SWS Computersysteme AG

SWS
COMPUTERSYSTEME
Member of ACP Group

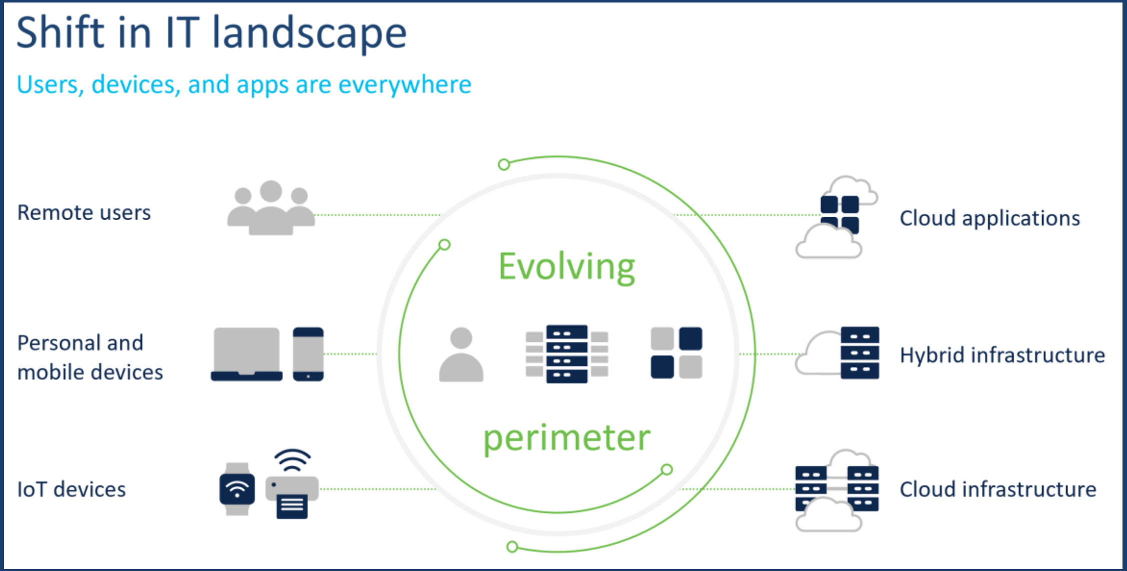
Cisco Secure Endpoint und Cisco Umbrella - Better together

Agenda

- Endpoint und Perimeter Security
- Cisco EDR – Secure Endpoint
- Secure Endpoint – Visibility, Threat Hunting - Demo
- Cisco SASE – Umbrella SIG
- Umbrella SIG - Demo
- Q&A

Endpoint und Perimeter Security

- Bedrohung durch Malware und Sicherheitslücken
- Verschiebung des Perimeters in Richtung Internet
- Cloud Nutzung
- Homeoffice and Remote Worker

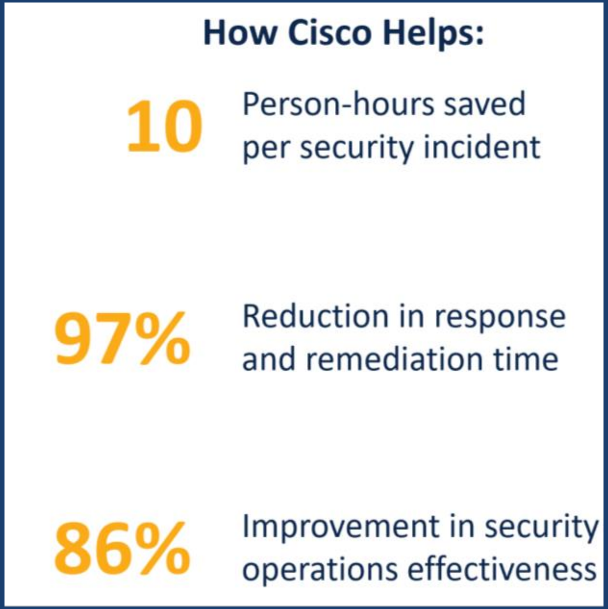


Shift in IT landscape

Users, devices, and apps are everywhere

Endpoint Security Herausforderungen

- Expertise
  - Bedrohungen analysieren, bewerten und abwehren
- Zeitmanagement
  - Alarme und Ereignisse bearbeiten
- Ursachenfindung
  - Patient Zero ausfindig machen und Lücken schließen

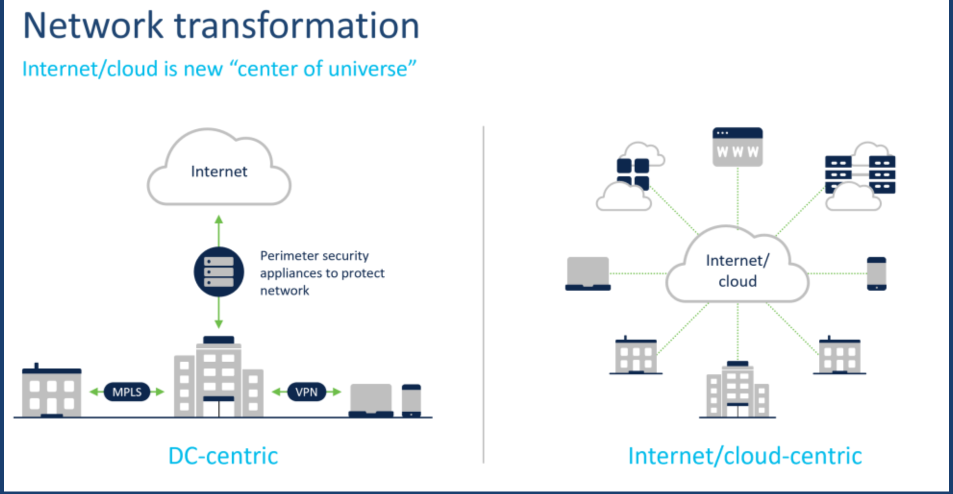


How Cisco Helps:

10	Person-hours saved per security incident
97%	Reduction in response and remediation time
86%	Improvement in security operations effectiveness

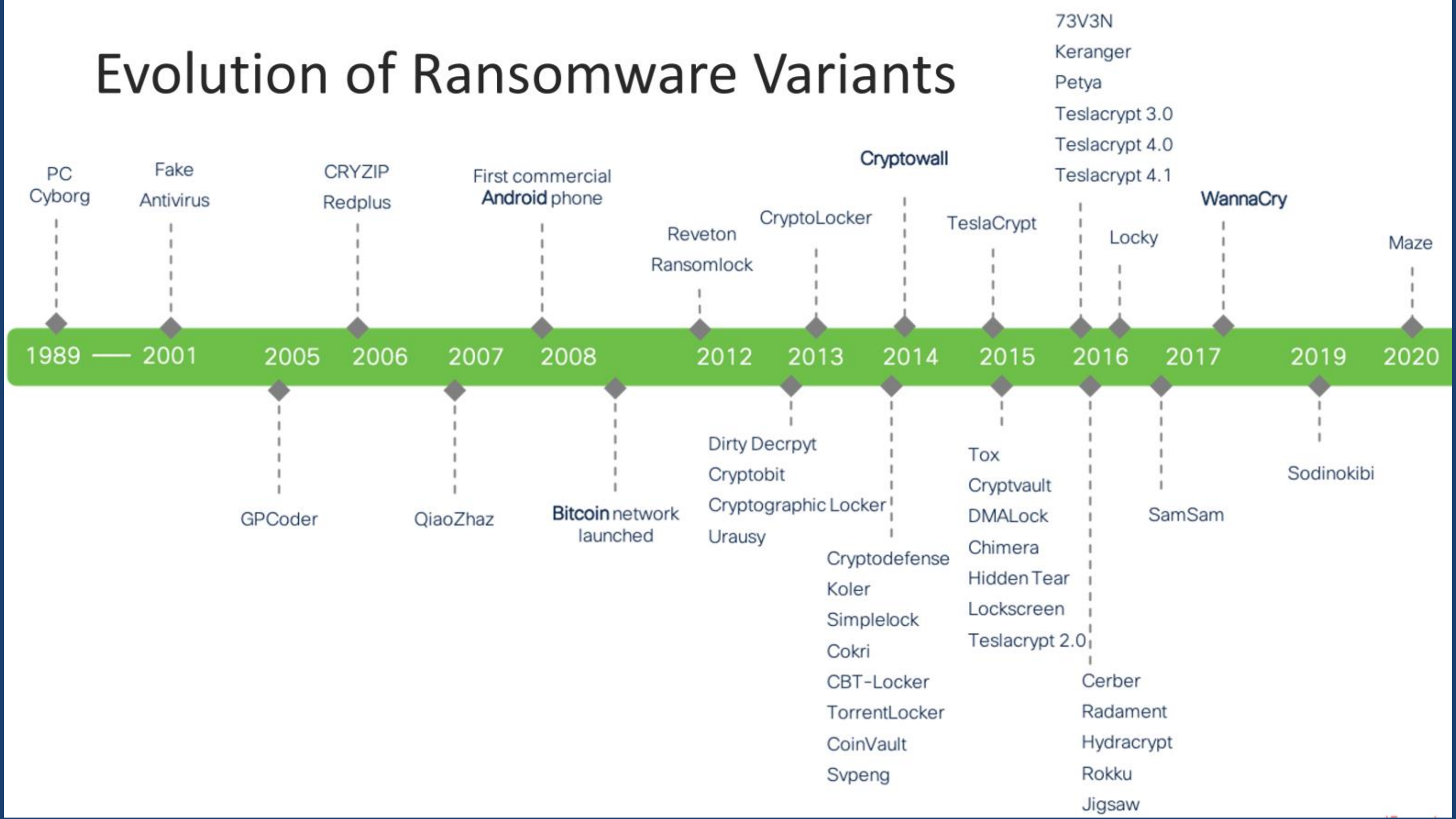
Perimeter Security Herausforderungen

- Konnektivität
  - Ressourcen müssen von überall erreichbar sein
- Einheitliche Security Richtlinien & Management
  - Zentrale Security vs Dezentrale Security
- Undurchsichtige Produktlandschaft
  - Sehr viele Hersteller mit unterschiedlichen Ansätzen und Dashboards



Network transformation

Internet/cloud is new “center of universe”



Evolution of Ransomware Variants

1989 — 2001 2005 2006 2007 2008 2012 2013 2014 2015 2016 2017 2019 2020

PC Cyborg

Fake Antivirus

GPCoder

CRYZIP
Redplus

QiaoZhaz

First commercial **Android** phone

Bitcoin network launched

Reveton
Ransomlock

CryptoLocker

Dirty Decrpyt
Cryptobit
Cryptographic Locker
Urausy

Cryptowall

Cryptodefense
Koler
Simplelock
Cokri
CBT-Locker
TorrentLocker
CoinVault
Svpeng

TeslaCrypt

Tox
Cryptvault
DMALock
Chimera
Hidden Tear
Lockscreen
Teslacrypt 2.0

73V3N
Keranger
Petya
Teslacrypt 3.0
Teslacrypt 4.0
Teslacrypt 4.1

Locky

Cerber
Radament
Hydracrypt
Rokku
Jigsaw

WannaCry

SamSam

Sodinokibi

Maze

Letzte Bastion - Endpoint

- Endpunkte sind ein beliebtes Angriffsziel
- Mitarbeiter können so direkt angesprochen werden -> Identity Fraud und Phishing
- Facettenreiche Schutzszenarien erforderlich durch Homeoffice, Remote Workers, usw.
- Verschlüsselte Verbindungen erschweren die Schutzmöglichkeiten durch Firewalls, IPS,…

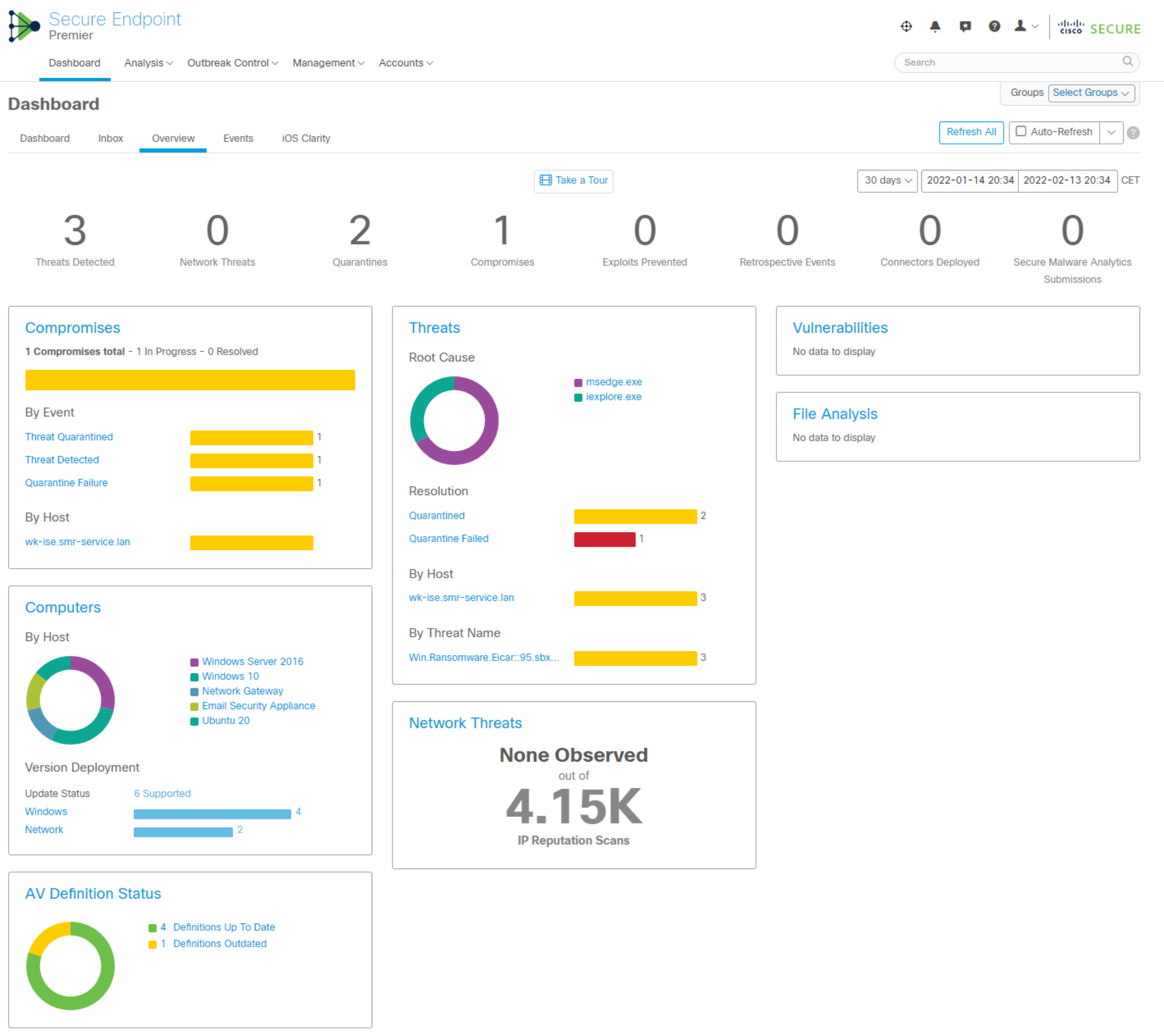
Image source: https://commons.wikimedia.org/wiki/File:Soccer_goalkeeper.jpg (public domain)

Agenda

- Endpoint und Perimeter Security
- Cisco EDR – Secure Endpoint
- Secure Endpoint – Visibility, Threat Hunting - Demo
- Cisco SASE – Umbrella SIG
- Umbrella SIG - Demo
- Q&A

Secure Endpoint

- Cloud Managed Dashboard
- Connectoren für Windows, Linux, Mac, Android, iOS
- Powered by Talos Intelligence
- EU Datacenter in Irland
- Datei Sandboxing, Hash Analyse, uvm.
- Integration mit Cisco Secure Portfolio
- Threat Hunting mit SecureX



Dashboard

2022-01-14 20:34 2022-02-13 20:34 CET

3	0	2	1	0	0	0	0
Threats Detected	Network Threats	Quarantines	Compromises	Exploits Prevented	Retrospective Events	Connectors Deployed	Secure Malware Analytics Submissions

Compromises

1 Compromises total - 1 In Progress - 0 Resolved

By Event

Threat Quarantined	1
Threat Detected	1
Quarantine Failure	1

By Host

wk-ise.smr-service.lan

Computers

By Host

■ Windows Server 2016
■ Windows 10
■ Network Gateway
■ Email Security Appliance
■ Ubuntu 20

Version Deployment

Update Status	6 Supported
Windows	4
Network	2

AV Definition Status

■ 4 Definitions Up To Date
■ 1 Definitions Outdated

Threats

Root Cause

■ msedge.exe
■ iexplore.exe

Resolution

Quarantined	2
Quarantine Failed	1

By Host

wk-ise.smr-service.lan	3

By Threat Name

Win.Ransomware.Eicar::95.sbx...	3

Network Threats

None Observed

out of

4.15K

IP Reputation Scans

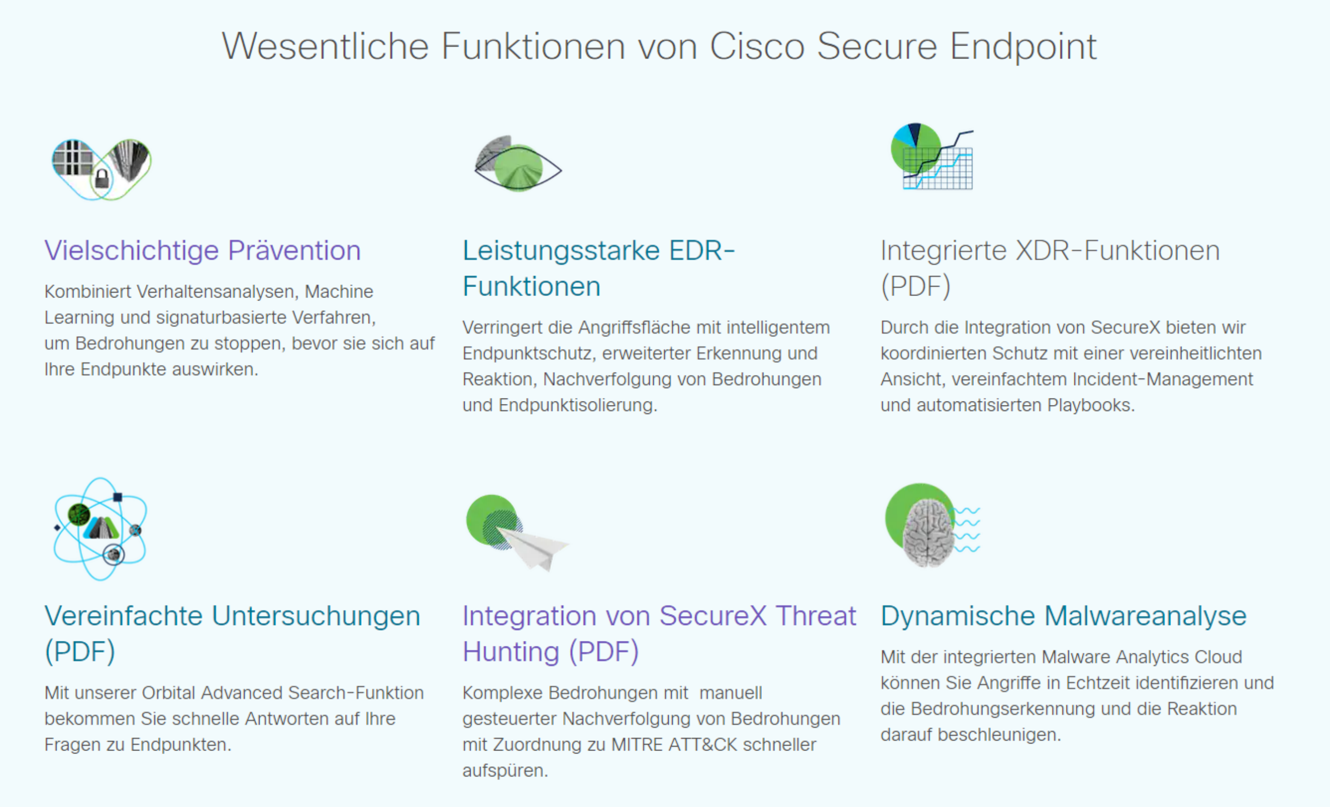
Vulnerabilities

No data to display

File Analysis

No data to display

Secure Endpoint



Wesentliche Funktionen von Cisco Secure Endpoint

Vielschichtige Prävention

Kombiniert Verhaltensanalysen, Machine Learning und signaturbasierte Verfahren, um Bedrohungen zu stoppen, bevor sie sich auf Ihre Endpunkte auswirken.

Leistungsstarke EDR-Funktionen

Verringert die Angriffsfläche mit intelligentem Endpunktschutz, erweiterter Erkennung und Reaktion, Nachverfolgung von Bedrohungen und Endpunktisolierung.

Integrierte XDR-Funktionen (PDF)

Durch die Integration von SecureX bieten wir koordinierten Schutz mit einer vereinheitlichten Ansicht, vereinfachtem Incident-Management und automatisierten Playbooks.

Vereinfachte Untersuchungen (PDF)

Mit unserer Orbital Advanced Search-Funktion bekommen Sie schnelle Antworten auf Ihre Fragen zu Endpunkten.

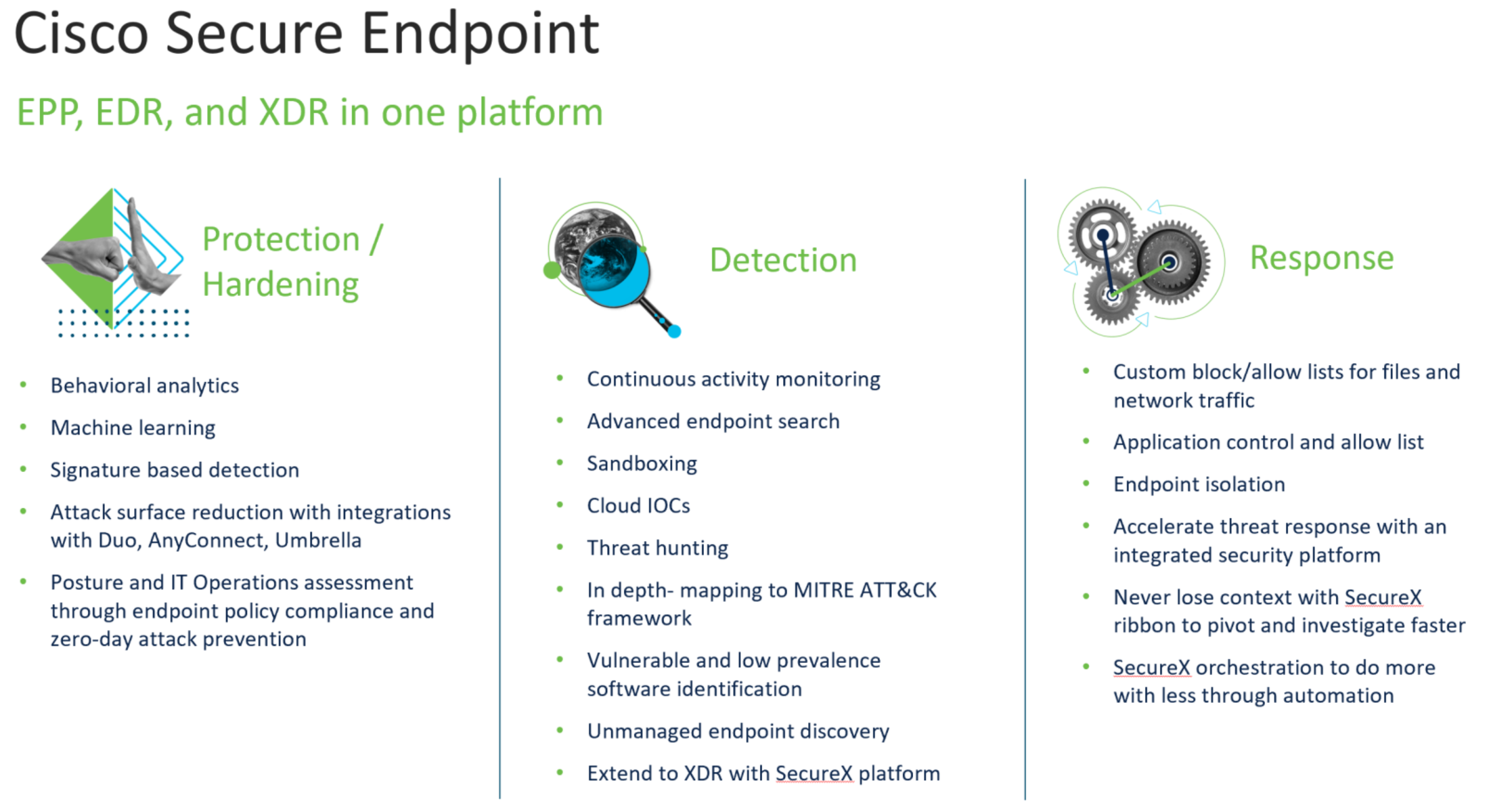
Integration von SecureX Threat Hunting (PDF)

Komplexe Bedrohungen mit manuell gesteuerter Nachverfolgung von Bedrohungen mit Zuordnung zu MITRE ATT&CK schneller aufspüren.

Dynamische Malwareanalyse

Mit der integrierten Malware Analytics Cloud können Sie Angriffe in Echtzeit identifizieren und die Bedrohungserkennung und die Reaktion darauf beschleunigen.

