YOU DESERVE THE BEST SECURITY

DATASHEET

QUANTUM IOT PROTECT NETWORK SECURTY

SECURE EVERY NEW IOT ATTACK SURFACE

Integrated into every aspect of our lives, internet of things (IoT) devices and operational technology (OT) assets automate and streamline operations. Yet every time a smart device is added to our network, it expands the attack surface. This is because connected devices are inherently vulnerable and easy to hack. This explains why 67% of enterprises have already experienced an IoT-related security incident, where the enterprise network was breached. Additionally, Check Point Research (CPR) reported that in the first two months of 2023 alone, there was a 41% increase in the average number of weekly attacks per organization targeting IoT devices, compared to 2022.

Easy to Hack, but Difficult to Patch

While IoT environments have become increasingly complex, IT security solutions have remained far behind, with limited visibility and control over IoT devices and their associated risks. When it comes to securing these devices, the challenge lies in the variety of vulnerabilities found in IoT: legacy Operating Systems, hardcoded or weak passwords, unpatched, and more.

A Complete Network and On-Device IoT Security Solution

From IP cameras to smart elevators, the full Quantum IoT Protect solution secures your company with IoT network security and on-device IoT security. Learn more about on-device IoT Security here.

Focusing on securing the network, Check Point's Quantum IoT Protect Network identifies and analyzes every IoT device in the network. By discovering and turning the IoT devices' attributes, risk parameters, and risk level into a granular IoT policy, and applying the relevant policy across the network on Check Point Quantum firewalls, the IoT attack surface can be minimized.

Secure IoT with AI/ML Powered Cloud Services

Check Point's Quantum IoT Protect's integrated IoT AI/ML engines analyze IoT meta-data found from continuous discovery to identify possible IoT threats and keep you protected. Granular security rules based on device attributes and risks, allow for zero trust network segmentation and prevent unauthorized access to and from IoT devices. As the cybersecurity industry is learning, the high velocity and sophistication of modern cyberattacks makes it impossible for human-managed models to fully protect organizations in real-time. Blocking the most evasive attacks requires innovative technologies that can take the stress away from security professionals.

Secondly, the industry has not effectively leveraged the true power of the cloud to enhance and accelerate on-premises security to keep up with the pace of business. Customers now expect their on-premises network security to quickly evolve with new requirements. Check Point has made strategic developments to quickly and seamlessly expand on-premises Quantum firewall capabilities through cloud-based services, but without forced downtime or otherwise impacting day-to-day operations. Thirdly, there is a huge global shortage of security expertise, and policy creation has become more complex than ever – driving the importance of automation. Security administrators need automation and greater efficiency to eliminate labor-intensive security administration and management.

Lastly, Quantum IoT Protect transforms what used to take security professionals months to achieve (deployment, defining policies, mapping connected assets, and more), and completes everything from deployment and discovery to threat prevention and protection within minutes.

