



Cisco Security Architecture Summit: For partners to receive updates and roadmaps from the BUs on the solutions and technologies being developed.

## Firewall Protection:

### Secure Firewall:

- **Firewall +AI Assistant:** Use AI Assist function within CDO console. (Dec 2023)
- **Firewall + SSE = ZTNA:** Client based ZTNA access no matter where user is. (Future)
- **200G & 400G Network modules & Optics:** Faster interface support. (v7.6)
- **Clustering with Multi-Instance on 3100 & 4200:** Data Center deployments. (v7.6)
- **Integration with Secure Client for NVM:** Network Visibility Module. (v7.6)

### Meraki MX:

- **Z4 Advanced Teleworker:** All basic security plus additional features. (Nov 2023)
- **Improved Performance:** Up to 3x on MX75, MX250, MC450. (MX18.2)
- **vMX in AWS:** SDWAN Firewall with up to 10Gbps VPN throughput. (MX18.2)
- **Firewall Logging Live Tool:** See firewall log flows live on console. (MX18.2)
- **Trusted Traffic Exclusions:** Bypass AMP or IDS/IPS inspection as needed. (MX18.2)
- **Adaptive Policy – Cloud-Managed TrustSec:** Security Group Tags. (MX18.2)
- **Multi-WAN:** 2 Active (primary uplinks) + 1 Backup. (MX18.2)
- **Firewall Simplification:** 1 network-level FW policy spanning L3, L7 & VPN. (Future)
- **Org-Level Unified Firewall:** Spanning MX and Cisco+ Secure Connect. (Future)

## User Protection:

### Cisco Duo:

- **IP Based Config:** Configure IP lists for corporate infrastructure. (GA)
- **RBA Monitoring Mode:** Score and display risky authentications. (Early Access)
- **Browser-based Cont. Trust:** Encrypt tokens, prevent stolen cookies. (1H2024)
- **OIDC Refresh Tokens:** Extend sessions without frequent re-auth. (Jan 2024)<sup>1</sup>
- **AD Password Mgmt.:** Enable user to reset expired password. (Jan 2024)<sup>1</sup>
- **Unenrolled User Lockout:** Set number of days a user must enroll. (Jan 2024)
- **Duo Desktop for Linux:** Red Hat/CentOS, Debian, Ubuntu. (Sept 2023)
- **Zero Trust from Apple Devices:** All Applications, Ports, Protocols. (Soon)
- **Device API Support for Linux:** API support for Linux to sync w/Duo. (Dec 2023)
- **VM & Win Server Support:** Device Health App for VM & Win Server. (Dec 2023)

### Identity Services Engine (ISE):

- **Wi-Fi Edge Analytics:** Device Analytics attributes for Apple/Intel/Samsung. (v3.3)
- **AI Analytics:** Machine Learning, Endpoint Smart Grouping in cloud. (v3.3)
- **Secure RADIUS & TACACS w/IPSec:** Device Admin using 3<sup>rd</sup> party. (v3.3)
- **Enhanced ISE + Duo Integration for MFA:** AD integration supported. (v3.3.1)

### Cisco Secure Access:

- **Resource Connectors - AWS:** Inside to out L4-7 tunnels from RCs. (Jan 2024)

### Umbrella:

- **FedRAMP Moderate:** For Federal and SLED consideration. (July 2024)<sup>1</sup>

## Breach Protection:

### Extended Detection & Response (XDR):

- **Identity Threat Detection & Response:** Coming from recent Oort acquisition. (Soon)
- **New Incident Generation:** Secure Email, Secure Endpoint, Proofpoint, etc. (Jan 2024)<sup>1</sup>
- **New Incident Generation:** Meraki, Oort, Secure Access, Checkpoint, etc. (July 2024)<sup>1</sup>

### Secure Endpoint: Bonus!

- **Compensating Controls:** Temporary fix/patch with Exploit Prevention. (Future)
- **Response Initiated Actions:** Remote scripts powered by Orbital (EDR & XDR). (Oct 2023)
- **Host Firewall Controls:** API and Console-based Rules Management (Win & Mac). (Future)

### Secure Network Analytics (SNA): Bonus!

- **Firewall logs to Detections:** SNA detections with a firewall as a telemetry source. (Dec 2024)
- **Backward Compatibility (SW):** Re-use Managers, Flow Collectors & Sensors. (Dec 2024)
- **New Detections:** LDAP Connection & Outbound LDAP Spikes, Protocol Forgery etc. (v7.4.2)

### Secure Email Threat Defense: Bonus!

- **Compromised Account Detection:** Alert on suspicious patterns or origin. (Beta)
- **Inline Mode:** Message Acceptance (inbound / outbound). (Apr 2024)
- **Inline Mode:** Filtering, Advanced Policy & Quarantine. (July 2024)

Bonus: Items not fully covered at the Partner Security Architecture Summit

## Cloud Protection:

### Multicloud Defense: (GA Sept 2023)

- **Hybrid Cloud:** Integration of CDO to manage on-premise ASA and FTD. (July 2024)<sup>1</sup>

### Panoptica: (Cloud Application Security)

- **Serverless Scanning:** Azure & GCP. (Dec 2023)
- **MITRE Dashboard:** (Dec 2023)
- **Recon.Cloud port to V2:** (Dec 2023)
- **OWASP GenAI Top Ten:** (Future)

## Random Related Links:

<a href="#">Summit Presentations</a>	<a href="#">Firewall Essentials</a>	<a href="#">Secure Access</a>
<a href="#">Summit Q&amp;A Team Room</a>	<a href="#">Firewall Performance Estimator</a>	<a href="#">XDR</a>
<a href="#">Fire Jumper Academy</a>	<a href="#">Firewall Migration Tool</a>	<a href="#">Multicloud Defense</a>
<a href="#">Security Suites At-a-Glance</a>	<a href="#">Feature Matrix</a>	<a href="#">Panoptica</a>
<a href="#">SalesConnect – Sec Products</a>	<a href="#">Cisco Defense Orchestrator</a>	<a href="#">Secure Connect</a>