



CISCO SECURITY

Kovaci Petru-Dan
Senior Presales Engineer



IMPORTANCE of CYBER SECURITY

- The importance of security in today's digital landscape, with cyber threats becoming increasingly sophisticated and frequent.
- The impact of security breaches on organizations, including financial loss, damage to reputation, and loss of customer trust.
- The need for a holistic and proactive approach to security that leverages advanced technologies and best practices, and how Cisco devices and solutions can help.

C.I.A Triad

- **Confidentiality** makes sure that only authorized personnel are given access or permission to modify data
- **Integrity** helps maintain the trustworthiness of data by having it in the correct state and immune to any improper modifications
- **Availability** means that the authorized users should be able to access data whenever required



Goals of Information Security



Prevention refers to preventing computer or information violations from occurring. Security breaches are also referred to as incidents.



Detection refers to identifying events when they occur. Detection is a very difficult problem in many situations



Response refers to developing strategies and techniques to deal with an attack or loss

Overview of Networks

The Internet is a global network that connects computer and networks together

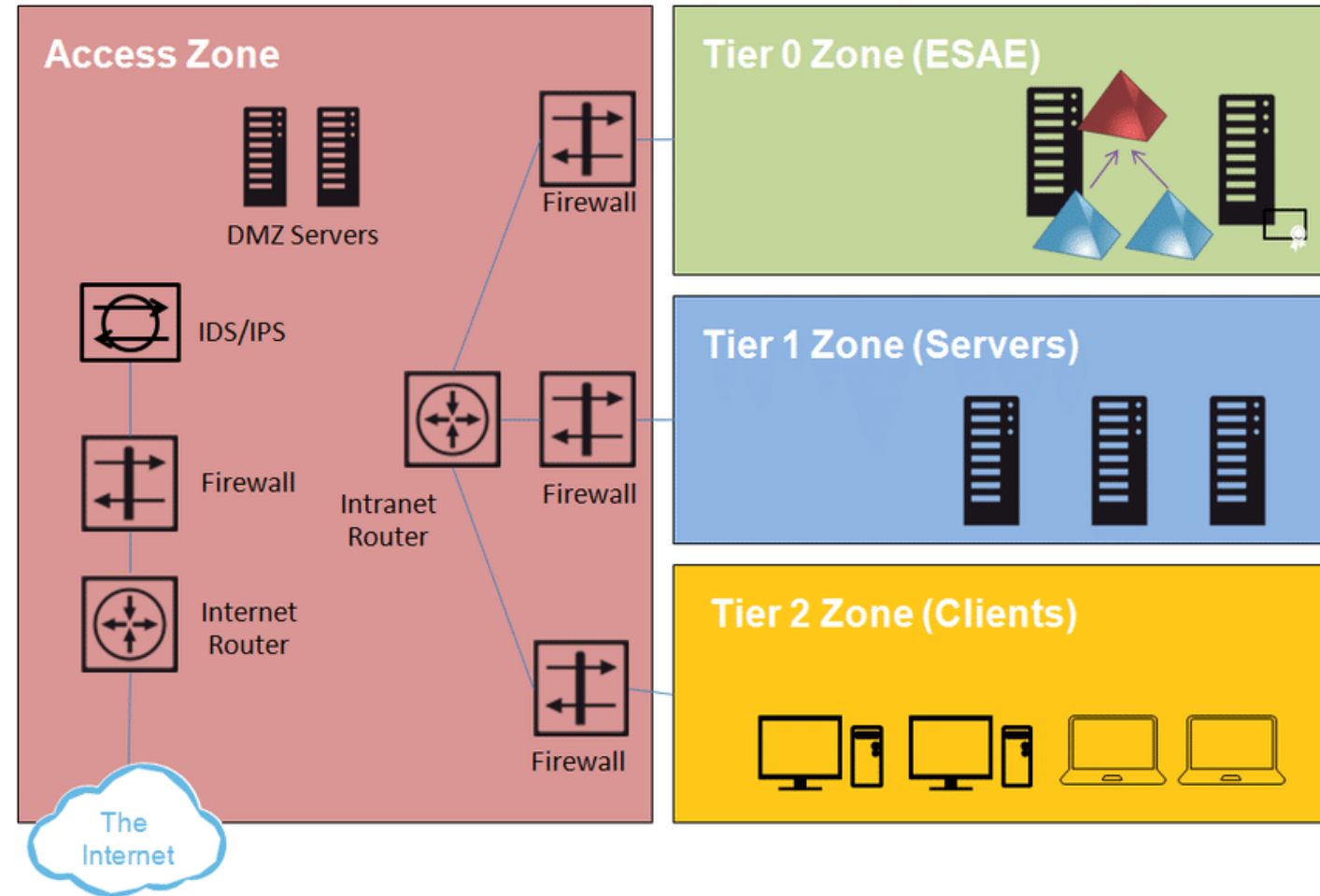
Intranets are private networks implemented and maintained by an individual company or organization

Extranets/WAN extend Intranets to include outside connections to partnersn

DMZ A Demilitarized Zone (DMZ) is an area where you can place a public server for access by people you might not trust otherwise.

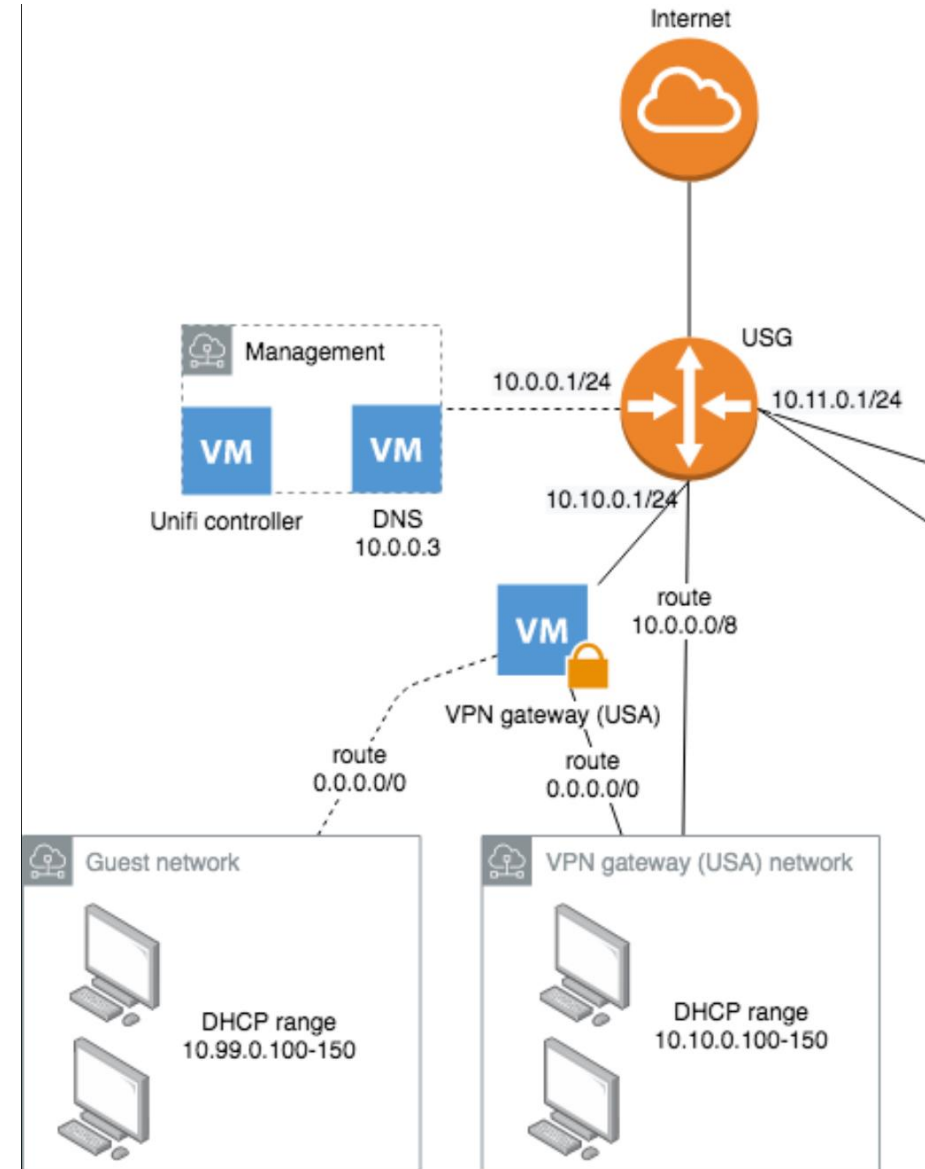
Designing Security Zones

- Security zone design is an important aspect of computer security.
- You have many different approaches to accomplish a good solid design.
- You can create layers of security to protect systems from less secure connection, and you can use address translation to hide resources.
- New methods and tools to design secure networks are being introduced on a regular basis.



Technologies

- One of the nice things about technology is that it is always changing.
- One of the bad things about technology is that it is always changing.
- Several relatively new technologies have become available to help you create a less vulnerable system.
- The three technologies this section will focus on are Virtual Local Area Networks(VLANs), Network Address Translation (NAT) and Tunneling

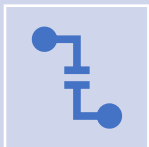




VLANs allow you to create groups of users and systems and segment them on the network. This segmentation allows you to hide segments of the network from other segments and control access.



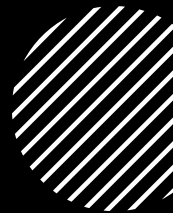
NAT creates a unique opportunity to assist in the security of a network. Originally, NAT extended the number of usable Internet addresses.