Why Check Point for IoT Network Security

Discovers and protects unmanaged IoT devices in minutes vs weeks or months

Automates everything from discovery to zero trust policy enforcement

Consolidates IT and IoT security into one unified cybersecurity architecture

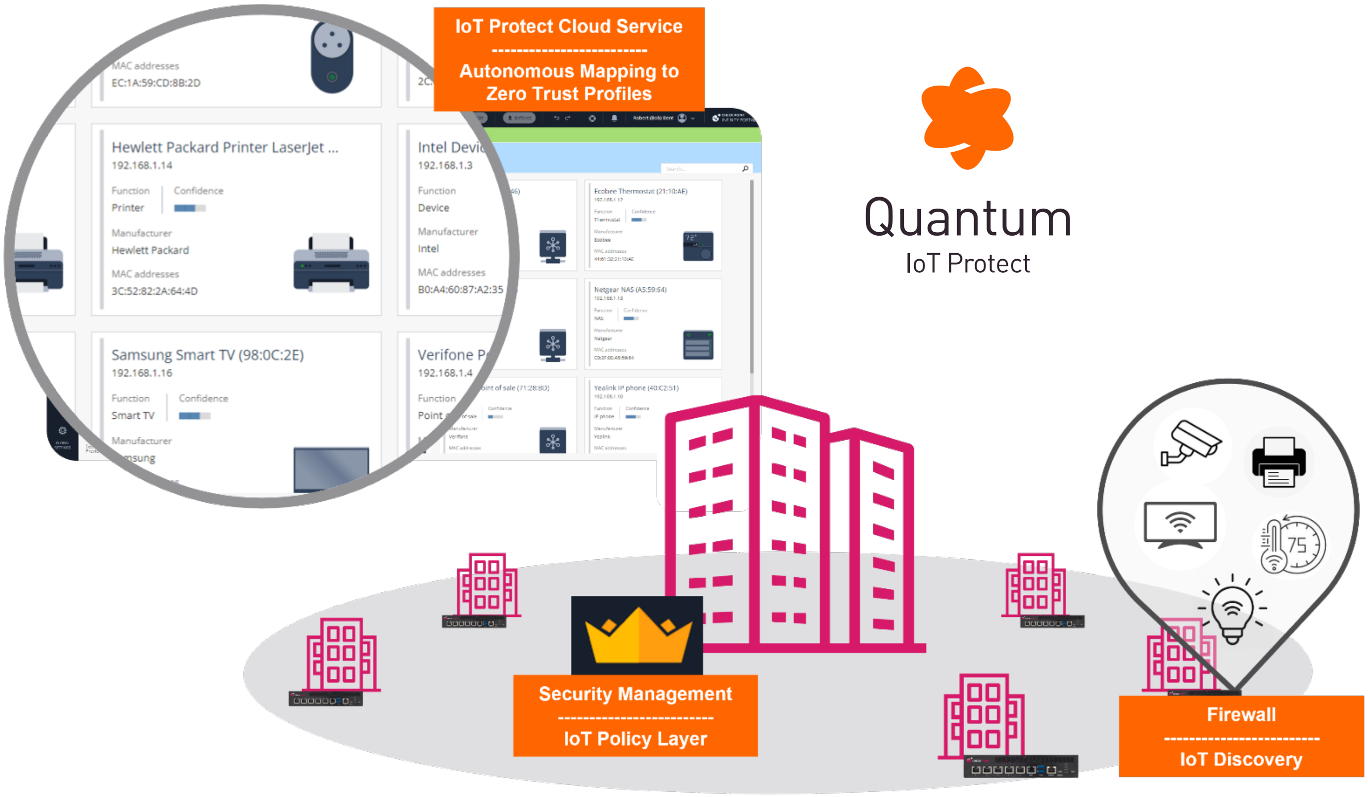
Multi-layered cyber defense solution to protect IoT devices

Highest rated threat prevention against the most evasive IoT cyber attacks

Choice of rugged, small business, branch, and enterprise firewalls

Augments firewall discovery without needing additional equipment

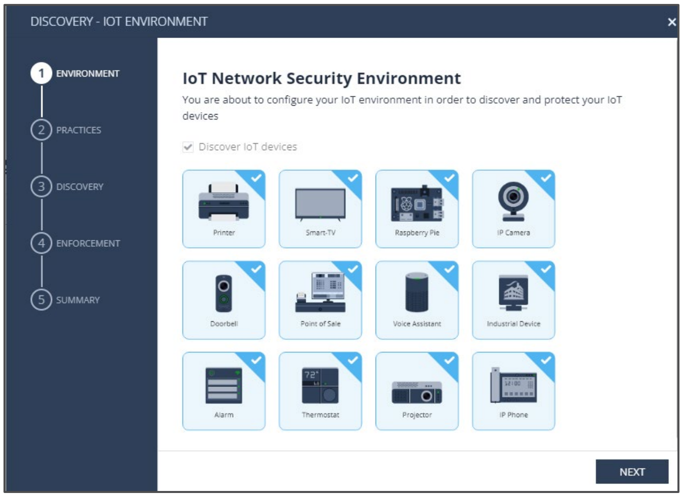
© 2023 Check Point Software Technologies Ltd. All rights reserved. | May 21, 2023



