



# Spotit, Cisco and the Shield Framework: what's in it for you?

Bruno Mekeirele – Gert Tilburgs







\*\* The right technology matters \*\*\*

17.400,-

Op voorraad : Levering binnen 1-2 werkdagen

- 1 +

Voeg toe aan winkelwagen



Vragen? Stel ze gerust! →



# FALLING IN LOVE

## DOGMA F STARRY RED

# Ook AG2R-renners waren eerst bezorgd over Decathlon-fiets: "Maar ik ben weggeblazen", zegt Oliver Naesen

di 28 november 2023 | 09:06



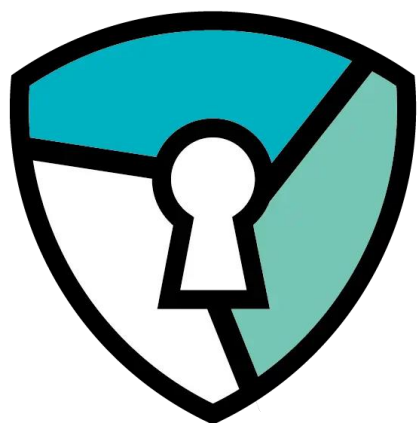
Van Duijn: het racefietsmerk van Decathlon is de nieuwe fiets van de AG2R-renners

\*\* Beyond Technology: The Right Strategy\*\*





# Frame Agreement for Network/NextGen Firewalls



**SHIELD**<sub>vzw</sub>



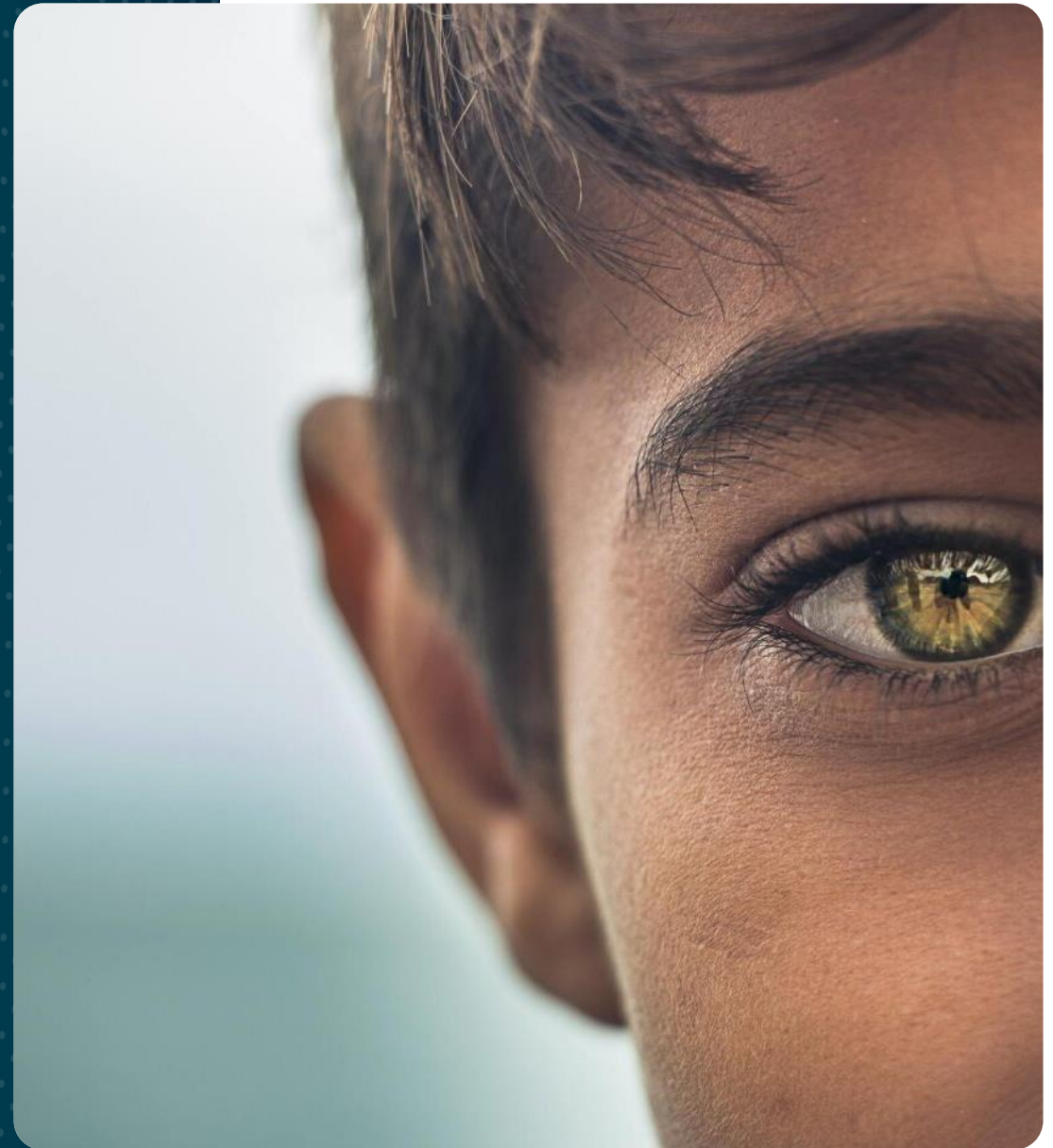
**spotit**  
YOUR SECURITY & NETWORK LAYER





Who is spotit?

---



# Who is spotit?

SECURITY & NETWORKING IS A COMPANY VISION!



› ° 2014 – privately owned



› HQ in Belgium



› 28 million euros in 2023



› Security and Network



› Quality and honour



› Spotit Academy



› +120 experts



› >200 customers



› Your strategic partner

# NPS INVESTIGATION



NPS SCORE SPOTIT 2024



Big enough to  
deliver, small  
enough to care.