Tunneling refers to the ability to create a virtual dedicated connection between two systems or networks. The tunnel is created between the two ends by encapsulating the data in a mutually agreed upon protocol for transmission.



Vulnerability vs Threat vs Risk



A vulnerability is a weakness, flaw or other shortcoming in a system (infrastructure, database or software), but it can also exist in a process, a set of controls, or simply just the way that something has been implemented or deployed.



a threat is anything that could exploit a vulnerability, which could affect the confidentiality, integrity or availability of your systems, data, people and more.



Risk is the probability of a negative (harmful) event occurring as well as the potential of scale of that harm.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

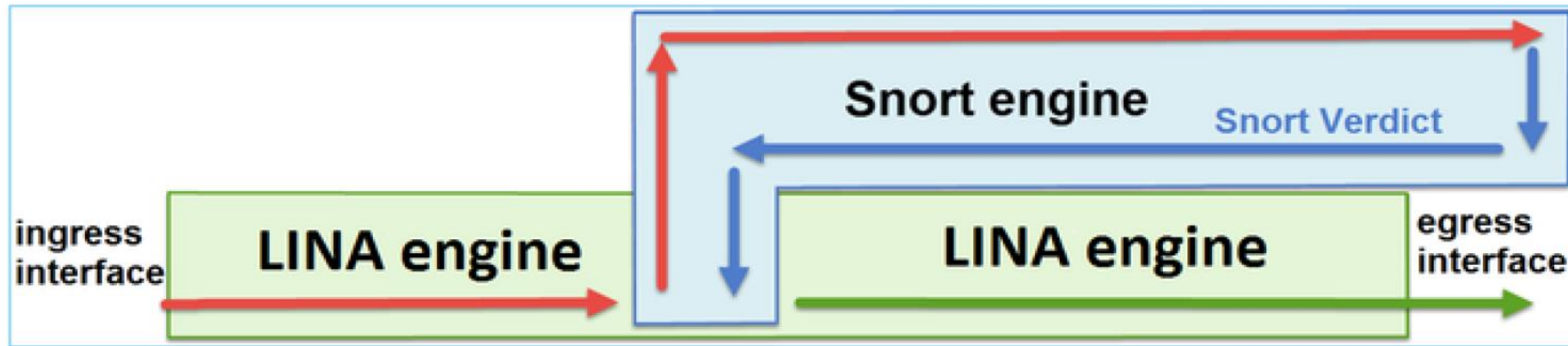


**TIME IT TAKES
A HACKER TO
BRUTE FORCE
YOUR
PASSWORD
IN 2022**

CISCO FirePower

- Next-generation firewall that uses advanced threat detection and prevention technologies.
- Provides intrusion prevention, URL filtering, and application control features to detect and respond to threats more quickly.
- Protects against a wide range of attacks including malware, viruses, and ransomware.
- Uses machine learning and artificial intelligence (AI) to detect and respond to threats faster and more accurately.
- Can be deployed as a physical or virtual appliance, or as a cloud-based service.

FTD Software Architecture – The Big Picture



- **LINA engine** (multiple instances of Data Path) - Focused on **L2-L4** functionality
 - **Snort engine** (multiple instances of Snort) - Focused on **L7** functionality
1. A packet enters the ingress interface and it is **handled by the LINA engine**
 2. If the policy dictates so the packet is **inspected by the Snort engine**
 3. Snort engine **returns a verdict** (whitelist or blacklist) for the packet
 4. The **LINA engine drops or forwards** the packet based on Snort's verdict

Secure Firewall Appliances

Supporting your choice of FTD or ASA software

880 Mbps* AVC+IPS	2.3-4.9 Gbps* AVC+IPS	2.6-10.4 Gbps* AVC+IPS	Stand-alone device: 10-45 Gbps* AVC+IPS 8 node cluster: Up to 288 Gbps* AVC + IPS	Stand-alone device: 15.5-53 Gbps* AVC+IPS 16 node cluster: Up to 680 Gbps* AVC+IPS	One Module: 55-70 Gbps* AVC+IPS 16 node cluster: Up to 950 Gbps* AVC+IPS
-------------------	-----------------------	------------------------	--	---	---

New

FPR 1010

FPR 1120/40/50

FPR 2110/20/30/40

FPR 3110/20/30/40
3105 (New in 2023)

FPR 4110/12/15/25/45

FPR 9300 Series
SM-40
SM-48
SM-56

SMB

Branch Office

Mid Enterprise

Data Center

Service Provider

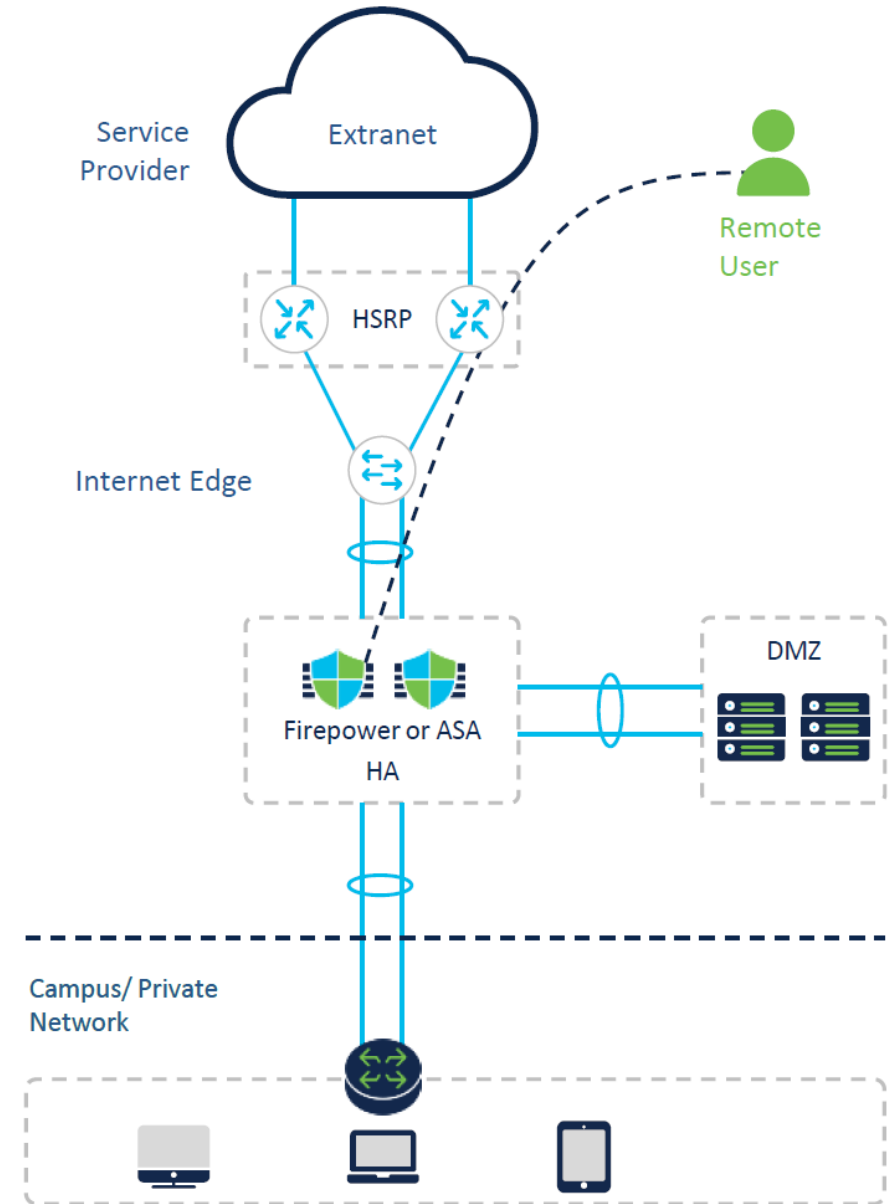
Remote Access VPN (RA VPN)

Key Functions

- Resilience (and scalability)
- Advanced Access Control
- Block access to malicious IP's, URL's, DNS
- Dynamic NAT/PAT and Static NAT
- Remote Access VPN
- Site to Site VPN
- Detecting malicious network traffic
- Visibility and tracking of file transfers, Blocking of malicious files
- Dynamic analysis of unknown files

Key Capabilities

- VPN load balancing
- IPSEC and SSL
- Talos Security Intelligence
- AD, LDAP and Radius
- IKEv2
- RADIUS CoA
- Snort IPS
- Advanced Malware Protection
- Malware Analytics Integration



RA VPN Identity Integration and Monitoring

- Dashboard widgets show VPN usage by user
- User Activity event page gives details of logon and logoff events
- Active Sessions page shows status of active sessions
- Administrator may monitor and terminate specific sessions

The screenshot displays the 'Access Controlled User Statistics' dashboard with the 'VPN' tab selected. It features four data widgets:

- VPN Users by Data Transferred:** A table listing users and their total bytes transferred.
- VPN Users by Duration:** A table listing users and their connection durations.
- VPN Users by Client Country:** A table listing client countries and their counts.
- VPN Users by Client Application:** A table listing client applications and their counts.

At the bottom of the dashboard, it shows the last login information: 'Last login on Wednesday, 2016-12-07 at 15:44:10 PM from 10.151.34.199'.