Large Organization with Headquarters and Multiple Branch Offices

GET STARTED WITH IOT PROTECT NETWORK

When you connect the Quantum IoT Protect Cloud Service with your existing Check Point Quantum Smart-1 management and firewalls, it automatically creates the communication infrastructure necessary to discover IoT assets and protect them. There's no need to add additional software or hardware. The Smart-1 Security Management objects and security logs are shared with the IoT Protect Cloud Service. Admins then launch a first-time wizard and select the firewalls they want to initiate the IoT discovery. An agent is then installed on the firewalls, and they begin collecting and sharing discovered IoT asset meta data with the Quantum IoT Protect Cloud Service. Check Point patented technology automatically analyzes, and maps the data into common zones that define the ordered IoT zero-trust policy layer generated for the Smart-1 security management server. When installed on the firewalls in prevent mode, then only the communications necessary for normal operations is allowed. First begin in a Learning/Detect mode to allow any other connections. When ready, change to the Prevent mode to drop any anomalous communications, protecting your IoT devices and preventing infected IoT devices from being used as a launch point by threat actors into your organization.



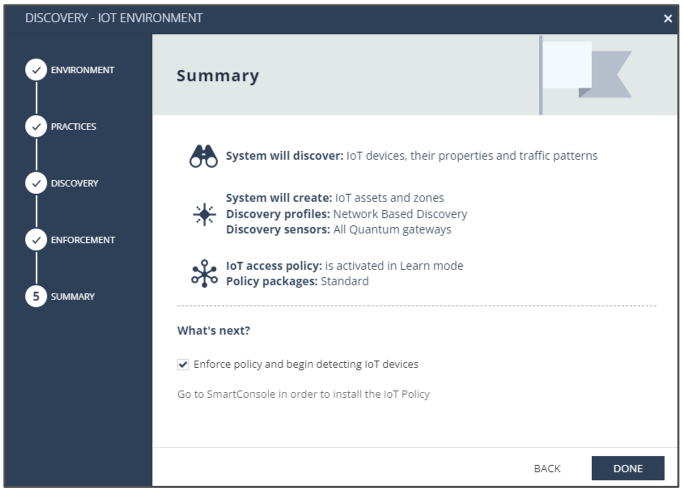
DISCOVERY - IOT ENVIRONMENT

1 ENVIRONMENT
2 PRACTICES
3 DISCOVERY
4 ENFORCEMENT
5 SUMMARY

IoT Network Security Environment

You are about to configure your IoT environment in order to discover and protect your IoT devices

☑ Discover IoT devices



DISCOVERY - IOT ENVIRONMENT

✓ ENVIRONMENT
✓ PRACTICES
✓ DISCOVERY
✓ ENFORCEMENT
5 SUMMARY

Summary

System will discover: IoT devices, their properties and traffic patterns

System will create: IoT assets and zones
Discovery profiles: Network Based Discovery
Discovery sensors: All Quantum gateways

IoT access policy: is activated in Learn mode
Policy packages: Standard

What's next?