# OUR PORTFOLIO

## SECURITY AND NETWORKING STRATEGY

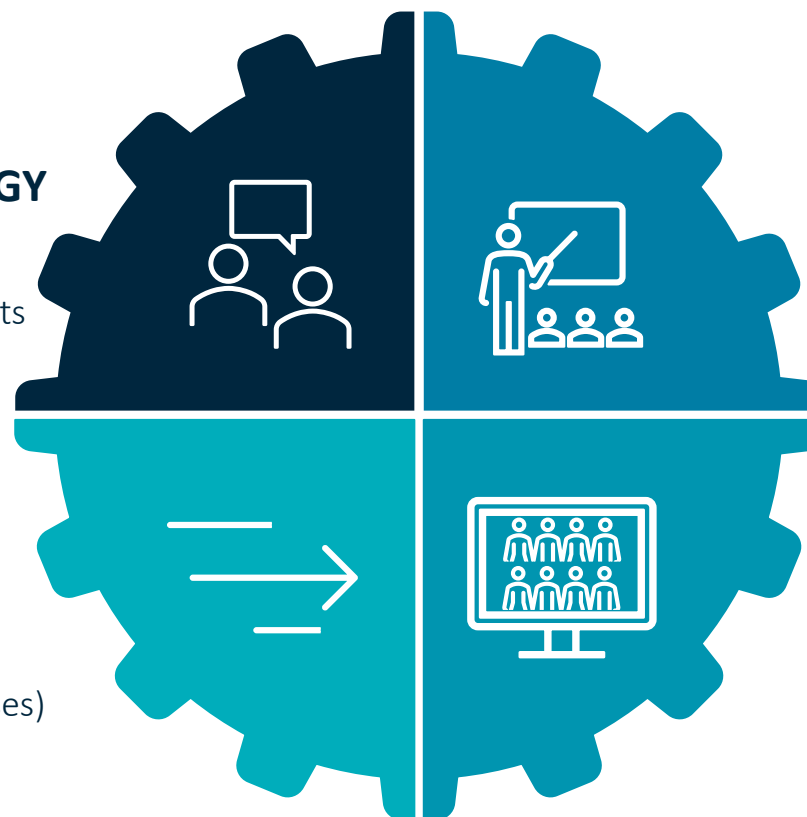
Accelerate your journey

Security and networking consultancy / assessments

## IMPLEMENTATION & OPTIMISATION

Extend, integrate, maintain and optimize

Security and networking solutions (HW, SW, licenses)



## STRATEGIC SECURITY SERVICES

Security Governance

CISO / DPO / security awareness

## MANAGED SERVICES/ NOC / MSOC

Leave it to us

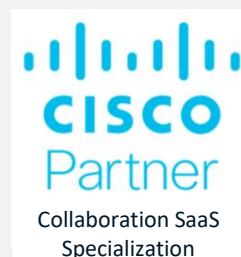
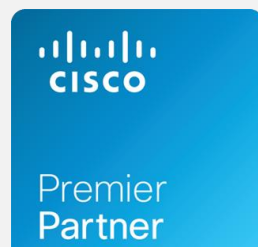
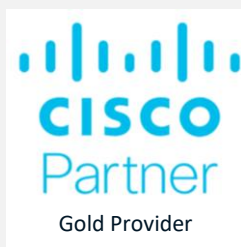
24/7 monitoring and assurance

## OUR PARTNERS



# CISCO CAPABILITIES

## Our Specializations



# 31

## certified individuals

- › CCIE Enterprise Infrastructure
- › CCIE Routing and Switching Written Exam 400-101
- › CCNA
- › CCNA Cyber Ops
- › CCNP Security Specialized
- › CCNP DataCenter
- › CCNP Enterprise
- › CCS Data Center Core
- › CCS Data Center Operations
- › CCS Enterprise Advanced Infrastructure Implementation
- › CCS Enterprise Core
- › CCS Enterprise Design
- › Implementing-Operating Cisco EN Core Tech 350-401 v1
- › And many more



# Shield offering

---

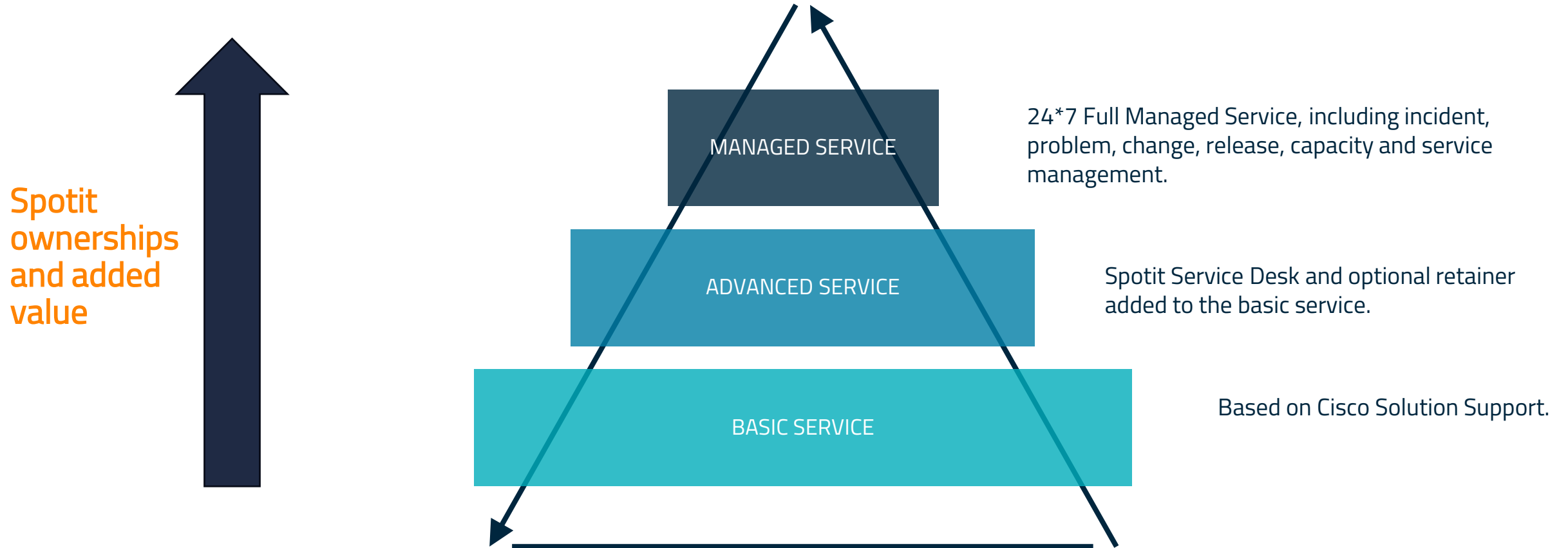




# SPOTIT OFFERING FOR SHIELD MEMBERS



# Operational Services



# Why would you go for this offer?

- Strong Cisco portfolio tailored to the healthcare & education market
- Spotit expertise & innovation combined with a flexible service offering
- Aggressive discounts
- Highest quality services
- Human-to-human approach
- Local service delivery
- Big enough to deliver, small enough to care
- Strong partnership Cisco - spotit



INVITATION

# Cybersecurity Seminar 2025: Trends, Insights and Expert Perspectives

- 20-03-2025
  - Communicatieloft Gent
  - Be present to learn more
    - about the 2025 threat landscape
    - and how to defend your business
  - For IT decision makers where cybersecurity is a focus or priority
  - Visit spotit website
- [Cybersecurity Seminar | Spotit](#)


Together  
we can.



