CHECK POINT

Secure Your Branch Office in the Age of IoT

Secure your connections and IoT devicees with Quantum IoT Protect

Closing Branch Security Gaps in the Age of IoT

Cyber criminals are getting smarter, leveraging highly sophisticated attacks, and adapting their tactics to identify and exploit any weaknesses in systems to achieve their goals. A growing number of cyber criminals are targeting internet connected IoT devices at branch offices and remote locations which are often far less secure and more vulnerable than the company headquarters.

Any lack of visibility into connected devices that is lacking at an organization's main location is often compounded by a factor of N for every additional remote branch office. Not only are the remote locations not staffed by the same IT or security experts at headquarters, but they are also maintained and operated by different employees and third-party vendors.

Before any IoT devices such as printers, cameras and other Smart systems at these remote offices can be secured, they must first be identified and assessed for risk. Furthermore, significant efforts and resources are then needed to build effective security policies that can protect against the risk these IoT devices create across the various branch locations. This requires allowing normal operational connections for managing, monitoring, and updating the devices while preventing other connections to or from the devices.

These large and geographically distributed organizations need an IoT security solution that automates the discovery and visibility of any connected IoT devices and automatically applies immediate protection of the device and network - all centrally managed from a cloud service with real time IoT threat intelligence.

Protecting Your Branch Offices for Business Success

As organizations move to cloud and SaaS applications, branch offices are also increasing their adoption of Software-defined Wide Area Network (SD-WAN) technologies which offer connections back to corporate via legacy MPLS and direct connections to the Internet. This creates a broad attack surface that can be used to enter the remote network, gain direct access back to headquarters, and possibly cause significant damage.

Take for example the story of a casino in North America where a group of cyber criminals hacked a fish tank in order to steal data from a casino.[1] This specific fish tank was connected to the Internet via the casino's network for remote monitoring—temperature adjustment, feedings, salinity, etc. The hackers were able to steal 10 gigabytes of data from the casino after they had just installed it.

Check Point Quantum IoT Protect

Quantum IoT Protect provides complete protection for your devices within minutes, delivering autonomous threat prevention and zero trust policies to secure your organization and your managed and unmanaged IoT devices.

Quantum IoT Protect provides the ability to autonomously locate, analyze, and determine the security risk of all IoT devices connected to the network. The devices are automatically categorized by device type, category, and vendor and protected with zero trust IoT security policies, preventing unauthorized access all within minutes.

Check Point Quantum Firewalls

Check Point Quantum IoT Protect is integrated into Check Point Quantum R81.xx firewalls providing customers with autonomous policy enforcement and IoT discovery. IoT objects discovered are sent directly to the customer's IoT Protect cloud service tenant. If needed, firewall IoT discovery can be improved and augmented using other network infrastructure components such as SNMP, DHCP and Cisco ISE.

Check Point Quantum Security Management

Check Point firewalls are managed centrally using either on-premises security management server or Smart-1 Cloud. The firewalls receive policies from the management server and in turn send security events and traffic logs to the management server – consolidating security management and threat visibility into a single console.

The security management server shares objects, such as the firewalls it manages and the logs from these firewalls, with the IoT Protect cloud service. In turn, the management server receives IoT objects and the policies from the IoT Protect cloud service and installs it on managed firewalls.

Quantum IoT Protect Cloud Services

After the Quantum security management server is connected to the IoT Protect cloud service, tokens are exchanged, and trust is established to the customer's tenant. With trust established, the management server sends logs and objects to the IoT Protect cloud service. Within Infinity Portal, customers navigate to IoT Protect and launch the Getting Started wizard to choose which firewalls they want to do IoT discovery. Clicking finish sends instructions to the Quantum security management server which enables discovery on the firewalls.

Within minutes, discovered IoT devices are seen in the IoT Protect cloud service and are automatically mapped to zero trust profiles. This becomes a firewall IoT security policy that is sent to the security management server to be installed on the firewalls.

Moving from Detect to Prevent

Initially the policy is set to Learning mode where the default action for the firewall policy is to allow any connections. When ready customers can change this default action to drop so that connections not needed for normal operations are prevented.

Multilayer Security Design for IoT Devices

Quantum IoT Protect empowers businesses to easily secure their IoT devices from headquarters to branch office location through multiple layers of protection:

- Instant IoT Discovery and Risk Analysis
- Autonomous IoT Zero-Trust Network Access.
- Best-of-breed IoT Threat Prevention.
- Unified policy events and management.

Large Organization with Headquarters and Multiple Branch Offices

Benefits

- Eliminate the complexity of managing IoT with an autonomous solution that instantly maps, profiles, and assesses risk for any connected IoT device
- Minimize the attack surface with continuous discovery and full IoT visibility that blocks zero-day attacks with zero-trust profiles
- Prevent malicious IoT traffic with 1000s of NGFW IPS protections, augmented with threat prevention services, and real-time threat intelligence
- Segment IoT devices from production networks to block access to and from infected devices with proven security gateways

About Check Point

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

GET A DEMO:
https://pages.checkpoint.com/iot-demo.html

GET IoT SECURITY CHECKUP:
https://pages.checkpoint.com/iot-security-checkup.html

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

www.checkpoint.com