Secure Endpoint



Cisco Secure Endpoint

EPP, EDR, and XDR in one platform

Protection / Hardening

- Behavioral analytics
- Machine learning
- Signature based detection
- Attack surface reduction with integrations with Duo, AnyConnect, Umbrella
- Posture and IT Operations assessment through endpoint policy compliance and zero-day attack prevention

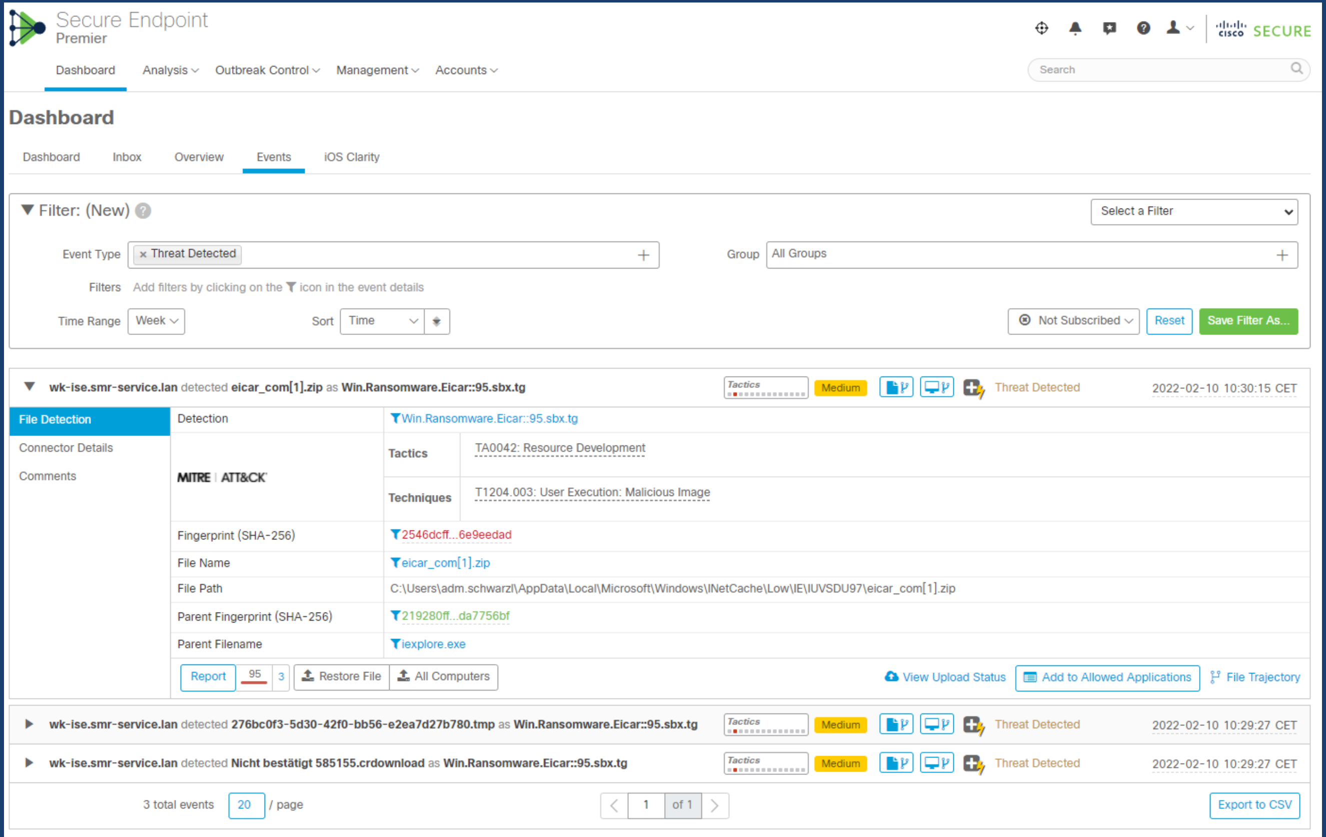
Detection

- Continuous activity monitoring
- Advanced endpoint search
- Sandboxing
- Cloud IOCs
- Threat hunting
- In depth- mapping to MITRE ATT&CK framework
- Vulnerable and low prevalence software identification
- Unmanaged endpoint discovery
- Extend to XDR with SecureX platform

Response

- Custom block/allow lists for files and network traffic
- Application control and allow list
- Endpoint isolation
- Accelerate threat response with an integrated security platform
- Never lose context with SecureX ribbon to pivot and investigate faster
- SecureX orchestration to do more with less through automation

Secure Endpoint - Detection



Filter: (New)

Select a Filter

Event Type: × Threat Detected

Group: All Groups

Filters: Add filters by clicking on the icon in the event details

Time Range: Week

Sort: Time

wk-ise.smr-service.lan detected **eicar_com[1].zip** as **Win.Ransomware.Eicar::95.sbx.tg** | Tactics | Medium | Threat Detected | 2022-02-10 10:30:15 CET

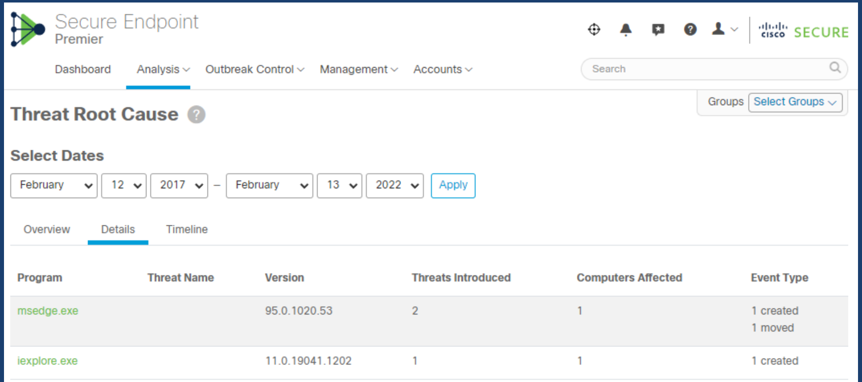
Detection	Win.Ransomware.Eicar::95.sbx.tg	
MITRE ATT&CK	Tactics	TA0042: Resource Development
	Techniques	T1204.003: User Execution: Malicious Image
Fingerprint (SHA-256)	2546dcff...6e9eedad	
File Name	eicar_com[1].zip	
File Path	C:\Users\adm.schwarzl\AppData\Local\Microsoft\Windows\INetCache\Low\IE\IUVSDU97\eicar_com[1].zip	
Parent Fingerprint (SHA-256)	219280ff...da7756bf	
Parent Filename	iexplore.exe	

wk-ise.smr-service.lan detected **276bc0f3-5d30-42f0-bb56-e2ea7d27b780.tmp** as **Win.Ransomware.Eicar::95.sbx.tg** | Tactics | Medium | Threat Detected | 2022-02-10 10:29:27 CET

wk-ise.smr-service.lan detected **Nicht bestätigt 585155.crdownload** as **Win.Ransomware.Eicar::95.sbx.tg** | Tactics | Medium | Threat Detected | 2022-02-10 10:29:27 CET

3 total events 20 / page

Secure Endpoint - Detection



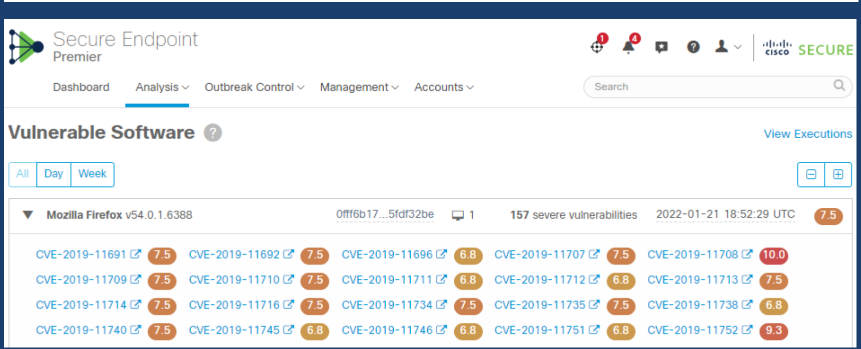
Threat Root Cause

Select Dates

February 12 2017 – February 13 2022 Apply

Overview | Details | Timeline

Program	Threat Name	Version	Threats Introduced	Computers Affected	Event Type
msedge.exe		95.0.1020.53	2	1	1 created 1 moved
iexplore.exe		11.0.19041.1202	1	1	1 created



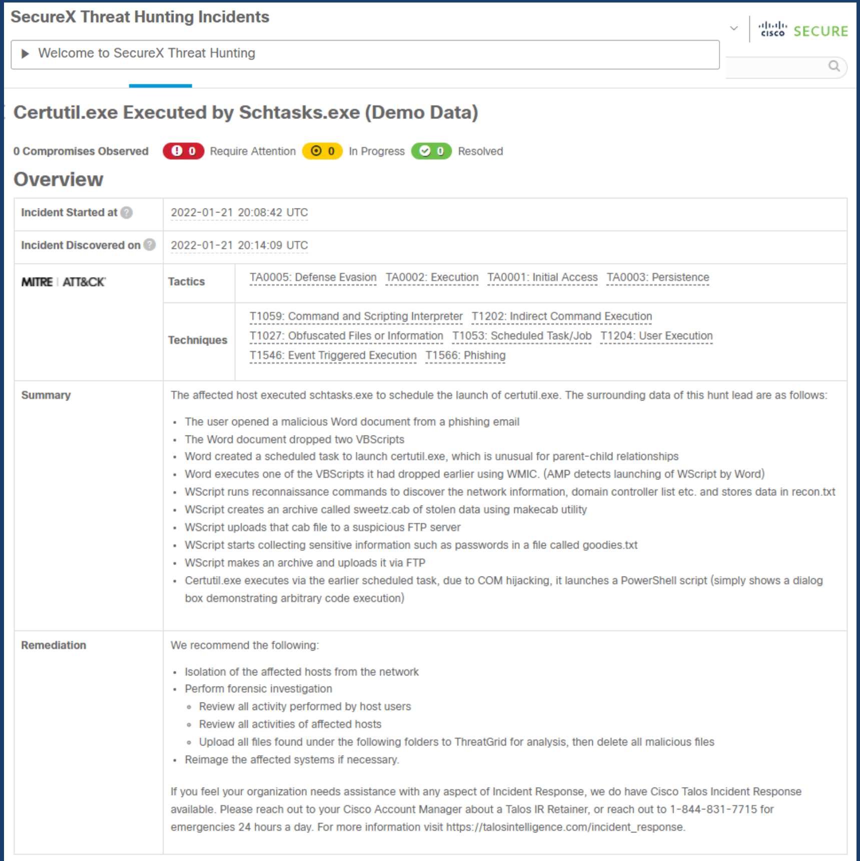
Vulnerable Software

View Executions

All | Day | Week

▼ **Mozilla Firefox** v54.0.1.6388 0fff6b17...5fdf32be 1 **157** severe vulnerabilities 2022-01-21 18:52:29 UTC 7.5

CVE-2019-11691	7.5	CVE-2019-11692	7.5	CVE-2019-11696	6.8	CVE-2019-11707	7.5	CVE-2019-11708	10.0
CVE-2019-11709	7.5	CVE-2019-11710	7.5	CVE-2019-11711	6.8	CVE-2019-11712	6.8	CVE-2019-11713	7.5
CVE-2019-11714	7.5	CVE-2019-11716	7.5	CVE-2019-11734	7.5	CVE-2019-11735	7.5	CVE-2019-11738	6.8
CVE-2019-11740	7.5	CVE-2019-11745	6.8	CVE-2019-11746	6.8	CVE-2019-11751	6.8	CVE-2019-11752	9.3



SecureX Threat Hunting Incidents

▶ Welcome to SecureX Threat Hunting

Certutil.exe Executed by Schtasks.exe (Demo Data)

0 Compromises Observed 0 Require Attention 0 In Progress 0 Resolved

Overview

Incident Started at	2022-01-21 20:08:42 UTC	
Incident Discovered on	2022-01-21 20:14:09 UTC	
MITRE ATT&CK	**Tactics**	TA0005: Defense Evasion TA0002: Execution TA0001: Initial Access TA0003: Persistence
	Techniques	T1059: Command and Scripting Interpreter T1202: Indirect Command Execution T1027: Obfuscated Files or Information T1053: Scheduled Task/Job T1204: User Execution T1546: Event Triggered Execution T1566: Phishing

Summary

The affected host executed schtasks.exe to schedule the launch of certutil.exe. The surrounding data of this hunt lead are as follows:

- The user opened a malicious Word document from a phishing email
- The Word document dropped two VBScripts
- Word created a scheduled task to launch certutil.exe, which is unusual for parent-child relationships
- Word executes one of the VBScripts it had dropped earlier using WMIC. (AMP detects launching of WScript by Word)
- WScript runs reconnaissance commands to discover the network information, domain controller list etc. and stores data in recon.txt
- WScript creates an archive called sweetz.cab of stolen data using makecab utility
- WScript uploads that cab file to a suspicious FTP server
- WScript starts collecting sensitive information such as passwords in a file called goodies.txt
- WScript makes an archive and uploads it via FTP
- Certutil.exe executes via the earlier scheduled task, due to COM hijacking, it launches a PowerShell script (simply shows a dialog box demonstrating arbitrary code execution)

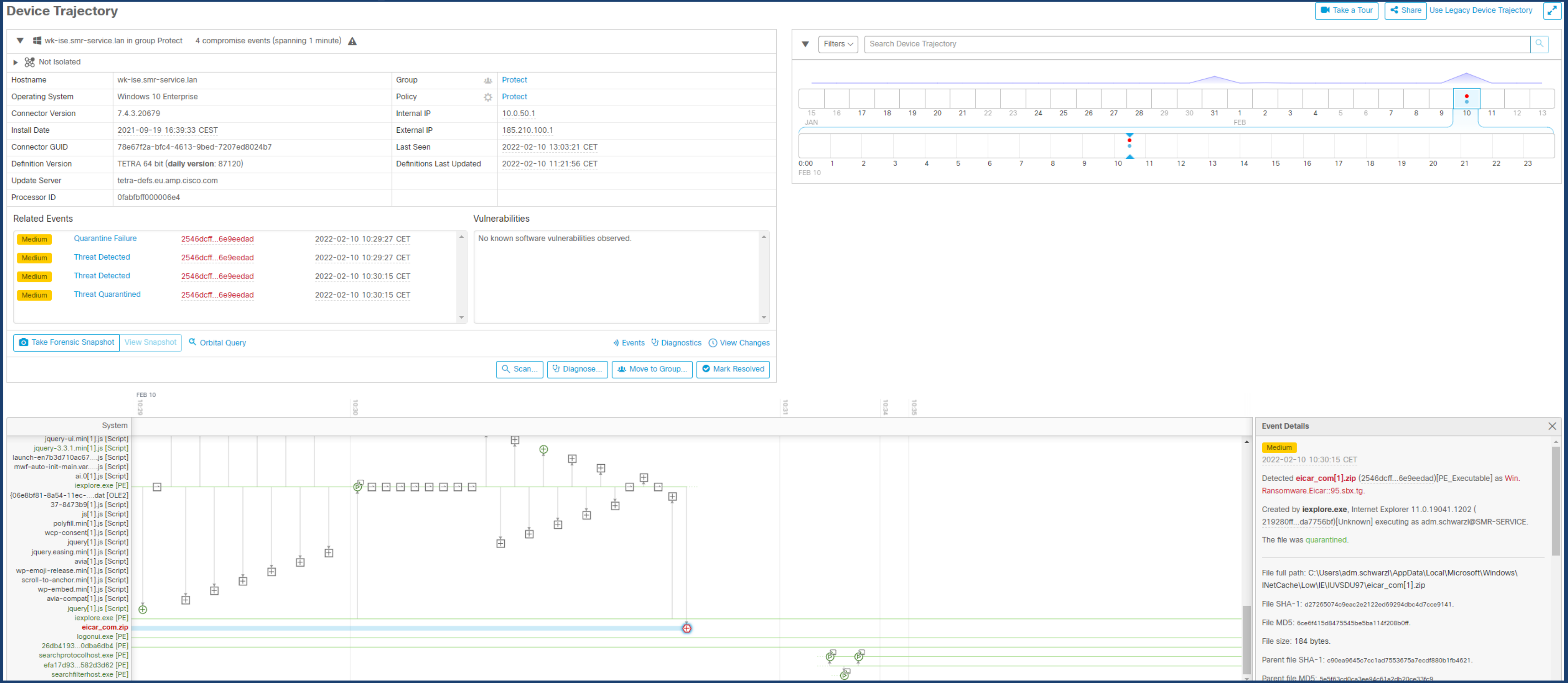
Remediation

We recommend the following:

- Isolation of the affected hosts from the network
- Perform forensic investigation
  - Review all activity performed by host users
  - Review all activities of affected hosts
  - Upload all files found under the following folders to ThreatGrid for analysis, then delete all malicious files
- Reimage the affected systems if necessary.

If you feel your organization needs assistance with any aspect of Incident Response, we do have Cisco Talos Incident Response available. Please reach out to your Cisco Account Manager about a Talos IR Retainer, or reach out to 1-844-831-7715 for emergencies 24 hours a day. For more information visit https://talosintelligence.com/incident_response.

Secure Endpoint - Detection



Device Trajectory

wk-ise.smr-service.lan in group Protect 4 compromise events (spanning 1 minute)

Not Isolated

Hostname	wk-ise.smr-service.lan	Group	Protect
Operating System	Windows 10 Enterprise	Policy	Protect
Connector Version	7.4.3.20679	Internal IP	10.0.50.1
Install Date	2021-09-19 16:39:33 CEST	External IP	185.210.100.1
Connector GUID	78e67f2a-bfc4-4613-9bed-7207ed8024b7	Last Seen	2022-02-10 13:03:21 CET
Definition Version	TETRA 64 bit (**daily version**: 87120)	Definitions Last Updated	2022-02-10 11:21:56 CET
Update Server	tetra-defs.eu.amp.cisco.com		
Processor ID	0fabfbff000006e4		

Related Events

Medium	Quarantine Failure	2546dcff...6e9eedad	2022-02-10 10:29:27 CET
Medium	Threat Detected	2546dcff...6e9eedad	2022-02-10 10:29:27 CET
Medium	Threat Detected	2546dcff...6e9eedad	2022-02-10 10:30:15 CET
Medium	Threat Quarantined	2546dcff...6e9eedad	2022-02-10 10:30:15 CET

Vulnerabilities

No known software vulnerabilities observed.

Take Forensic Snapshot
View Snapshot
Orbital Query
Events
Diagnostics
View Changes
Scan...
Diagnose...
Move to Group...
Mark Resolved
FEB 10
10:29
10:30
10:31
10:34
10:35
System
jquery-ui.min[1].js [Script]
jquery-3.3.1.min[1].js [Script]
launch-en7b3d710ac67....js [Script]
mwf-auto-init-main.var.....js [Script]
ai.0[1].js [Script]
iexplore.exe [PE]
{06e8bf81-8a54-11ec-....dat [OLE2]
37-8473b9[1].js [Script]
js[1].js [Script]
polyfill.min[1].js [Script]
wcp-consent[1].js [Script]
jquery[1].js [Script]
jquery.easing.min[1].js [Script]
avia[1].js [Script]
wp-emoji-release.min[1].js [Script]
scroll-to-anchor.min[1].js [Script]
wp-embed.min[1].js [Script]
avia-compat[1].js [Script]
jquery[1].js [Script]
iexplore.exe [PE]
eicar_com.zip
logonui.exe [PE]
26db4193...0dba6db4 [PE]
searchprotocolhost.exe [PE]
efa17d93...582d3d62 [PE]
searchfilterhost.exe [PE]

Event Details

Medium

2022-02-10 10:30:15 CET

Detected **eicar_com[1].zip** (2546dcff...6e9eedad)[PE_Executable] as Win.Ransomware.Eicar::95.sbx.tg.

Created by **iexplore.exe**, Internet Explorer 11.0.19041.1202 (219280ff...da7756bf)[Unknown] executing as adm.schwarzl@SMR-SERVICE.

The file was quarantined.

File full path: C:\Users\adm.schwarzl\AppData\Local\Microsoft\Windows\INetCache\Low\IE\IUVSDU97\eicar_com[1].zip

File SHA-1: d27265074c9eac2e2122ed69294dbc4d7cce9141.

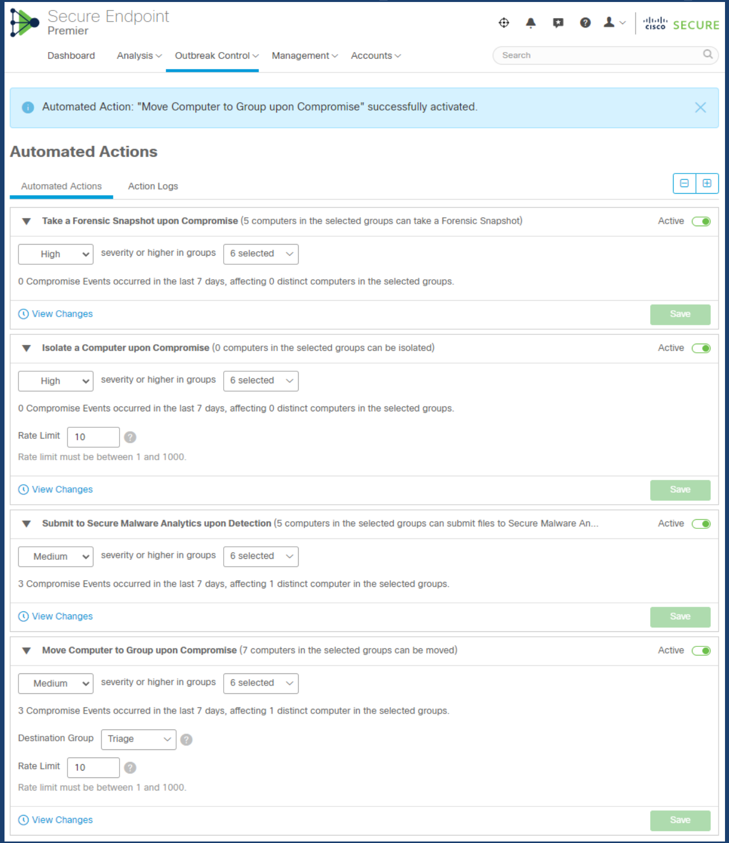
File MD5: 6ce6f415d8475545be5ba114f208b0ff.

File size: 184 bytes.

Parent file SHA-1: c90ea9645c7cc1ad7553675a7ecdf880b1fb4621.

Parent file MD5: 5e5f63cd0ca3ee94c61a2db20ce33fc9

Secure Endpoint - Response



Secure Endpoint Premier — SECURE

Dashboard | Analysis | Outbreak Control | Management | Accounts | Search

Automated Action: "Move Computer to Group upon Compromise" successfully activated.

Automated Actions

Automated Actions | Action Logs

Take a Forensic Snapshot upon Compromise (5 computers in the selected groups can take a Forensic Snapshot) — Active

High severity or higher in groups 6 selected

0 Compromise Events occurred in the last 7 days, affecting 0 distinct computers in the selected groups.

View Changes — Save

Isolate a Computer upon Compromise (0 computers in the selected groups can be isolated) — Active

High severity or higher in groups 6 selected

0 Compromise Events occurred in the last 7 days, affecting 0 distinct computers in the selected groups.

Rate Limit 10

Rate limit must be between 1 and 1000.

View Changes — Save

Submit to Secure Malware Analytics upon Detection (5 computers in the selected groups can submit files to Secure Malware An... — Active

Medium severity or higher in groups 6 selected

3 Compromise Events occurred in the last 7 days, affecting 1 distinct computer in the selected groups.

View Changes — Save

Move Computer to Group upon Compromise (7 computers in the selected groups can be moved) — Active

Medium severity or higher in groups 6 selected

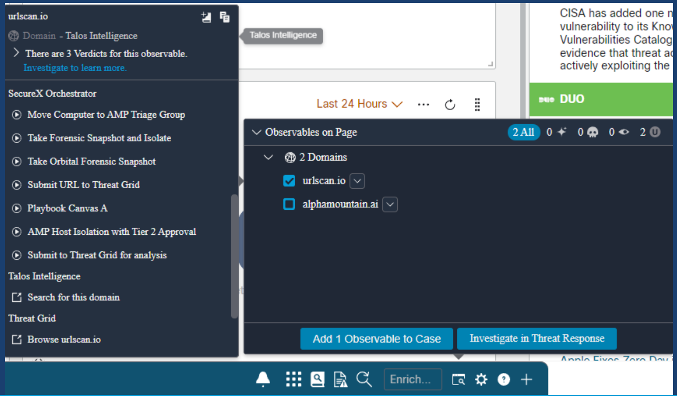
3 Compromise Events occurred in the last 7 days, affecting 1 distinct computer in the selected groups.

Destination Group Triage

Rate Limit 10

Rate limit must be between 1 and 1000.

View Changes — Save



urlscan.io

Domain - Talos Intelligence

There are 3 Verdicts for this observable.
Investigate to learn more.

SecureX Orchestrator
- Move Computer to AMP Triage Group
- Take Forensic Snapshot and Isolate
- Take Orbital Forensic Snapshot
- Submit URL to Threat Grid
- Playbook Canvas A
- AMP Host Isolation with Tier 2 Approval
- Submit to Threat Grid for analysis

Talos Intelligence
- Search for this domain

Threat Grid
- Browse urlscan.io

Talos Intelligence

CISA has added one n... vulnerability to its Kno... Vulnerabilities Catalog... evidence that threat a... actively exploiting the...

DUO

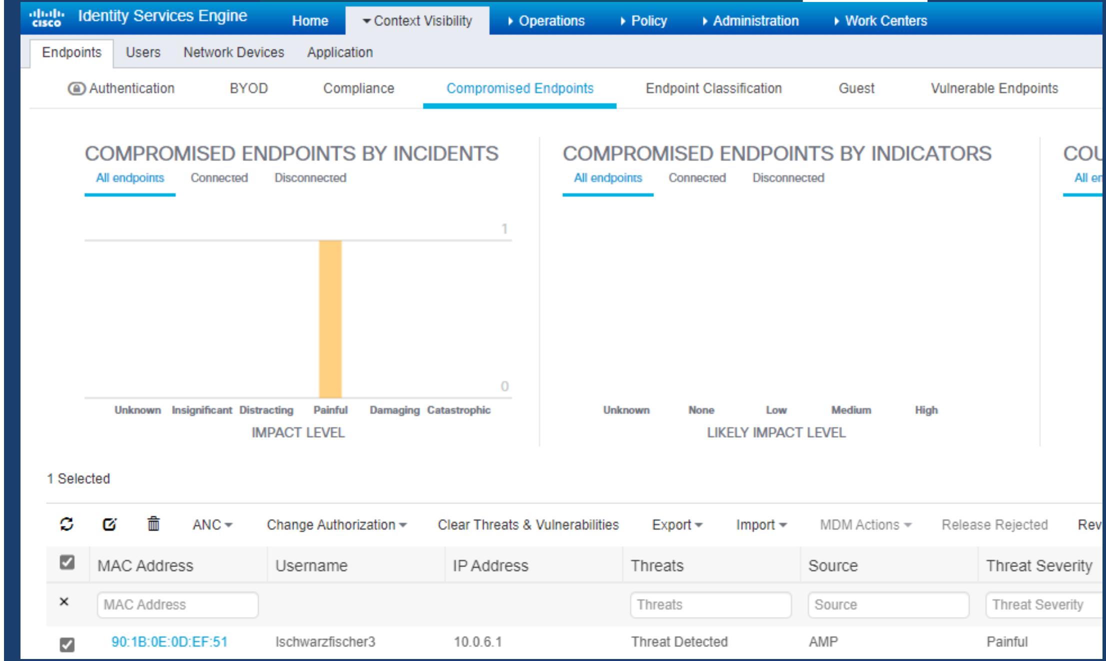
Last 24 Hours

Observables on Page — 2 All 0 0 0 2

2 Domains
- ☑ urlscan.io
- □ alphamountain.ai

Add 1 Observable to Case | Investigate in Threat Response

Enrich...