# LET'S CONNECT

## CONTACT INFORMATION

 [www.spotit.be](http://www.spotit.be)

 [info@spotit.be](mailto:info@spotit.be)

 +32 (0)9 394 44 41

## SOCIAL MEDIA

 [linkedin.com/company/spotit](https://www.linkedin.com/company/spotit)

 [@spotitbv](https://www.facebook.com/spotitbv)

## LOCATIONS

**SPOTIT HEADQUARTERS**  
Guldensporenpark 30/C  
9820 Merelbeke  
Belgium

**SPOTIT ANTWERPEN**  
Noorderlaan 133/ 38  
2030 Antwerpen  
Belgium

**SPOTIT HERK-DE-STAD**  
Steenweg 3, Blok 402  
3540 Herk-de-Stad  
Belgium





# Cisco Security for Healthcare

## Zero Trust & Resiliency

# Zero Trust

- ▶ Never assume trust
- ▶ Always verify
- ▶ Enforce least privilege

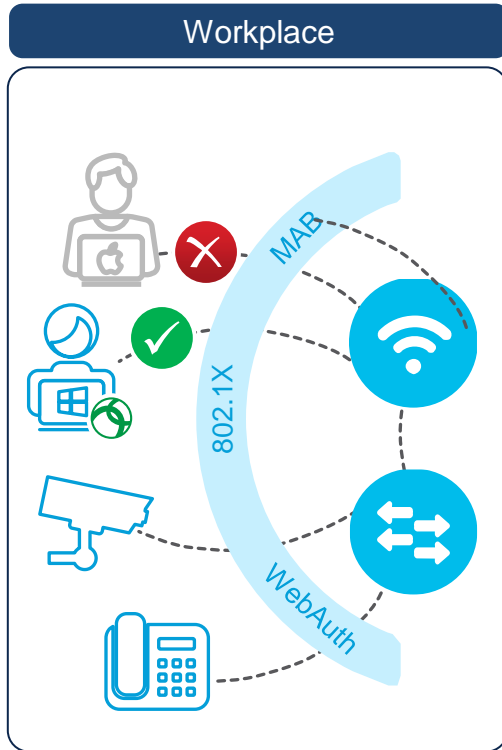
# Resiliency

Healthcare resilience is the ability to adapt before, during, or after disruptions to ensure continuous patient care — no matter the circumstances

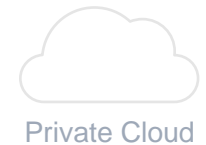


# Campus: Establishing Trust

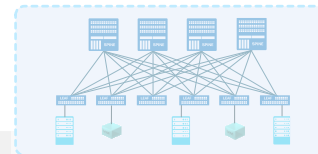
*Limiting the network to authorized devices & users*



Internet Applications



Private Applications

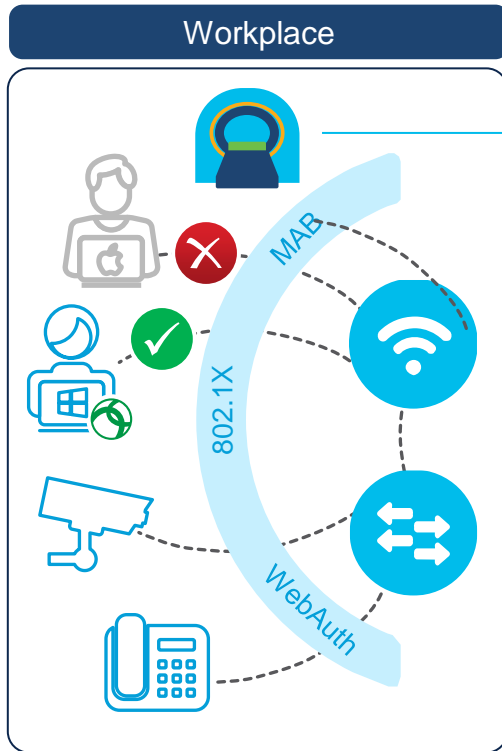


**Identity Services Engine**  
Policy Server for Network Access Control

**Authentication**  
802.1x & MAB  
Limiting the network to Trusted devices only.

# Campus: Establishing Trust

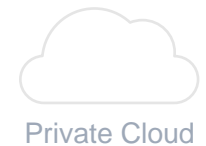
*Limiting the network to authorized devices & users*



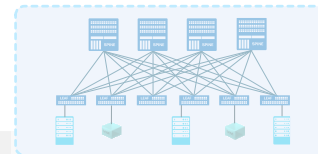
Manageable?  
Vulnerable?