Username	VPN Total Bytes
penguin	666,666,660
gordon	131,412
batman	100,495
hooter	62,544
camona	62,144
ichigo	61,440
draco	32,704
gordon	32,575
joker	22,400
riddler	14,722

Username	Connection Duration
gordon	5 minutes
batman	5 minutes
gordon	1 minute
joker	15 seconds
riddler	6 seconds
naruto	5 seconds

VPN Client Country	Count
USA (United States)	31
BHB (Bahrain)	19
BLM (Saint Barthelemy)	19
ARG (Argentina)	12
3206d	1

VPN Client Application	Count
Cisco AnyConnect for Windows	49
Cisco AnyConnect VPN Agent for Windows 4.0.00051	27
Cisco AnyConnect for Mac OS	20

Talos Collective Security Intelligence

Who



What



Where



When



How



1.6 million

global sensors

100 TB

of data received per day

150 million+

deployed endpoints

600+

engineers, technicians

35%

worldwide email traffic

13 billion

web requests

24x7x365

operations

40+

languages

Discover, Enforce, Harden

Detect, Block, Defend

Scope, Contain, Remediate

BEFORE

Firewall

VPN

NGFW

UTM

Secure Access + Identity Services

DURING

NGIPS

Web Security

Email Security

AFTER

Advanced Malware Protection

Network Behavior Analysis

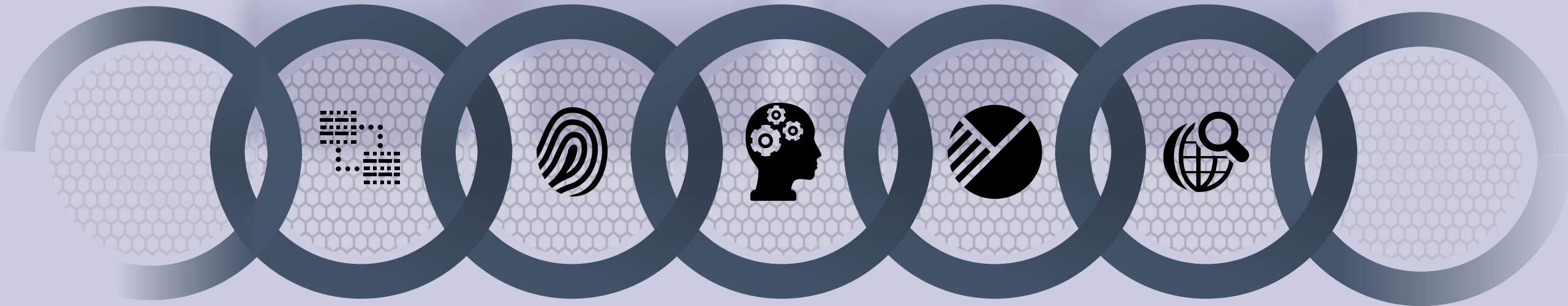
Advanced Malware Protection (AMP)

AMP for Networks

- Snort understands network protocols
- Files can be carved out of the network traffic
- AMP detection techniques can be applied to the file
 - Hash lookups – both SHA 256 and Spero hashes
 - Local malware analysis (Clam AV) on the firewall
 - Submitting the file to Cisco Threat Grid for sandboxing
- File transfers can be blocked
 - Based on file type – this can be determined using the first block of the file. The entire file will be blocked.
 - Based on malware verdict – this requires analyzing the entire file. Only the last piece of the file transfer will be blocked.

Malware Detection Methods

All detection is less than 100%



One-to-One
Signature

Fuzzy
Finger-Printing

Machine
Learning

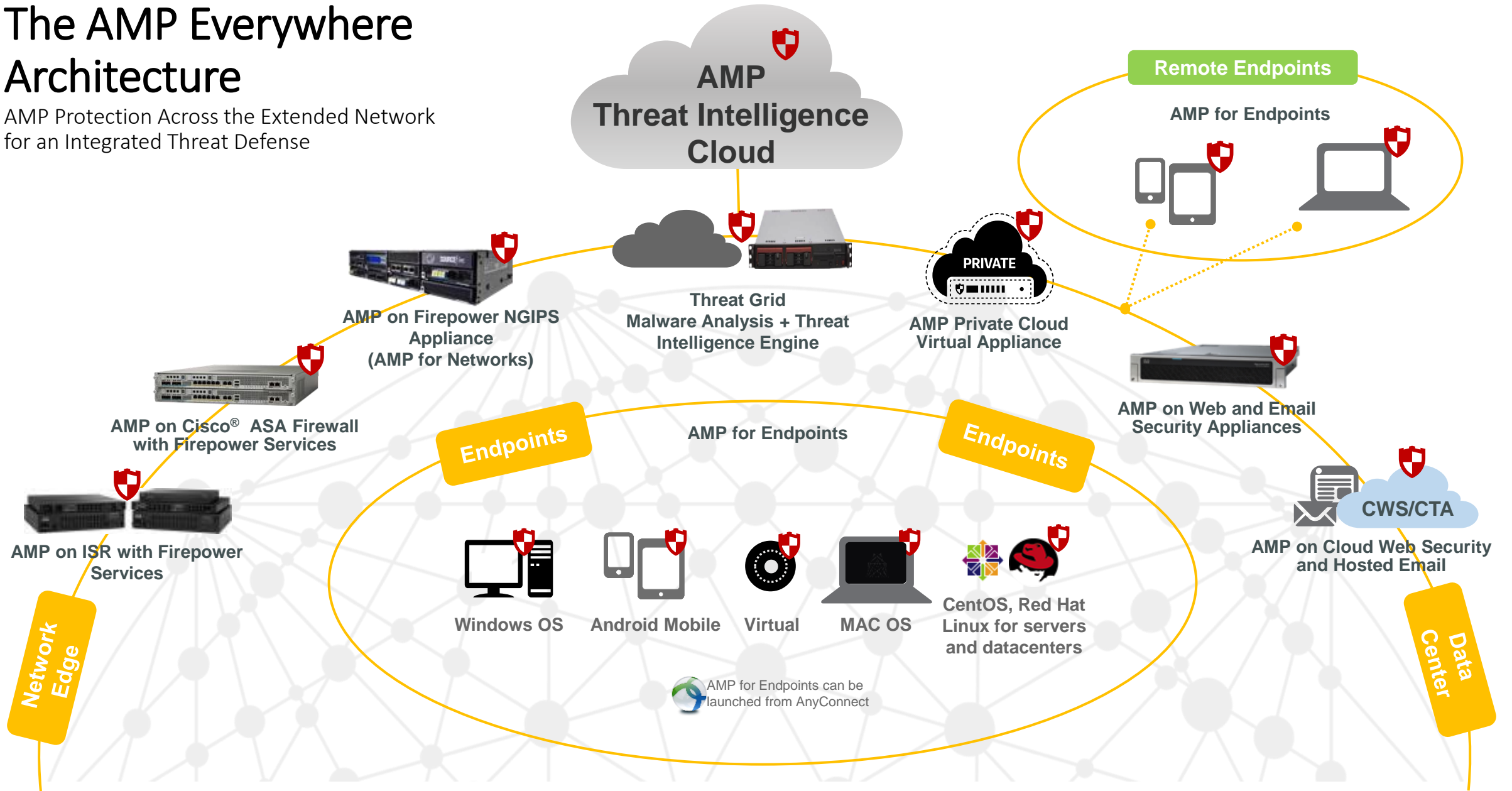
Advanced Analytics

Dynamic
Analysis

Reputation Filtering and File Sandboxing

The AMP Everywhere Architecture

AMP Protection Across the Extended Network for an Integrated Threat Defense



Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)

Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)

Event Count 7

Seen On 4 hosts

Seen On Breakdown 2 senders → 3 receivers

Trajectory



Events Transfer Block Create Move Execute Scan Retrospective Quarantine

Dispositions Unknown Malware Clean Custom Unavailable

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score [High](#)

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)

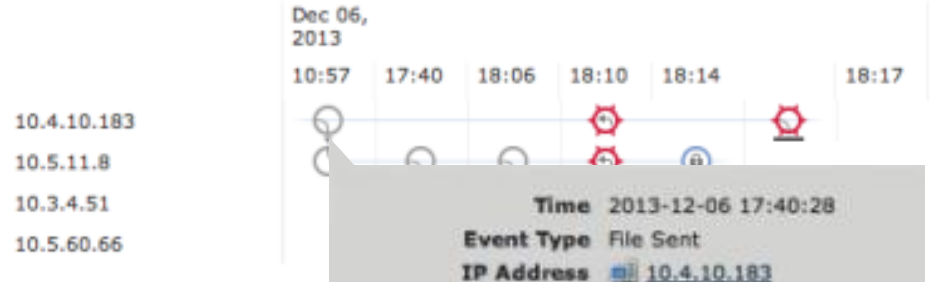
Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)

Event Count 7

Seen On 4 hosts

Seen On Breakdown 2 senders → 3 receivers

Trajectory



Time 2013-12-06 17:40:28

Event Type File Sent

IP Address [10.4.10.183](#)

Sent To [10.5.11.8](#)

File Name [WindowsMediaInstaller.exe](#)

Disposition [Unknown](#)

Action [Malware Cloud Lookup](#)

Application Protocol [HTTP](#)

Client [Firefox](#)

An unknown file is present on IP: 10.4.10.183, having been downloaded from Firefox

Events

Time	Event Type	IP Address	IP Address	File Name	Disposition	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score [High](#)

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)

Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)

Event Count 7

Seen On 4 hosts

Seen On Breakdown 2 senders → 3 receivers

Trajectory



Events Transfer

Dispositions Unknown

Time 2013-12-06 17:40:28

Event Type File Received

IP Address [10.5.11.8](#)

Received From [10.4.10.183](#)

File Name [WindowsMediaInstaller.exe](#)

Disposition [Unknown](#)

Action [Malware Cloud Lookup](#)

Application Protocol [HTTP](#)

Client [Firefox](#)

At 10:57, the unknown file is from IP 10.4.10.183 to IP: 10.5.11.8

Events

Time	Event Type	IP Address	Received From	File Name	Disposition	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score [High](#)

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)