Identity Services Engine — Home | Context Visibility | Operations | Policy | Administration | Work Centers

Endpoints | Users | Network Devices | Application

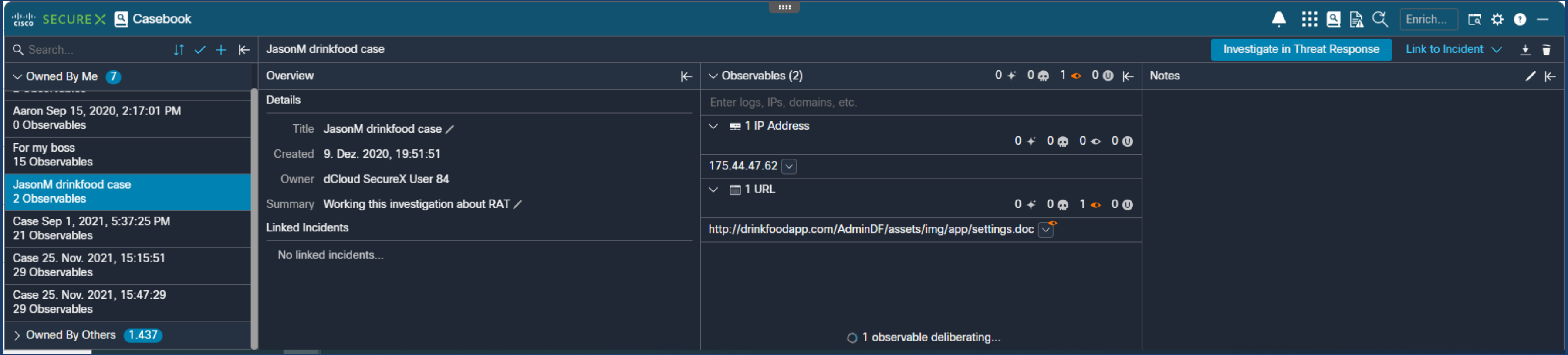
Authentication | BYOD | Compliance | Compromised Endpoints | Endpoint Classification | Guest | Vulnerable Endpoints

1 Selected

ANC | Change Authorization | Clear Threats & Vulnerabilities | Export | Import | MDM Actions | Release Rejected | Rev

☑	MAC Address	Username	IP Address	Threats	Source	Threat Severity
×	MAC Address			Threats	Source	Threat Severity
☑	90:1B:0E:0D:EF:51	lschwarzfischer3	10.0.6.1	Threat Detected	AMP	Painful

Secure Endpoint – Detection / Threat Hunting



JasonM drinkfood case

Owned By Me 7

- Aaron Sep 15, 2020, 2:17:01 PM
0 Observables
- For my boss
15 Observables
- JasonM drinkfood case
2 Observables
- Case Sep 1, 2021, 5:37:25 PM
21 Observables
- Case 25. Nov. 2021, 15:15:51
29 Observables
- Case 25. Nov. 2021, 15:47:29
29 Observables

Owned By Others 1.437

Details

Title	JasonM drinkfood case
Created	9. Dez. 2020, 19:51:51
Owner	dCloud SecureX User 84
Summary	Working this investigation about RAT

Linked Incidents

No linked incidents...

Observables (2) 0 0 1 0

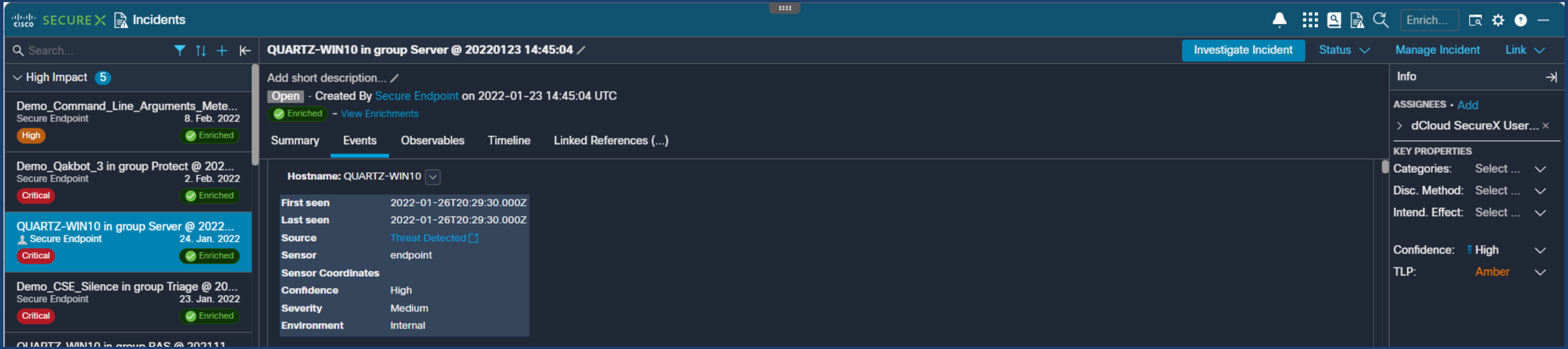
1 IP Address 0 0 0 0

175.44.47.62

1 URL 0 0 1 0

http://drinkfoodapp.com/AdminDF/assets/img/app/settings.doc

1 observable deliberating...



High Impact 5

- Demo_Command_Line_Arguments_Mete...
Secure Endpoint 8. Feb. 2022
High Enriched
- Demo_Qakbot_3 in group Protect @ 202...
Secure Endpoint 2. Feb. 2022
Critical Enriched
- QUARTZ-WIN10 in group Server @ 2022...
Secure Endpoint 24. Jan. 2022
Critical Enriched
- Demo_CSE_Silence in group Triage @ 20...
Secure Endpoint 23. Jan. 2022
Critical Enriched
- QUARTZ-WIN10 in group RAS @ 202111

QUARTZ-WIN10 in group Server @ 20220123 14:45:04

Add short description...

Open · Created By Secure Endpoint on 2022-01-23 14:45:04 UTC

Enriched – View Enrichments

Hostname: QUARTZ-WIN10

First seen	2022-01-26T20:29:30.000Z
Last seen	2022-01-26T20:29:30.000Z
Source	Threat Detected
Sensor	endpoint
Sensor Coordinates	
Confidence	High
Severity	Medium
Environment	Internal

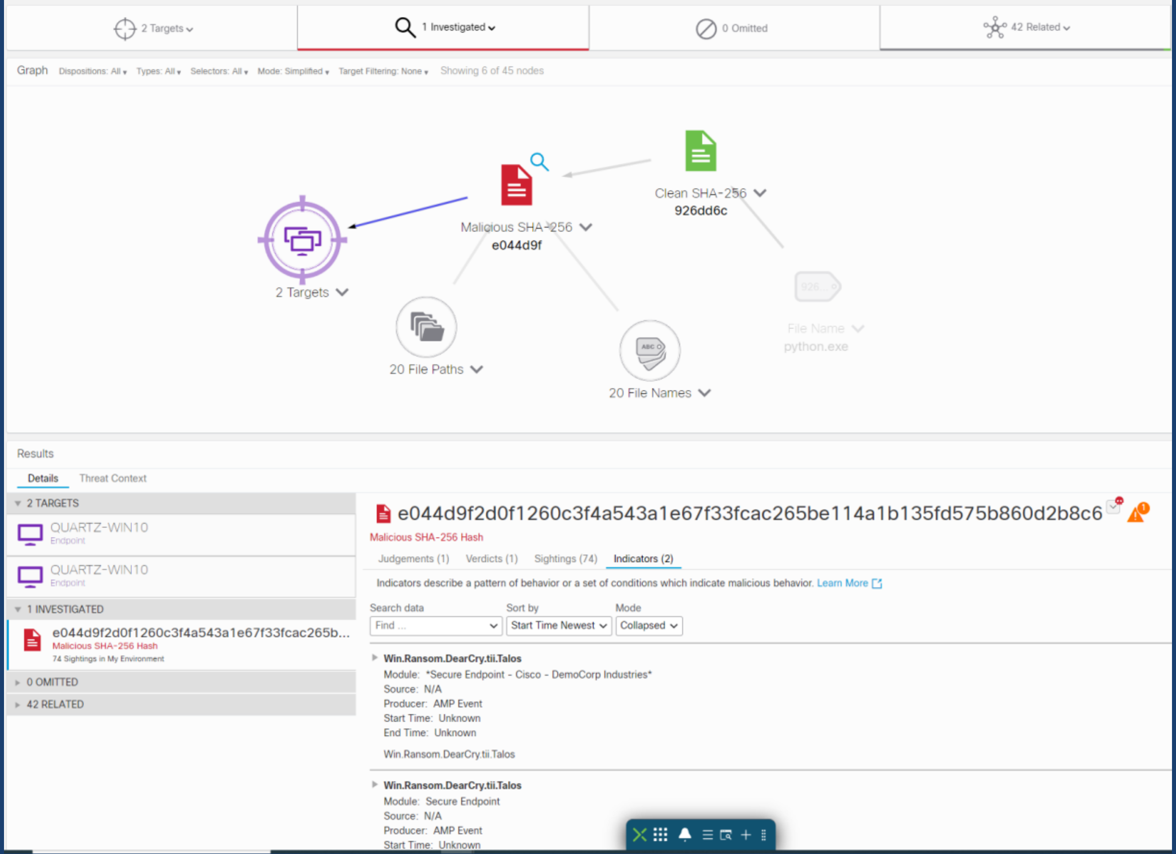
ASSIGNEES · Add

dCloud SecureX User...

KEY PROPERTIES

Categories:	Select ...
Disc. Method:	Select ...
Intend. Effect:	Select ...
Confidence:	High
TLP:	Amber

Secure Endpoint – Detection / Threat Hunting



2 Targets | 1 Investigated | 0 Omitted | 42 Related

Graph Dispositions: All Types: All Selectors: All Mode: Simplified Target Filtering: None Showing 6 of 45 nodes

Results

Details Threat Context

2 TARGETS

QUARTZ-WIN10
Endpoint

QUARTZ-WIN10
Endpoint

1 INVESTIGATED

e044d9f2d0f1260c3f4a543a1e67f33fcac265b...
Malicious SHA-256 Hash
74 Sightings in My Environment

0 OMITTED

42 RELATED

e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6

Malicious SHA-256 Hash

Judgements (1) Verdicts (1) Sightings (74) Indicators (2)

Indicators describe a pattern of behavior or a set of conditions which indicate malicious behavior. Learn More

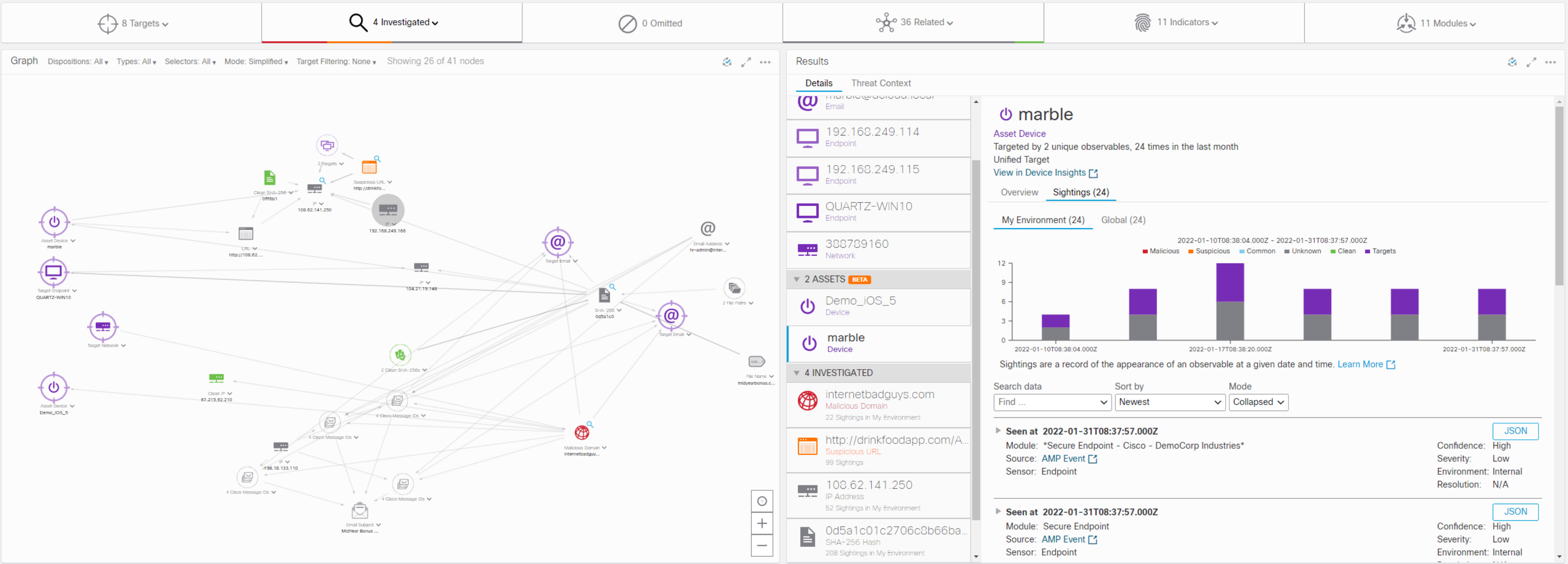
Search data: Find ...
Sort by: Start Time Newest
Mode: Collapsed

Win.Ransom.DearCry.tii.Talos
Module: *Secure Endpoint - Cisco - DemoCorp Industries*
Source: N/A
Producer: AMP Event
Start Time: Unknown
End Time: Unknown

Win.Ransom.DearCry.tii.Talos

Win.Ransom.DearCry.tii.Talos
Module: Secure Endpoint
Source: N/A
Producer: AMP Event
Start Time: Unknown

Secure Endpoint – Detection / Threat Hunting



marble@dcloud.local
Email

192.168.249.114
Endpoint

192.168.249.115
Endpoint

QUARTZ-WIN10
Endpoint

388789160
Network

2 ASSETS BETA

Demo_iOS_5
Device

marble
Device

4 INVESTIGATED

internetbadguys.com
Malicious Domain
22 Sightings in My Environment

http://drinkfoodapp.com/A...
Suspicious URL
99 Sightings

108.62.141.250
IP Address
52 Sightings in My Environment

0d5a1c01c2706c8b66ba...
SHA-256 Hash
208 Sightings in My Environment

marble
Asset Device
Targeted by 2 unique observables, 24 times in the last month
Unified Target
View in Device Insights

Overview | Sightings (24)

My Environment (24) | Global (24)

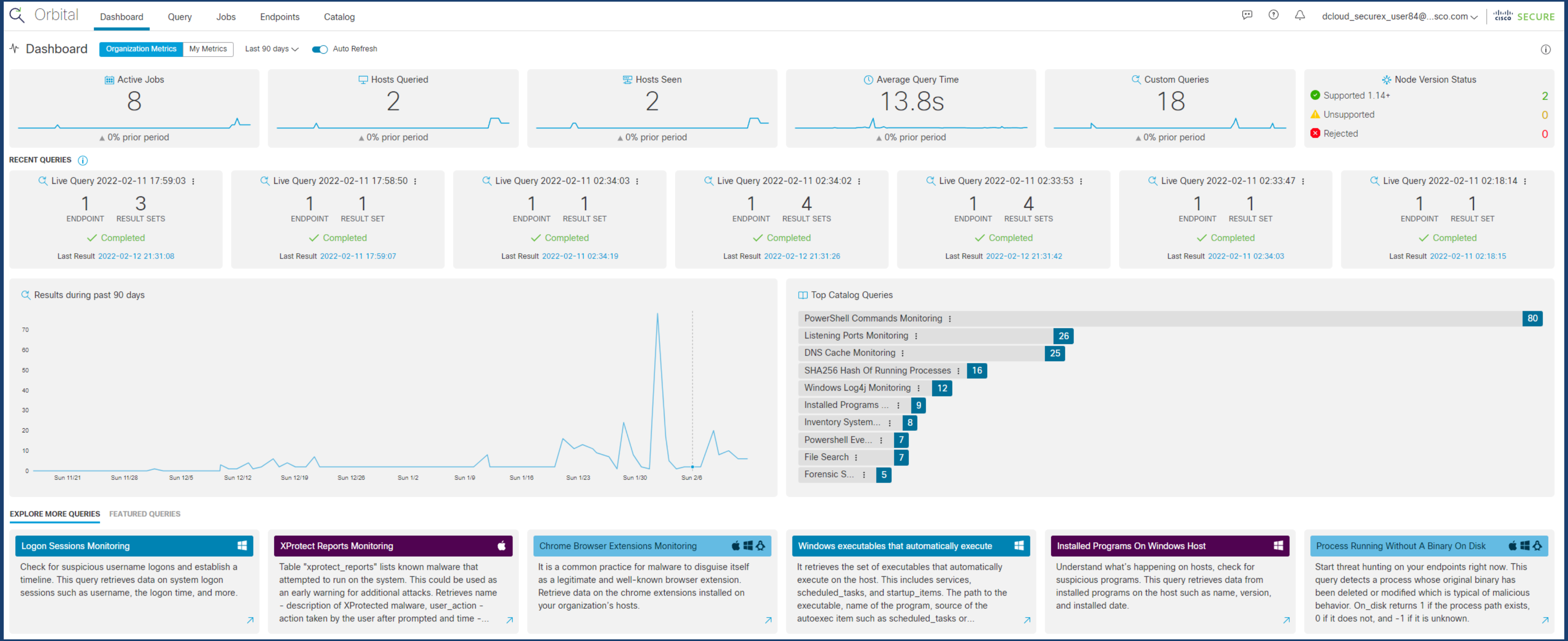
Sightings are a record of the appearance of an observable at a given date and time. Learn More

Search data: Find ...
Sort by: Newest
Mode: Collapsed

Seen at 2022-01-31T08:37:57.000Z
Module: *Secure Endpoint - Cisco - DemoCorp Industries*
Source: AMP Event
Sensor: Endpoint
Confidence: High
Severity: Low
Environment: Internal
Resolution: N/A

Seen at 2022-01-31T08:37:57.000Z
Module: Secure Endpoint
Source: AMP Event
Sensor: Endpoint
Confidence: High
Severity: Low
Environment: Internal

Secure Endpoint – Detection / Threat Hunting mit Orbital



Dashboard

Active Jobs	Hosts Queried	Hosts Seen	Average Query Time	Custom Queries
8	2	2	13.8s	18
▲ 0% prior period	▲ 0% prior period	▲ 0% prior period	▲ 0% prior period	▲ 0% prior period

Node Version Status

✓ Supported 1.14+	2
⚠ Unsupported	0
✕ Rejected	0

RECENT QUERIES

Query	Endpoint	Result sets	Status	Last Result
Live Query 2022-02-11 17:59:03	1 ENDPOINT	3 RESULT SETS	✓ Completed	2022-02-12 21:31:08
Live Query 2022-02-11 17:58:50	1 ENDPOINT	1 RESULT SET	✓ Completed	2022-02-11 17:59:07
Live Query 2022-02-11 02:34:03	1 ENDPOINT	1 RESULT SET	✓ Completed	2022-02-11 02:34:19
Live Query 2022-02-11 02:34:02	1 ENDPOINT	4 RESULT SETS	✓ Completed	2022-02-12 21:31:26
Live Query 2022-02-11 02:33:53	1 ENDPOINT	4 RESULT SETS	✓ Completed	2022-02-12 21:31:42
Live Query 2022-02-11 02:33:47	1 ENDPOINT	1 RESULT SET	✓ Completed	2022-02-11 02:34:03
Live Query 2022-02-11 02:18:14	1 ENDPOINT	1 RESULT SET	✓ Completed	2022-02-11 02:18:15

Results during past 90 days

Top Catalog Queries

PowerShell Commands Monitoring	80
Listening Ports Monitoring	26
DNS Cache Monitoring	25
SHA256 Hash Of Running Processes	16
Windows Log4j Monitoring	12
Installed Programs ...	9
Inventory System...	8
Powershell Eve...	7
File Search	7
Forensic S...	5

EXPLORE MORE QUERIES　FEATURED QUERIES

Logon Sessions Monitoring
Check for suspicious username logons and establish a timeline. This query retrieves data on system logon sessions such as username, the logon time, and more.

XProtect Reports Monitoring
Table "xprotect_reports" lists known malware that attempted to run on the system. This could be used as an early warning for additional attacks. Retrieves name - description of XProtected malware, user_action - action taken by the user after prompted and time -...

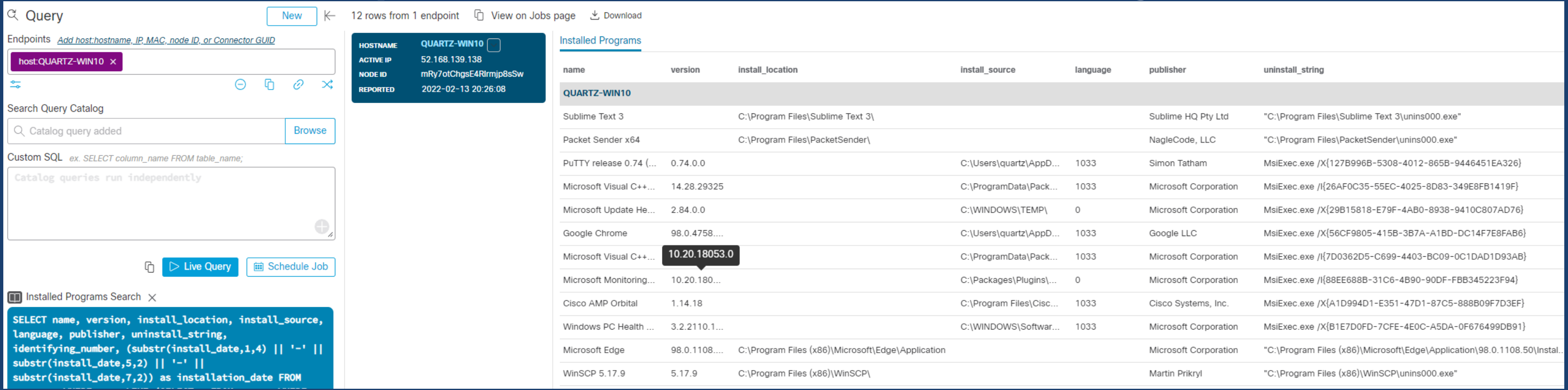
Chrome Browser Extensions Monitoring
It is a common practice for malware to disguise itself as a legitimate and well-known browser extension. Retrieve data on the chrome extensions installed on your organization's hosts.

Windows executables that automatically execute
It retrieves the set of executables that automatically execute on the host. This includes services, scheduled_tasks, and startup_items. The path to the executable, name of the program, source of the autoexec item such as scheduled_tasks or...

Installed Programs On Windows Host
Understand what's happening on hosts, check for suspicious programs. This query retrieves data from installed programs on the host such as name, version, and installed date.

Process Running Without A Binary On Disk
Start threat hunting on your endpoints right now. This query detects a process whose original binary has been deleted or modified which is typical of malicious behavior. On_disk returns 1 if the process path exists, 0 if it does not, and -1 if it is unknown.

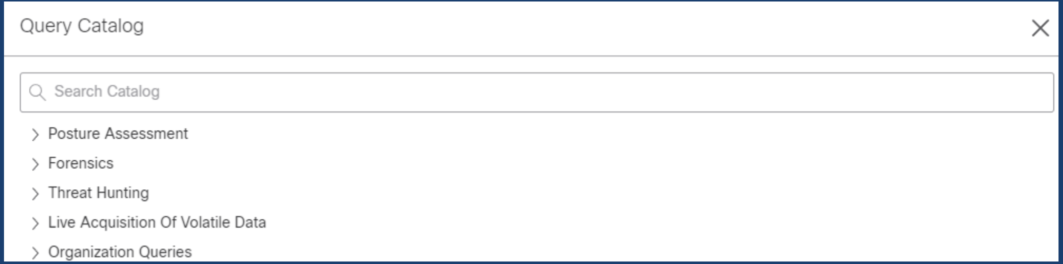
Secure Endpoint – Detection / Threat Hunting mit Orbital



```
SELECT name, version, install_location, install_source,
language, publisher, uninstall_string,
identifying_number, (substr(install_date,1,4) || '-' ||
substr(install_date,5,2) || '-' ||
substr(install_date,7,2)) as installation_date FROM
```

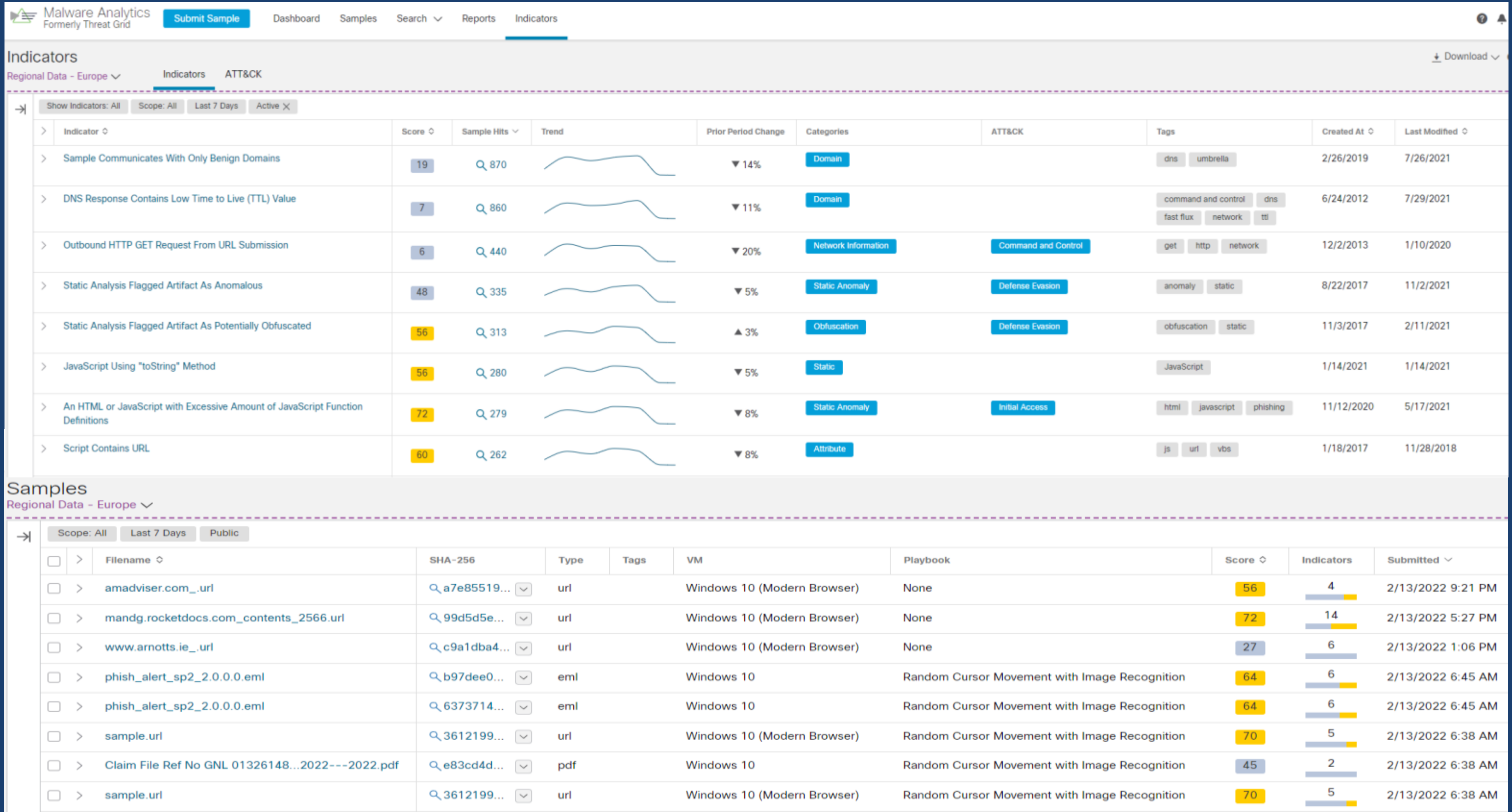
HOSTNAME	QUARTZ-WIN10
ACTIVE IP	52.168.139.138
NODE ID	mRy7otChgsE4Rlrmjp8sSw
REPORTED	2022-02-13 20:26:08

name	version	install_location	install_source	language	publisher	uninstall_string
QUARTZ-WIN10						
Sublime Text 3		C:\Program Files\Sublime Text 3\			Sublime HQ Pty Ltd	"C:\Program Files\Sublime Text 3\unins000.exe"
Packet Sender x64		C:\Program Files\PacketSender\			NagleCode, LLC	"C:\Program Files\PacketSender\unins000.exe"
PuTTY release 0.74 (...	0.74.0.0		C:\Users\quartz\AppD...	1033	Simon Tatham	MsiExec.exe /X{127B996B-5308-4012-865B-9446451EA326}
Microsoft Visual C++...	14.28.29325		C:\ProgramData\Pack...	1033	Microsoft Corporation	MsiExec.exe /I{26AF0C35-55EC-4025-8D83-349E8FB1419F}
Microsoft Update He...	2.84.0.0		C:\WINDOWS\TEMP\	0	Microsoft Corporation	MsiExec.exe /X{29B15818-E79F-4AB0-8938-9410C807AD76}
Google Chrome	98.0.4758....		C:\Users\quartz\AppD...	1033	Google LLC	MsiExec.exe /X{56CF9805-415B-3B7A-A1BD-DC14F7E8FAB6}
Microsoft Visual C++...			C:\ProgramData\Pack...	1033	Microsoft Corporation	MsiExec.exe /I{7D0362D5-C699-4403-BC09-0C1DAD1D93AB}
Microsoft Monitoring...	10.20.180...		C:\Packages\Plugins\...	0	Microsoft Corporation	MsiExec.exe /I{88EE688B-31C6-4B90-90DF-FBB345223F94}
Cisco AMP Orbital	1.14.18		C:\Program Files\Cisc...	1033	Cisco Systems, Inc.	MsiExec.exe /X{A1D994D1-E351-47D1-87C5-888B09F7D3EF}
Windows PC Health ...	3.2.2110.1...		C:\WINDOWS\Softwar...	1033	Microsoft Corporation	MsiExec.exe /X{B1E7D0FD-7CFE-4E0C-A5DA-0F676499DB91}
Microsoft Edge	98.0.1108....	C:\Program Files (x86)\Microsoft\Edge\Application			Microsoft Corporation	"C:\Program Files (x86)\Microsoft\Edge\Application\98.0.1108.50\Instal...
WinSCP 5.17.9	5.17.9	C:\Program Files (x86)\WinSCP\			Martin Prikryl	"C:\Program Files (x86)\WinSCP\unins000.exe"