Internet Applications



Private Applications

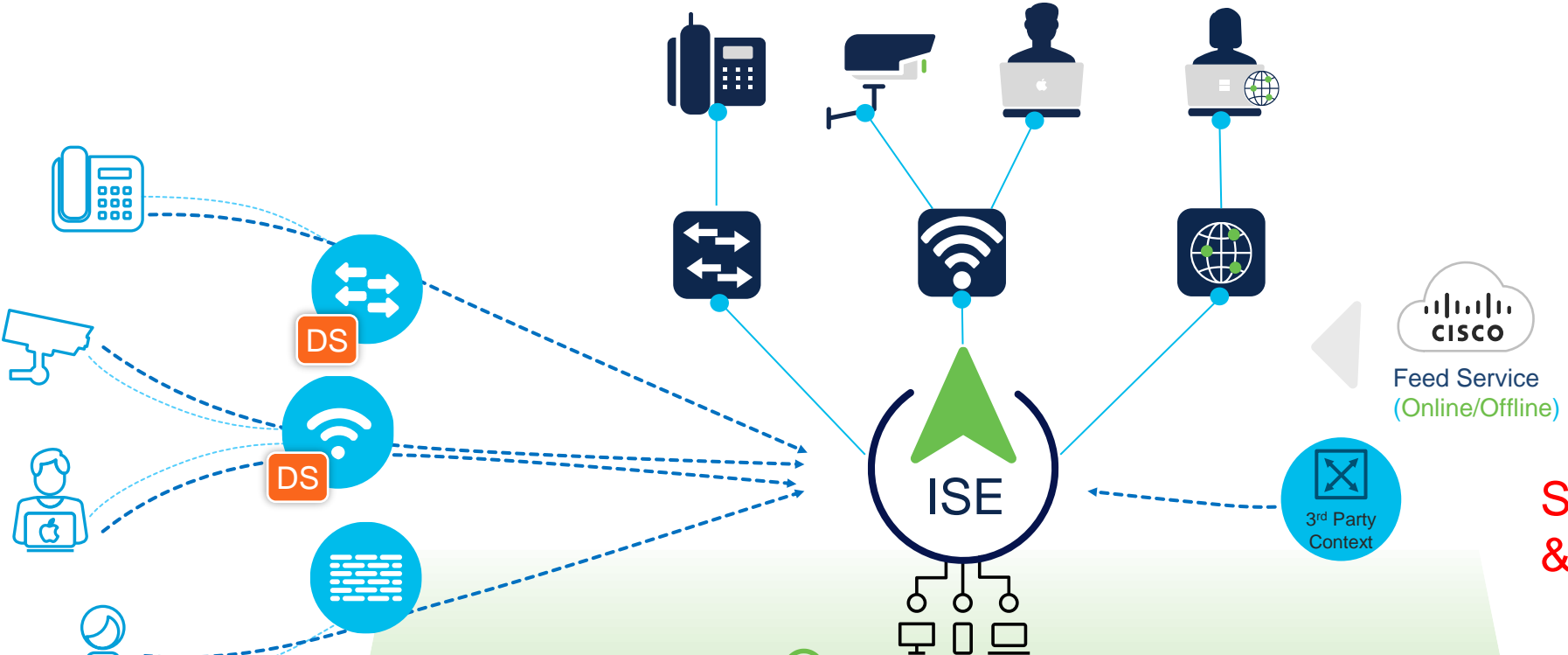


Datacenters

**Identity Services Engine**  
Policy Server for Network Access Control

**Authentication**  
802.1x & MAB  
Limiting the network to Trusted devices only.

# Multi-Factor Classification on ISE



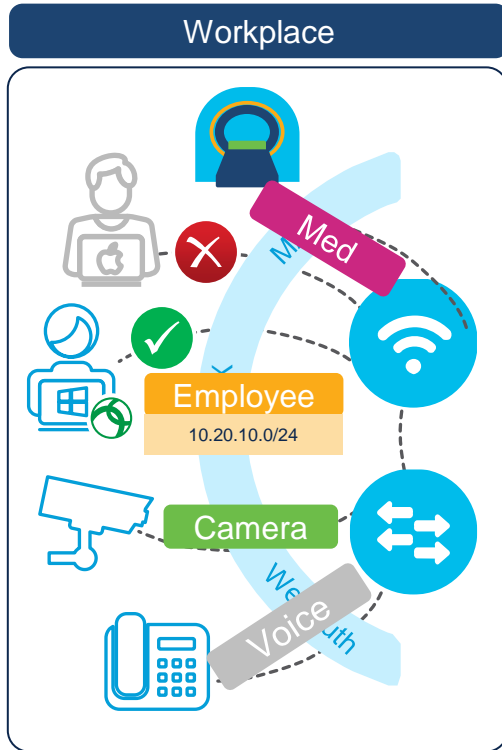
Shield Device Database & Risk Scoring!



Manufacturer	Device Type	Model	OS
<ul style="list-style-type: none"> <li>Cisco (IP-Phone)</li> <li>Arlo (Camera)</li> <li>Apple (Laptop)</li> <li>Lenovo (Laptop)</li> </ul>	<ul style="list-style-type: none"> <li>IP-Phone</li> <li>Camera</li> <li>Laptop</li> <li>Laptop</li> </ul>	<ul style="list-style-type: none"> <li>IP Phone 7980</li> <li>Pro wireless Cam</li> <li>MacBook Pro</li> <li>Thinkpad 540</li> </ul>	<ul style="list-style-type: none"> <li>iOS</li> <li>Linux</li> <li>macOS 12.0</li> <li>Windows Enterprise</li> </ul>

# Campus: Establishing Trust

## Segmentation on the Network

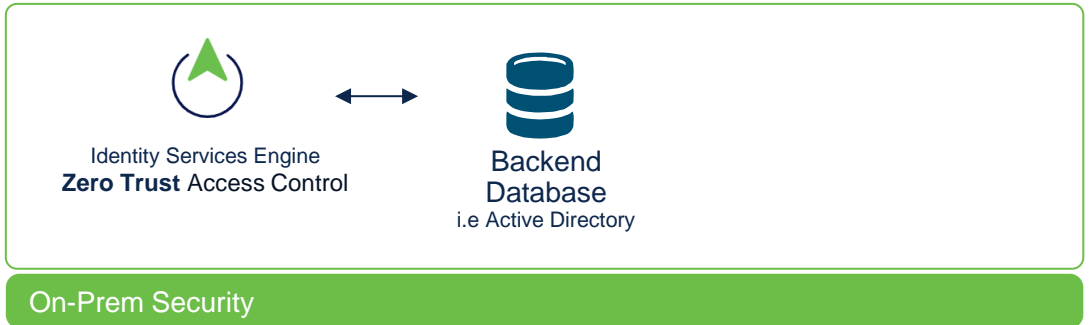


```

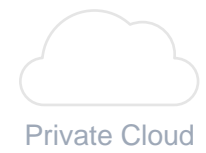
access-list 102 deny udp 167.160.188.162 0.0.0.255 gt 4230 248.11.187.246 0.255.255.255 eq 2165
access-list 102 deny udp 32.124.217.1 255.255.255.255 lt 907 11.38.130.82 0.0.31.255 gt 428
access-list 102 permit ip 64.98.77.248 0.0.0.127 eq 639 122.201.132.164 0.0.31.255 gt 1511
access-list 102 deny tcp 247.54.117.116 0.0.0.127 gt 4437 136.68.158.104 0.0.1.255 gt 1945
access-list 102 permit icmp 136.196.101.101 0.0.0.255 lt 2361 90.186.112.213 0.0.31.255 eq 116
access-list 102 deny udp 242.4.189.142 0.0.1.255 eq 1112 19.94.101.166 0.0.0.127 eq 959
access-list 102 deny tcp 82.1.221.1 255.255.255.255 eq 2587 174.222.14.125 0.0.31.255 lt 4993
access-list 102 deny tcp 103.10.93.140 255.255.255.255 eq 970 71.103.141.91 0.0.0.127 lt 848
access-list 102 deny ip 32.15.78.227 0.0.0.127 eq 1493 72.92.200.157 0.0.0.255 gt 4878
access-list 102 permit icmp 100.211.144.227 0.0.1.255 lt 4962 94.127.214.49 0.255.255.255 eq 1216
access-list 102 deny icmp 88.91.79.30 0.0.0.255 gt 26 207.4.250.132 0.0.1.255 gt 1111
access-list 102 deny ip 167.17.174.35 0.0.1.255 eq 3914 140.119.154.142 255.255.255.255 eq 4175
access-list 102 permit tcp 37.85.170.24 0.0.0.127 lt 3146 77.26.232.98 0.0.0.127 gt 1462
access-list 102 permit tcp 155.237.22.232 0.0.0.127 gt 1843 239.16.35.19 0.0.1.255 lt 4384
access-list 102 deny udp 167.160.188.162 0.0.0.255 gt 4230 248.11.187.246 0.255.255.255 eq 2165
access-list 102 deny udp 32.124.217.1 255.255.255.255 lt 907 11.38.130.82 0.0.31.255 gt 428
    
```

**Security Policy based on IP address**

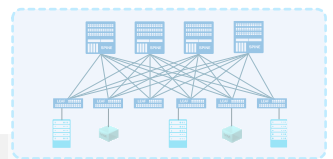
No Microsegmentation	Not Scalable	Difficult to Manage
----------------------	--------------	---------------------