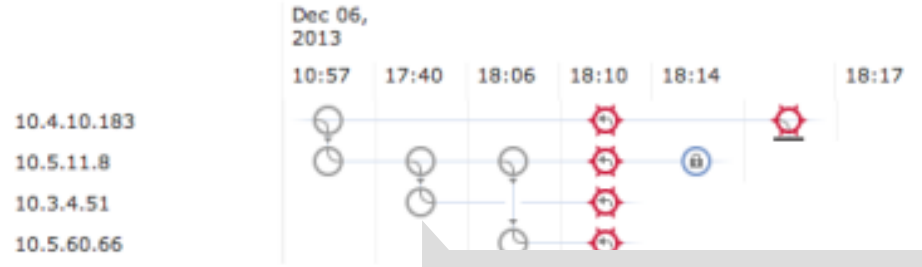
Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)

Event Count 7

Seen On 4 hosts

Seen On Breakdown 2 senders → 3 receivers

Trajectory



Events Transfer Block

Dispositions Unknown Malware

Time 2013-12-06 18:06:03

Event Type File Received

IP Address [10.3.4.51](#)

Received From [10.5.11.8](#)

File Name [WindowsMediaInstaller.exe](#)

Disposition [Unknown](#)

Action

Application Protocol [NetBIOS-ssn \(SMB\)](#)

Seven hours later the file is then transferred to a third device (10.3.4.51) using an SMB application

Events

Time	Event Type	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospec...			
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller.... Unkn... Malware Cloud L... HTTP Firefox Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller.... Unkn... NetBIOS-... Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller.... Unkn... NetBIOS-... Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...			Malwa...
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller.... Malwa...
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller.... Malwa... Malware Block HTTP Firefox

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score [High](#)

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)

Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)

Event Count 7

Seen On 4 hosts

Seen On Breakdown 2 senders → 3 receivers

Trajectory



Events Transfer Block Unknown Malware

Dispositions Unknown Malware

Time 2013-12-06 18:10:03

Event Type File Received

IP Address [10.5.60.66](#)

Received From [10.5.11.8](#)

File Name [WindowsMediaInstaller.exe](#)

Disposition Unknown

Action NetBIOS-ssn (SMB)

The file is copied yet again onto a fourth device (10.5.60.66) through the same SMB application a half hour later

Events

Time	Event Type	Source IP	Destination IP	File Name	Disposition	Action	Application Protocol	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...								Retrospective Event, Fri Dec 6 ...
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInsta...	Unknown				Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...				
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...				
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox	

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score [High](#)

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)

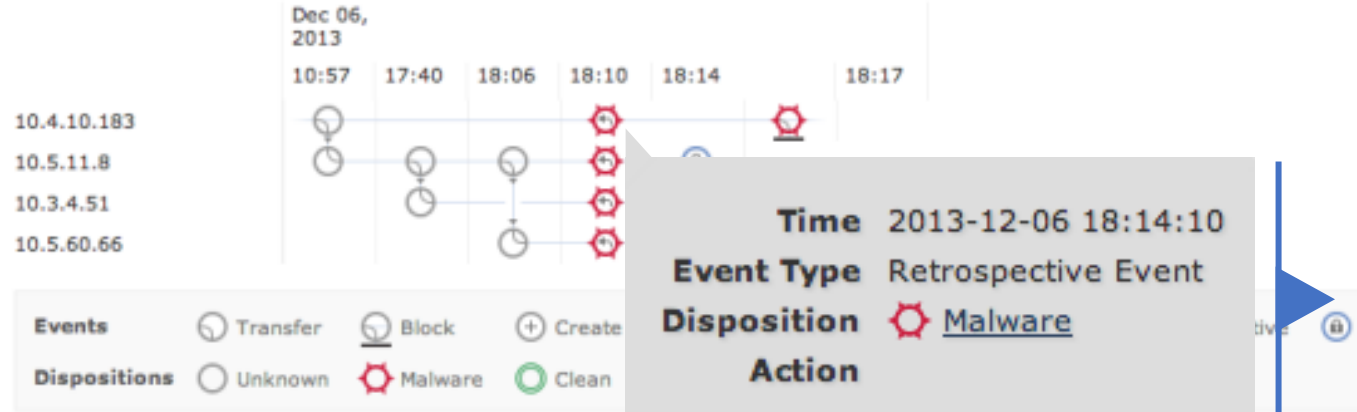
Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)

Event Count 7

Seen On 4 hosts

Seen On Breakdown 2 senders → 3 receivers

Trajectory



The Cisco Collective Security Intelligence Cloud has learned this file is malicious and a retrospective event is raised for all four devices immediately.

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)

Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)

Event Count 7

Seen On 4 hosts

Seen On Breakdown 2 senders → 3 receivers

Trajectory



Events Transfer Block Create Malware

Dispositions Unknown Malware Clean Quarantined

Time 2013-12-06 18:14:23

Event Type File Quarantined

IP Address [10.5.11.8](#)

File Name [WindowsMediaInstaller.exe](#)

Disposition [Malware](#)

Action

At the same time, a device with the FireAMP endpoint connector reacts to the retrospective event and immediately stops and quarantines the newly detected malware

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disposition	Action	Protocol	Browser	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...				
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox	Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...				
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...				
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox	

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score [High](#)

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)

Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)

Event Count 7

Seen On 4 hosts

Seen On Breakdown 2 senders → 3 receivers

Trajectory



Events Transfer Block Create Move

Dispositions Unknown Malware Clean Custom

Time 2013-12-06 18:17:27

Event Type File Sent

IP Address [10.4.10.183](#)

Blocked Recipient [10.5.11.8](#)

File Name [WindowsMediaInstaller.exe](#)

Disposition Malware

Action [Malware Block](#)

Application Protocol HTTP

Client Firefox

8 hours after the first attack, the Malware tries to re-enter the system through the original point of entry but is recognized and blocked.

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...					Malwa...				
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...					Malwa...				
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		



URL Filtering

- Provides ability to block specific URLs or define policies based on the category of the URL like Gambling, Social Media, Gaming etc.
- Provides visibility based on the categories of URL being visited by the users of the network

URL Filtering Implementation

HTTP or decrypted HTTPS

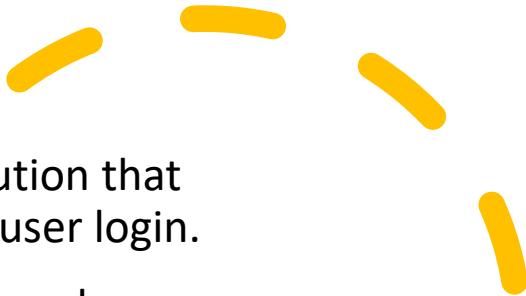
- Snort identifies HTTP protocol
- Snort parses HTTP request header – extracts URL
- Looks up URL in local database – if miss, optionally can do a cloud lookup

Un-decrypted HTTPS

- Snort identifies SSL protocol
- Snort parses SSL client hello and certificate – extracts FQDN from SNI or certificate
- Looks up FQDN in local database – if miss, optionally can do a cloud lookup

A large orange circle with a smaller blue circle at the bottom left. The text "CISCO DUO" is centered in white.

CISCO DUO

- 
- A decorative yellow dashed arc in the top right corner.
- Multi-factor authentication (MFA) solution that provides an extra layer of security for user login.
 - Requires two forms of authentication, such as a password and a fingerprint, to grant access to sensitive systems and data.
 - Supports a wide range of authentication methods, including push notifications, phone calls, and hardware tokens.
 - Provides easy integration with existing IT systems and applications, including VPNs and cloud services.
 - Offers advanced reporting and analytics to help identify security trends and potential threats.

Why customers use Cisco Secure Access By Duo



Block use of stolen credentials

Duo MFA and **Duo Passwordless** prevents unauthorized access to attackers even when their passwords are compromised

Mitigate attacks that bypass MFA

Verified Duo Push and **FIDO2 authentication options** prevent sophisticated phishing attacks that bypass MFA

Implement Zero Trust Access

Single sign-on, device trust and risk-based authentication allow organizations to implement granular per-application policies without creating user friction

Protect Microsoft Applications

Duo comes with out of box integrations with Microsoft applications and other 3rd party applications, enabling organizations to consolidate multiple siloed solutions

Verify Device Trust

Duo Device Trust provides comprehensive visibility into all devices that access protected applications and verifies their posture before granting access.

Start your Passwordless Journey

Duo Passwordless enables organizations to start their journey towards a passwordless future securely in a cost-efficient manner

Compliance and Regulations

All Duo editions can help organizations meet compliance requirements and regulatory framework guidelines.

Current IT Landscape

Users, devices, and apps are everywhere

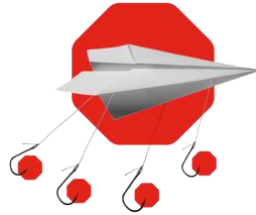


Threat Landscape Today



Attack surface is growing with cloud migration and hybrid work

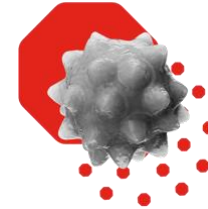
As your apps and data moves to the cloud, it has also become more accessible to bad actors increasing your attack surface.



Stolen credentials account for >80% of web app attacks

Weak passwords and bad security practices such as password reuse or sharing increase the risk of a data breach.

Source: 2022 Verizon DBIR



Attacks bypassing security are on the rise

Attackers can use readily available phishing kits to bypass MFA, turning push notification, one-time passcodes and authentication device enrollment into a security risk.

A new approach to security is needed – **Zero Trust** – to address evolving threats

Duo Access Management

Zero Trust for the Workforce

CORPORATE
RESOURCES

Cloud, On-premise, Public,
Private, Hybrid



Authenticate users

- ✓ MFA
- ✓ Passwordless
- ✓ Employees, contractors, vendors, external 3rd parties, etc.



