CHECK POINT™

QUANTUM SOFTWARE R82

FEATURE LIST

Threat Prevention

1. AI-based Prevention Engines

- ThreatCloud Graph—knowledgebase to form relationship attack patterns
- Kronos—Behavioral algorithms detecting malicious activity
- Deep Brand Clustering—Prevent phishing campaigns based on local/global brands
- Dynamic classification of uncategorized websites—Dynamic URL categorization

2. Improved DNS Security Capabilities

- Advanced DNS protection against Non-Existent Domain (NXNS) Attack
- Support for DNS over HTTPS (DoH) protocol
- Configuration granularity—Adv DNS Security settings in the Threat Prevention profile
- Detailed DNS Security statistics—Now available in the SmartView Dashboard

3. Automatic Security Services

- Zero Phishing, Anti-Virus, Anti-Bot and IPS blades more accessible, simpler and easier user experience
  - Zero Phishing Automatic mode—simplifying the configuration to make activation even easier
  - Anti-Virus and Anti-Bot blades are now activated by default in newly created gateways/clusters—SK182106
  - Automatically load and update SNORT rules file as IoC feed, enforced as new IPS protections

4. Web Security

- Support of HTTP/3 protocol over QUIC transport (UDP) for Network Security, Threat Prevention, and Sandboxing

5. HTTPS Inspection

- **Enhanced UI—fully managed from SmartConsole**
  - Enhanced policies
    - Dedicated policy for inbound inspection
    - Enhanced default outbound policy
    - Certificate management views for inbound and outbound policies
  - Trusted CA package—New view to manage Trusted certs
  - Advanced settings—New view to configure advanced settings, including R82 new features
- **Client Side Fail mode**
  - Automatically detect client-side SSLi failures, such as pinned certs, and automatically flags connections to be bypassed in future attempts. AI learning capabilities from these failures to identify similar connections.
  - Endpoint Detection—Identifies endpoints without deployed outbound CA certificate
- **Bypass under load**
  - Optional bypass in case of high CPU load
- **Learning mode**
  - Gradual & Smart deployment
    - Activated during deployment of SSLi, inspecting minor percentage of traffic over two weeks
  - Network Learning
    - Collects insights into network behavior and detects potential connectivity issues for AI consideration
  - Performance Prediction
    - Estimates the performance impact on Security Gateways when HTTPS inspection is fully implemented
- **HTTPS Inspection Monitoring**
  - SSLi statistics view within SmartView, including bypass/inspect stats

Security Gateway

1. New Clustering Technology

- ElasticXL (active/active Orchestrator-less cluster)
  - Single management object (SMO) for simplified configuration of all cluster members
  - Automatic sync of configuration and software packages between all cluster members

2. Dynamic Access Layer

- Fully automated API-controlled dynamic policy layer implementing changes to the GW in seconds

3. Identity Awareness

- New PDP-Only mode allowing GW to act only as a policy decision point
- New identity sharing cache mode to improve resiliency
- Gateway's can now use IDP's defined within Infinity Portal. Centralizing managed identities across multiple products

4. Remote Access

- Gateway's support IKEv2 protocol for Client to Site remote access (E88.40 or higher)

5. Performance and Infrastructure

- HyperFlow support for SMB/CIFS and QUIC protocols

6. IPsec VPN

- **Support for ML-KEM (Kyber768), required for FIPS 203. Uses Post-Quantum Cryptography (PQC)**
- **Automatic detection and adjustments of configuration changes in AWS, Azure, and GCP**
- **Enhanced Link Selection**
  - Interoperability
    - Uses Public IP address as tunnel identifies to establish separate tunnels for each link
    - Support for Dead Peer Detection (DPD) as link probing
  - Redundancy—VPN tunnel redundancy including third-party and native cloud VPN peers
  - Granularity—Ability for the gateway to use different VPN interfaces in different VPN communities
- **Advanced VPN Monitoring tool showing health and performance of tunnel**

7. Mobile Access

- **Mobile Access Policy and Capsule Workspace configurations are now in SmartConsole**
- **SAML authentication support for Mobile Access clients**
- **New Management API calls for Capsule Workspace configuration**

8. Dynamic Routing

- **Added support for new dynamic routing capabilities**
  - BGP Extended Communities (RFC 4360)
  - BGP Conditional Route Advertisement and Injection
  - Routing Table Monitor for Event Triggers
  - IPv4 and IPv6 Router Discovery on cluster members
  - Router Preference and Route Information option
  - Route age information
  - IPv4 PIM-SSM with non-default prefixes
  - IPv4 PIM with BFD
  - IPv4 PIM neighbor filtering
  - IPv4 PIM RPT to SPT switchover control
  - IPv6 Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD)
- **Added support for new dynamic routing API calls**
  - REST API calls for: BGP, PIM, MLD, Route Redistribution, Inbound Route Filters, NAT pools, and IGMP

9. Quantum Maestro, Scalable Chassis, and ElasticXL

- Support REST API calls on Maestro Orchestrator to configure and monitoring Security Groups, Sites, and Ports. Including Gaia REST APIs on Scalable Platform Members
- Support First Time Wizard on Orchestrators, with ability to configure Maestro Site settings
- Support for SNMP queries on each Scalable Platform Member
- Support for LLDP on Uplink, Sync, and Management ports of Orchatrators
- New Ports page showing a summary and interactive view of port configuration
- New Cluster Management pafe showing state and performance of Scalable Platform Members
- New CLI tool "insights" to monitor entire cluster in both Expert and gClish
- New gClish commands "show cluster" and "set cluster"
- Improved boot time and reduction in required reboots of Scalable Platform Members when there is a change in the Gaia OS config
- Automatic CPUSE Deployment Agent updates on Scalable Platforms
- Removed the requirement of "sp_upgrade" script starting with upgrades to R82 or higher
- Additional snapshot mechanism for small Gaia OS snapshots (lightshots)