Internet Applications



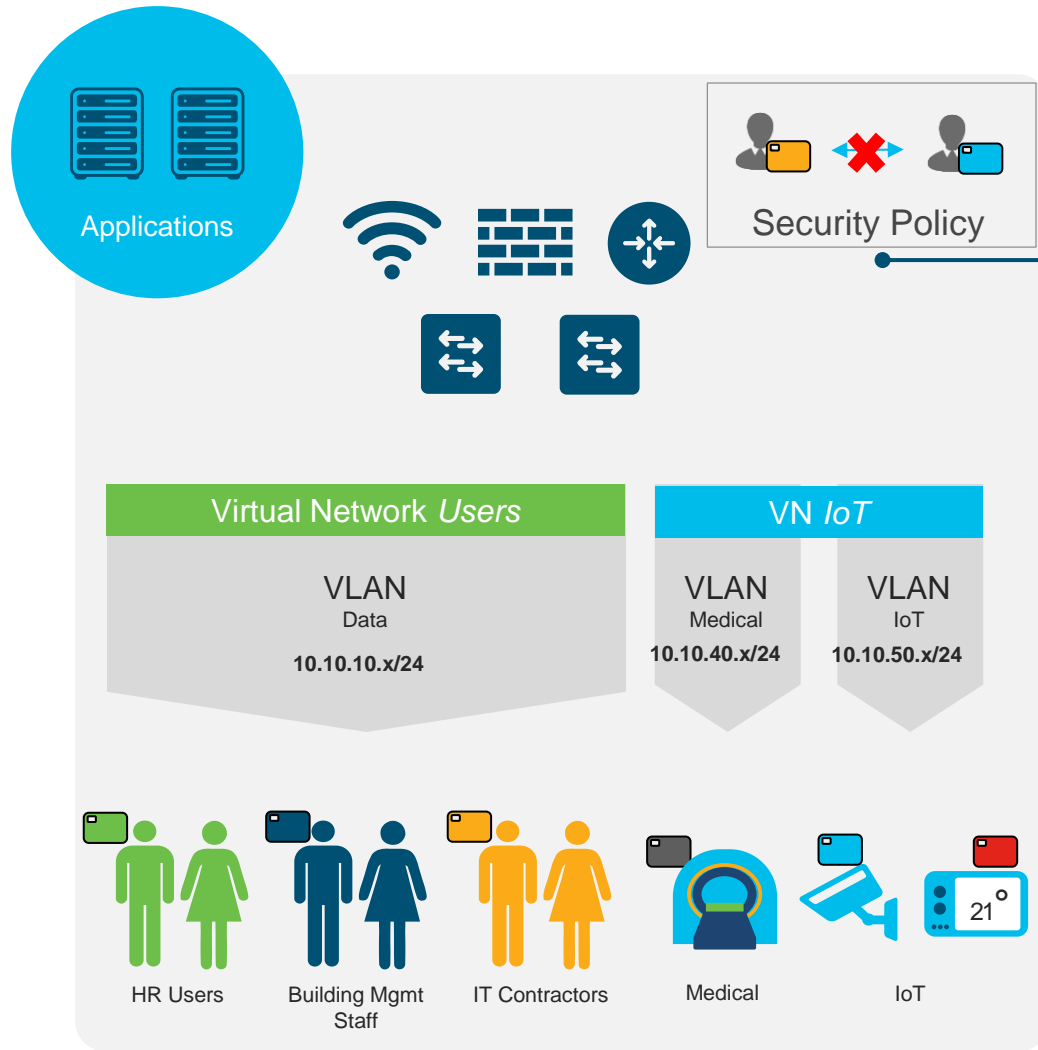
Private Applications



**Identity Services Engine**  
Policy Server for Network Access Control

**Authentication**  
802.1x & MAB  
Limiting the network to Trusted devices only.

# Micro-segmentation using Scalable Group



Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Group-Based Access Control IP Based Access Control Application Traffic Copy Virtu

Policies (12091) Enter full screen

Filter Deploy

Contractors → Guests Custom Set to Default Policy

Policy Status Enabled

Contract: Change Contract

#	Action	Application	Protocol	Source / Destination	Port	Logging
1	DENY	netbios-dgm	TCP/UDP	Destination	138	OFF
2	DENY	netbios-ssn	TCP/UDP	Destination	139	OFF
3	DENY	netbios-ns	TCP/UDP	Destination	137	OFF
4	DENY	telnet	TCP	Destination	23	OFF
5	DENY	ssh	TCP	Destination	22	OFF
6	DENY	advanced	ICMP	Source Destination		OFF
7	DENY	http	TCP	Destination	80	OFF
8	DENY	advanced	TCP	Source Destination	80	OFF
9	DENY	ftp	TCP	Destination	21,21000	OFF

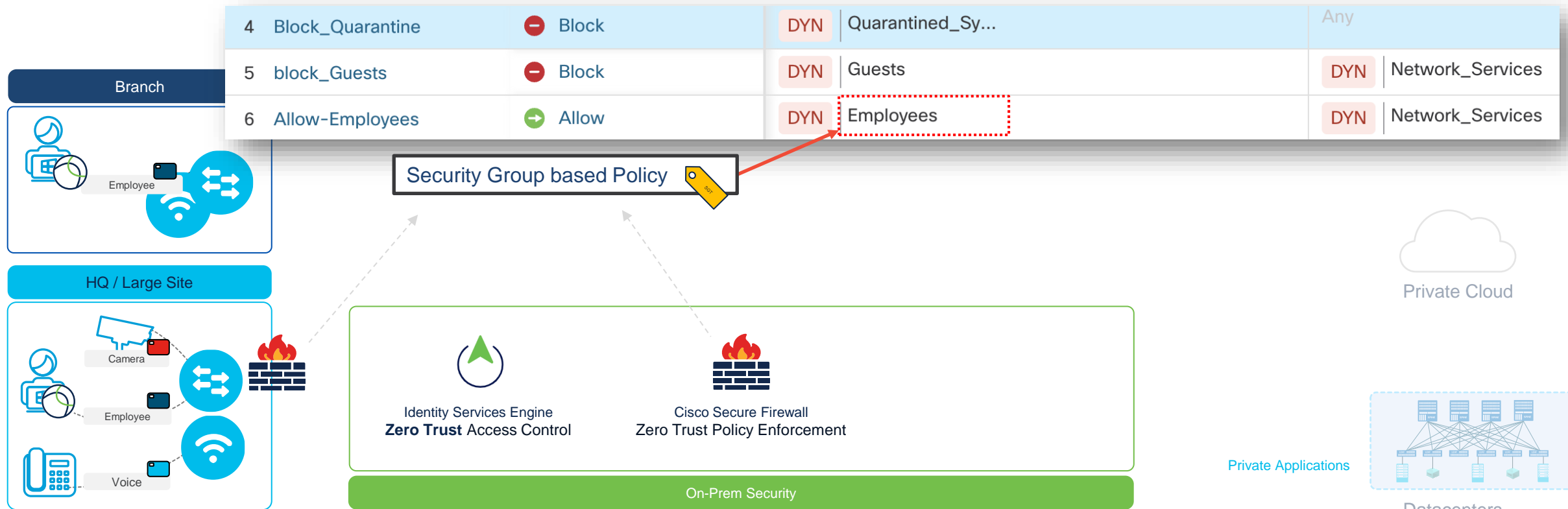
Default Action PERMIT Logging OFF

Cancel Save

Can you tell who is allowed to talk to who?

