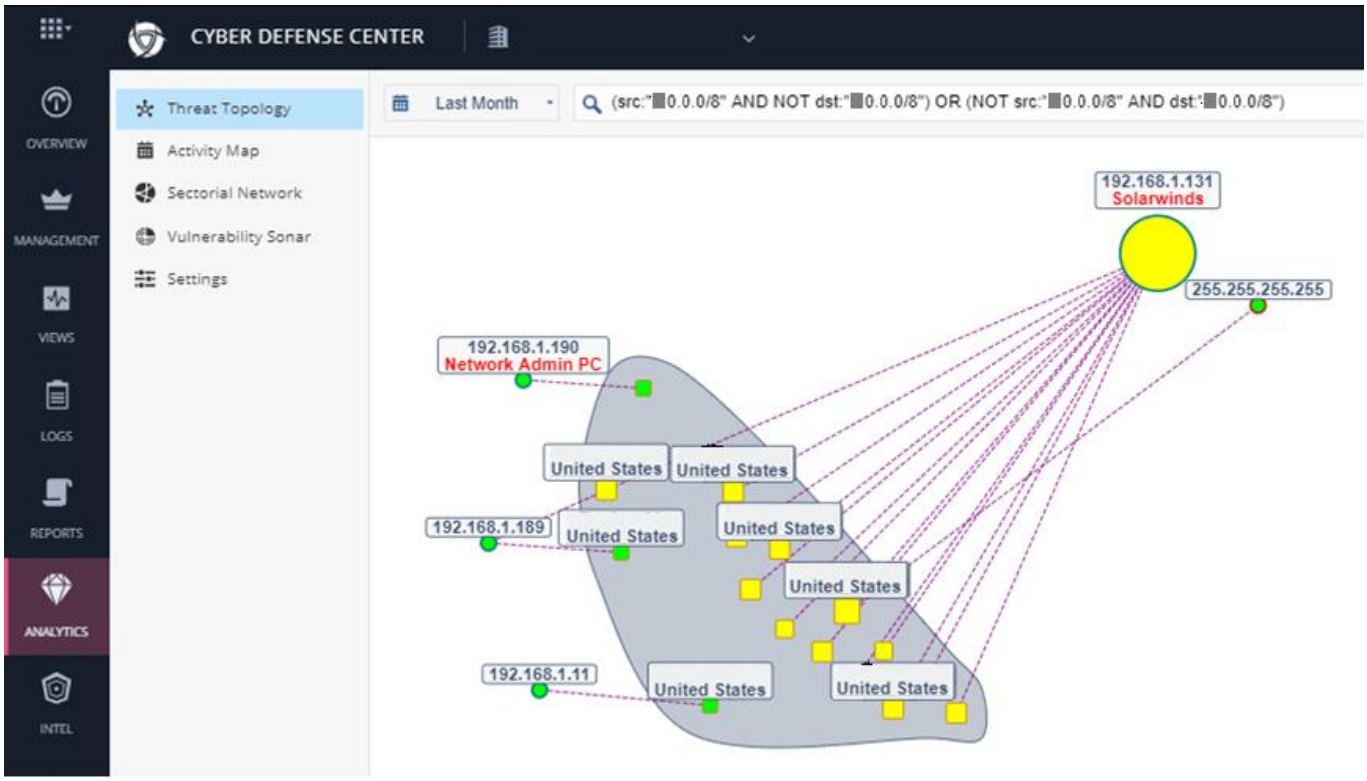
TLS-encrypted network traffic can be transparently decrypted by the CloudGuard IaaS TAP's patent-pending, revolutionary Cooperative Inspection capability. Cooperative Inspection provides true plug and play operation, with no need to pre-register protected servers nor import their certificates. Ultra-fast, 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. Alternatively, CloudGuard IaaS TAP can inspect TLS traffic in its encrypted form, analyzing envelope data, including SNI and certificate attributes, as well as peer endpoints and traffic volumes and periodicity.