- Malware Persistence oder Schwachstellen prüfen (log4j,…)
- Hosts File, Routing Table Monitoring
- Disabled Accounts / Failed Logon Monitoring
- Installierte Programme, Drucker, Zertifikate,… überwachen
- SMBv1 Nutzung, SSH-Konfiguration

Secure Endpoint – Sandbox Secure Malware Analytics Cloud



Indicators

Regional Data - Europe

Indicators | ATT&CK

Show Indicators: All | Scope: All | Last 7 Days | Active

Indicator	Score	Sample Hits	Trend	Prior Period Change	Categories	ATT&CK	Tags	Created At	Last Modified
Sample Communicates With Only Benign Domains	19	870		▼ 14%	Domain		dns umbrella	2/26/2019	7/26/2021
DNS Response Contains Low Time to Live (TTL) Value	7	860		▼ 11%	Domain		command and control dns fast flux network ttl	6/24/2012	7/29/2021
Outbound HTTP GET Request From URL Submission	6	440		▼ 20%	Network Information	Command and Control	get http network	12/2/2013	1/10/2020
Static Analysis Flagged Artifact As Anomalous	48	335		▼ 5%	Static Anomaly	Defense Evasion	anomaly static	8/22/2017	11/2/2021
Static Analysis Flagged Artifact As Potentially Obfuscated	56	313		▲ 3%	Obfuscation	Defense Evasion	obfuscation static	11/3/2017	2/11/2021
JavaScript Using "toString" Method	56	280		▼ 5%	Static		JavaScript	1/14/2021	1/14/2021
An HTML or JavaScript with Excessive Amount of JavaScript Function Definitions	72	279		▼ 8%	Static Anomaly	Initial Access	html javascript phishing	11/12/2020	5/17/2021
Script Contains URL	60	262		▼ 8%	Attribute		js url vbs	1/18/2017	11/28/2018

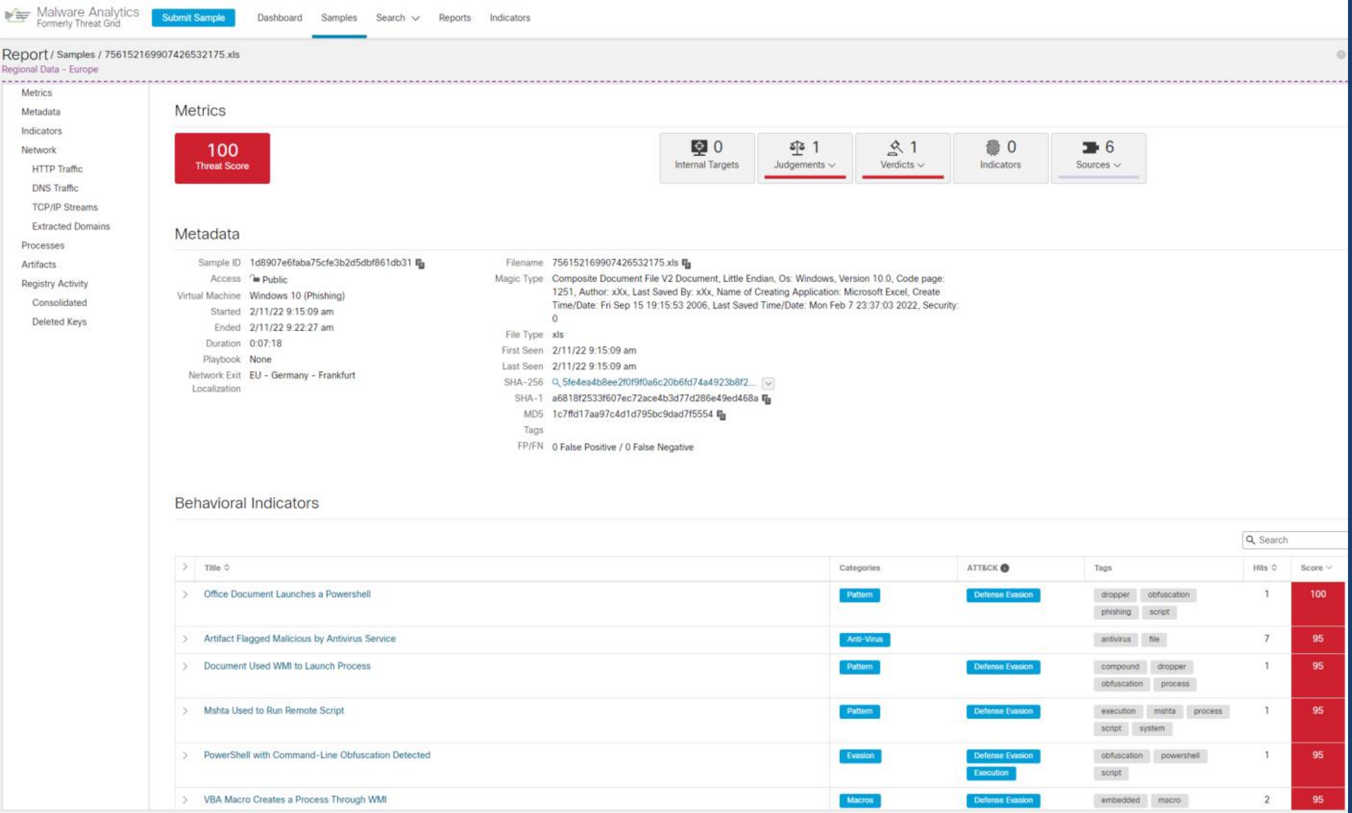
Samples

Regional Data - Europe

Scope: All | Last 7 Days | Public

□	Filename	SHA-256	Type	Tags	VM	Playbook	Score	Indicators	Submitted
□	amadviser.com_.url	a7e85519...	url		Windows 10 (Modern Browser)	None	56	4	2/13/2022 9:21 PM
□	mandg.rocketdocs.com_contents_2566.url	99d5d5e...	url		Windows 10 (Modern Browser)	None	72	14	2/13/2022 5:27 PM
□	www.arnotts.ie_.url	c9a1dba4...	url		Windows 10 (Modern Browser)	None	27	6	2/13/2022 1:06 PM
□	phish_alert_sp2_2.0.0.0.eml	b97dee0...	eml		Windows 10	Random Cursor Movement with Image Recognition	64	6	2/13/2022 6:45 AM
□	phish_alert_sp2_2.0.0.0.eml	6373714...	eml		Windows 10	Random Cursor Movement with Image Recognition	64	6	2/13/2022 6:45 AM
□	sample.url	3612199...	url		Windows 10 (Modern Browser)	Random Cursor Movement with Image Recognition	70	5	2/13/2022 6:38 AM
□	Claim File Ref No GNL 01326148...2022---2022.pdf	e83cd4d...	pdf		Windows 10	Random Cursor Movement with Image Recognition	45	2	2/13/2022 6:38 AM
□	sample.url	3612199...	url		Windows 10 (Modern Browser)	Random Cursor Movement with Image Recognition	70	5	2/13/2022 6:38 AM

Secure Endpoint – Sandbox Secure Malware Analytics Cloud



Report / Samples / 7561521699074265321 75.xls
Regional Data - Europe

Metrics

100 Threat Score	0 Internal Targets	1 Judgements	1 Verdicts	0 Indicators	6 Sources

Metadata

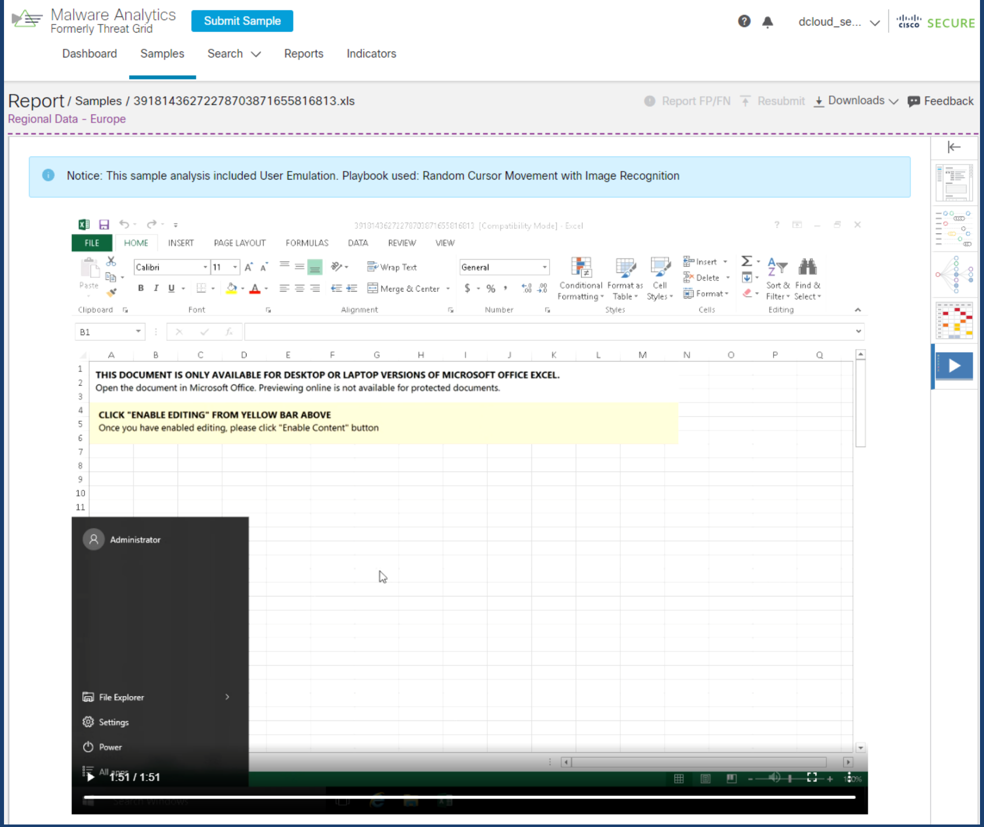
Sample ID	1d8907e6faba75cfe3b2d5dbf861db31
Access	Public
Virtual Machine	Windows 10 (Phishing)
Started	2/11/22 9:15:09 am
Ended	2/11/22 9:22:27 am
Duration	0:07:18
Playbook	None
Network Exit Localization	EU - Germany - Frankfurt

Filename	756152169907426532175.xls
Magic Type	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: xXx, Last Saved By: xXx, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Sep 15 19:15:53 2006, Last Saved Time/Date: Mon Feb 7 23:37:03 2022, Security: 0
File Type	xls
First Seen	2/11/22 9:15:09 am
Last Seen	2/11/22 9:15:09 am
SHA-256	5fe4ea4b8ee2f0f9f0a6c20b6fd74a4923b8f2...
SHA-1	a6818f2533f607ec72ace4b3d77d286e49ed468a
MD5	1c7ffd17aa97c4d1d795bc9dad7f5554
Tags	
FP/FN	0 False Positive / 0 False Negative

Behavioral Indicators

Title	Categories	ATT&CK	Tags	Hits	Score
Office Document Launches a Powershell	Pattern	Defense Evasion	dropper obfuscation phishing script	1	100
Artifact Flagged Malicious by Antivirus Service	Anti-Virus		antivirus file	7	95
Document Used WMI to Launch Process	Pattern	Defense Evasion	compound dropper obfuscation process	1	95
Mshta Used to Run Remote Script	Pattern	Defense Evasion	execution mshta process script system	1	95
PowerShell with Command-Line Obfuscation Detected	Evasion	Defense Evasion Execution	obfuscation powershell script	1	95
VBA Macro Creates a Process Through WMI	Macros	Defense Evasion	embedded macro	2	95

Secure Endpoint – Sandbox Secure Malware Analytics Cloud



Report / Samples / 39181436272278703871655816813.xls

Regional Data - Europe

Notice: This sample analysis included User Emulation. Playbook used: Random Cursor Movement with Image Recognition

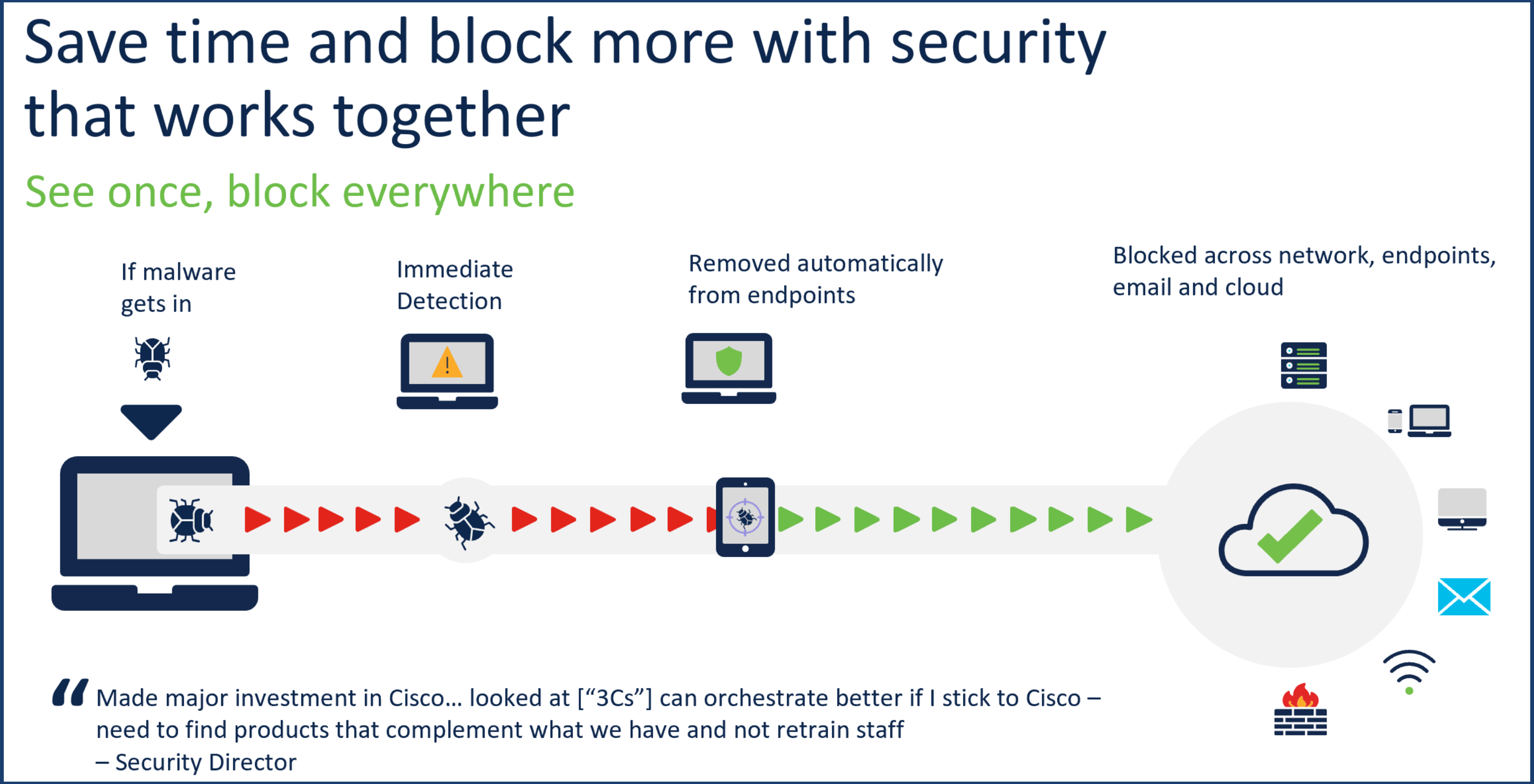
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.

Open the document in Microsoft Office. Previewing online is not available for protected documents.

CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE

Once you have enabled editing, please click "Enable Content" button

Secure Endpoint – Integration AMP Everywhere



Save time and block more with security that works together

See once, block everywhere

If malware gets in

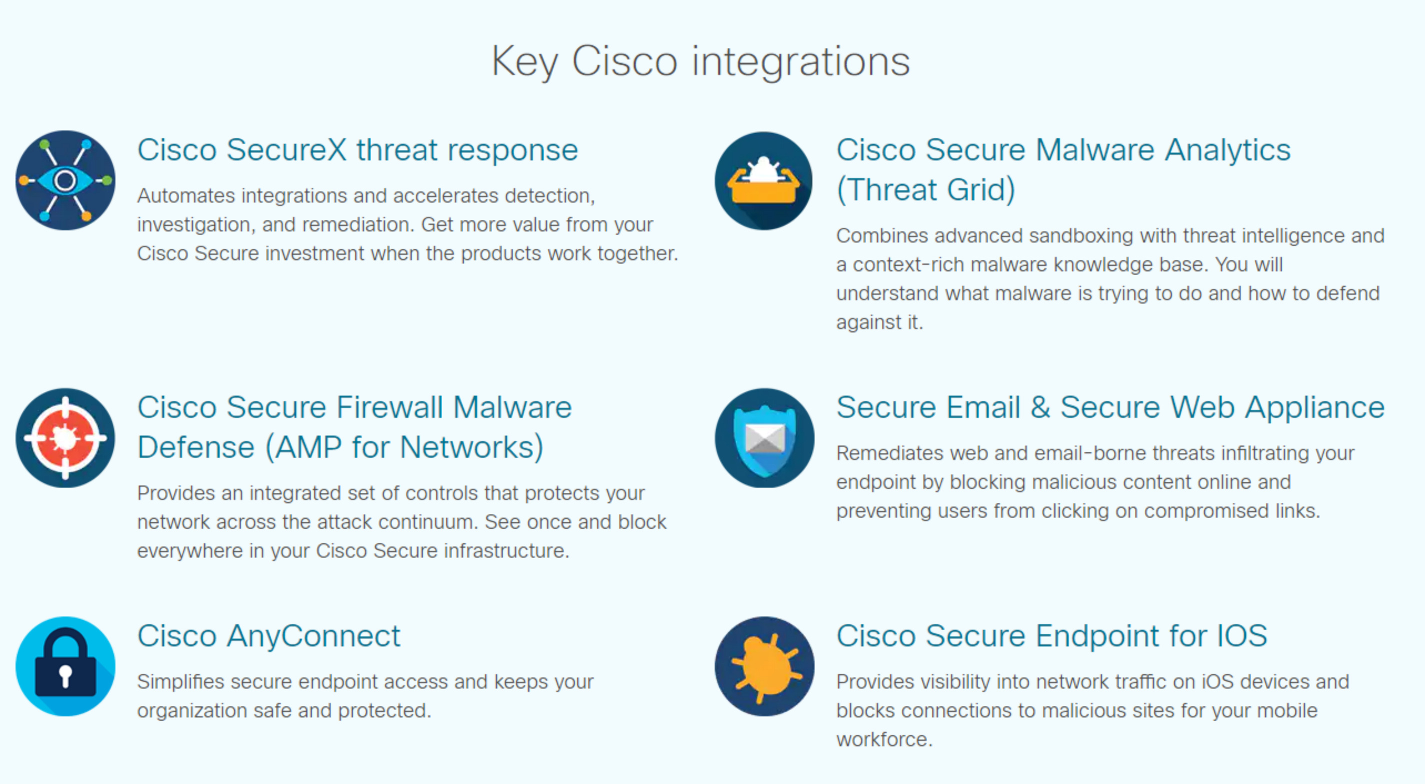
Immediate Detection

Removed automatically from endpoints

Blocked across network, endpoints, email and cloud

“ Made major investment in Cisco… looked at [“3Cs”] can orchestrate better if I stick to Cisco – need to find products that complement what we have and not retrain staff
– Security Director

Secure Endpoint – Integration AMP Everywhere



Key Cisco integrations

Cisco SecureX threat response

Automates integrations and accelerates detection, investigation, and remediation. Get more value from your Cisco Secure investment when the products work together.

Cisco Secure Malware Analytics (Threat Grid)

Combines advanced sandboxing with threat intelligence and a context-rich malware knowledge base. You will understand what malware is trying to do and how to defend against it.

Cisco Secure Firewall Malware Defense (AMP for Networks)

Provides an integrated set of controls that protects your network across the attack continuum. See once and block everywhere in your Cisco Secure infrastructure.

Secure Email & Secure Web Appliance

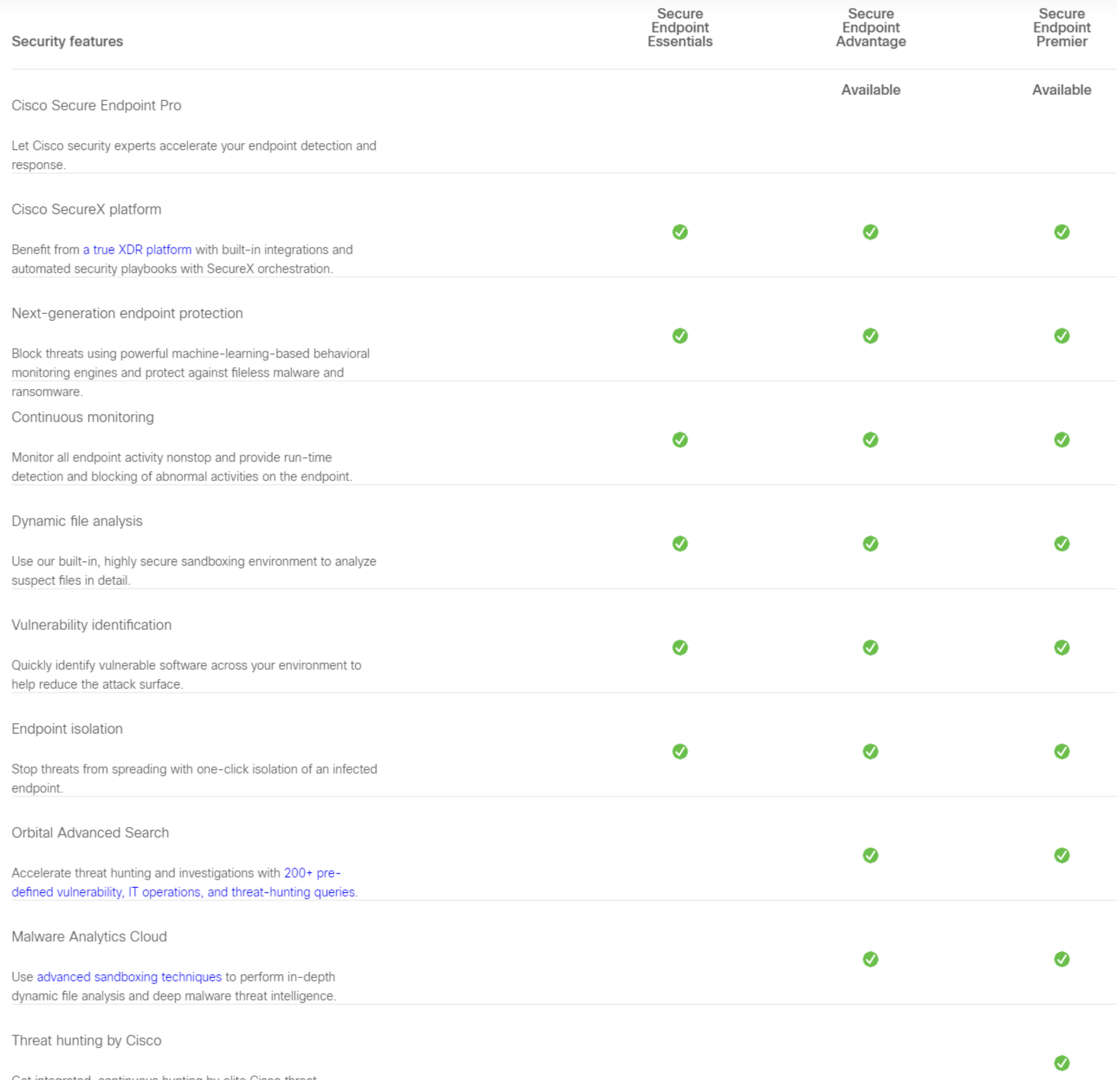
Remediates web and email-borne threats infiltrating your endpoint by blocking malicious content online and preventing users from clicking on compromised links.

Cisco AnyConnect

Simplifies secure endpoint access and keeps your organization safe and protected.

Cisco Secure Endpoint for IOS

Provides visibility into network traffic on iOS devices and blocks connections to malicious sites for your mobile workforce.