# Campus / Branch: Enforcing Trust Based Access

*Define Who can do What on the Network*



# Cisco Secure Firewall Hardware Portfolio

890 Mbps  
AVC+IPS

2.3-5.3 Gbps AVC+IPS

6-9 Gbps AVC+IPS

10-45 Gbps AVC+IPS  
5.5 - 39.4 Gbps IPsec VPN  
8 Node Cluster:  
Up to 288 Gbps AVC+IPS

19-53 Gbps AVC+IPS  
16-node cluster:  
Up to 678 Gbps AVC+IPS

65-140 Gbps AVC+IPS  
45-140 Gbps IPsec VPN  
16-node cluster:  
Up to 1.7 Tbps AVC+IPS

55-68 Gbps AVC+IPS  
16-node cluster:  
Up to 950 Gbps AVC+IPS



1010



1120/40/50



1200



3105/10/20/30/40



4112/15/25/45



4215/25/45



9300 Series  
SM-40  
SM-48  
SM-56



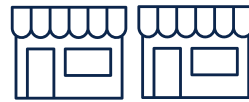
SMB



Branch Office



Mid Enterprise



Large Enterprise



Data Center



Service Provider

All appliances can run either ASA or FTD applications, FP9300 can run both on different SMs

# Firewall Policy Optimizer

**i** Policy Analysis and Optimization

Anomalies found from the initial scan: Out of **1234** rules, there are **323** duplicate rules found. These include **153** fully shadowed rules and **170** fully redundant rules.

Fully Shadowed Rules (153)      Fully Redundant Rules (170)      Total rules 1234

[View Details](#)

---

We recommend you take one of the following actions on the duplicate rules:

[Disable all](#)      [Delete all](#)

[Regenerate](#)



# Secure IPS based on SNORT 3

**Summary**

Rule Distribution

Alert	512
Block	11893
Disabled	37672

Base Configuration

Base Policy: Balanced Security and Connectivity

Recommendations

Usage: **In Use**

Security Level:

Generated on 2022-10-03 10:56:03 UTC

Rule State 6682 rules recommended for 2 networks

---

**Effective Policy**

51 items View Groups

Rule Action: Alert Block Disabled Overridden

Presets: Alert ( 512 ) | Block ( 11,893 ) | Disabled ( 37,672 ) | Overridden ( 17,197 )

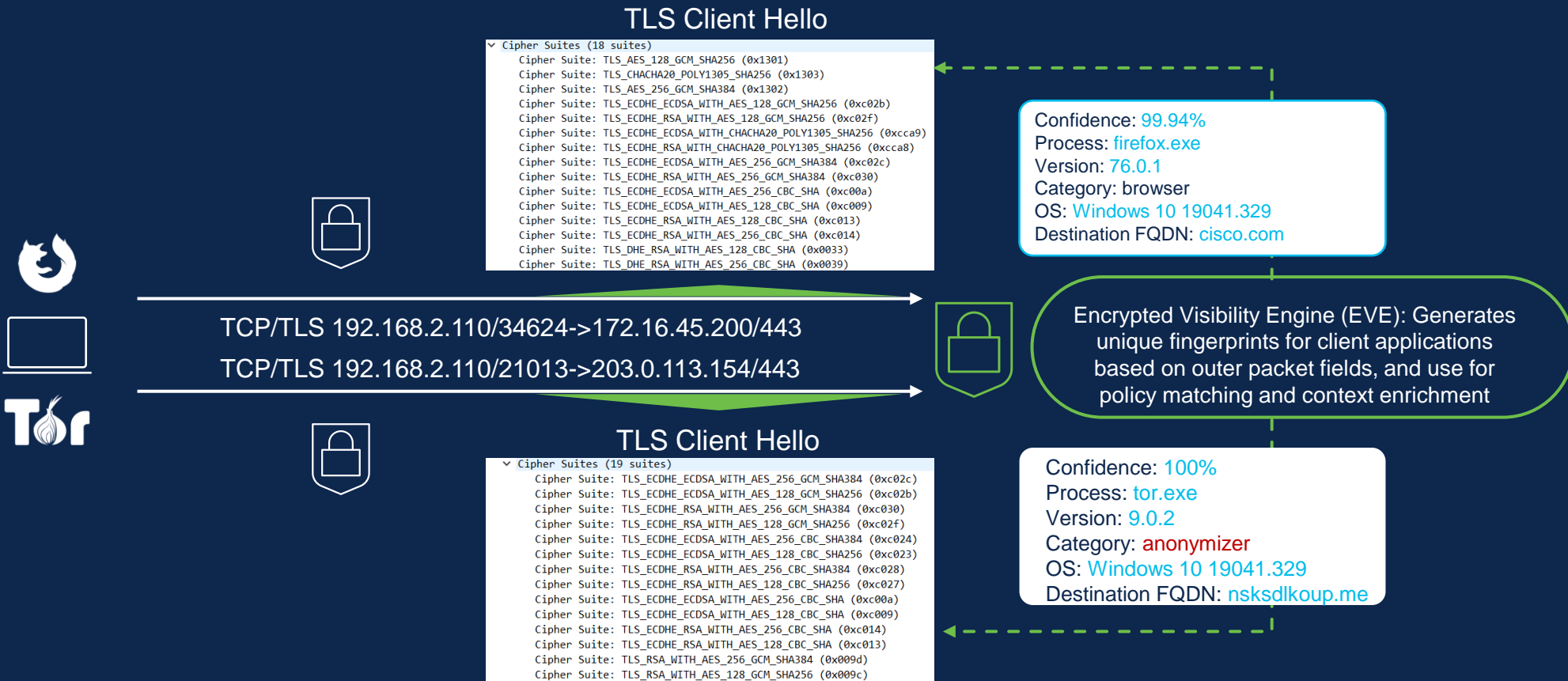
Advanced Filters

Rule Action	Search by CVE, SID, Reference Info, or Rule Message	Set By	Assigned Groups
50,077 rules			
All Rules			
Rule Categories (9 groups)			
<input type="checkbox"/> 125:8 (ftp_server) FTP bounce ...	Alert	Rule Override	Builtins
<input type="checkbox"/> 125:2 (ftp_server) invalid FTP c...	Alert	Rule Override	Builtins
<input type="checkbox"/> 125:1 (ftp_server) TELNET cmd ...	Alert	Rule Override	Builtins
<input type="checkbox"/> 119:16 (http_inspect) chunk leng...	Alert	Rule Override	Builtins
<input type="checkbox"/> 119:19 (http_inspect) HTTP head...	Alert	Rule Override	Builtins
<input type="checkbox"/> 119:2 (http_inspect) URI contai...	Alert	Rule Override	Builtins
<input type="checkbox"/> 119:1 (http_inspect) URI has pe...	Alert	Rule Override	Builtins
<input type="checkbox"/> 119:6 (http_inspect) URI has tw...	Alert	Rule Override	Builtins

Context Menu Options:

- Rule Action
- Block
- Alert
- Rewrite
- Drop
- Reject
- Disable (Default)
- Revert to default