☑ Enforce policy and begin detecting IoT devices

Go to SmartConsole in order to install the IoT Policy

IoT Protect Network 5 Step Getting Started Wizard

KEY CAPABILITIES

IoT Discovery

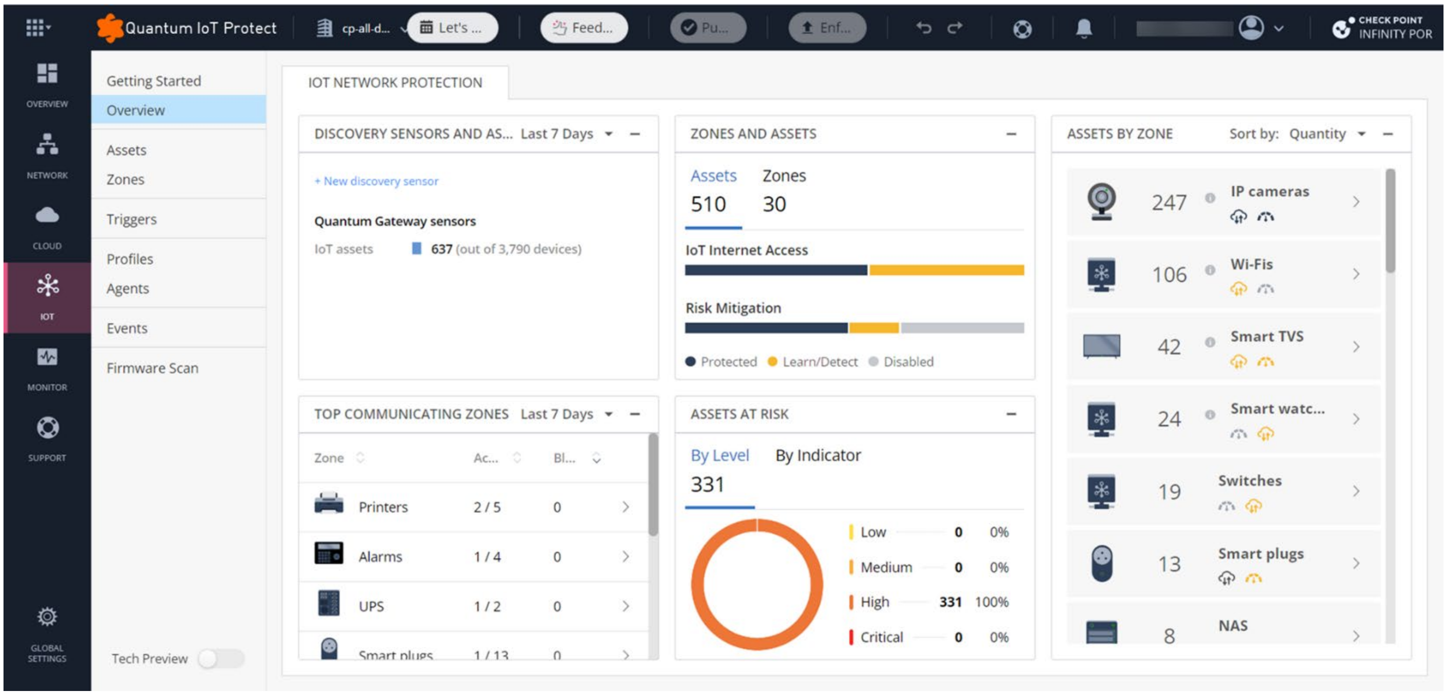
When enabled on Quantum firewalls (enterprise and small business models), discovery uses one of these protocols to query and retrieve data: DNS, Multi DNS (mDNS), uPnP, and SNMP. In some environments, the firewalls may not have visibility into every part of the network. In these cases, additional sensors can be enabled such as SNMP, MS-DHCP (Logs Read from Local Directory), MS-DHCP (Logs Read from Splunk), Unix DHCP (Syslog), Cisco ISE, and Infoblox DHCP (Syslog).