Security features	Secure Endpoint Essentials	Secure Endpoint Advantage	Secure Endpoint Premier
Cisco Secure Endpoint Pro Let Cisco security experts accelerate your endpoint detection and response.		Available	Available
Cisco SecureX platform Benefit from a true XDR platform with built-in integrations and automated security playbooks with SecureX orchestration.	✓	✓	✓
Next-generation endpoint protection Block threats using powerful machine-learning-based behavioral monitoring engines and protect against fileless malware and ransomware.	✓	✓	✓
Continuous monitoring Monitor all endpoint activity nonstop and provide run-time detection and blocking of abnormal activities on the endpoint.	✓	✓	✓
Dynamic file analysis Use our built-in, highly secure sandboxing environment to analyze suspect files in detail.	✓	✓	✓
Vulnerability identification Quickly identify vulnerable software across your environment to help reduce the attack surface.	✓	✓	✓
Endpoint isolation Stop threats from spreading with one-click isolation of an infected endpoint.	✓	✓	✓
Orbital Advanced Search Accelerate threat hunting and investigations with 200+ pre-defined vulnerability, IT operations, and threat-hunting queries.		✓	✓
Malware Analytics Cloud Use advanced sandboxing techniques to perform in-depth dynamic file analysis and deep malware threat intelligence.		✓	✓
Threat hunting by Cisco Get integrated, continuous hunting by elite Cisco threat			✓

Agenda

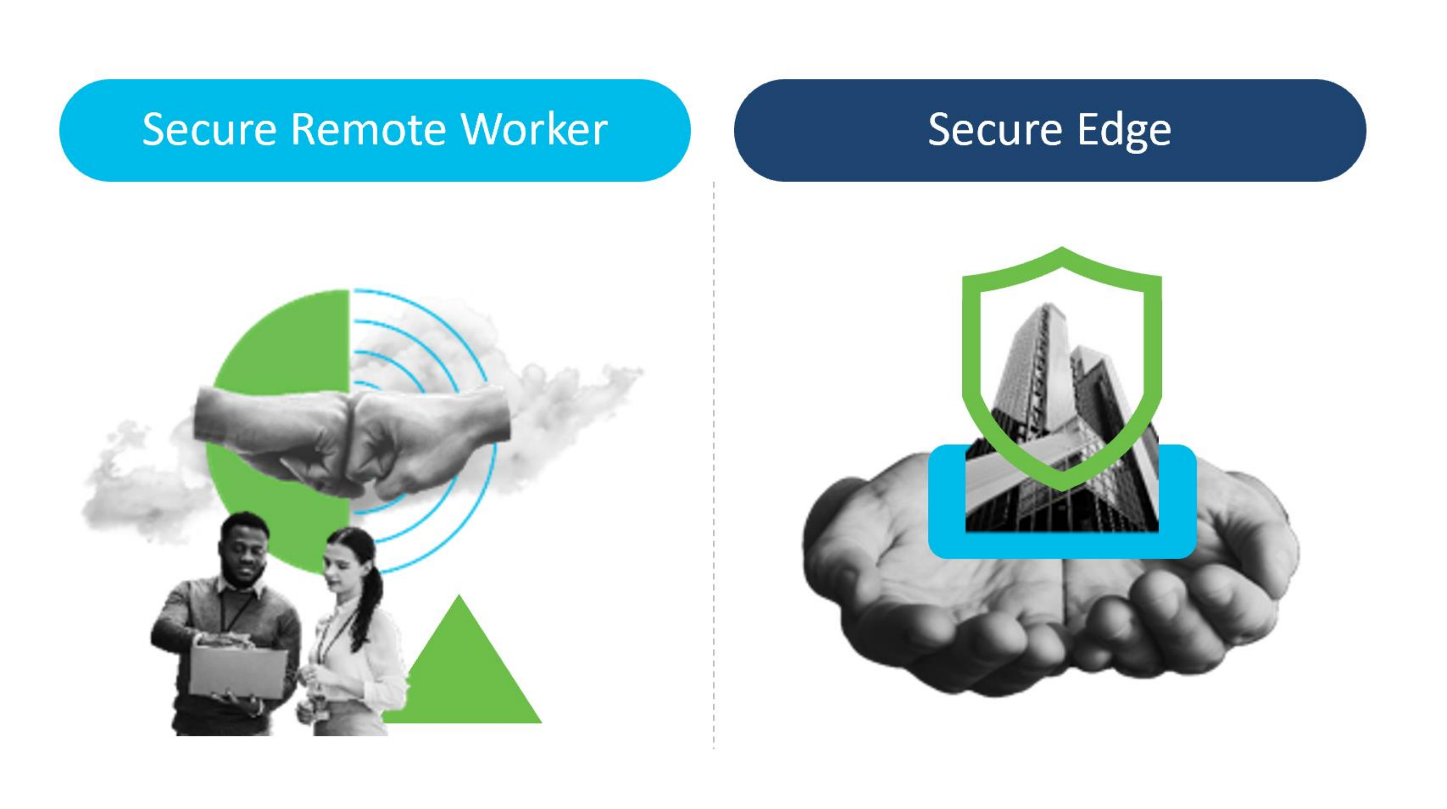
- Endpoint und Perimeter Security
- Cisco EDR – Secure Endpoint
- Secure Endpoint – Visibility, Threat Hunting - Demo
- Cisco SASE – Umbrella SIG
- Umbrella SIG - Demo
- Q&A

SWS COMPUTERSYSTEME Member of ACP Group

Agenda

- Endpoint und Perimeter Security
- Cisco EDR – Secure Endpoint
- Secure Endpoint – Visibility, Threat Hunting - Demo
- Cisco SASE – Umbrella SIG
- Umbrella SIG - Demo
- Q&A

SASE – Secure Access Service Edge

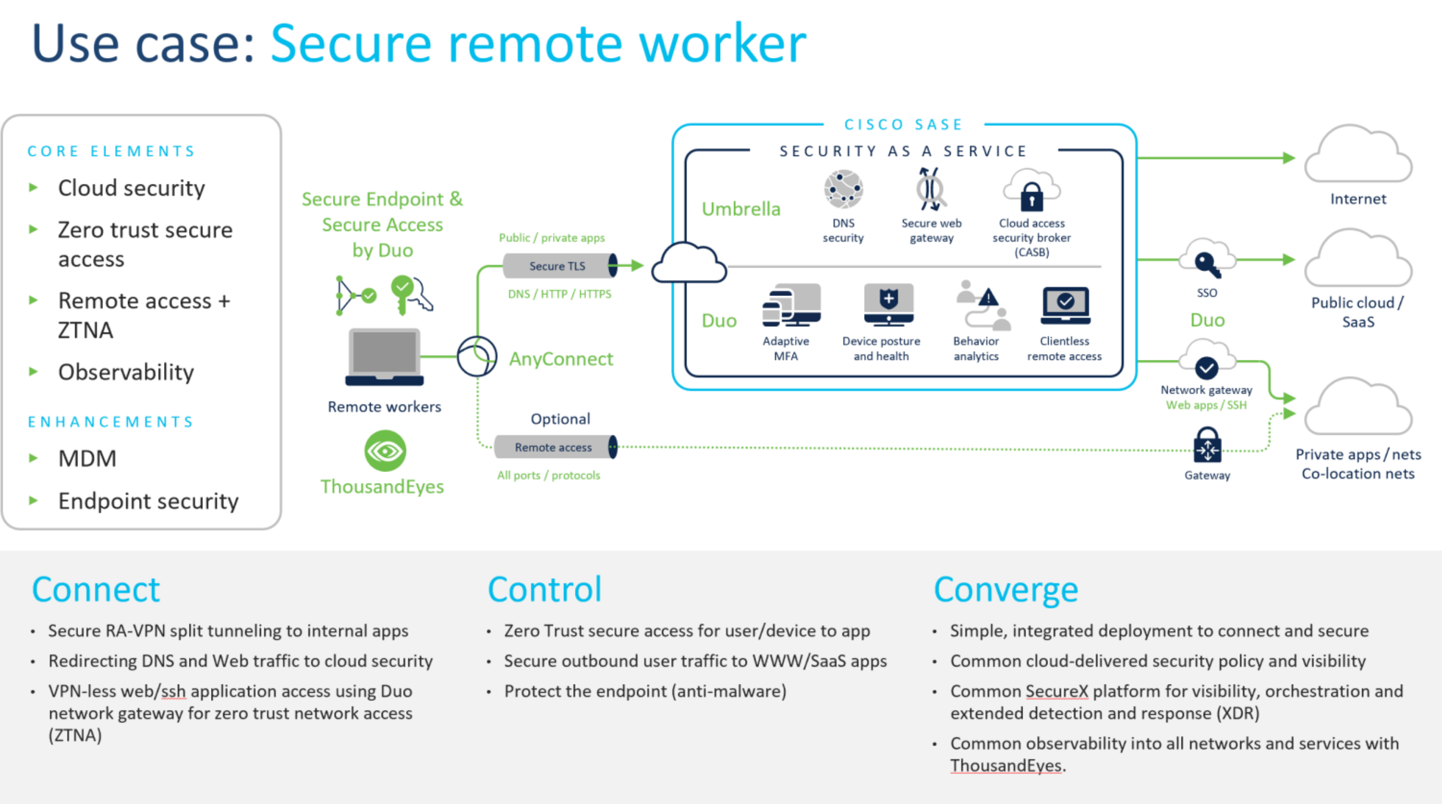


SASE – Secure Access Service Edge

Networking
Security
Zero Trust

SWS COMPUTERSYSTEME
Member of ACP Group

SASE – Secure Access Service Edge



Use case: Secure remote worker

CORE ELEMENTS

- Cloud security
- Zero trust secure access
- Remote access + ZTNA
- Observability

ENHANCEMENTS

- MDM
- Endpoint security

Connect

- Secure RA-VPN split tunneling to internal apps
- Redirecting DNS and Web traffic to cloud security
- VPN-less web/ssh application access using Duo network gateway for zero trust network access (ZTNA)

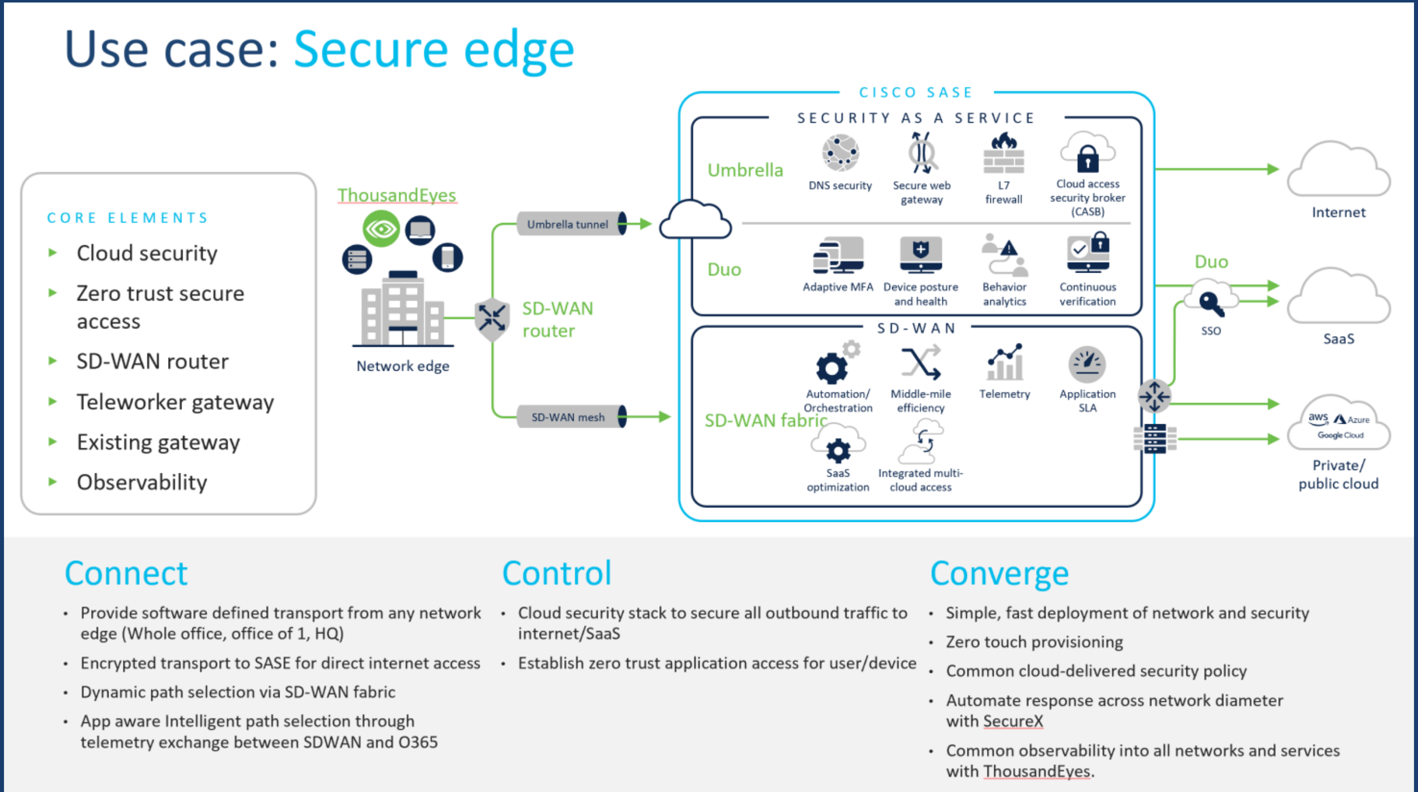
Control

- Zero Trust secure access for user/device to app
- Secure outbound user traffic to WWW/SaaS apps
- Protect the endpoint (anti-malware)

Converge

- Simple, integrated deployment to connect and secure
- Common cloud-delivered security policy and visibility
- Common SecureX platform for visibility, orchestration and extended detection and response (XDR)
- Common observability into all networks and services with ThousandEyes.

SASE – Secure Access Service Edge



Use case: Secure edge

CORE ELEMENTS

- Cloud security
- Zero trust secure access
- SD-WAN router
- Teleworker gateway
- Existing gateway
- Observability

Connect

- Provide software defined transport from any network edge (Whole office, office of 1, HQ)
- Encrypted transport to SASE for direct internet access
- Dynamic path selection via SD-WAN fabric
- App aware Intelligent path selection through telemetry exchange between SDWAN and O365

Control

- Cloud security stack to secure all outbound traffic to internet/SaaS
- Establish zero trust application access for user/device

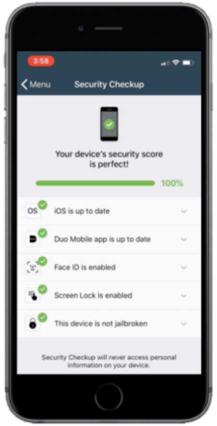
Converge

- Simple, fast deployment of network and security
- Zero touch provisioning
- Common cloud-delivered security policy
- Automate response across network diameter with SecureX
- Common observability into all networks and services with ThousandEyes.

SWS COMPUTERSYSTEME
Member of ACP Group

SASE – Secure Access Service Edge

SaaS apps flow capabilities & experience

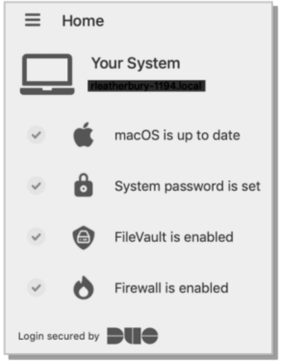

3:58
Menu
Security Checkup

Your device's security score is perfect!

100%

- OS iOS is up to date
- Duo Mobile app is up to date
- Face ID is enabled
- Screen Lock is enabled
- This device is not jailbroken

Security Checkup will never access personal information on your device.

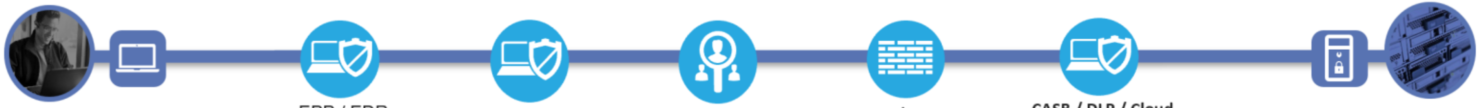

Home

Your System
[redacted]

- ✓ macOS is up to date
- ✓ System password is set
- ✓ FileVault is enabled
- ✓ Firewall is enabled

Login secured by DUO

Cisco webex
slack
Office 365
salesforce
workday.
amazon web services
Google Apps
Dropbox



Remote Worker

EPP / EDR (Secure Endpoint)

DNS / IP Security Content Filtering (Umbrella Roaming)

SAML / MFA Device Trust (DUO)

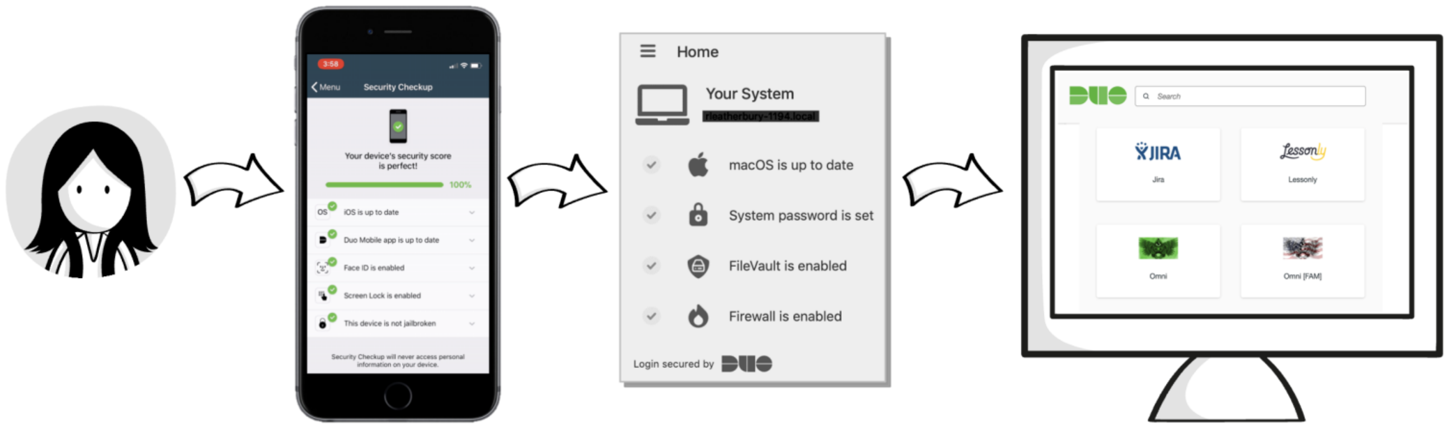
Secure Web Gateway Decryption / Inspection / File Sandboxing (Umbrella)

CASB / DLP / Cloud Malware Protection / Tenant Controls (Umbrella)

Public Application (SaaS)

SASE – Secure Access Service Edge

Private apps flow capabilities & experience



3:58

Menu

Security Checkup

Your device's security score is perfect!

100%

- OS iOS is up to date
- Duo Mobile app is up to date
- Face ID is enabled
- Screen Lock is enabled
- This device is not jailbroken

Security Checkup will never access personal information on your device.

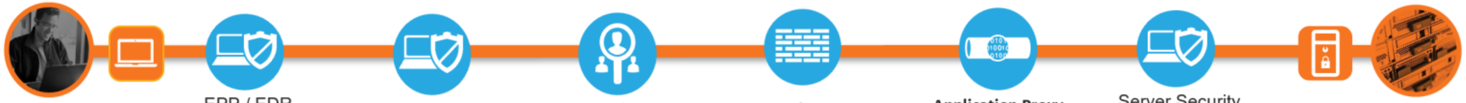
Home

Your System

[redacted]

- ✓ macOS is up to date
- ✓ System password is set
- ✓ FileVault is enabled
- ✓ Firewall is enabled

Login secured by DUO



Remote Worker

EPP / EDR (Secure Endpoint)

DNS / IP Security Content Filtering (Umbrella Roaming)

SAML / MFA Device Trust (DUO)

Secure Web Gateway Decryption / Inspection / File Sandboxing (Umbrella)

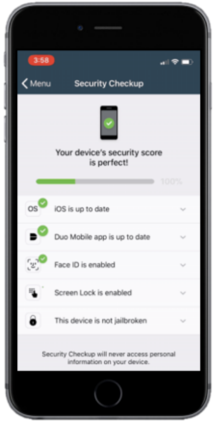
Application Proxy (DUO Net Gateway)

Server Security (Secure Workload)

Private App (web / ssh) (Private DC / IaaS)

SASE – Secure Access Service Edge

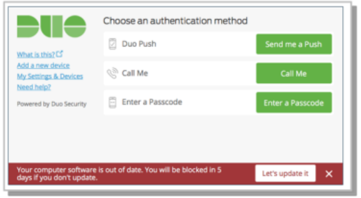
VPN based apps flow capabilities & experience



Your device's security score is perfect!

- OS iOS is up to date
- Duo Mobile app is up to date
- Face ID is enabled
- Screen Lock is enabled
- This device is not jailbroken

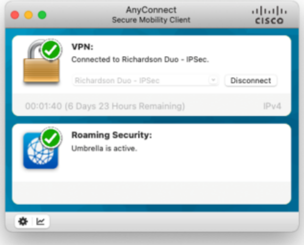
Security Checkup will never access personal information on your device.



Choose an authentication method

Duo Push	Send me a Push
Call Me	Call Me
Enter a Passcode	Enter a Passcode

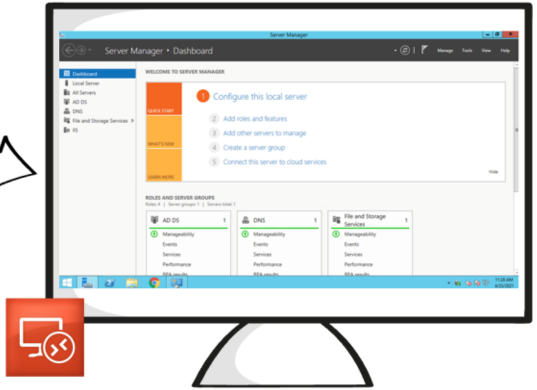
Your computer software is out of date. You will be blocked in 5 days if you don't update.



VPN:
Connected to Richardson Duo - IPSec.

00:01:40 (6 Days 23 Hours Remaining) IPv4

Roaming Security:
Umbrella is active.

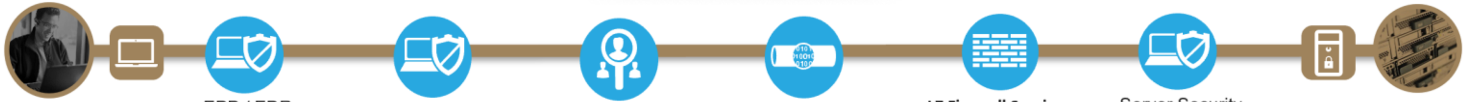


WELCOME TO SERVER MANAGER

1. Configure this local server
2. Add roles and features
3. Add other servers to manage
4. Create a server group
5. Connect this server to cloud services

ROLES AND SERVER GROUPS
Roles: 4 | Server groups: 1 | Servers total: 1

AD DS 1	DNS 1	File and Storage Services 1
Manageability	Manageability	Manageability
Events	Events	Events
Services	Services	Services
Performance	Performance	Performance
BPA results	BPA results	BPA results



Remote Worker

EPP / EDR
(Secure Endpoint)

DNS / IP Security
Content Filtering
(Umbrella Roaming)

SAML / MFA
Device Trust
(DUO)

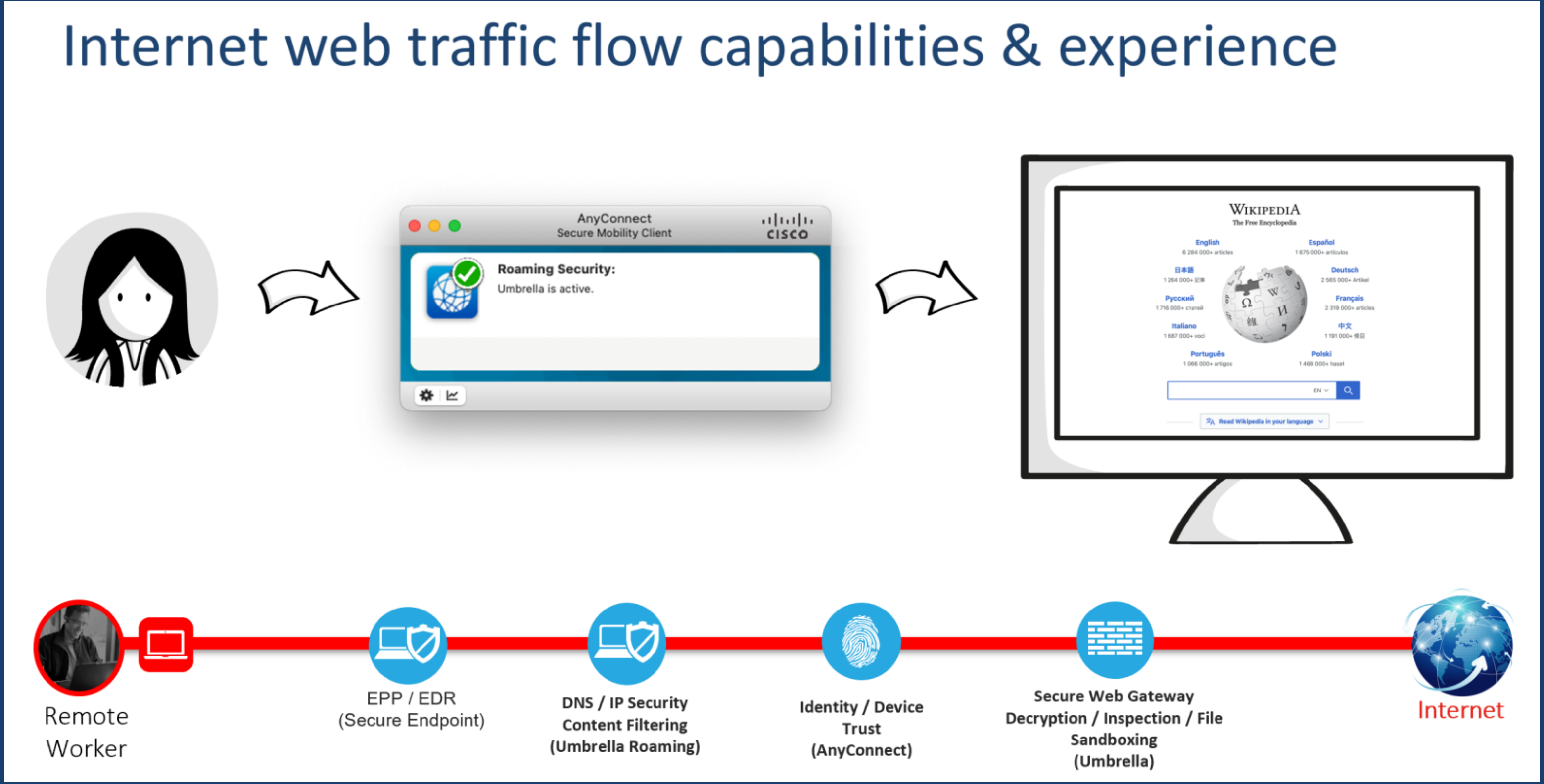
RA VPN / Always On
(AnyConnect)

L7 Firewall Services
(ASA / Firepower)

Server Security
(Secure Workload)

Private App (any tcp/udp)
(Private DC / IaaS)

SASE – Secure Access Service Edge



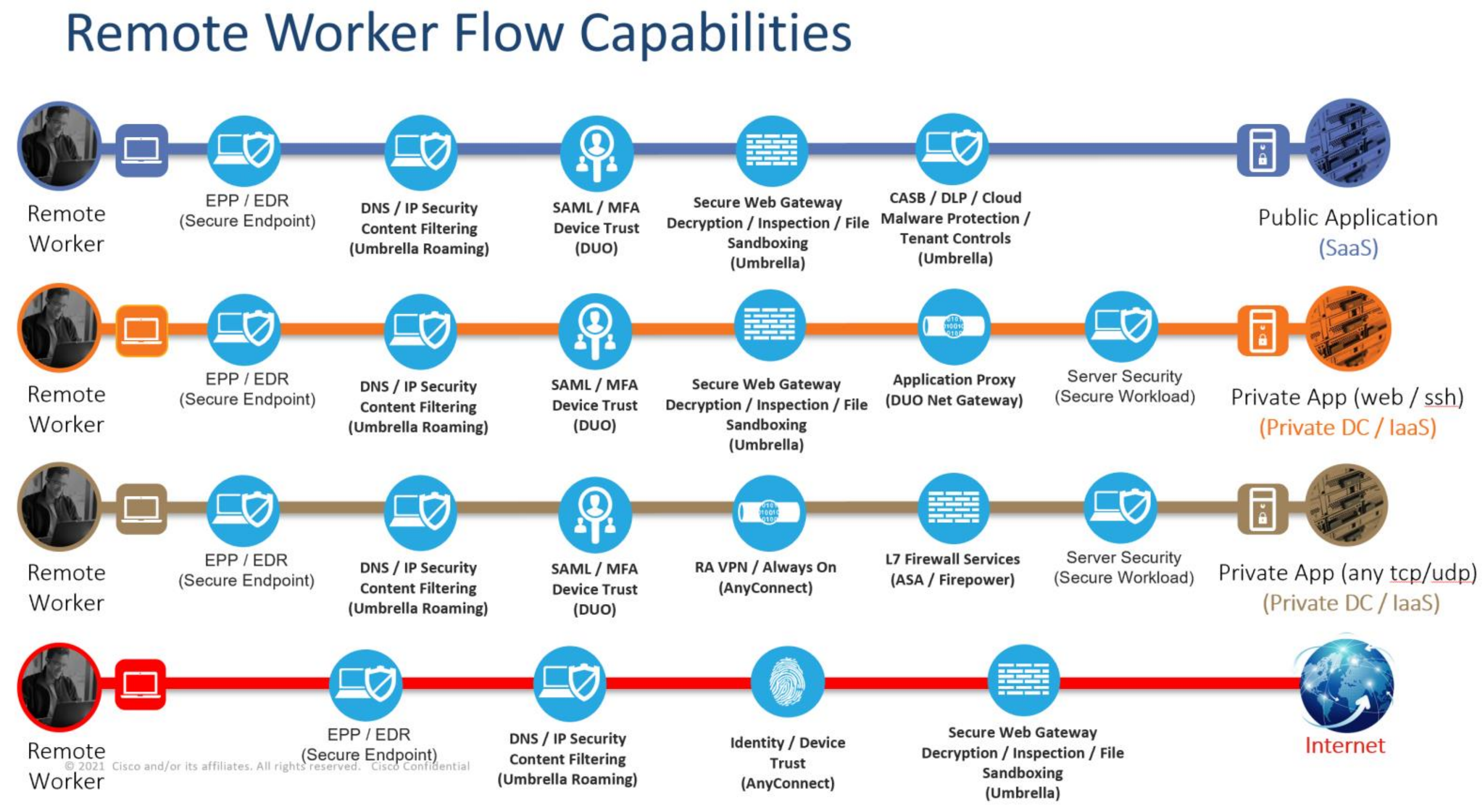
Internet web traffic flow capabilities & experience

AnyConnect
Secure Mobility Client

Roaming Security:
Umbrella is active.