# Encrypted Visibility without Decryption



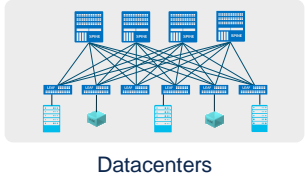
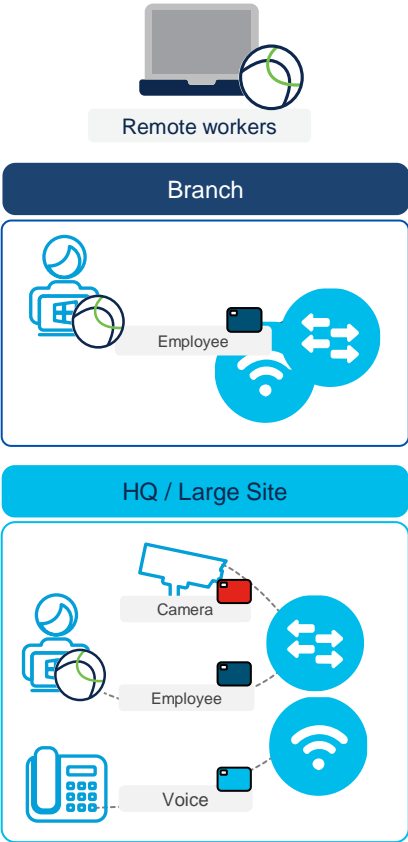
Views... IOIC Triggered x Select... Refresh

Showing all 2 events (2) 2022-07-21 10:59:07 EDT → 2022-07-21 11:59:07 EDT 1h Go Live

Time	Detection Type	Encrypted Visibility Process Confidence Score	Encrypted Visibility Process Name	Encrypted Visibility Threat Confidence	Encrypted Visibility Threat Confidence Score	IOC	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application
2022-07-21 11:56:57	AppID	97%	_malware	Very High	97%	Triggered	49161 / tcp	443 (https) / tcp	
2022-07-21 11:29:51	AppID	97%	_malware	Very High	97%	Triggered	49161 / tcp	443 (https) / tcp	

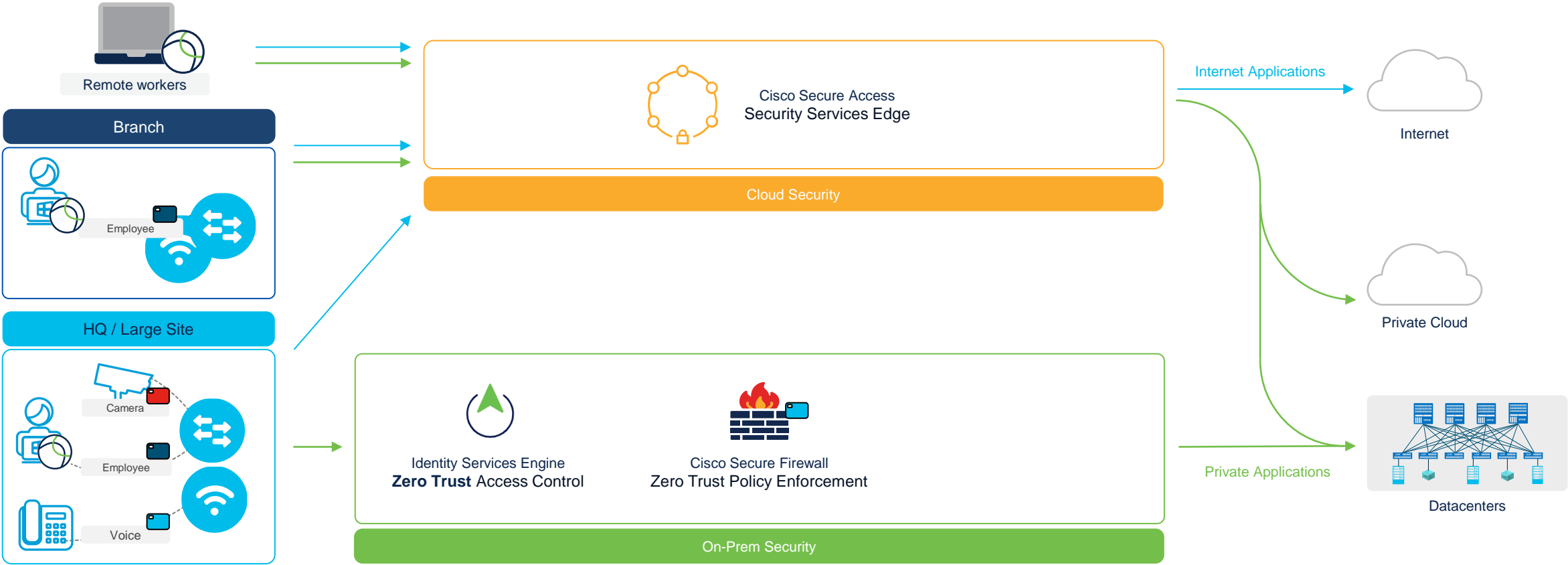
# Hybrid Work: *Extending* Trust based Enforcement

*Unify policies for Secure Internet and Private Access*



# Hybrid Work: *Extending* Trust based Enforcement

*Unify policies for Secure Internet and Private Access*



# Resiliency

Am I capable of detecting, reporting and recovering from a breach?

*NIS2 & Compliancy*

# NDR using Cisco Secure Network Analytics

## Network Detection & Response

### Global threat intelligence

(powered by Talos)

Intelligence of global threat campaigns mapped to local alarms for faster mitigation



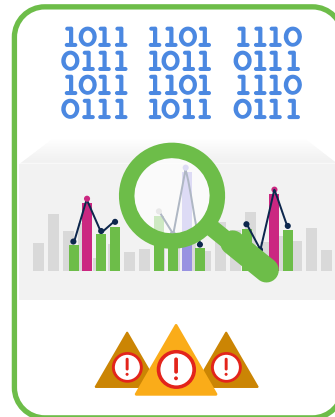
### Security Event Detection

Initial check for the real threats like Ddos, Packet floods etc.



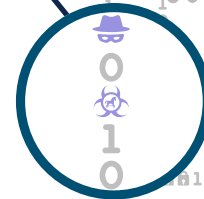
### Behavioral modeling

Behavioral analysis of every activity within the network to pinpoint anomalies



### Encrypted Traffic Analytics

Malware detection without any decryption using enhanced telemetry from the new Cisco devices



### Data collection

Rich telemetry from the existing network or Cloud infrastructure



- Netflow
- SPAN
- VPC logs
- GCP logs
- NSG logs
- ISE
- Firewalls
- Proxies
- DHCP
- Active Directory
- ETA