DISCOVERY OPTIONS

- The **Network Sensor** runs on the Check Point Quantum Firewall and detects this asset meta-data: source IP and MAC addresses, destination IP and MAC addresses, DHCP traffic from the DHCP server, HTTP information from the "User Agent" header in HTTP(S) packets.
- The **SNMP Sensor** typically runs on the Smart-1 Security Management server (can also run on the firewall) and retrieves MAC and IP addresses that are detected by an SNMP server. A common SNMP server example is a router.
- The **DHCP Sensor** typically runs on the Smart-1 Security Management server and collects data from these DHCP servers: MS-DHCP, Unix DHCP, Unix DHCP (Syslog feed), Infoblox DHCP Server (Syslog feed).
- The **Cisco ISE Sensor** runs on the firewall and collects data from a Cisco Platform Exchange Grid (pxGrid) system.

Asset Mapping

The IOT Protect Cloud Service AI/ML engines enrich the meta-data collected from discovery and map the IoT devices into common categories, e.g. printers, IP cameras, etc. Asset data includes name, function, manufacturer, model, IP and MAC addresses plus the risk level of the IoT device and confidence level in the mapping process. More detailed information is also available including: VLAN, and security logs associated with the device.



Quantum Gateway sensors

IoT assets 637 (out of 3,790 devices)

Assets	Zones
510	30

Zone	Ac...	Bl...
Printers	2 / 5	0
Alarms	1 / 4	0
UPS	1 / 2	0
Smart plugs	1 / 13	0

Low	0	0%
Medium	0	0%
High	331	100%
Critical	0	0%

247	IP cameras
106	Wi-Fis
42	Smart TVS
24	Smart watc...
19	Switches
13	Smart plugs
8	NAS

IoT Protect Cloud Service Dashboard (orange indicates a Learn/Detect mode policy action)

© 2023 Check Point Software Technologies Ltd. All rights reserved. | May 21, 2023

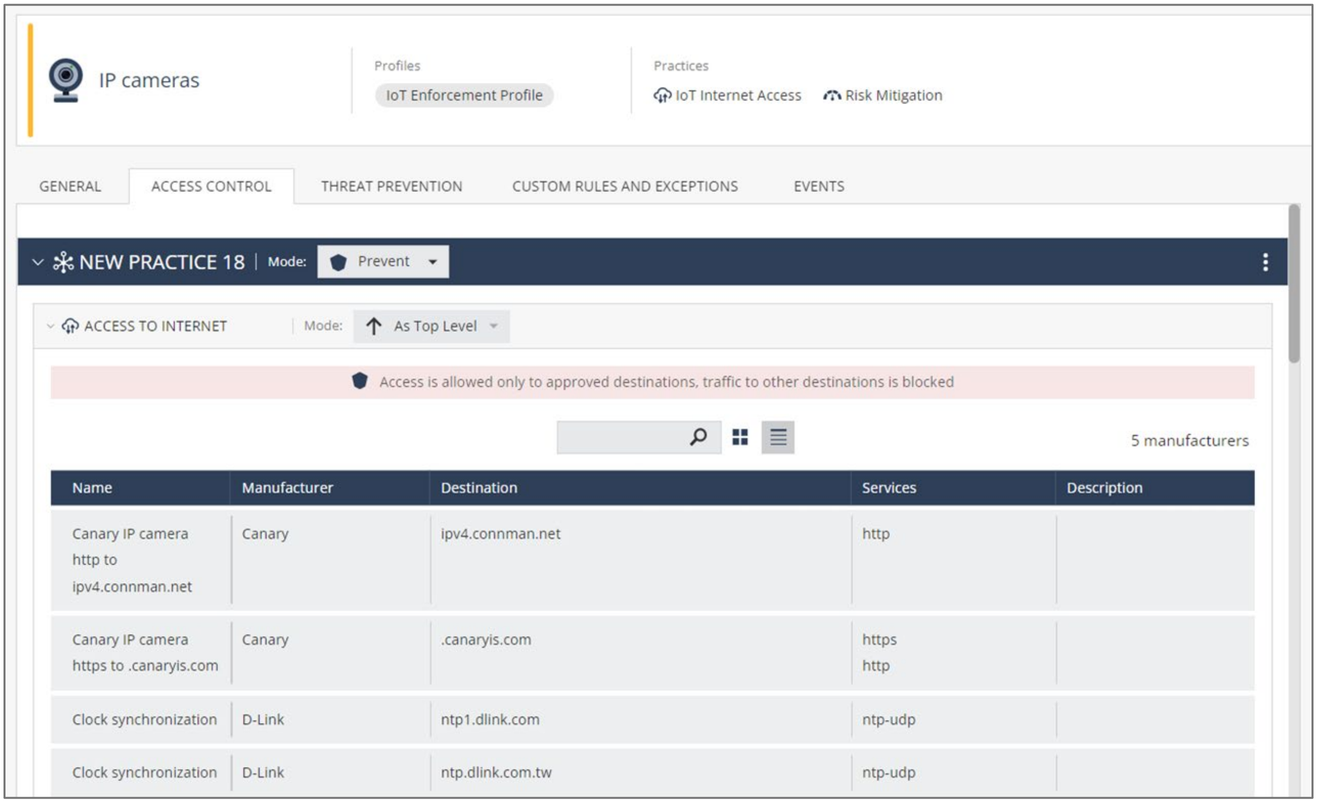
Zone Access Controls, Threat Prevention and Event Logs