Remote Worker → EPP / EDR (Secure Endpoint) → DNS / IP Security Content Filtering (Umbrella Roaming) → Identity / Device Trust (AnyConnect) → Secure Web Gateway Decryption / Inspection / File Sandboxing (Umbrella) → Internet

SASE – Secure Access Service Edge



Remote Worker Flow Capabilities

Remote Worker → EPP / EDR (Secure Endpoint) → DNS / IP Security Content Filtering (Umbrella Roaming) → SAML / MFA Device Trust (DUO) → Secure Web Gateway Decryption / Inspection / File Sandboxing (Umbrella) → CASB / DLP / Cloud Malware Protection / Tenant Controls (Umbrella) → Public Application (SaaS)

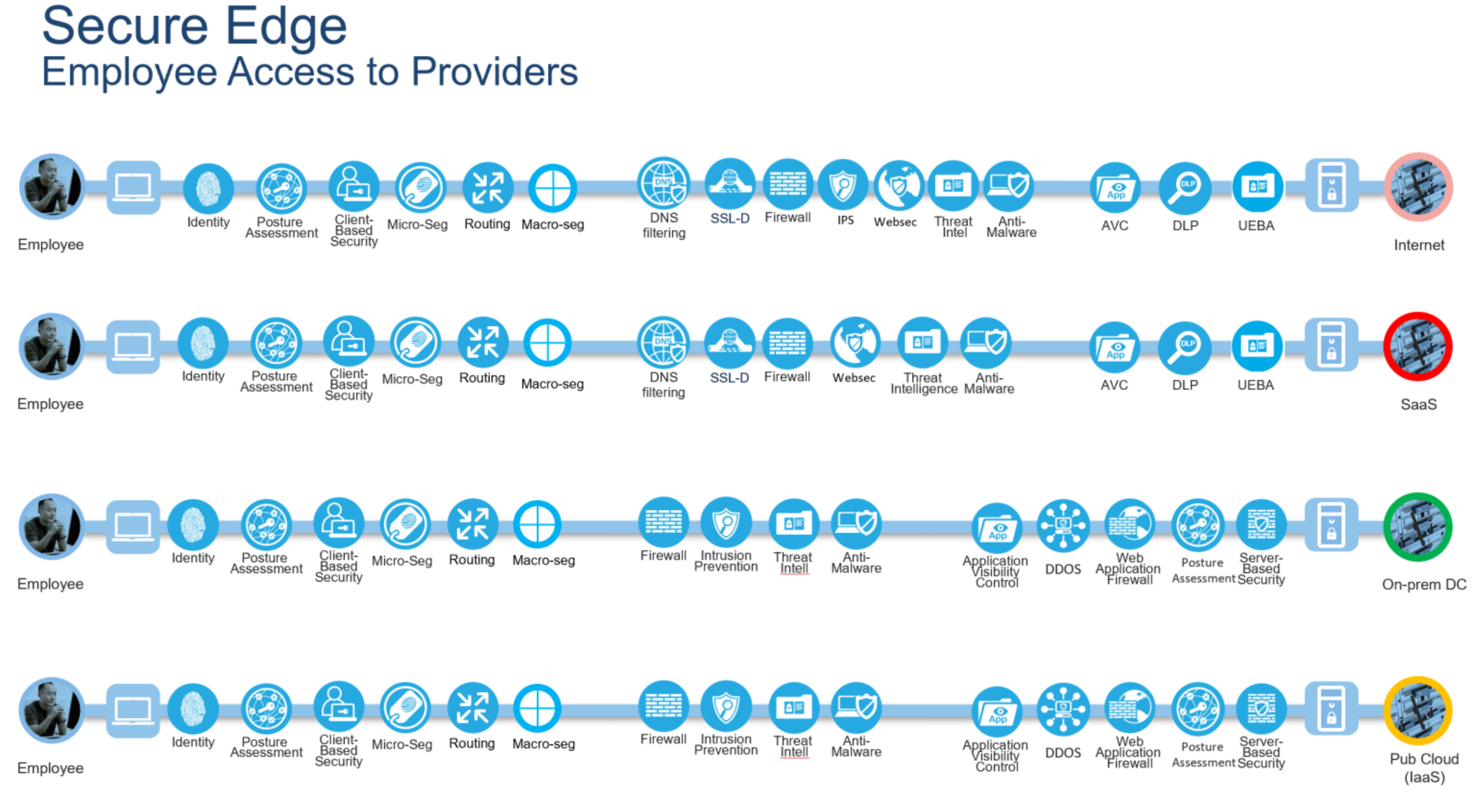
Remote Worker → EPP / EDR (Secure Endpoint) → DNS / IP Security Content Filtering (Umbrella Roaming) → SAML / MFA Device Trust (DUO) → Secure Web Gateway Decryption / Inspection / File Sandboxing (Umbrella) → Application Proxy (DUO Net Gateway) → Server Security (Secure Workload) → Private App (web / ssh) (Private DC / IaaS)

Remote Worker → EPP / EDR (Secure Endpoint) → DNS / IP Security Content Filtering (Umbrella Roaming) → SAML / MFA Device Trust (DUO) → RA VPN / Always On (AnyConnect) → L7 Firewall Services (ASA / Firepower) → Server Security (Secure Workload) → Private App (any tcp/udp) (Private DC / IaaS)

Remote Worker → EPP / EDR (Secure Endpoint) → DNS / IP Security Content Filtering (Umbrella Roaming) → Identity / Device Trust (AnyConnect) → Secure Web Gateway Decryption / Inspection / File Sandboxing (Umbrella) → Internet

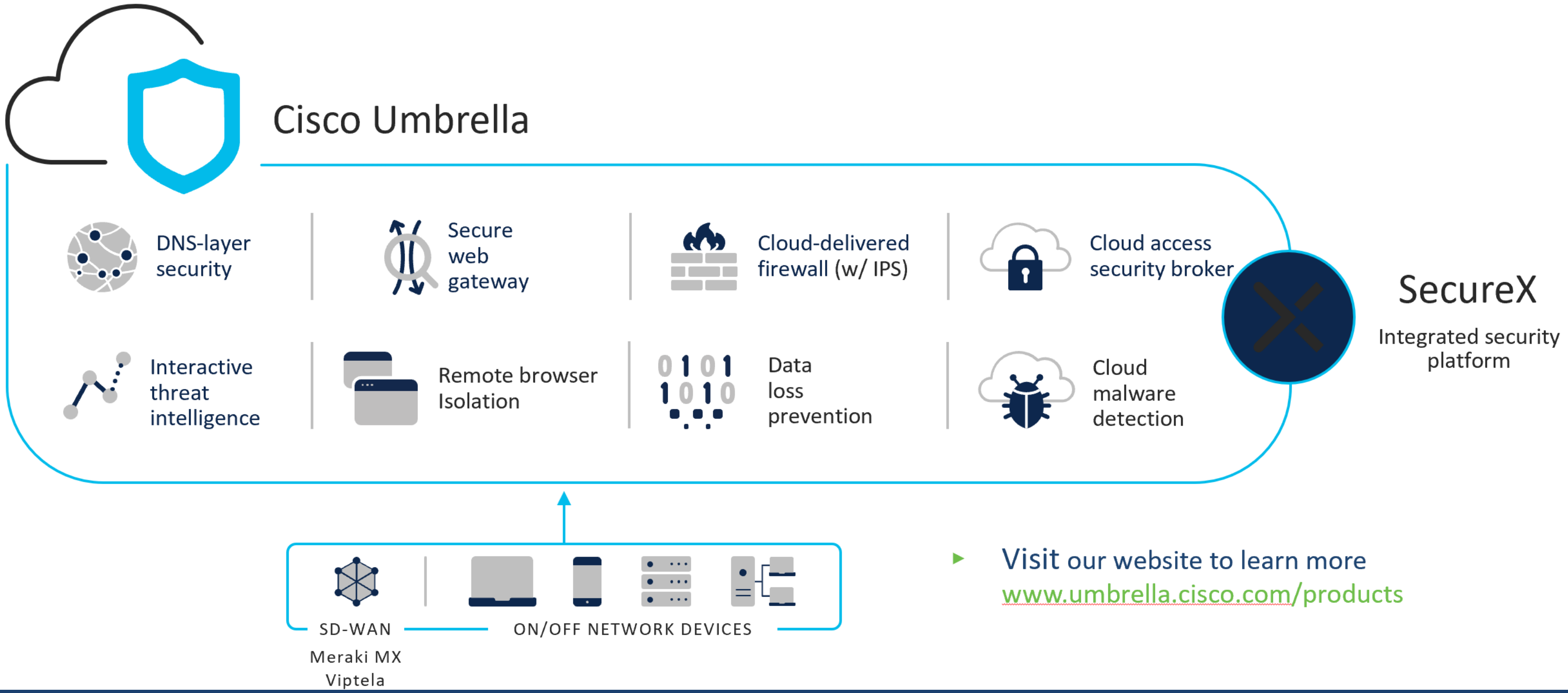
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

SASE – Secure Access Service Edge



Secure Edge
Employee Access to Providers

Cisco Umbrella SIG



Cisco Umbrella

DNS-layer security

Secure web gateway

Cloud-delivered firewall (w/ IPS)

Cloud access security broker

Interactive threat intelligence

Remote browser Isolation

Data loss prevention

Cloud malware detection

SecureX

Integrated security platform

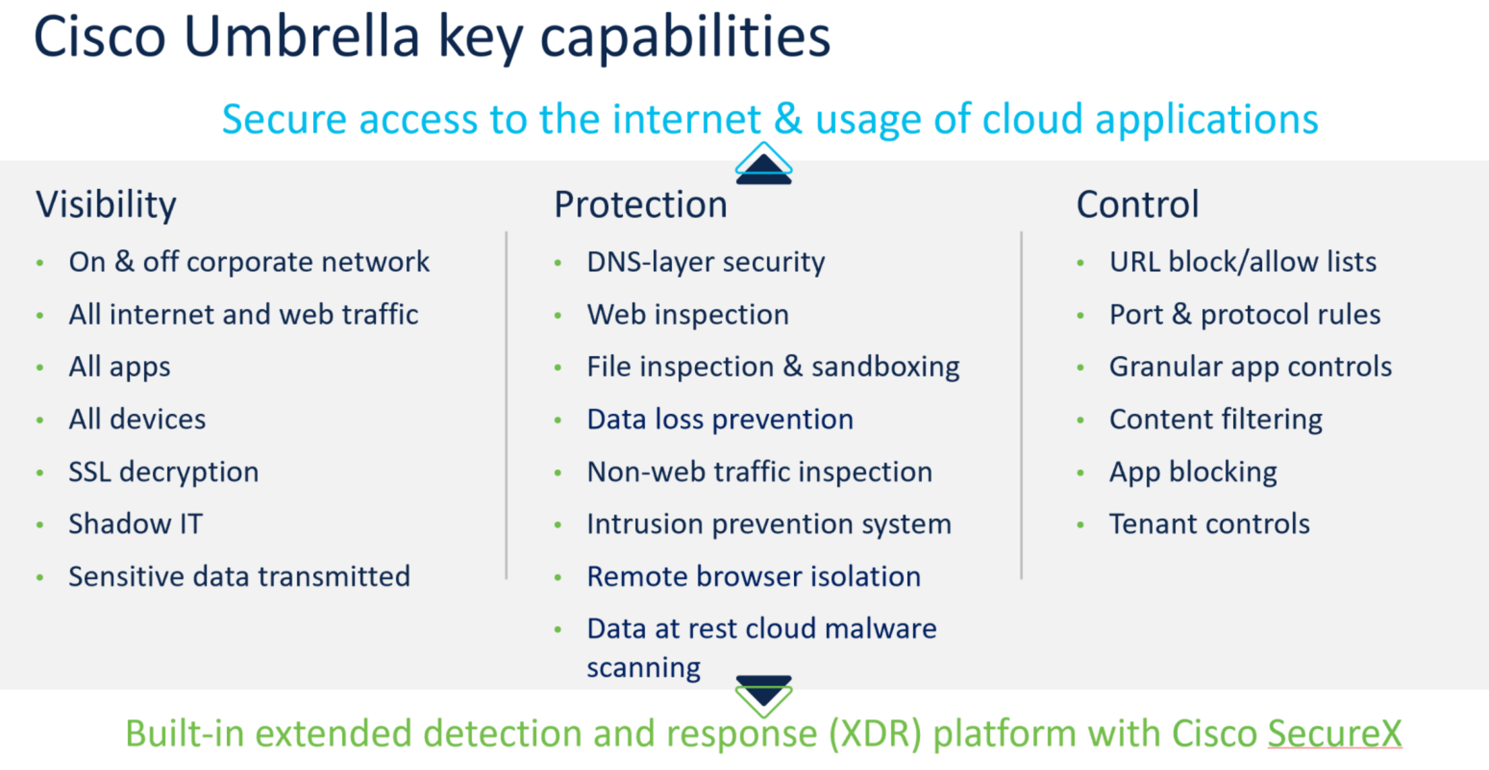
SD-WAN

Meraki MX
Viptela

ON/OFF NETWORK DEVICES

- Visit our website to learn more
  www.umbrella.cisco.com/products

Cisco Umbrella SIG



Cisco Umbrella key capabilities

Secure access to the internet & usage of cloud applications

Visibility

- On & off corporate network
- All internet and web traffic
- All apps
- All devices
- SSL decryption
- Shadow IT
- Sensitive data transmitted

Protection

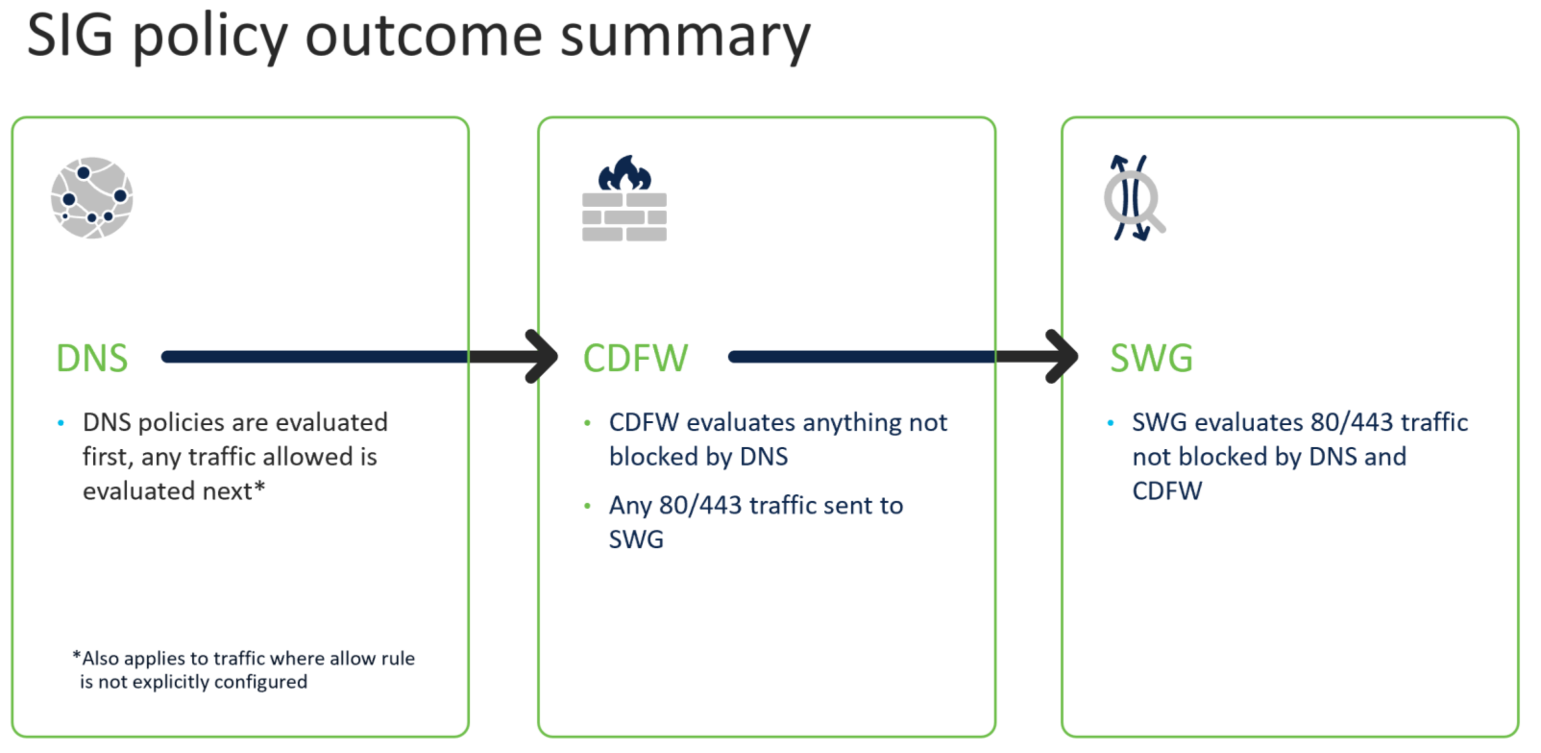
- DNS-layer security
- Web inspection
- File inspection & sandboxing
- Data loss prevention
- Non-web traffic inspection
- Intrusion prevention system
- Remote browser isolation
- Data at rest cloud malware scanning

Control

- URL block/allow lists
- Port & protocol rules
- Granular app controls
- Content filtering
- App blocking
- Tenant controls