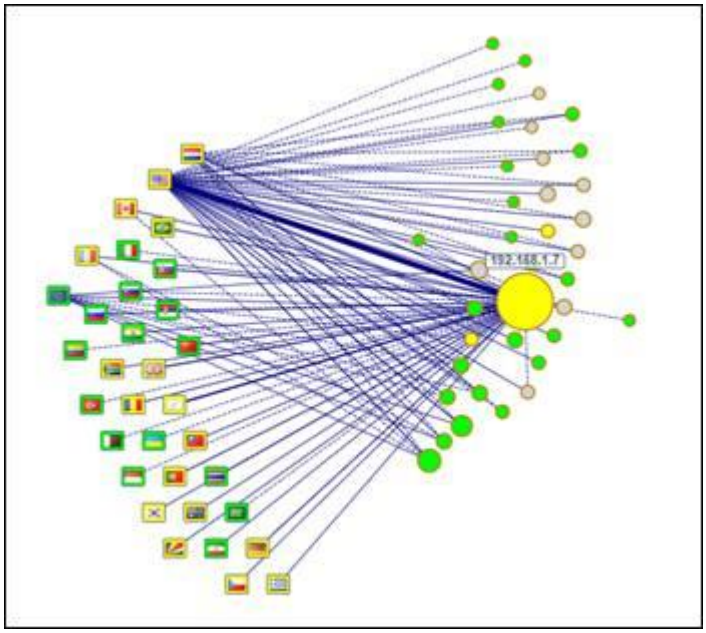
The Cyber Defense Center is a scalable, multi-tenant, multi-tier platform, allowing customers to enjoy cyber defense as a service from Check Point service partners. Tiering support also enables delegation of duties, so that complex environments can be divided into subdomains, while retaining a birds-eye view and reporting capability for the entire estate, on a single pane of glass. Furthermore, the same unparalleled CloudGuard IaaS TAP capabilities can also be incorporated into private cloud and legacy networks, providing end-to-end observability of all IT assets. In addition to SaaS, the Cyber Defense Center can alternatively be purchased as a self-contained private cloud solution.