Policy for all IoT devices is managed in zones. This simplifies the creation of security policy for thousands of IoT devices. Many devices fall into common categories such as printers or IP cameras. Access control rules are automatically created, saving admins what would take days or weeks to create if they had to do the task manually. If needed, security admins can also create exceptions to the IoT Protect policy, customizing their security to better fit their organization's environment.

Example zones include IP cameras, printers, TVs, VoIP devices, security systems, speakers/amps, doorbells, IP phones, Smart Plugs, thermostats, UPS, remote controls, light objects, Smart Meters, HVAC, sprinklers, conferencing equipment, solar panels, sensors and more.

In addition to the access control policy, there are threat prevention settings. Manage your IoT risk by enabling protections for devices from restricted vendors, devices that use default passwords, have vulnerabilities, and communicate with known bad services. Policy actions Learn/Detect, Prevent, Disable and Block can be applied separately to the Access Control and Threat Prevention policies.

Firewall and IoT security events showing the network communications for each zone are also available in the zones view. When in Prevent mode anomalies stand out as drop events letting you easily see the effectiveness of the IoT Protect autonomous policy for that zone.



NEW PRACTICE 18 | Mode: Prevent

ACCESS TO INTERNET | Mode: As Top Level

Access is allowed only to approved destinations, traffic to other destinations is blocked

5 manufacturers

Name	Manufacturer	Destination	Services	Description
Canary IP camera http to ipv4.connman.net	Canary	ipv4.connman.net	http	
Canary IP camera https to .canaryis.com	Canary	.canaryis.com	https http	
Clock synchronization	D-Link	ntp1.dlink.com	ntp-udp	
Clock synchronization	D-Link	ntp.dlink.com.tw	ntp-udp	

IoT Protect Cloud Service IP Camera Zone Access Control Policy in Prevent Mode

IoT Network Segmentation Prevents Known and Unknown Threats

Fully integrated into our industry-leading Next Generation Firewalls, IoT Protect blocks exploits of known vulnerabilities, and automatically and continuously enforces a zero-trust policy for existing and newly discovered IoT devices. Enable your security and network operations teams to do more with less. Leverage your existing security infrastructure to discover and manage IoT security in minutes.

Smart-1 Security Management Enhanced with IoT Cloud Orchestration

Customers access the IoT Protect Cloud Service via a web browser login to an Infinity Portal tenant. The Infinity Portal provides a single access point to all of Check Point's cloud services. This also includes Smart-1 Cloud security management which is hosted in the cloud. Simply sign up for each service. Objects and logs are shared between the two cloud services. Customers who use on-premises Smart-1 create a trusted connection to their tenant via a simple and secure process and enable object and log sharing. Smart-1 security management then proxies the connections from the IoT Cloud Service to the firewalls it manages. The process enables discovery on the firewalls and creates an IoT policy layer on Smart-1. Because the policy is created by the IoT Protect Cloud service, admins see it as Read-Only in the Smart-1 SmartConsole graphical user interface (GUI).