Verify devices

- ✓ Device Trust
- ✓ Device health & compliance
- ✓ Mac, Win, Linux, iOS, Android, BYOD



Enable access

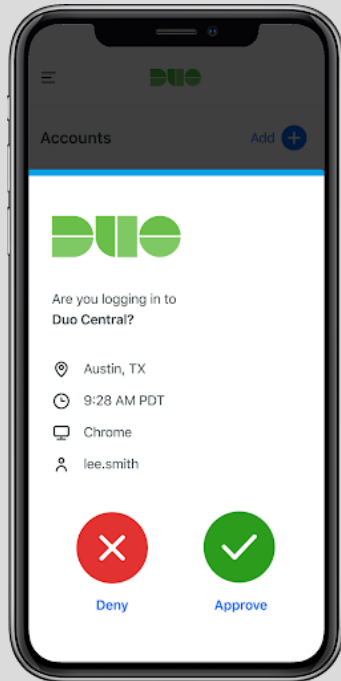
- ✓ Single Sign-On (SSO)
- ✓ VPN-less remote access
- ✓ All apps – cloud, on-prem and private



Continuous Trusted Access with Risk Based Authentication

Authenticate Users

Verify the trustworthiness devices before granting access



Provide Strong Multi Factor Authentication

Protects against unauthorized access using valid credentials



Prevent Push Phishing Attacks

Ensures users don't fall victim to push phishing attacks



Start Passwordless Journey

Increase security and user productivity by enabling secure login without a password

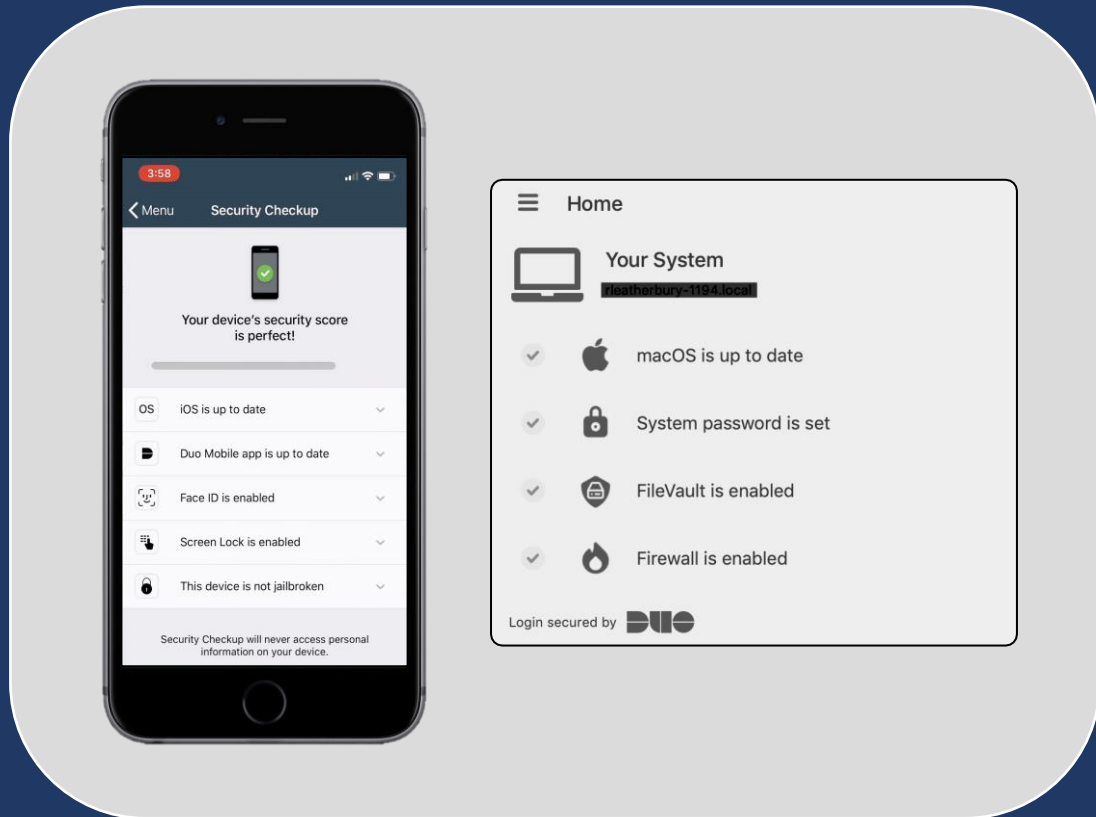


Quickly deploy and be protected

Cloud native and designed to be user friendly from the start, any IT professional can implement Duo at lightening speed

Verify Devices

Verify the trustworthiness devices before granting access



Assess Security Posture

Deny access to compromised or out of compliance devices



Verify Endpoint Trust

Prevent attackers from accessing applications with their own devices



Guide self-remediation

Eliminate vulnerabilities and lower IT costs by empowering users to remediate their device

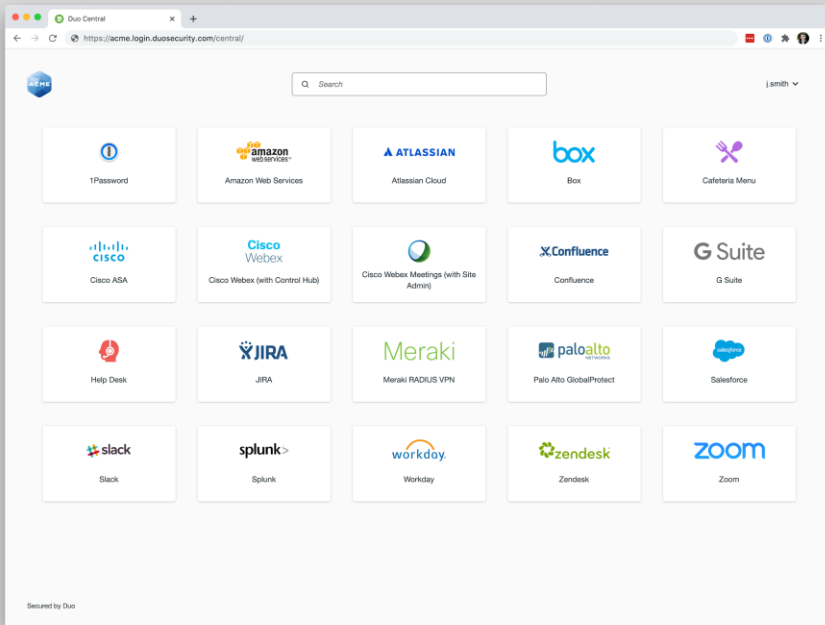


Provide Complete Visibility

Gain complete visibility into all laptops and mobile devices accessing your resources

Enable Access

Simplify user experience while easily controlling who can access which corporate applications



