Security SEVT (February 2021)

Notice: The content listed below are just a few highlights from the latest Cisco Security SEVT. For more detailed updates, refer to the Community link posted or contact your Cisco Channel team.

Cisco Partner

Cisco Security **SEVT:** Quarterly session for internal and select partners to receive updates and roadmaps from the BUs on the solutions and technologies being developed.

SecureX & SASE:

SecureX:

- **Posture as a Service**: Data from *Duo, Orbital, MDM* etc. into 1 holistic view (July 2021)
- Cisco will **host relays** in cloud for supported 3rd party devices (coming soon)
- **False Positive/Negative** feedback option (coming soon)
- **Auto Omit** in Threat Response (coming soon)

SASE:

- New SASE "**Bundle**" offer (coming soon)
- **SASE subscription** service (future)

Access & Endpoint:

Secure Endpoint: *(formerly AMP for Endpoints)*

- **USB** device access control (July 2021)
- Expanded Linux support: **AWS Linux**, **SUSE**, **Debian** (July 2021)
- **False positive/negative** reporting in console (July 2021)
- Orbital support on macOS (CY2022)
- **Secure Client**: (e.g., *Secure Endpoint Orbital, Umbrella, Duo, AnyConnect*) (Nov 2021)

Secure Malware Analytics: *(formerly Threat Grid)*

- New ***Suspicious*** Verdict: Previously Clean, Malicious & Unknown (July 2021)
- **macOS support**: macOS Binaries for analysis (CY2022)

Secure Email: v14.0 *(formerly ESA and CES)*

- Password protected file analysis (July 2021)
- *Internal Mailbox Defense* embedded *in Cloud Email Security* interface (July 2021)

Secure Cloud Mailbox: *(formerly Cloud Mailbox Defense)*

- GrayMail Classifications (March 2021)
- dCloud Instance (GA)
- Rolling 30-day POV reporting: showing incremental value over MS (Spring 2021)

Network Security:

Meraki MX:

- AnyConnect on Meraki MX16 firmware (all but MX64) w/PLUS License (Open Beta)
- Network Based Application Recognition (**NBAR2**) on Meraki MX, MS & MR (MX16 Beta)
- **Adaptive Policy** on MX is similar to SGT's (Security Group Tag) (MX16 Beta)
  - Provide enforcement on Tags
  - Enforce access entire SD-WAN fabric
- **IDS** (Snort v3) Multi-Threaded increased throughput (not on MX64/65) (MX16 Beta)
- **SD-WAN over Cellular**: Use LTE as an active uplink for any policy (MX16 Beta)

Cloud Security:

Umbrella:

- **De-ID:** Anonymization Reporting w/in Dashboard (GA)
- **Recategorization Tool** – FP & FN reporting available for customers (future)
- **DNS over TLS:** DNSsec for encryption and support DNS over HTTPS (future)
- **SIG Advantage:** New package with L7 CDFW (Malware Analytics capable) (July 2021)

Secure Web Gateway (SWG):

- **Full Proxy** capabilities for all Web Traffic including additional functions (GA)
- **AnyConnect**: Entitlement to AnyConnect w/SIG Essentials package (GA)
- **Time Based Policy:** Time of Day/Week, apply rule to a specific rule (April 2021)
- **SSL Resumption** (NAT as a Service); persistent IP for HTTPS sessions (April 2021)
- **Rule Based Policy:** Apply to Identities, Users, Groups, Tunnels, Categories etc. (LA)
- **Remote Browser Isolation** (RBI): Available to Full-Proxy or DNS-only (July 2021)

Cloud Delivered Firewall (CDFW):

- **Layer-7 IDS/IPS**: Snort layer of detection of Malware, Botnet, CnC etc. (April 2021)

Cloud Access Security Broker (CASB):

- **App-Discovery**: Discover about 20,000 applications and control 3,000 (up 20%) (GA)
- **Cloud Malware**: Identify Malware at-rest with AMP & 3rd Party AV (in coming months)
- **In-Line DLP**: 80+ classifiers and configure custom key-words (in coming months)

Remote Access (RAaaS): (new)

- Secure Remote access to private apps using *AnyConnect* via *Umbrella* (Oct 2021) *
- Role Base Access & Posture control (future)

Secure Web: *(formerly WSA)*

- Umbrella integrations (July 2021)
- Mandatory Smart Licensing (July 2021)

** Initial release w/1k user min.*

Visibility & Segmentation:

Duo:

- **Passwordless:** *WebAuthn* standards (Windows Hello, Mac Touch ID etc.) (July 2021)
- **Trust Monitor**: Machine Learning to learn "normal behavior" of every user (GA)
- **Provisioning/De-provisioning:** Applications a new user needs & vise-versa (CY2022+)
- **Continuous Trusted Access**: Enforcement post log-in for SaaS Apps (CY2022+)

Secure Network Analytics: *(formerly Stealthwatch Enterprise)*

- **Network Visibility Module (NVM):** (July 2021)
  - Ingest off-premise data (regardless if assets is on someone else's network)
  - AnyConnect Agent as primary telemetry source (**nvzFlow**)
- **Cisco Telemetry Broker:** (new) (April 2021)
  - Telemetry FROM anything TO anything
  - Addition of **VPCFlowlogs** transforming to NetFlow, send *VPCFlowLogs* to on-prem

Available | Targeted availability | Estimate

SEVT PPT's and VOD's: https://community.cisco.com/t5/security-documents/training-global-security-sevt/ta-p/3609563