Built-in extended detection and response (XDR) platform with Cisco SecureX

Cisco Umbrella SIG



SIG policy outcome summary

DNS

- DNS policies are evaluated first, any traffic allowed is evaluated next*

*Also applies to traffic where allow rule is not explicitly configured

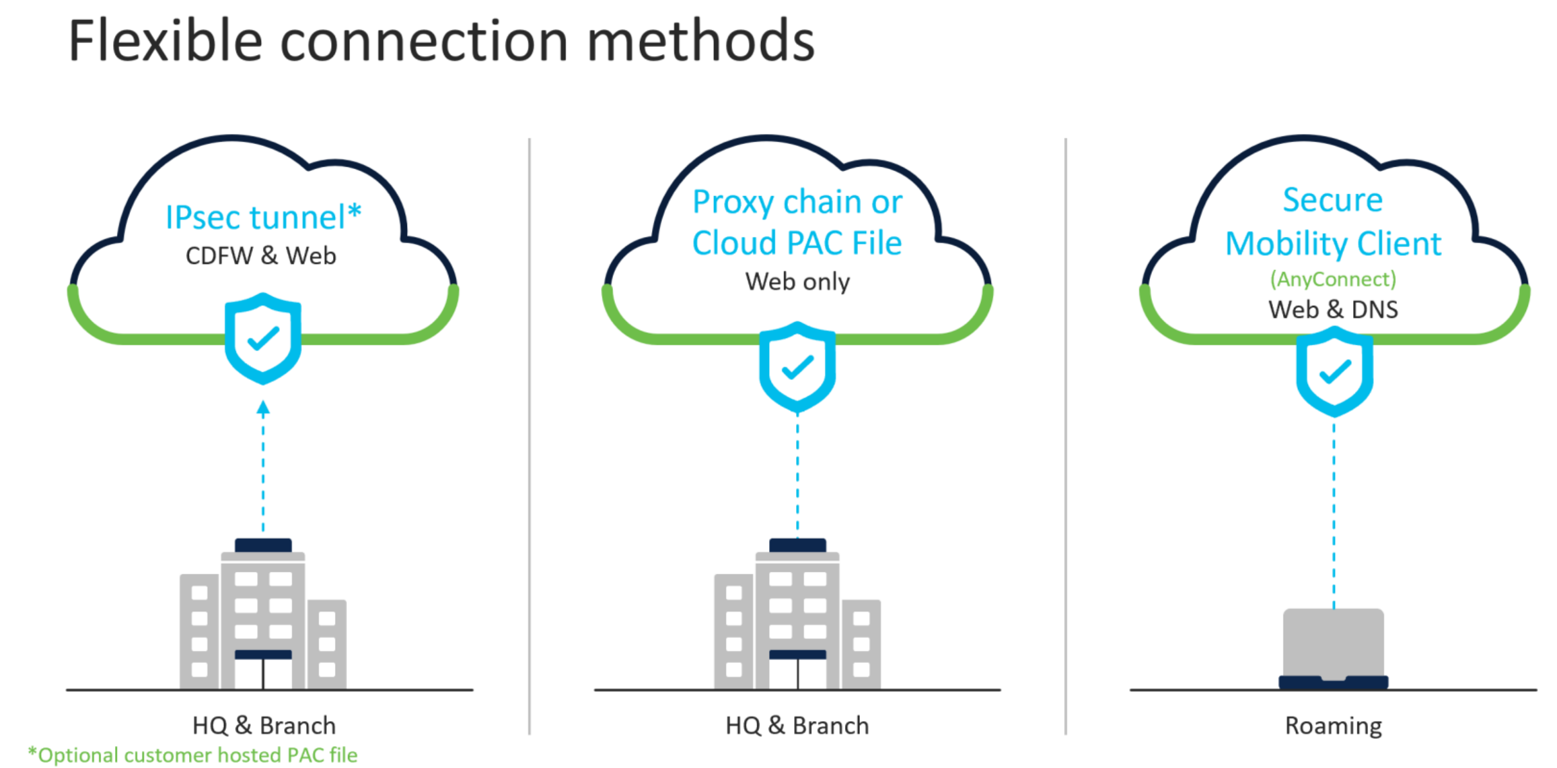
CDFW

- CDFW evaluates anything not blocked by DNS
- Any 80/443 traffic sent to SWG

SWG

- SWG evaluates 80/443 traffic not blocked by DNS and CDFW

Cisco Umbrella SIG



Flexible connection methods

IPsec tunnel*
CDFW & Web

HQ & Branch

Proxy chain or Cloud PAC File
Web only

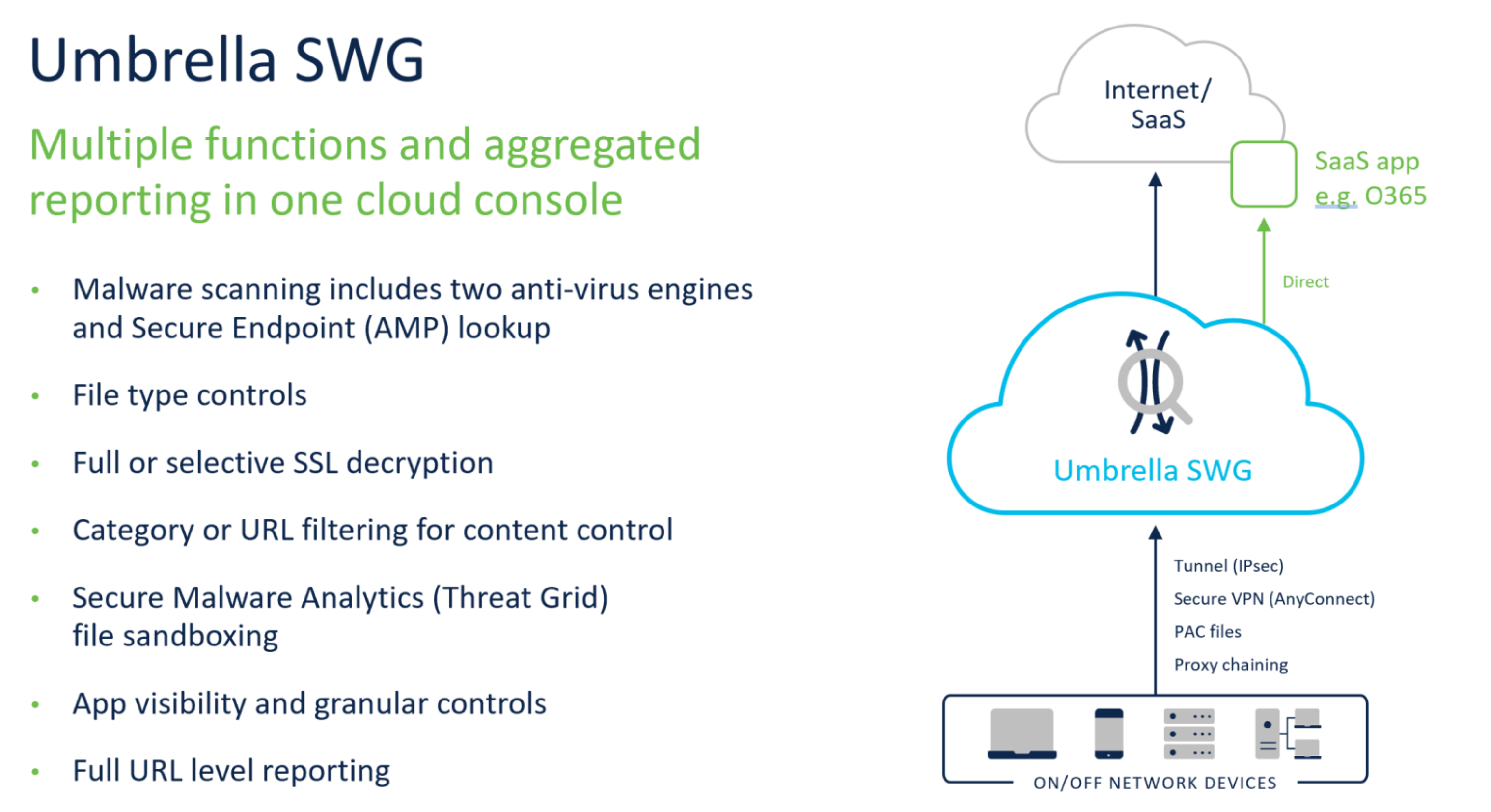
HQ & Branch

Secure Mobility Client
(AnyConnect)
Web & DNS

Roaming

*Optional customer hosted PAC file

Cisco Umbrella SIG – Secure Web Gateway

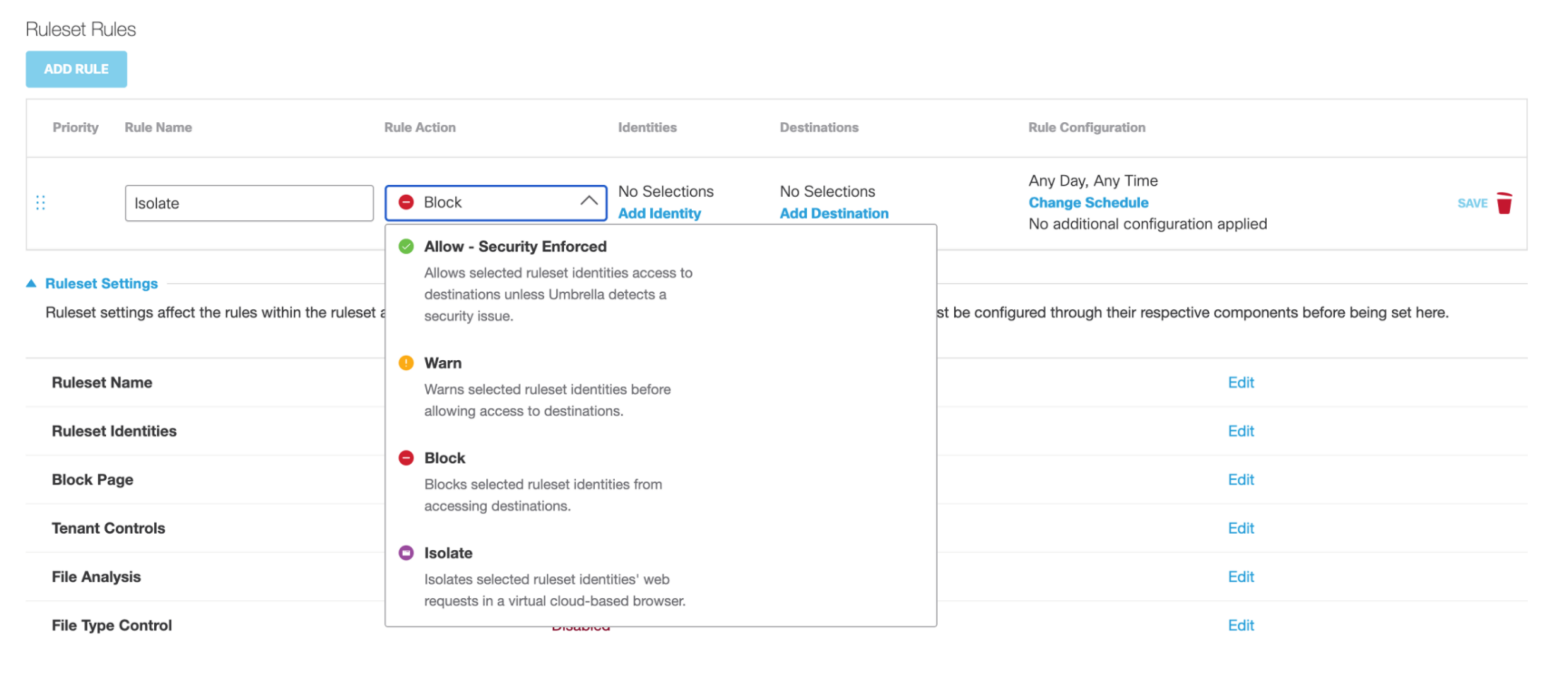


Umbrella SWG

Multiple functions and aggregated reporting in one cloud console

- Malware scanning includes two anti-virus engines and Secure Endpoint (AMP) lookup
- File type controls
- Full or selective SSL decryption
- Category or URL filtering for content control
- Secure Malware Analytics (Threat Grid) file sandboxing
- App visibility and granular controls
- Full URL level reporting

Cisco Umbrella SIG – Secure Web Gateway



Ruleset Rules

ADD RULE

Priority	Rule Name	Rule Action	Identities	Destinations	Rule Configuration	
	Isolate	Block	No Selections Add Identity	No Selections Add Destination	Any Day, Any Time Change Schedule No additional configuration applied	SAVE

Allow - Security Enforced
Allows selected ruleset identities access to destinations unless Umbrella detects a security issue.

Warn
Warns selected ruleset identities before allowing access to destinations.

Block
Blocks selected ruleset identities from accessing destinations.

Isolate
Isolates selected ruleset identities' web requests in a virtual cloud-based browser.

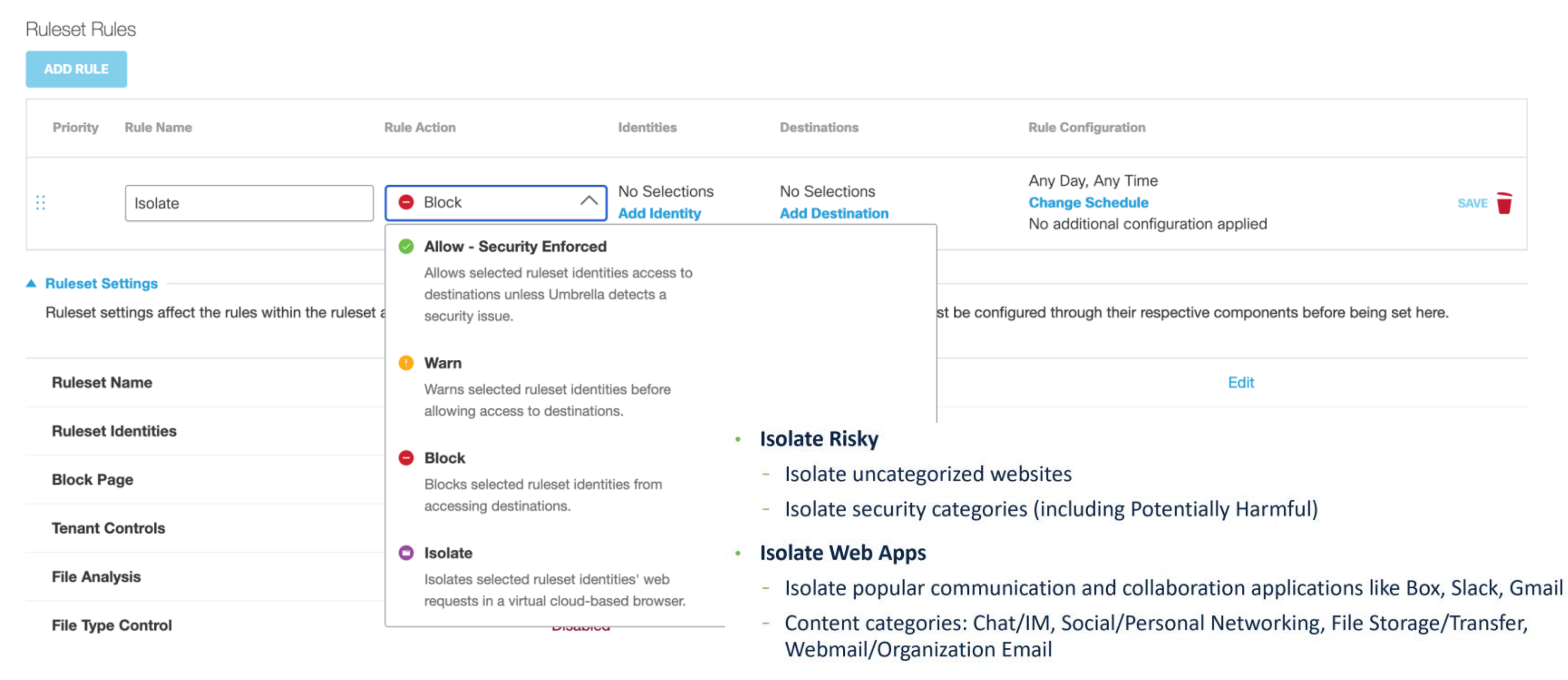
Ruleset Settings

Ruleset settings affect the rules within the ruleset a st be configured through their respective components before being set here.

Ruleset Name		Edit
Ruleset Identities		Edit
Block Page		Edit
Tenant Controls		Edit
File Analysis		Edit
File Type Control	Disabled	Edit

SWS COMPUTERSYSTEME Member of ACP Group

Cisco Umbrella SIG – Secure Web Gateway



Ruleset Rules

Priority	Rule Name	Rule Action	Identities	Destinations	Rule Configuration
⁝	Isolate	Block	No Selections Add Identity	No Selections Add Destination	Any Day, Any Time Change Schedule No additional configuration applied

Allow - Security Enforced
Allows selected ruleset identities access to destinations unless Umbrella detects a security issue.

Warn
Warns selected ruleset identities before allowing access to destinations.

Block
Blocks selected ruleset identities from accessing destinations.

Isolate
Isolates selected ruleset identities' web requests in a virtual cloud-based browser.

▲ Ruleset Settings

Ruleset settings affect the rules within the ruleset a … st be configured through their respective components before being set here.

Ruleset Name	Edit
Ruleset Identities	
Block Page	
Tenant Controls	
File Analysis	
File Type Control	Disabled

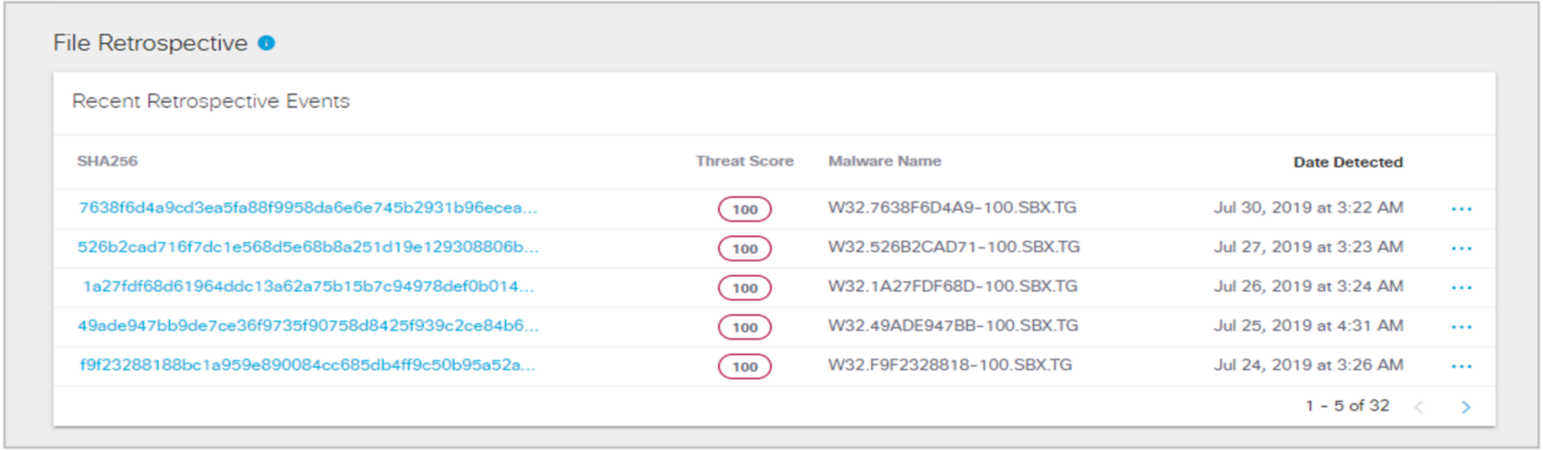
- **Isolate Risky**
  - Isolate uncategorized websites
  - Isolate security categories (including Potentially Harmful)
- **Isolate Web Apps**
  - Isolate popular communication and collaboration applications like Box, Slack, Gmail
  - Content categories: Chat/IM, Social/Personal Networking, File Storage/Transfer, Webmail/Organization Email
- **Isolate Any**
  - Isolate any chosen destination, including content categories, security categories, destination lists, applications, uncategorized, etc.

Cisco Umbrella SIG – Secure Web Gateway

Secure Malware Analytics (Threat Grid)

Sandbox inspection

- Files that make it through the anti-virus and malware scan by Cisco SecureX Malware Analytics and third-party tools (less than 50 Mb in size)
- Files that haven’t been seen before by Cisco Secure Malware Analytics and have attributes that the Cisco Secure Malware Analytics model targets
- We are using libmagic for file type detection as well as listed file extension



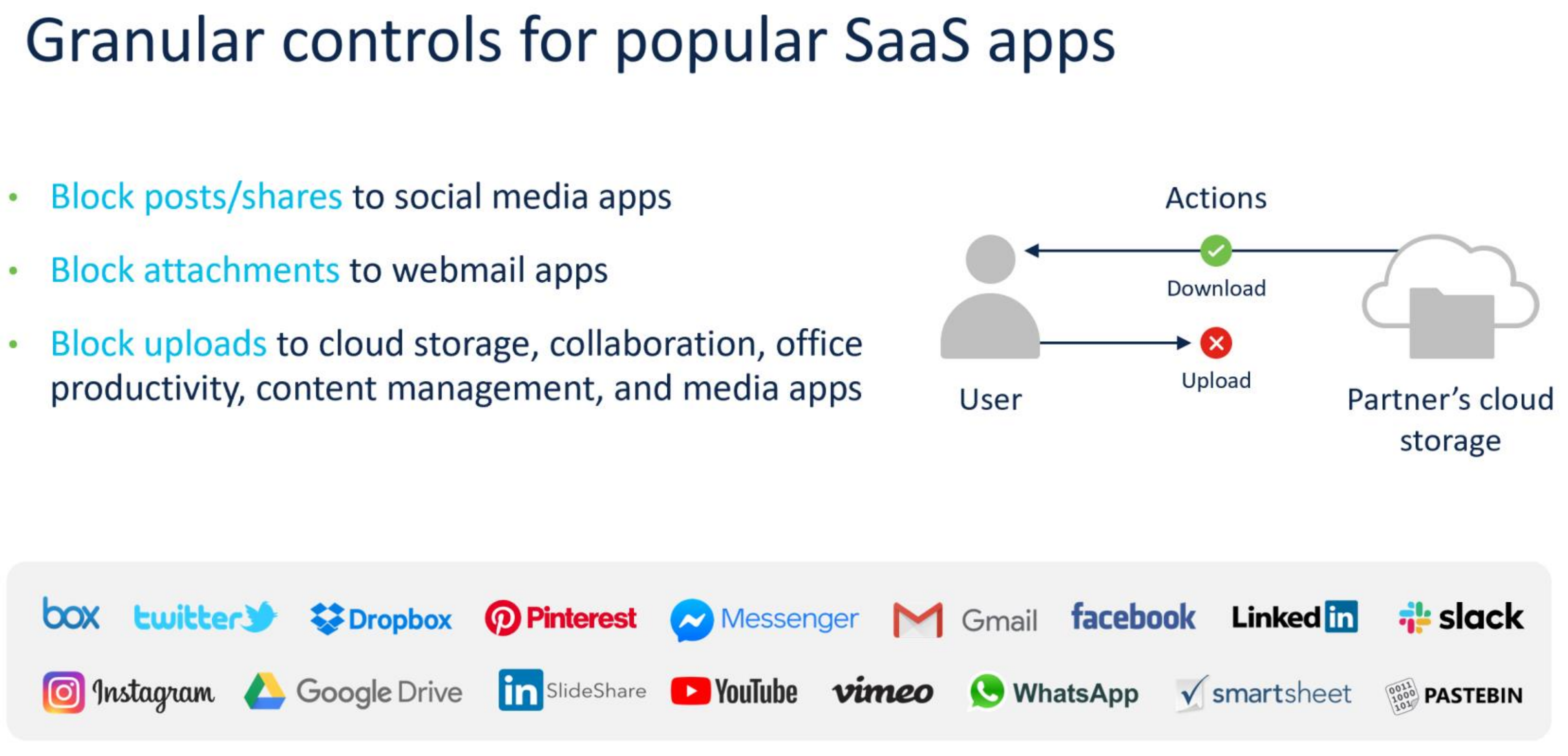
File Retrospective

Recent Retrospective Events

SHA256	Threat Score	Malware Name	Date Detected	
7638f6d4a9cd3ea5fa88f9958da6e6e745b2931b96ecea...	100	W32.7638F6D4A9-100.SBX.TG	Jul 30, 2019 at 3:22 AM	···
526b2cad716f7dc1e568d5e68b8a251d19e129308806b...	100	W32.526B2CAD71-100.SBX.TG	Jul 27, 2019 at 3:23 AM	···
1a27fdf68d61964ddc13a62a75b15b7c94978def0b014...	100	W32.1A27FDF68D-100.SBX.TG	Jul 26, 2019 at 3:24 AM	···
49ade947bb9de7ce36f9735f90758d8425f939c2ce84b6...	100	W32.49ADE947BB-100.SBX.TG	Jul 25, 2019 at 4:31 AM	···
f9f23288188bc1a959e890084cc685db4ff9c50b95a52a...	100	W32.F9F2328818-100.SBX.TG	Jul 24, 2019 at 3:26 AM	···

1 - 5 of 32 ‹ ›

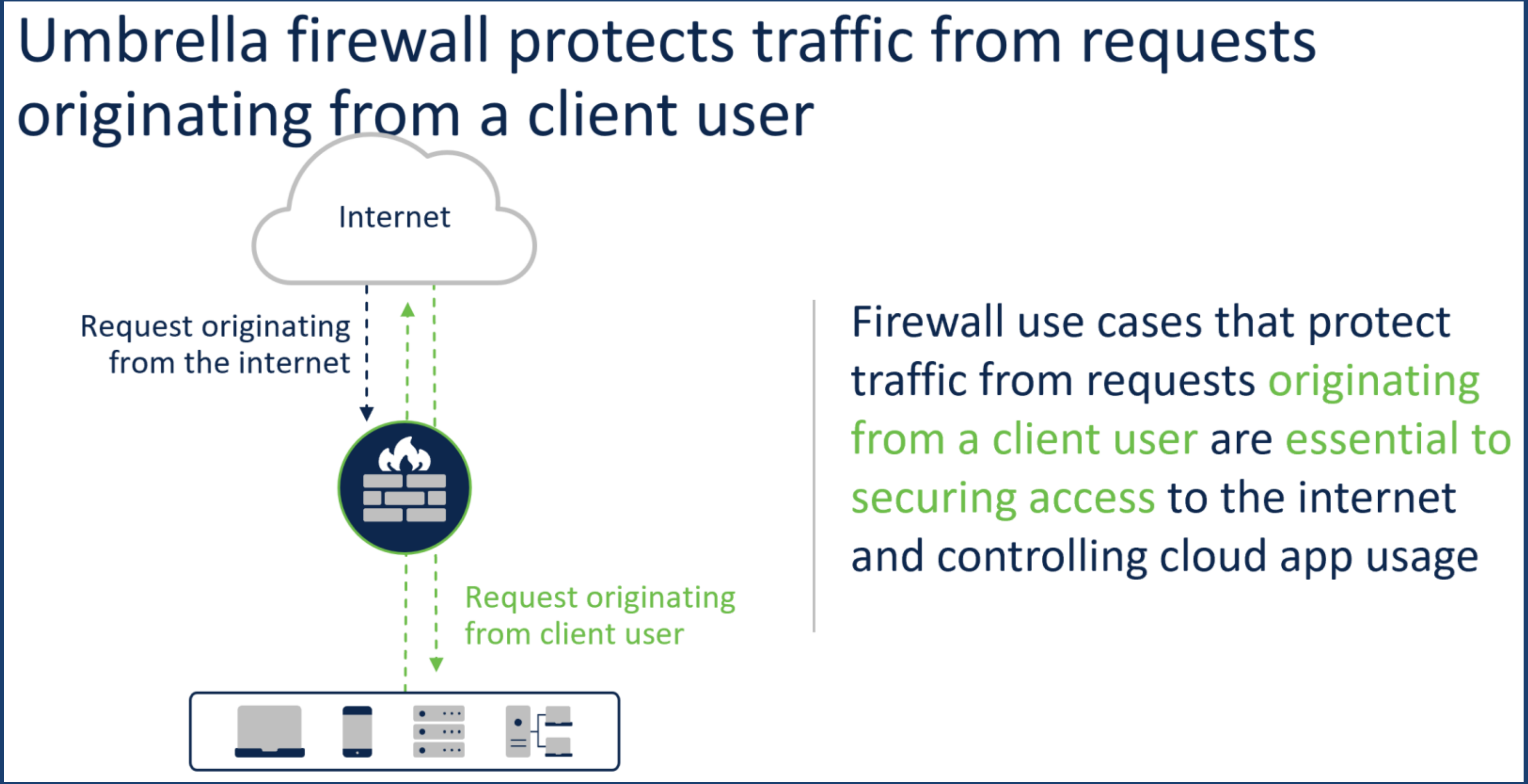
Cisco Umbrella SIG – Secure Web Gateway



Granular controls for popular SaaS apps

- Block posts/shares to social media apps
- Block attachments to webmail apps
- Block uploads to cloud storage, collaboration, office productivity, content management, and media apps

Cisco Umbrella SIG – Cloud Delivered Firewall

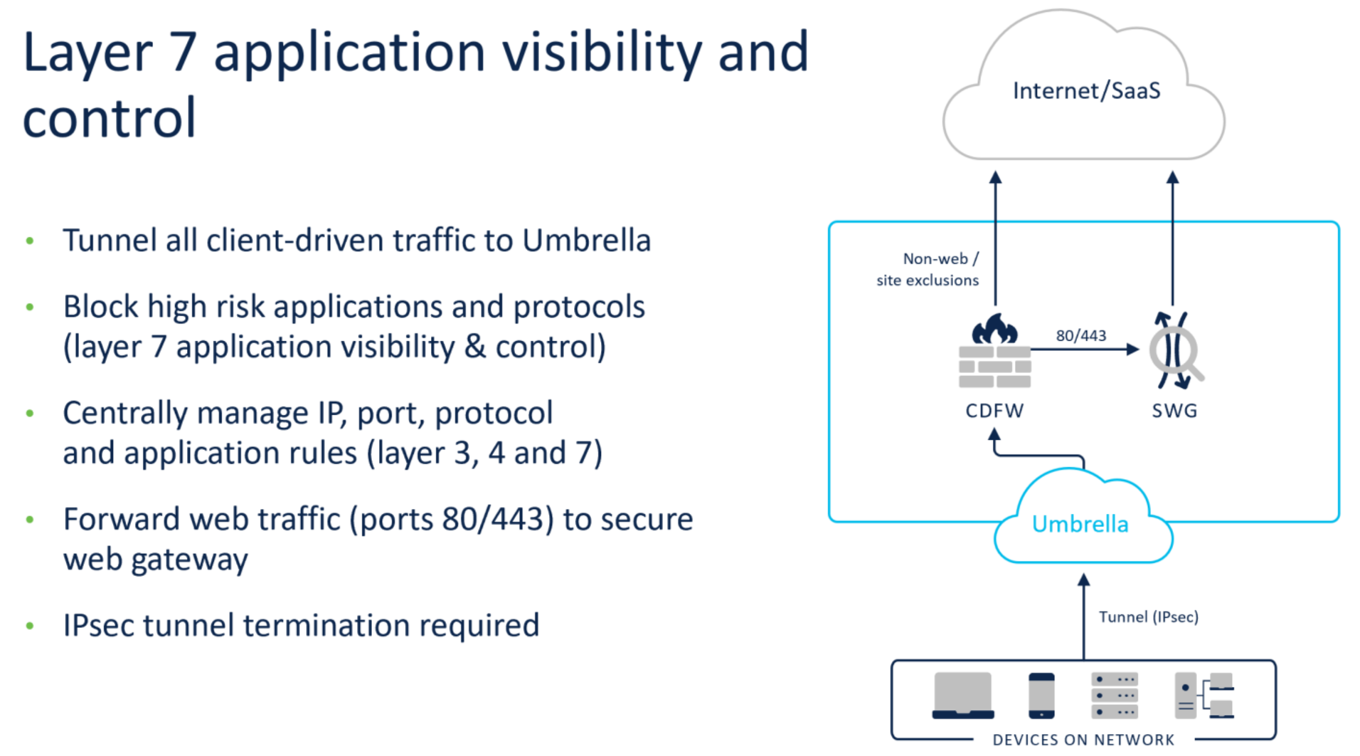


Umbrella firewall protects traffic from requests originating from a client user

Internet
Request originating from the internet
Request originating from client user

Firewall use cases that protect traffic from requests originating from a client user are essential to securing access to the internet and controlling cloud app usage

Cisco Umbrella SIG – Cloud Delivered Firewall

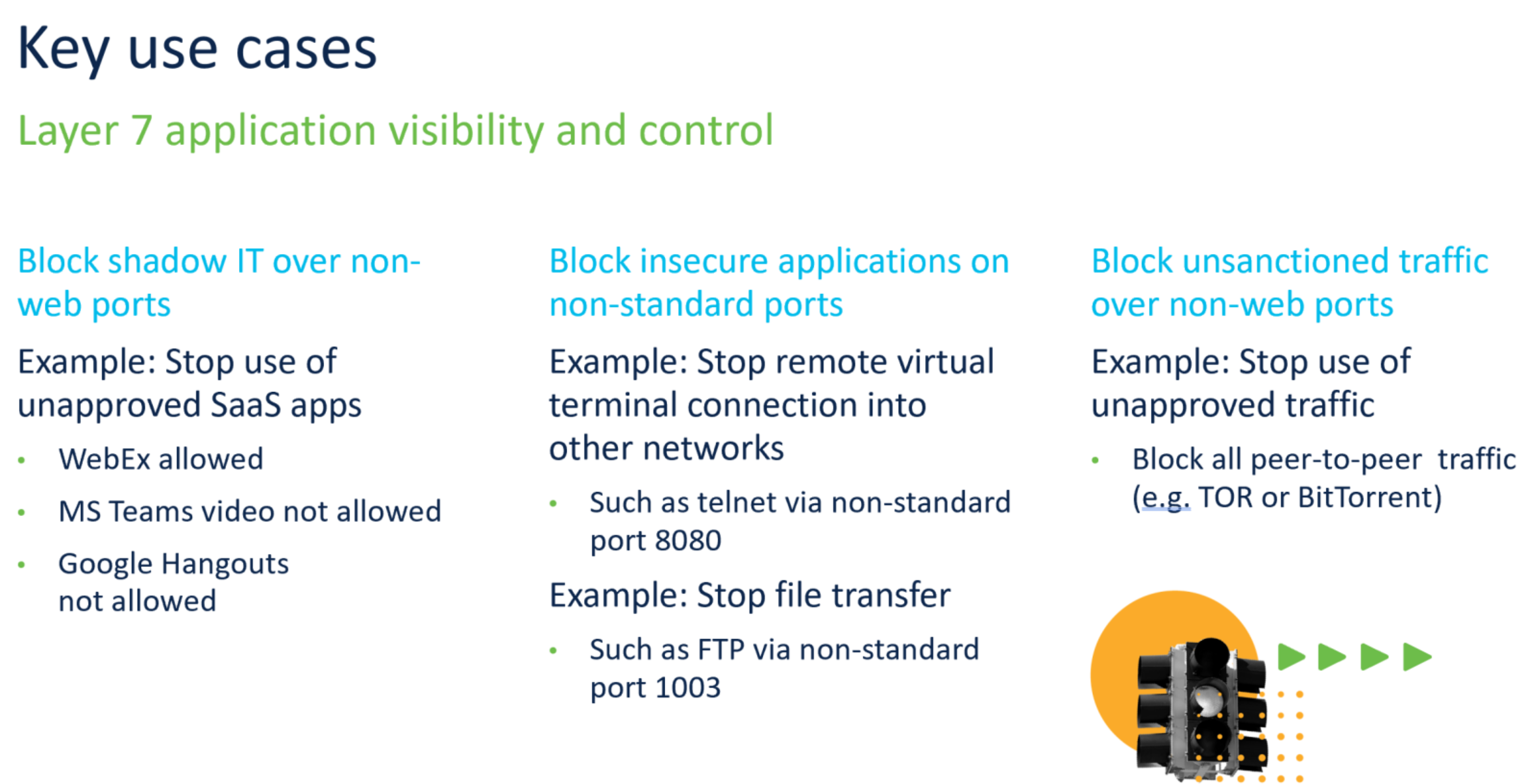


Layer 7 application visibility and control

- Tunnel all client-driven traffic to Umbrella
- Block high risk applications and protocols (layer 7 application visibility & control)
- Centrally manage IP, port, protocol and application rules (layer 3, 4 and 7)
- Forward web traffic (ports 80/443) to secure web gateway
- IPsec tunnel termination required