Secure any corporate application

Covers the widest array and unlimited number of applications



Single Sign-on

Allow users to login only once to access multiple applications

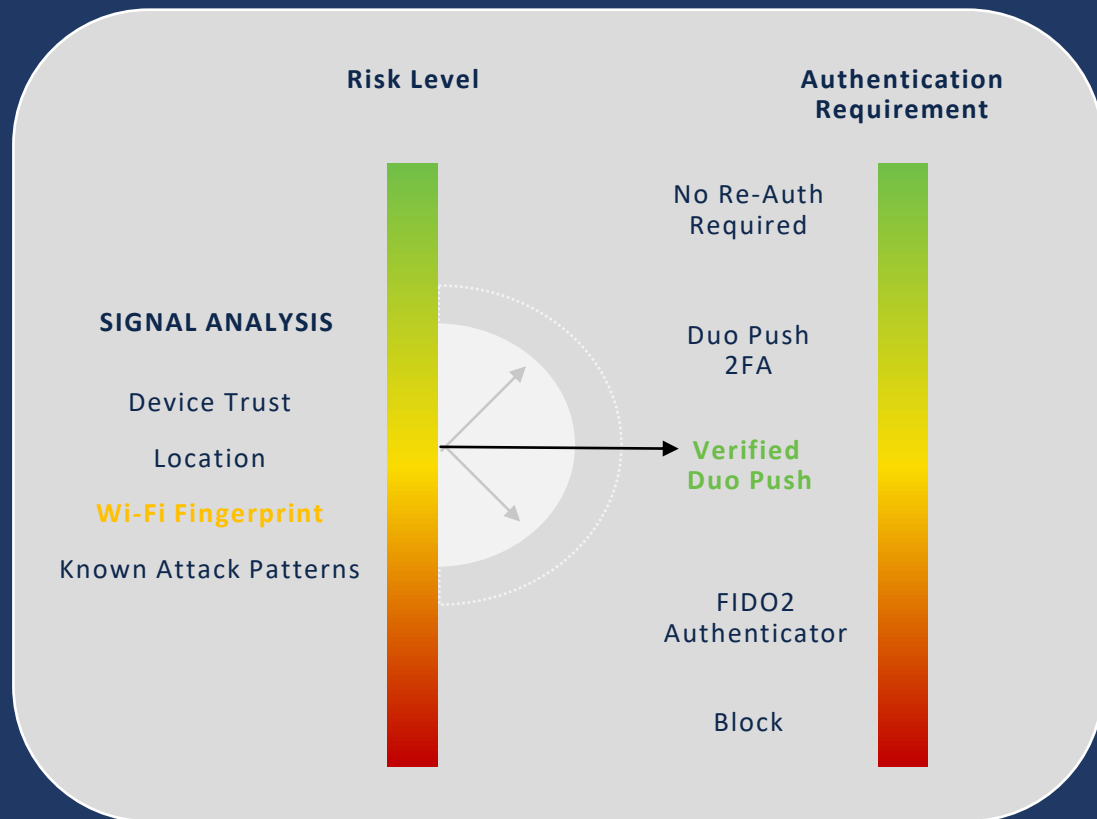


Provide VPN-less Remote Access

Enable users to securely and easily access on-premise resources

Risk Based Authentication

Maximize user productivity without compromising security



RBA

Adjust authentication requirements in real time based on risk levels



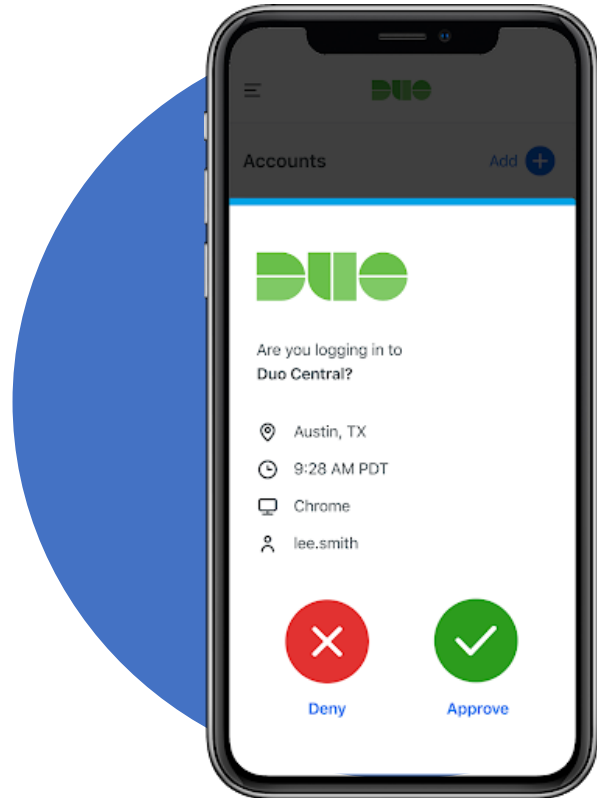
Patent pending risk signals analysis **Wi-Fi Fingerprint**

Determine risk levels without infringing on user privacy

The World's Easiest and Most Secure MFA

Easily prevent unauthorized access

- Instantly integrates with all apps
- Users self-enroll in minutes
- Users authenticate in seconds



Strong Multi-Factor Authentication (MFA) Options

Flexible MFA for every use case

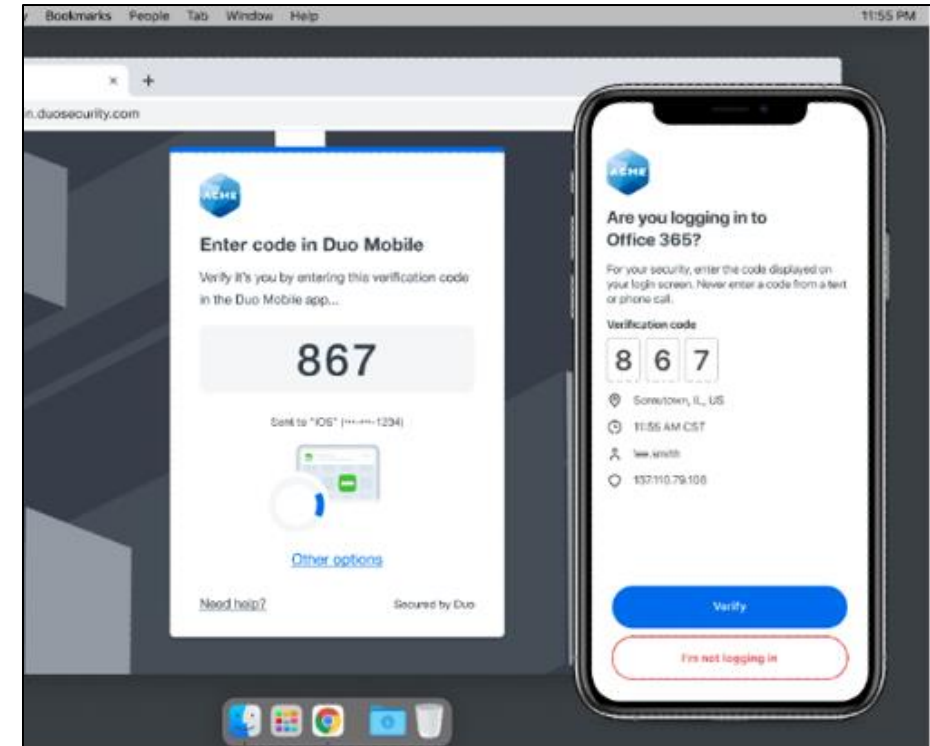
- Configure authentication options for each application or group of users
- Require phishing-resistant MFA (FIDO2) for critical applications and privileged users
- Enable multiple option for users for ease of use and flexibility



Prevent Push Phishing Attacks

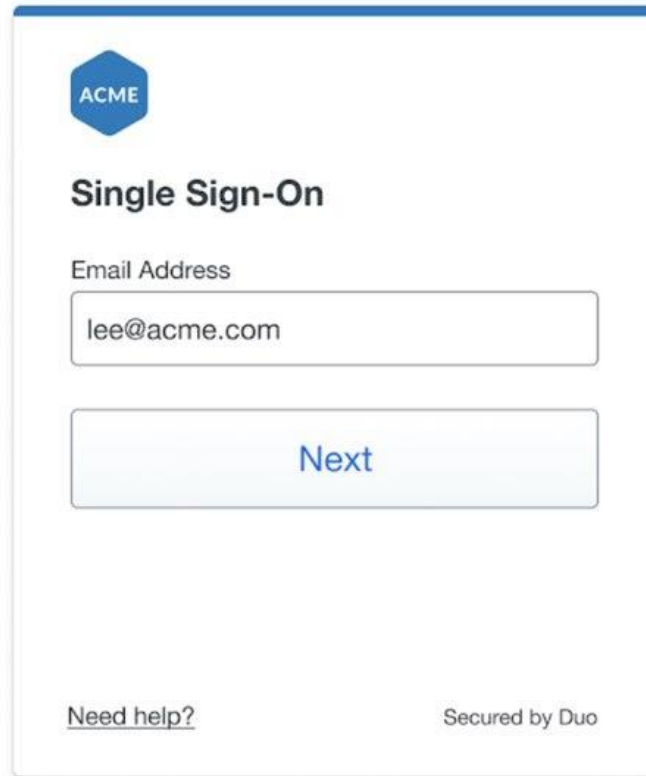
Strengthen MFA with Verified Duo Push

- Increases security of push-based MFA while preserving ease of use
- Customizable code length
- Can be triggered only when risk level increases to preserve user productivity



Start your passwordless journey

Duo Passwordless.1, 2, 3...you are in!



ACME

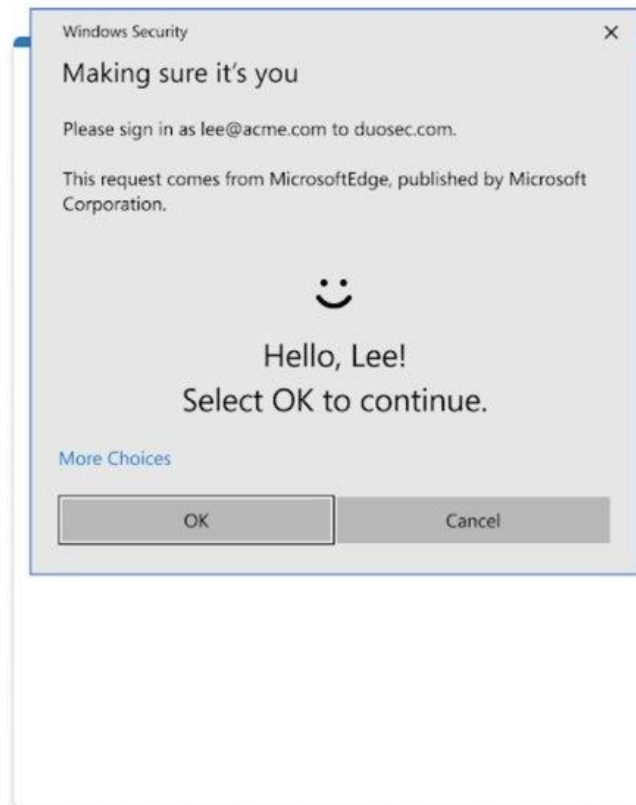
Single Sign-On

Email Address

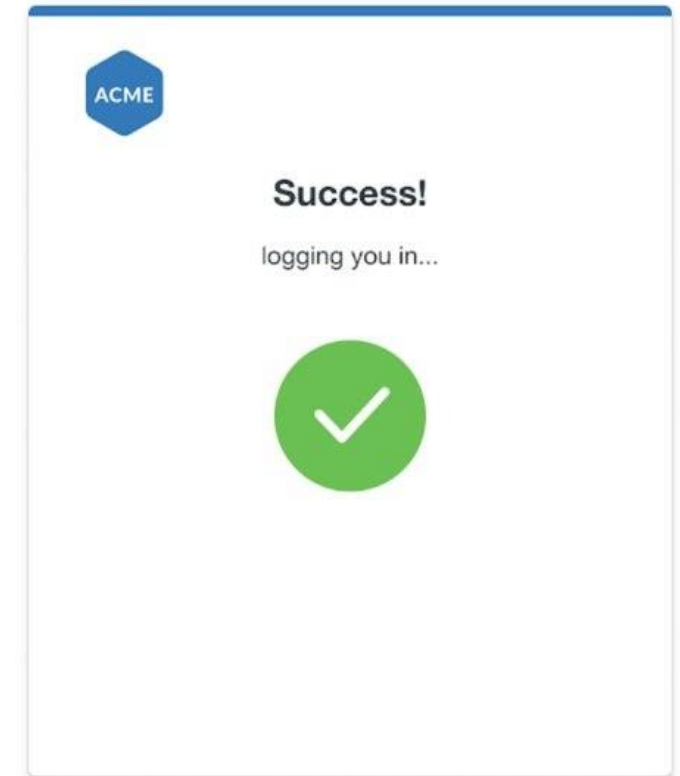
Next

[Need help?](#) Secured by Duo

Enter your current username



Use Passwordless Authenticators:
Platform Biometrics (TouchID, Windows Hello)
FIDO2 security Keys (Yubikey, Feitian)
Duo Mobile (passwordless push)

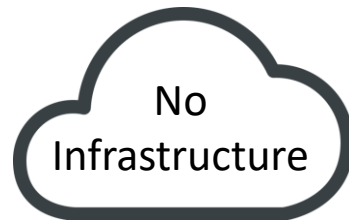


That's it!