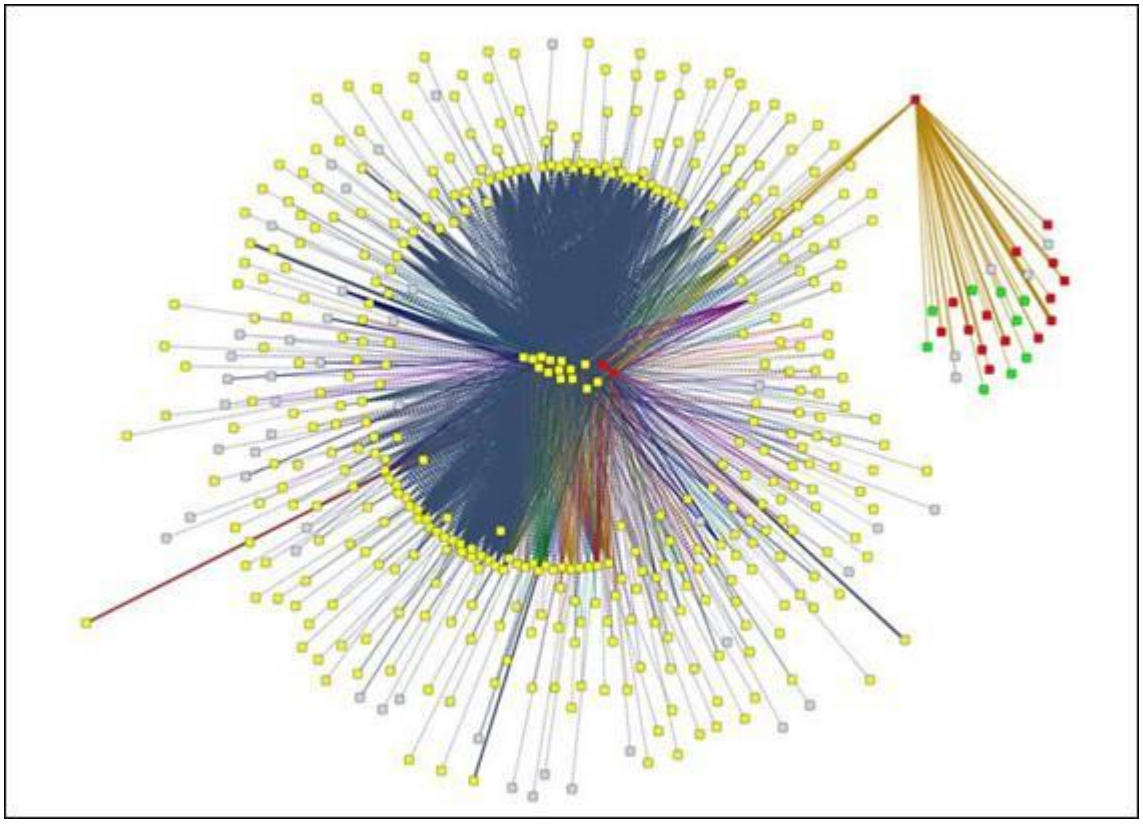
Highlights

- Multiple CloudGuard IaaS TAP instances can be launched for horizontal scalability and high availability, with detected events automatically consolidated on the Cyber Defense Center.
- Fully integrated, real time advanced threat detection capabilities include: IDS, Application fingerprinting, Anti-Virus and Anti-Bot, and Threat Emulation (evasion-resistant sandboxing).
- Some of the advanced analytical tools on the Cyber Defense Center include:
  - Threat Topology – a heuristics-based flexible graphical mapping of VPC network traffic, supporting rapid identification of anomalous behavior
  - 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 – AI-based detection of automation-based flows (i.e. bots)
  - AnalystMind – add-on AI Machine Learning-based identification of top-priority threats
- Integrated Threat Intelligence Platform (TIP) allows SOCs to manage custom threat indicators that augment Check Point's ThreatCloud intelligence. 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 threat intelligence sharing formats and protocols. The TIP's output feeds can also be consumed in real time by inline CloudGuard IaaS gateways, delivering a Detect – Analyze – Prevent cycle.
- Check Point ThreatCloud Managed Security Services and Incident Response Service can be purchased as an add-on, providing the customer's SOC with proactive and reactive support by the industry's cyber experts.

Screenshots





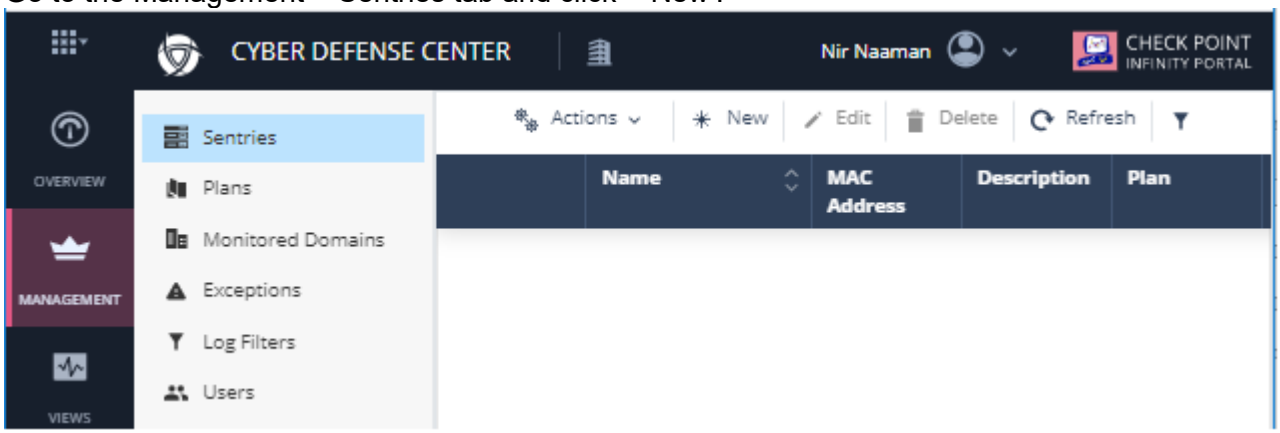


Pricing and Support Information

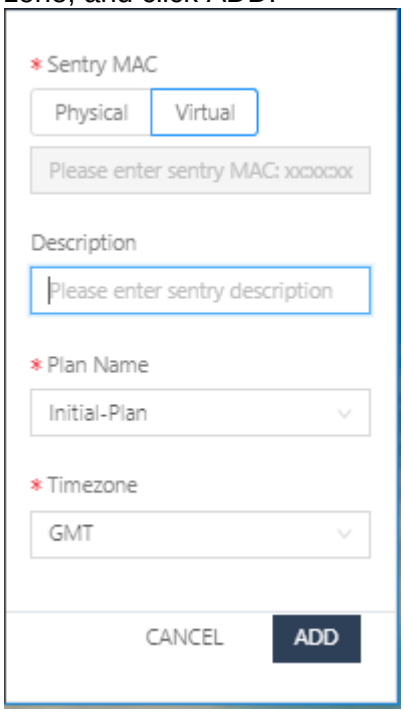
For the Early Availability period, this will be the same as for CloudGuard IaaS with Threat Prevention & SandBlast. Any purchase during this period guarantees the price for one year.