Internet/SaaS
Non-web / site exclusions
80/443
CDFW
SWG
Umbrella
Tunnel (IPsec)
DEVICES ON NETWORK

Cisco Umbrella SIG – Cloud Delivered Firewall



Key use cases

Layer 7 application visibility and control

Block shadow IT over non-web ports

Example: Stop use of unapproved SaaS apps

- WebEx allowed
- MS Teams video not allowed
- Google Hangouts not allowed

Block insecure applications on non-standard ports

Example: Stop remote virtual terminal connection into other networks

- Such as telnet via non-standard port 8080

Example: Stop file transfer

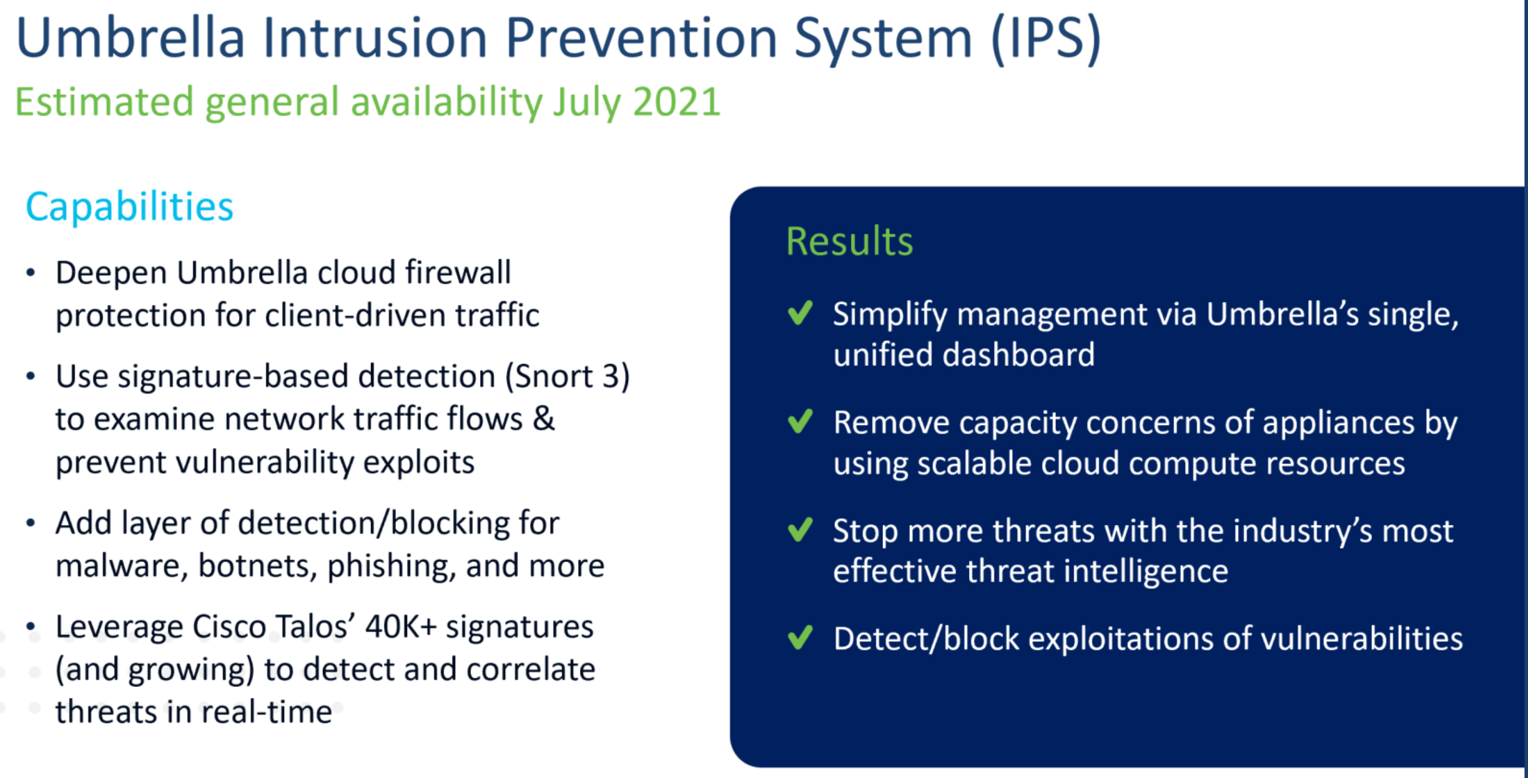
- Such as FTP via non-standard port 1003

Block unsanctioned traffic over non-web ports

Example: Stop use of unapproved traffic

- Block all peer-to-peer traffic (e.g. TOR or BitTorrent)

Cisco Umbrella SIG – Cloud Delivered Firewall



Umbrella Intrusion Prevention System (IPS)

Estimated general availability July 2021

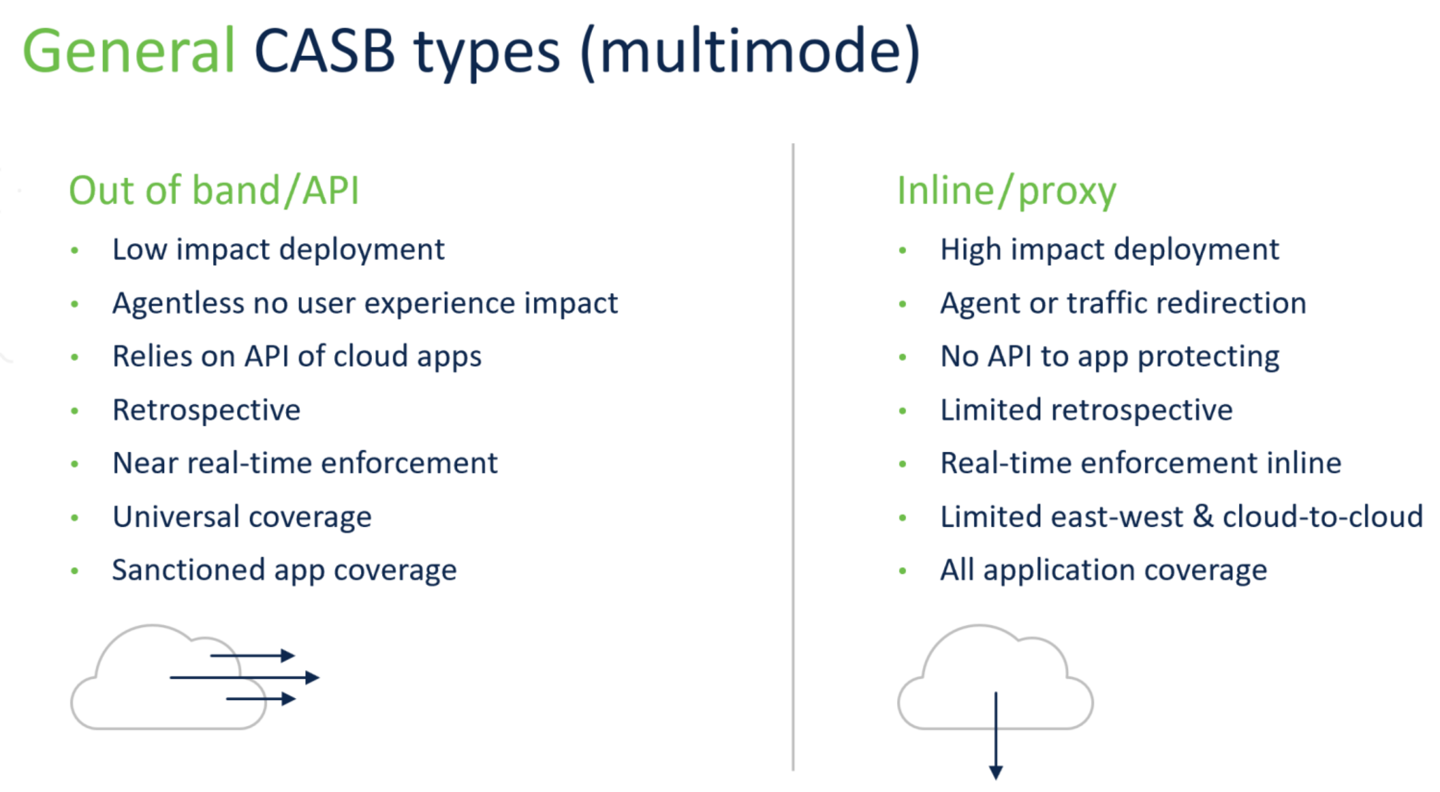
Capabilities

- Deepen Umbrella cloud firewall protection for client-driven traffic
- Use signature-based detection (Snort 3) to examine network traffic flows & prevent vulnerability exploits
- Add layer of detection/blocking for malware, botnets, phishing, and more
- Leverage Cisco Talos' 40K+ signatures (and growing) to detect and correlate threats in real-time

Results

- ✓ Simplify management via Umbrella's single, unified dashboard
- ✓ Remove capacity concerns of appliances by using scalable cloud compute resources
- ✓ Stop more threats with the industry's most effective threat intelligence
- ✓ Detect/block exploitations of vulnerabilities

Cisco Umbrella SIG – Cloud Access Security Broker



General CASB types (multimode)

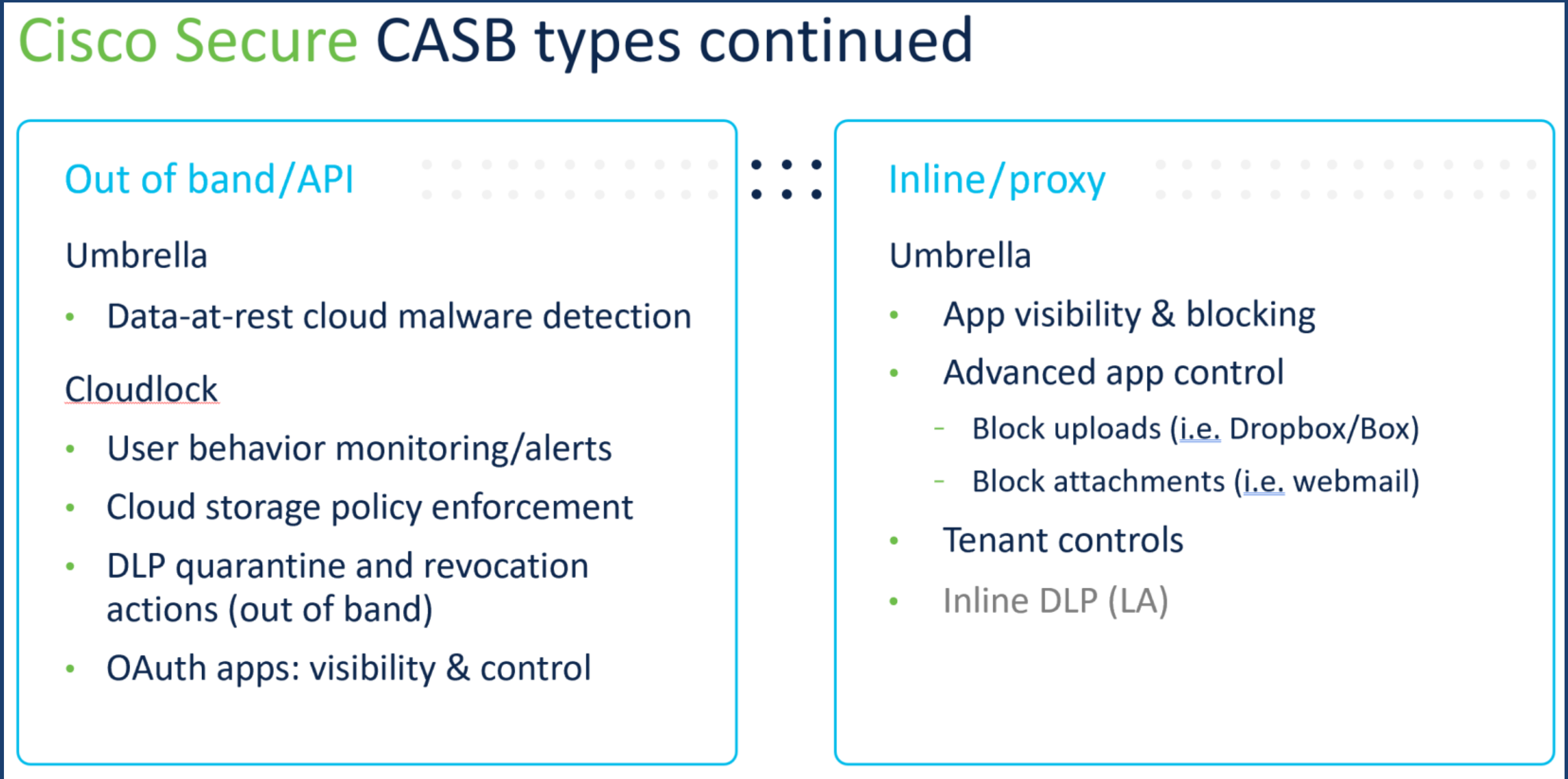
Out of band/API

- Low impact deployment
- Agentless no user experience impact
- Relies on API of cloud apps
- Retrospective
- Near real-time enforcement
- Universal coverage
- Sanctioned app coverage

Inline/proxy

- High impact deployment
- Agent or traffic redirection
- No API to app protecting
- Limited retrospective
- Real-time enforcement inline
- Limited east-west & cloud-to-cloud
- All application coverage

Cisco Umbrella SIG – Cloud Access Security Broker



Cisco Secure CASB types continued

Out of band/API

Umbrella

- Data-at-rest cloud malware detection

Cloudlock

- User behavior monitoring/alerts
- Cloud storage policy enforcement
- DLP quarantine and revocation actions (out of band)
- OAuth apps: visibility & control

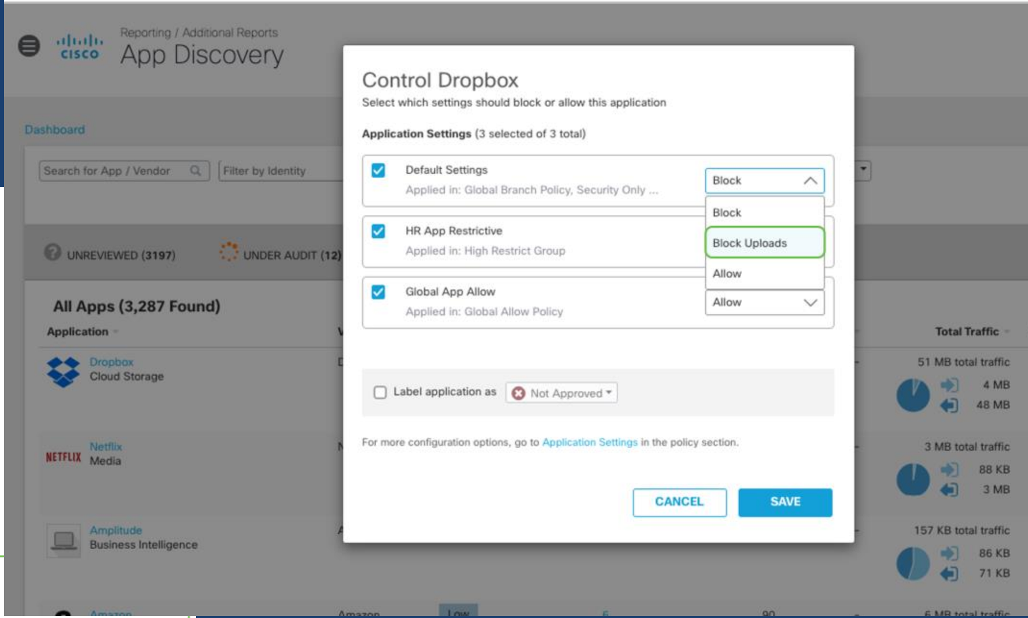
Inline/proxy

Umbrella

- App visibility & blocking
- Advanced app control
  - Block uploads (i.e. Dropbox/Box)
  - Block attachments (i.e. webmail)
- Tenant controls
- Inline DLP (LA)

Cisco Umbrella SIG – Cloud Access Security Broker

Granular app controls



Reporting / Additional Reports

App Discovery

Dashboard

Search for App / Vendor

Filter by Identity

UNREVIEWED (3197)

UNDER AUDIT (12)

All Apps (3,287 Found)

Application	Total Traffic
Dropbox Cloud Storage	51 MB total traffic 4 MB 48 MB
Netflix Media	3 MB total traffic 88 KB 3 MB
Amplitude Business Intelligence	157 KB total traffic 86 KB 71 KB

Control Dropbox

Select which settings should block or allow this application

Application Settings (3 selected of 3 total)

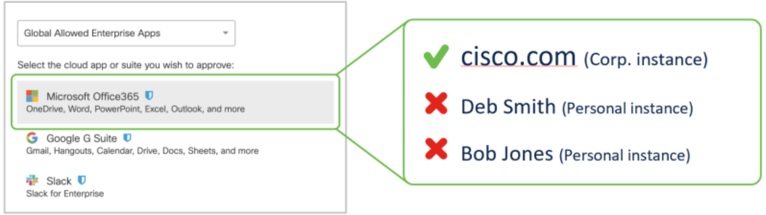
- ☑ Default Settings — Applied in: Global Branch Policy, Security Only ... — Block
- ☑ HR App Restrictive — Applied in: High Restrict Group — Block Uploads
- ☑ Global App Allow — Applied in: Global Allow Policy — Allow

□ Label application as: Not Approved

For more configuration options, go to Application Settings in the policy section.

Tenant controls

Select the instance(s) of Core SaaS applications that can be accessed by all users or by specific groups/individuals



Global Allowed Enterprise Apps

Select the cloud app or suite you wish to approve:

- Microsoft Office365 — OneDrive, Word, PowerPoint, Excel, Outlook, and more
- Google G Suite — Gmail, Hangouts, Calendar, Drive, Docs, Sheets, and more
- Slack — Slack for Enterprise

✓ cisco.com (Corp. instance)

✗ Deb Smith (Personal instance)

✗ Bob Jones (Personal instance)

Key Use Cases

Security
Ensure, sensitive data is created and stored in approved instances of cloud apps

Productivity
Only provide access to corporate instances of core SaaS apps

Cisco Umbrella SIG – Cloud Access Security Broker

Data-at-rest, cloud malware detection (API-based)

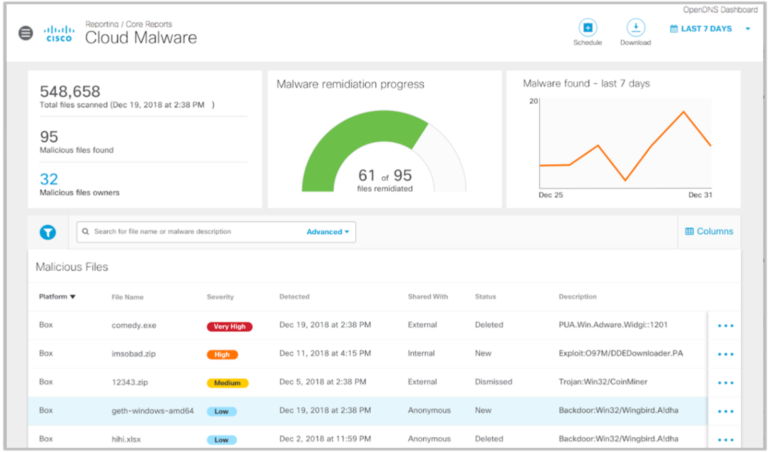
Files that contain malware in cloud repositories can do damage

Malware enters/exits via:

- Endpoints that aren’t covered by Cisco Secure Endpoint (AMP)
- Unmanaged devices
- External sharing- sharing files with other companies

Solution:

- Scan repositories and ongoing save events for cloud storage



Cloud Malware

548,658
Total files scanned (Dec 19, 2018 at 2:38 PM)

95
Malicious files found

32
Malicious files owners

Malware remidiation progress

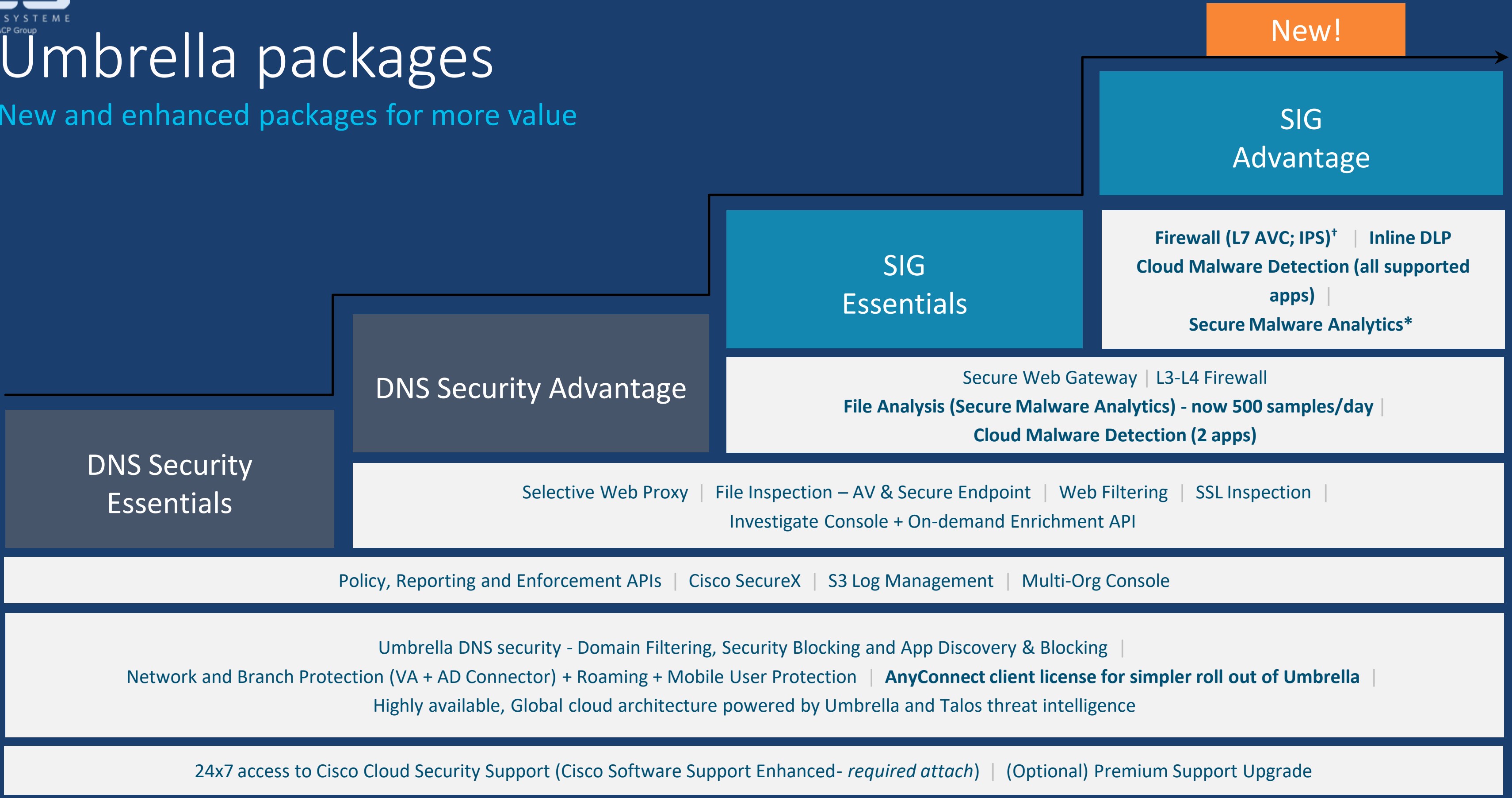
61 of 95
files remidiated

Malicious Files

Platform ▼	File Name	Severity	Detected	Shared With	Status	Description
Box	comedy.exe	Very High	Dec 19, 2018 at 2:38 PM	External	Deleted	PUA.Win.Adware.Widgi::1201
Box	imsobad.zip	High	Dec 11, 2018 at 4:15 PM	Internal	New	Exploit:O97M/DDEDownloader.PA
Box	12343.zip	Medium	Dec 5, 2018 at 2:38 PM	External	Dismissed	Trojan:Win32/CoinMiner
Box	geth-windows-amd64	Low	Dec 19, 2018 at 2:38 PM	Anonymous	New	Backdoor:Win32/Wingbird.A!dha
Box	hihi.xlsx	Low	Dec 2, 2018 at 11:59 PM	Anonymous	Deleted	Backdoor:Win32/Wingbird.A!dha

Umbrella packages

New and enhanced packages for more value



New!

SIG Advantage

Firewall (L7 AVC; IPS)† | **Inline DLP**
Cloud Malware Detection (all supported apps) |
Secure Malware Analytics*

SIG Essentials

Secure Web Gateway | L3-L4 Firewall
File Analysis (Secure Malware Analytics) - now 500 samples/day |
Cloud Malware Detection (2 apps)

DNS Security Advantage

Selective Web Proxy | File Inspection – AV & Secure Endpoint | Web Filtering | SSL Inspection |
Investigate Console + On-demand Enrichment API

DNS Security Essentials

Policy, Reporting and Enforcement APIs | Cisco SecureX | S3 Log Management | Multi-Org Console

Umbrella DNS security - Domain Filtering, Security Blocking and App Discovery & Blocking |
Network and Branch Protection (VA + AD Connector) + Roaming + Mobile User Protection | **AnyConnect client license for simpler roll out of Umbrella** |
Highly available, Global cloud architecture powered by Umbrella and Talos threat intelligence

24x7 access to Cisco Cloud Security Support (Cisco Software Support Enhanced- *required attach*) | (Optional) Premium Support Upgrade

** Secure Malware Analytics (formerly known as Threat Grid) for 3 admin users and unlimited sample submissions*
L7 Cloud Firewall includes IPS, †Also available as add-ons for SIG-Essentials

Agenda

- Endpoint und Perimeter Security
- Cisco EDR – Secure Endpoint
- Secure Endpoint – Visibility, Threat Hunting - Demo
- Cisco SASE – Umbrella SIG
- Umbrella SIG - Demo
- Q&A

Vielen Dank für Ihre Aufmerksamkeit.

Fragen?

Wir freuen uns auf Ihre weitere Anmeldung für unsere Webinar Serie:
- Netzwerkanalyse (Firewall, Stealthwatch)
- NAC und MFA