10. VSNext

- New VSX architecture
  - Simpler configuration, easier & faster provisioning, and a similar experience to a physical Security Gateway. Upgrade as a regular gateway
  - Unified management experience between physical Security Gateways and Virtual Gateways, including capability to manage each BS from a different Management Server
  - Management features and API parity between VS GW and physical GWs
  - Improved provisioning performance/experience
    - Create, modify, delete Virtual GWs and switches in Gaia portal, Clish, or REST API
  - Management of different Virtual Gateways with different Security Management Servers, in addition to different Domain Management Servers on the same Multi-Domain Security Management Server

11. New Tools and Utilities

- "connview"—consolidated troubleshooting tool for viewing connections on the Gateways running in User Space Firewall (USFW) mode
- "up_execute"—performs virtual Access Control / NAT Rule Base execution. Given inputs based on logs or connections, the execution provides detailed information such as matched rules and classification information

Gaia OS

(Applies to Gateways, Management and Log Servers)

1. New OS kernel

2. Enhancements in OS

- Support for Link Layer Discovery Protocol in VSX mode
- DHCPv6 server, DHCPv6 client, and DHCPv6 client for prefix-delegation in Gaia Portal and Gaia Clish
- Ability to configure order of "AAA" authentication (TACACS, RADIUS, Local auth) in Gaia Portal and Clish
- DNS Proxy forwarding of domains. Allows configuring specific DNS servers per DNS suffix

3. New items in OS

- Two-Factor Authentication for Gaia OS login using authenticator apps (Google/Microsoft Authenticator)
- Support NTP pools and a larger number of NTP servers
- NFSv4 configuration
- Keyboard layout
- TLS configuration for a remote Syslog server

4. Backups in Gaia Portal

- Support for cloud backup into Amazon S3 and MSFT Azure Storage
- Ability to notify on scheduled backups
- Restores provide must more detail
- Backup date, Hostname, Hardware, Version, JHF take, Role
- Restore verification checks if restoring into a different version/take

Management

1. SMS Enhancements

- Use of LDAP Account Unit object server name and cert for LDAP trust
- VSX GW and Cluster configurations via Management API
- Data Type object definition for DLP and Content Awareness via Management API
- Management of Gateways with SMS behind public cloud or third-party NAT device
- Manage up to 500 Gateways/Cluster Members with concurrent policy installation on all
- Support SAML login on SmartConsole with Gaia portal on a different port than 443. SK182032
- Ability to verify Access Control policy with unpublished changes

2. SmartConsole

- Enhanced Gateways & Server view to see and manage recommended JHF and Updates for Gateways and Host objects
- HealthCheck Point (HCP) tests are integrated and visible as part of the Gateway Status (disabled by default)

3. Central Software Deployment

- SmartConsole enhancements to include:
  - Uninstallation of Jumbo Hotfixes
  - ClusterXL High Availability mode "Switch to higher priority cluster member"
  - Ability to upgrade Secondary Management servers, Dedicated log servers, Dedicated SmartEvent servers, Standalone servers
  - Clusters of Spark appliances
  - Package Repository per Domain on Multi-Domain Management Server

4. Web SmartConsole new capabilities

- Threat Prevention rule base
- HTTPS Inspection rule base
- NAT rule base
- Rule base search

5. SmartProvisioning adding Star VPN community support for Maestro and VSX

6. Multi-Domain SMS

- Ability to clone an existing Domain on the same Multi-Domain SMS
- Improved upgrade time of large environments
- Support for IPv6 configurations
- Automatic refresh of modified Global objects
- Ability to select the Access Control, Threat Prevention, or both policies in a Policy Preset object

7. Compliance

- Gaia OS Best Practices for Maestro Security Groups, Quantum Spark Appliances, Management, and Log servers
- Added new regulations
  - Center for Internet Security Benchmarks
  - Cyber Essentials v3.1
  - Cybersecurity Maturity Model Certification
  - Essential Eight & Strategies to Mitigate Cyber Security Incidents
  - IEC 62443-2-1 201
  - ISO 27001:2022
  - Israeli Cyber Defense Methodology 2.0
  - Network and Information Systems Directive 2
  - PCI DSS 4.0
  - TISAX 5.1

CloudGuard Controller

- Identity Awareness PDP (Identity Sharing)
- Policy Mode APIs for importing of objects from NSX-T Manager
- Supports VMware NSX-T Global Manager to allow integration with VMware NSX-T v4.1
- Multi-Domain SMS support for Data Center Objects and queries within the Global Policy

Harmony

Endpoint Web Management

- **Client optimization for Windows Servers**
- **Performance Diagnostic checks as a push operation on endpoint clients**
  - Reports CPU and RAM status
  - Presents suggestion exclusions for performance improvements
- **Easier addition of exclusions for Global or Per Rule exclusion. Exclusions can now have a description added for comments**
- **Application control for macOS**
- **New/Updated Asset Management views**
  - Filters
  - Asset Management Table
  - Columns reorder
- **Linux Offline package support**
- **Harmony Endpoint Management API support for on-premises server (disabled by default)**

References

R82 Release Page with Key Links

sk181127—Check Point Quantum R82