Quickly deploy and be protected

Enable business agility and speed to security

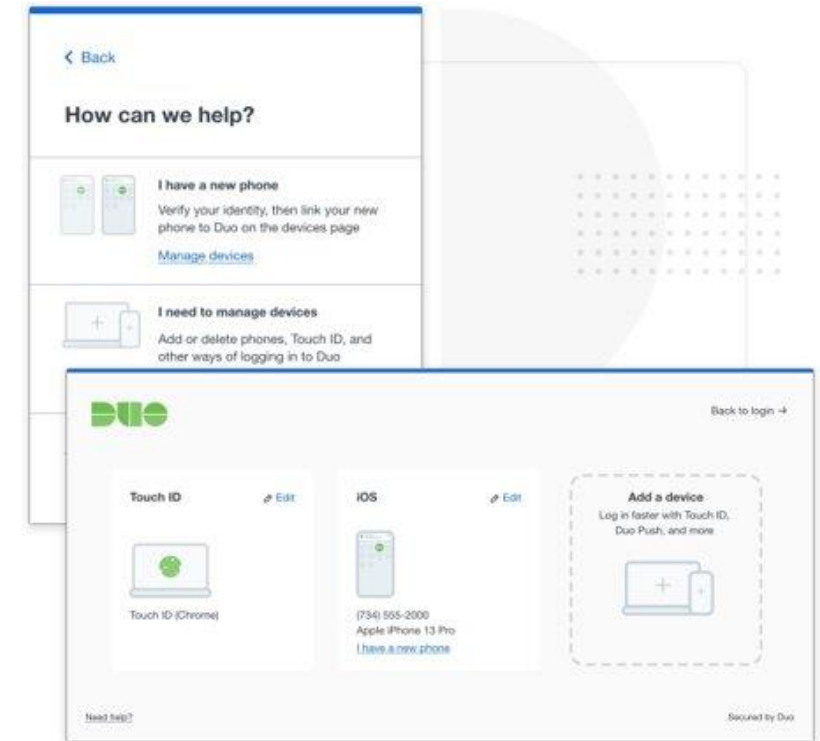
Cloud based



Deploy in hours

Duo Security FastTrack									
Success Planning									
Design Project Plan & Goals	Duo Policy Discussion								
Application Configuration & Testing									
Application Configuration & Testing					Pilot Users				
End User Communication									
Build Education Materials	Email - Pilot Group	Email: Duo/ZFA Overview	Email: Enrollment Info	Email: End User Guide	Email: Enroll Now	Email: Duo is Live			
Help Desk Enablement									
Training Session					Help Desk Supports End Users				
Go-live									
Duo Care Team Engagement									
Duo Care Team Introduction	Weekly Sync	Progress bar with 10 arrows						Deployment Review	

User self-service



CISCO Umbrella

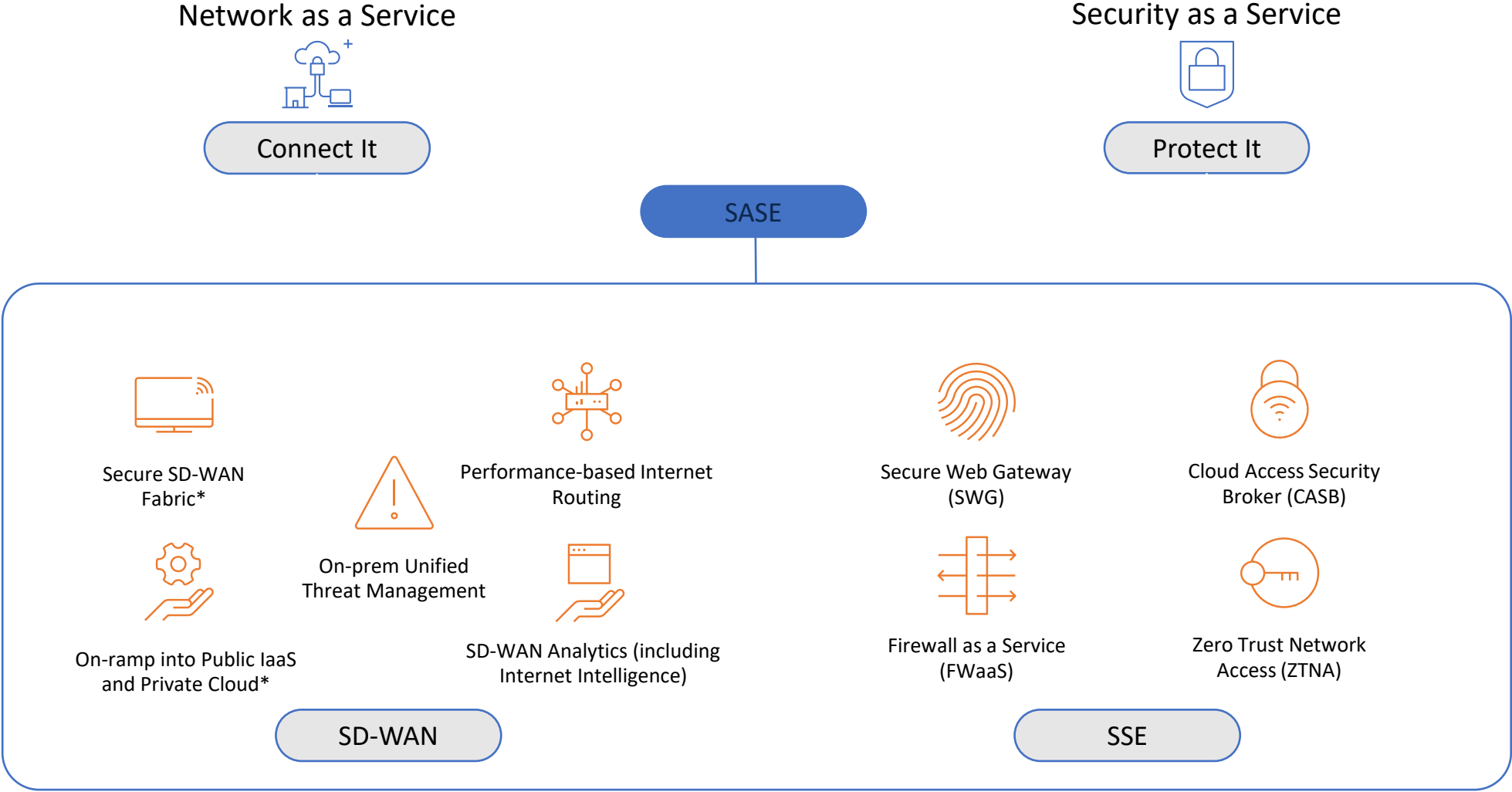
- Cloud-based security platform that provides DNS and web filtering, threat intelligence, and CASB capabilities.
- Blocks malicious domains and IP addresses to protect against malware, phishing, and other cyber threats.
- Uses a global network of threat intelligence to detect and block malicious activity.
- Provides granular visibility into all network activity to help identify potential threats.
- Offers seamless integration with other Cisco security products, such as Firepower and Meraki.

Common desired outcomes

- Protecting organization from threats
- Ensuring policy compliance
- Enforcing acceptable use policies
- Keeping sensitive data safe
- Achieving operational efficiency
- Delighting security administrators
- Maintaining end user satisfaction