- **IoT Protect Cloud Service Locations**: EU (Ireland AWS region) and US (North Virginia region), additional regions are planned
- **Meta-data shared with the Cloud**: MAC and IP address, HTTP User Agent, DHCP options, DHCP name and vendor, network and services objects, security logs, policy package objects.
- **Privacy you Can Trust**: IoT Protect Network is compliant with EU GDPR regulations.
- **Smart-1 Security Management Version**: On-prem Smart-1 Security Management R81.20 and above. Smart-1 Cloud is upgraded for you and supports IoT Protect Network.

Quantum Next Generation Firewalls

In addition to the discovery and IoT zero-trust policy enforcement of IoT Protect, Quantum Next Generation Firewalls also do full deep packet inspection to prevent both known and unknown zero-day threats. This is still managed in Smart-1 and includes IPS (intrusion prevention) to prevent exploits of known vulnerable IoT devices, providing IT staff time to safely patch their managed devices. Anti-bot, antivirus and AI/ML powered DNS security detect and block malware throughout the network and are automatically updated by Check Point ThreatCloud AI, Check Point's threat intelligence platform. Quantum firewalls also protect end users from unknown and zero-day threats with zero-phishing, sandboxing, and Content Disarm & Reconstruction technologies.

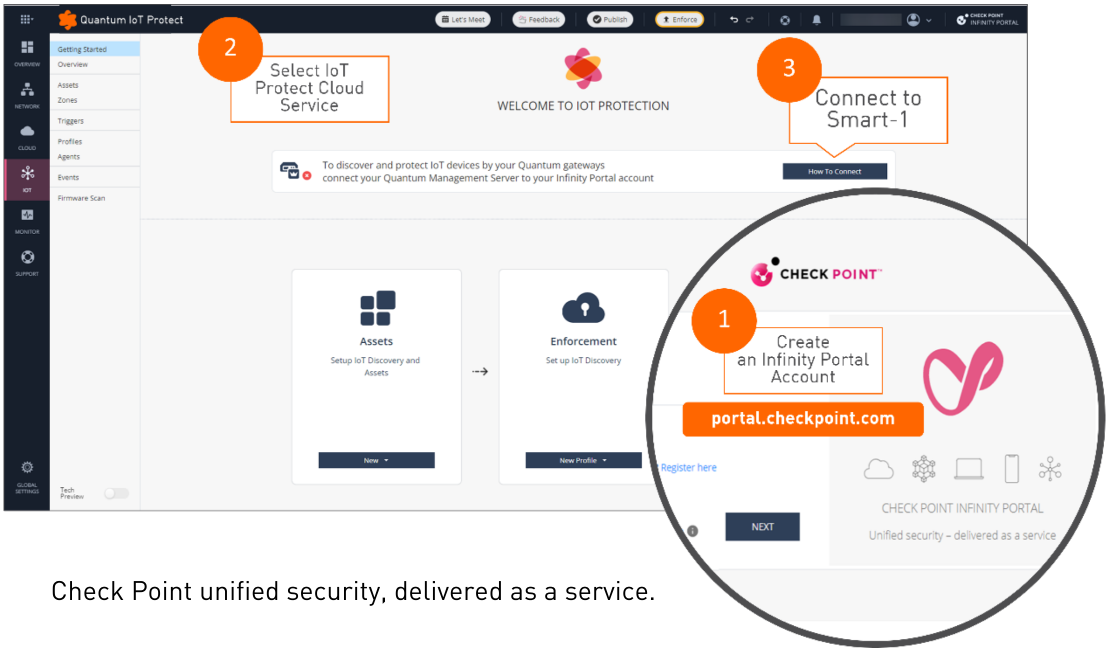
- **Quantum Firewall Version**: Quantum Next Gen Firewall version R81.20 and above (R81.10 support is planned as well)
- **Quantum Spark Version**: Quantum Spark firmware version R81.10.05 and above

TRIAL QUANTUM IOT PROTECT NETWORK TODAY

Create your personal tenant in the Infinity portal at portal.checkpoint.com, your access to Check Point unified security, delivered as a service, and activate IoT Protect.

