Security Architecture Summit (May 2023) v1

Notice: The content listed below are just a few highlights from the latest Security Architecture Summit. Not yet released features are subject to change. For more detailed updates, refer to the Community link posted.

Cisco Partner
https://cs.co/1page

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

Network Security: (Day 1)

Secure Firewall:

- **EVE:** Block malicious encrypted traffic based on threat score w/o decrypt (v7.4)
- **CSDAC:** Available in FMC, standalone and cloud-delivered form factors (v7.4)
- **WAN Summary:** WAN Summary dashboard for high-level overview (v7.4)
- **Hyper-V:** Support for Secure FMC Virtual (FMCv-25) (v7.4)
- **OpenConfig:** Streaming telemetry; interface metrics, CPU & memory util. (v7.4)
- **Multi-Instance:** As with 4100 & 9300, 3100's now support Multi-Instance (v7.4)
- **4200 Series:** VPN crypto accelerators, IPSec offload, FIPS compliance etc. (Future)

Multicloud Defense[1]**:** Secure cloud networking platform (GA - August 2023)

- Seamlessly access Cisco Multi-Cloud Defense from CDO portal
- Tiered licensing (Essentials, Advantage, Premier)
- Orchestrate, manage, control and secure cloud infrastructure

Cisco Defense Orchestrator (CDO):

- **Low Touch Provisioning (LTP):** Extend CDO onboarding for on-prem FMC's (v7.4)
- **RAVPN:** Consolidate RAVPN Monitoring Dashboard in CDO (v7.4)
- **FTD Provisioning:** Provision Firewall in any public cloud using a few clicks (Beta)
- **Migration Tool:** Cloud-delivered Migration Tool available as part of CDO (Beta)

SSE / Cloud: (Day 2)

Umbrella:

- **Multimode DLP:** Discover, enforce and maintain compliance (GA)
- **Real Time DLP:** Analyze data-in-transit, monitor and block file uploads (GA)
- **Exact Data Matching (EDM):** Increases accuracy, eliminate false positives (GA)
- **Generative AI:** App Category including ChatGPT support; monitor/block etc. (GA)
- **Compliance Data Classifications:** GDPR, HIPAA & PCI-DSS data violations (GA)
- **DNS Rulesets:** Extend workflow available in Web Policy to DNS Policy (EFT)
- **FedRAMP:** Authority to Operate (ATO) Gov DNS + shared controls (July 2024)
- **KeyAdmin API:** An API for managing APIs (GA)
- **BlueCat:** DNS, DHCP, IPAM (DDI) Provider (Available)

Cisco+ Secure Connect:

- **Enhanced Posture:** Anti-Malware, Firewall, Disk Encryption (GA)
- **Clientless ZTNA:** Turnkey solution for least privileged access (Regionally Avail.)
- **Policy Import:** Allows admins to import Meraki firewall policies (Available)
- **Unified SASE:** Unified experience, future-proof architecture (mid-July 2023)
- **Cisco+ Secure Connect NFR:** Available for all partners (March 2024)

Cisco Secure Access:

- **SSE Stack:** Evolution of Umbrella SIG to Unified SSE (Future - multi-phased)

Threat Intel, Detection & Response: (Day 3)

Extended Detection & Response (XDR):

- **Essentials:** Security analytics, Threat Intelligence, Response actions + more (GA – July 31)
- **Advantage:** Essentials + 3rd party telemetry (GA – July 31)
- **Premier:** Advantage + Managed Services (Soon)

Secure Endpoint (EDR):

- **Dashboard update:** Show more details in the UI, optimal for wide screens (Latest UI)
- **Computer Details:** Endpoint details, isolation events, Threat Hunting reports etc. (Latest UI)
- **Action Panel:** Easily take actions; starts isolation, forensic snapshot etc. (Latest UI)
- **Private Cloud:** Device Control, new Endpoint UI (v4.x)

Secure Network Analytics (NDR):

- **New Alerts:** LDAP connection spike, Repeated Umbrella Sinkhole, Protocol Forgery (v7.4.2)
- **Backward Compatibility:** No need for forklift upgrades to achieve success (v7.4.2)
- **M6 Hardware:** Performance for flow searches has been enhanced by at least 26% (v7.4.2)
- **Federal Certifications:** FIPS,CC, IPv6 and DoDIN (v7.5.0 – Jan 2024)

Secure Email Threat Defense (ETD):

- **Compromised Accounts:** Message based, location, additional Talos telemetry (July 2023)

Cisco Attack Surface Management (CASM): Formerly Cloud Insights

Zero Trust: (Day 4)

Cisco Duo:

- **Renamed packages:** Essentials (MFA), Advantage (Access), Premier (Beyond) (Available)
- **Trusted Endpoint:** Now available on all packages (Available)

Secure Workload:

- **Reporting:** Persona driven reporting dashboard and downloadable PDF reports (v3.8)
- **Domain based inventory:** Deeper visibility with the ability to view FQDN details (v3.8)
- **ADM Efficacy:** For Kubernetes or containerized workloads (v3.8)
- **Platform & Scale:** Large Appliance (75k Workloads), Small Appliance (20K Workloads) (v3.8)

Identity Services Engine (ISE):

- **ISE + Meraki:** Define groups (Tags), ACL's and policies (ISE 3.2 Patch 1)

Random Related Links:

Summit Presentations
Summit Q&A Team Room
Fire Jumper Academy

XDR SalesConnect
XDR At-a-Glance
XDR Buyers Guide

Secure FW Essentials
Secure FW AppID
Secure FW Migration
Partner Roadmap Series

[1] Name pending brand approval

Available | Targeted availability | Estimate

WO-06122023