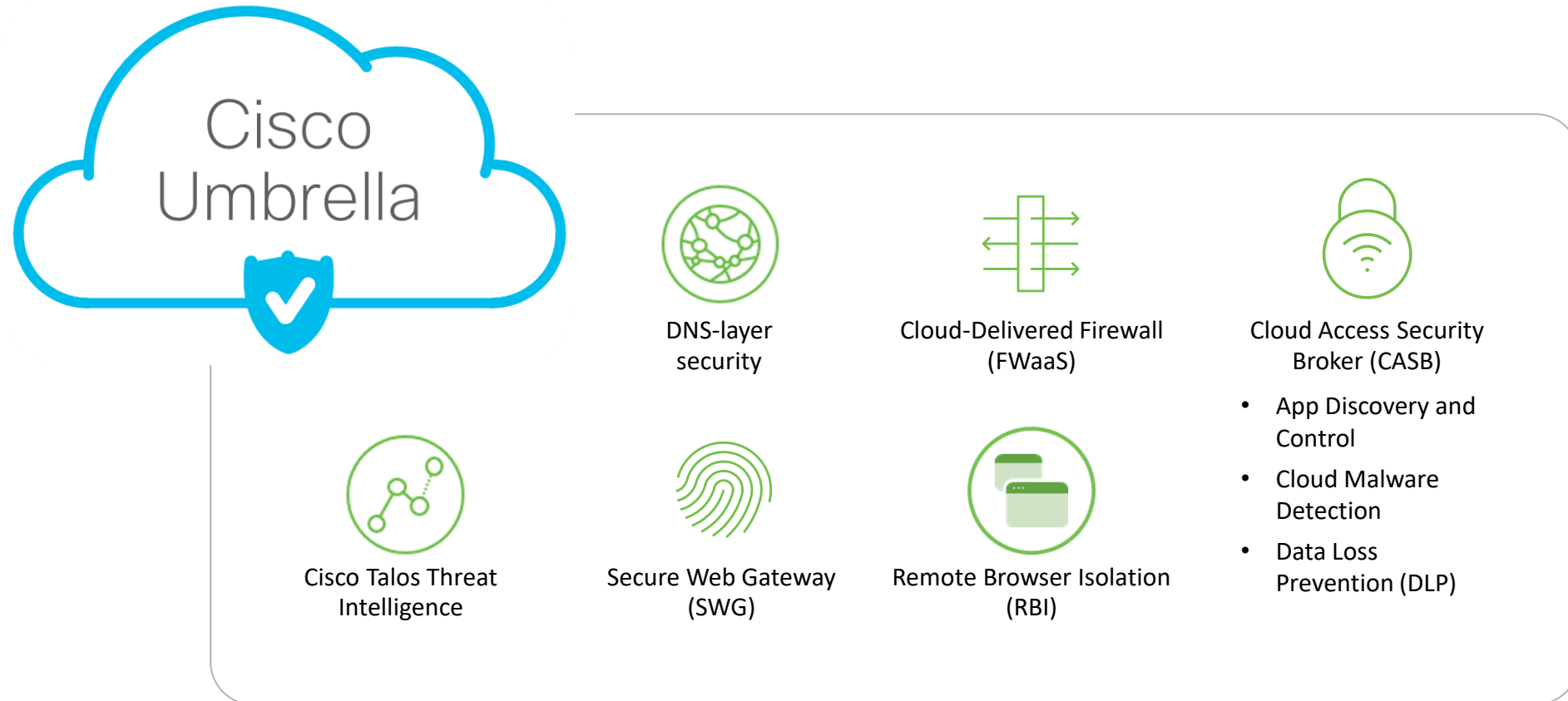


Secure Access Service Edge (SASE)



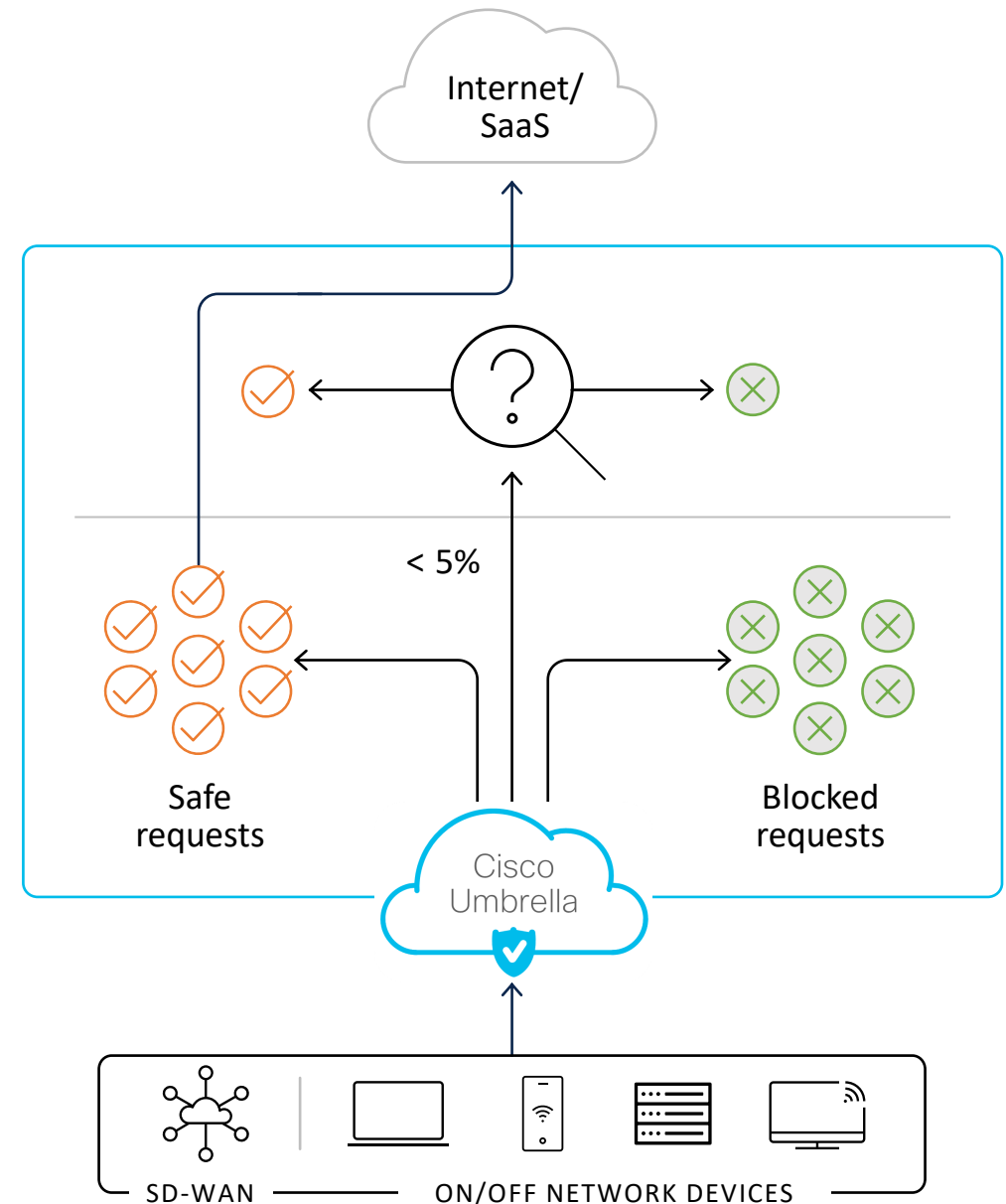
**with support for remote workers*

Umbrella: Core for your SSE and SASE journey



DNS-layer security

- Deploy enterprise-wide in minutes
- Block malware, phishing, CNC callbacks—from anywhere
- Prevent or limit visits to nefarious web sites from guest Wi-Fi networks
- Stop threats at the earliest point to reduce triage of alerts
- Accelerate internet access; only proxy risky domains



Secure Web Gateway: Full web proxy



- **Gain additional visibility** via full URL logging and cloud app discovery
- **Enforce acceptable use policy** via granular app controls, content filtering, and URL block/allow lists
- **Extend protection against malware** via SSL decryption and file inspection
- **Improve content security:** Sandboxing + retrospective alerts on malware that's evaded initial detection
- **View detailed reporting** with full URL addresses, network identity, allow/block actions, external IP addresses

CISCO Meraki

Cloud-based networking solution for routers, switches, and wireless access points.

Provides centralized management platform for monitoring and controlling network activity.

Easier to detect and respond to security threats with a single dashboard.

Provides end-to-end encryption to ensure data privacy and security. Offers advanced security features such as rogue access point detection and automatic firmware updates.

Provides automatic network segmentation to isolate compromised devices and prevent lateral movement of threats.

DNS integration with Meraki MX

- Simplest way to deploy Umbrella DNS on a wired network
- Conveniently enable Umbrella policies directly in the Meraki dashboard
- Create granular policies on a per-VLAN basis or by using Meraki group policies
- Achieve additional visibility into identifies

But wait there's MORE...



Simplified IPsec tunnel connectivity with Meraki MX

Meets diverse security requirements for distributed locations and users

- DNS-layer security, secure web gateway, cloud access security broker and an application-aware firewall
- Easily forward all outbound traffic to Umbrella for more advanced inspection and control of web and app traffic
- On and off network protection



“Secure Access Service Edge (SASE) is an emerging offering combining comprehensive WAN capabilities with comprehensive network security functions to support the dynamic secure access needs of digital enterprises.”

Neil MacDonald, Gartner



Advanced Protection for Meraki MX



Enhanced Threat Defense

Automatic protection against an ever-growing list of known malicious files, plus malware sandboxing with Threat Grid



Contextual Visibility

Security Center makes it easy to ensure you have the latest information about attacks on your network



Rapid Detection

Automatic alerting when a downloaded file is found to be malicious after the fact



Ease of Management

Enable best-in-class malware protection





Industry leading SD-WAN meets industry leading security



Meraki MX

On-prem security and SD-WAN

- Monitor and block malware and malicious traffic
- Restrict unauthorized users
- Prevent unwanted content or applications
- Firewall incoming traffic and VLAN to VLAN traffic
- Use secure site-to-site/in-tunnel VPN
- Detect and prevent intrusions (IDS/IPS)



Cisco Umbrella

Cloud-native security

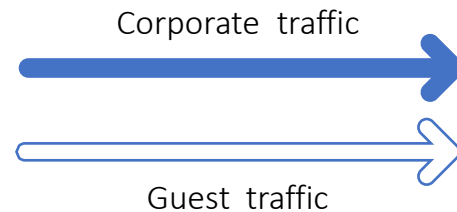
- Secure users at the edge with the best detection
- Increased reliability and performance with the speed and scale of the cloud
- Easily extend protection off-network
- Reduce the time, money, and resources required to identify and remediate threats

Flexible deployment & policies to meet needs

Competitive advantage over Zscaler and Fortinet



Meraki MX



Umbrella

Traffic type	Deployment	Feature requirements
Corporate traffic	IPsec tunnel or PAC file	<ul style="list-style-type: none">• Full logging• Deep inspection and controls
Guest traffic	DNS device integration (new MX feature)	<ul style="list-style-type: none">• Threat protection and attribution



SECURE