Already have an active tenant?

Just activate IoT Protect and connect to your Smart-1 management server.



1 Create an Infinity Portal Account

portal.checkpoint.com

2 Select IoT Protect Cloud Service

3 Connect to Smart-1

WELCOME TO IOT PROTECTION

To discover and protect IoT devices by your Quantum gateways connect your Quantum Management Server to your Infinity Portal account

Check Point unified security, delivered as a service.

ORDERING QUANTUM IOT PROTECT

Firewall Security Services Bundle Feature Sets

	NGFW	NGTP	SNBT
Firewall	✓	✓	✓
VPN	✓	✓	✓
Mobile Access	✓	✓	✓
Identity Awareness	✓	✓	✓
Application Control	✓	✓	✓
Content Awareness	✓	✓	✓
Intrusion Prevention System (IPS)	✓	✓	✓
URL Filtering		✓	✓
Antivirus and Anti-Bot		✓	✓
Anti-Spam and Email Security		✓	✓
DNS Security		✓	✓
Threat Emulation (sandboxing)			✓
Threat Extraction (Content Disarm and Reconstruction)			✓
Zero-phishing			✓
IoT Network Protection Services	Optional	Optional	Optional
SD-WAN Network Optimization Services	Optional	Optional	Optional

Optional security capabilities can be ordered a-la-carte or separately.

Firewall Security Service Descriptions

See the table above for security capabilities included in the NGFW, NGTP and SNBT services packages. IoT and SD-WAN are ordered a la carte.

SERVICE	SERVICES HIGHLIGHTS
Next-Gen Firewall (NGFW): segment networks and apply zero trust policy with IPS	• Accept, prevent, schedule, and apply traffic-shaping based controls to application traffic • 10,000+ pre-defined apps or customize your own application • Protect vulnerable systems with 12,000+ IPS protections
Next-Gen Threat Prevention (NGTP): AI Deep Learning DNS security with antivirus and anti-bot prevents threats	• DNS security prevents Command & Control (C2) connections and blocks data theft through DNS tunneling • Antivirus stops incoming malicious files and links in web, email, FTP and SMB content • Anti-Bot detects infected hosts and prevents communications with external C2 servers • Apply web and application control using 100+ categories or customize your own
SandBlast (SNBT): comprehensive, multi-layered defense with sandboxing protection from unknown and zero-day threats	• Average emulation time for unknown files that require full sandbox evaluation is under 100 seconds • Emulation OS Support: Windows XP, 7, 8.1, 10 applications • CPU-level, OS-level and static file analysis • Maximal file size for Emulation is 15 MB
IoT Network Protection: simple, effective, autonomous discovery and protection of IoT devices in minutes	• Passive and active discovery of enterprise IoT devices with autonomous mapping to 200+ profiles • IoT attributes include function, manufacturer, model, risk, confidence, VLAN, IP and MAC address • Automatically creates and applies an inline zero-trust IoT policy layer
SD-WAN: reliable and optimum network connectivity at the lowest cost	• Link aggregation and link prioritization according to latency, jitter, and packet loss • Advanced multi-path orchestration and steering for 10,000+ apps • Sub-second failover for overlay and supported applications • SLA monitoring and autonomous link swapping

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000

www.checkpoint.com

2023 Check Point Software Technologies Ltd. All rights reserved.