Deployment

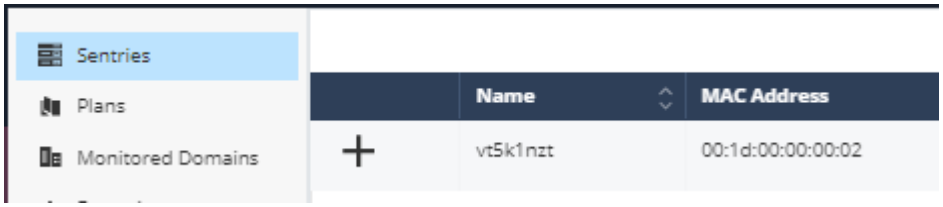
Spinning up a CloudGuard IaaS TAP in your VPC is a cinch!
First, you will purchase a CloudGuard IaaS gateway with Threat Prevention & SandBlast from the AWS marketplace.
A named customer domain must be provisioned on the Check Point now.checkpoint.com SaaS – during the Early Availability period, this must be performed by Check Point. To create a NOW domain fill in the NOW cloud registration form. You will receive an email with a registration link – click that, and a certificate will be automatically generated and provided to you for download and import into your browser.
(Note - some browsers, e.g. Google Chrome, require a restart for the certificate to be activated – kill all instances of the browser, and restart it.)
Now point your browser at now.checkpoint.com. You will be directed into your new domain.
Go to the Management > Sentries tab and click '* New':



The New Sentry pane will open – select 'Virtual', enter an optional description, verify the time zone, and click ADD:



A new sentry entry will appear. It will be uniquely identified by automatically generated ‘Name’ and ‘MAC Address’:



Download the CloudGuard IaaS TAP Terraform module from Github.
For your convenience, you may also download the TAP example files from CloudGuard IAAS Github - TAP example. Edit the example's terraform.tfvars file according to the instructions in the [Readme - Usage] section, using the sentry’s 'MAC Address’ for the *registration_key* variable.
Launch the module using Terraform. As described in the README, this module creates a Check Point CloudGuard IaaS TAP Gateway instance in the VPC specified by the user, along with traffic mirror filter and target, and two lambda functions: ‘TAP Lambda’ and ‘TAP Termination Lambda’. Once the Check Point CloudGuard IaaS TAP Gateway instance is deployed, the TAP Lambda is invoked and scans the entire VPC for mirrorable NITRO instances that meet the configured selection criteria.

Note
The CloudGuard IaaS TAP Gateway instance must have an authorized route out to the Internet established during its startup and normal operation.

Note
Due to an AWS limitation the **maximum number of mirror sources per target** depends on the TAP Gateway instance type.
For a non-dedicated instance type as target, the limit is 10 sources.
For a dedicated instance type, the limit is 100 sources.
CGI supports the following dedicated instance types: **c5.18xlarge** and **c5n.18xlarge**
For more information please refer to AWS Traffic Mirroring quotas and considerations page.

The CloudGuard IaaS TAP initialization typically takes up to 20 minutes. The sentry’s state will change to “Connected” in the now.checkpoint.com portal.
Check the Logs tab to see that network traffic is flowing into the sentry.

Usage

The Cyber Defense Center provides the following functions, selectable by the tabs in the left pane of the portal:

- Overview – an overview of the threat detections on the domain, broken down by threat category
- Management – allows you to manage sentries, plans (privacy policy), users, exceptions and log filters, and subdomains
- Views – traffic breakdowns by applications, attacks, and data flow
- Logs – individual logs, as well as associated packet captures and Threat Emulation reports
- Reports – a batch interface for scheduling various types of reports on the logs
- Analytics – analytical tools for network visualization and threat hunting
- Intel – the Cyber Defense Center TIP