# NDR using Secure Network Analytics

Network Detection & Response

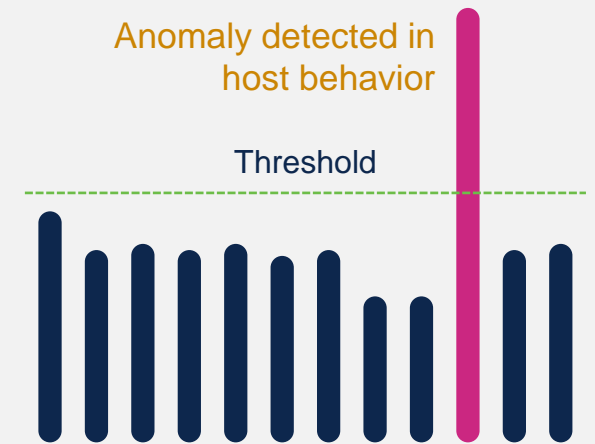
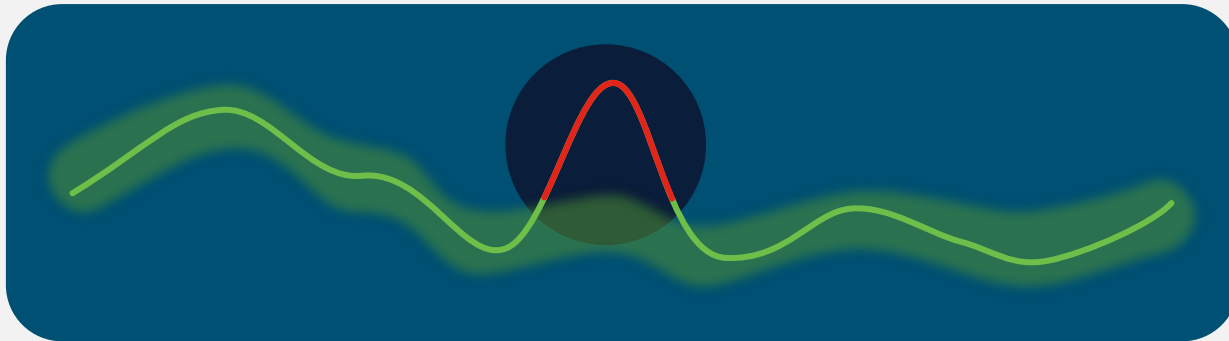
Global threat intelligence

(powered by Talos)

Intelligence of global threat campaigns mapped to local alarms for faster mitigation

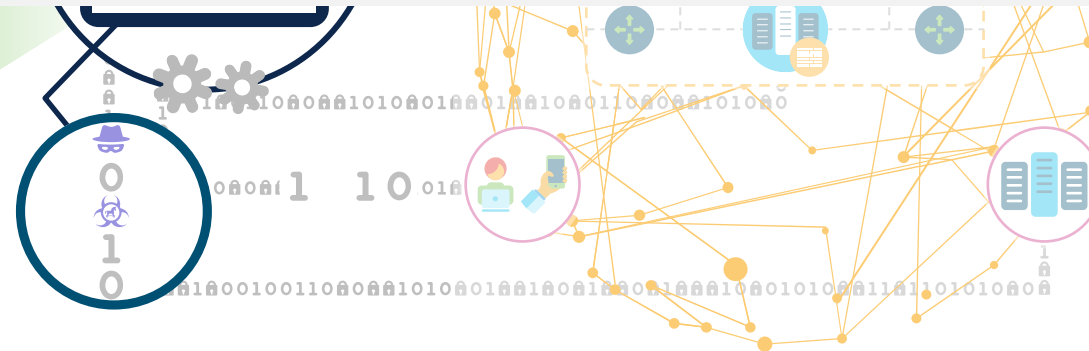


**Behavior Analytics:** Dynamic baselines = relevant anomalies



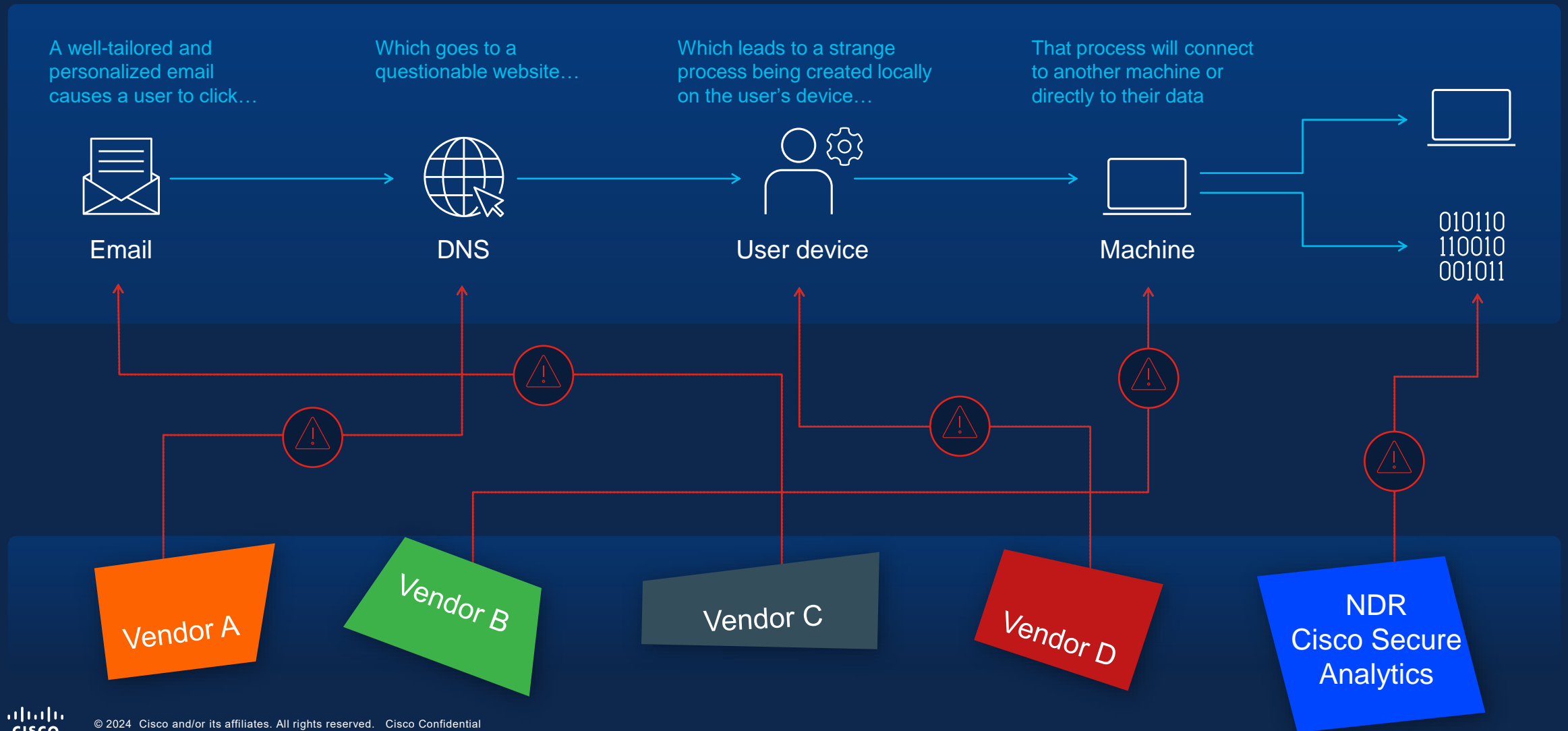
**Encrypted Traffic Analytics**

Malware detection without any decryption using enhanced telemetry from the new Cisco devices



Firewalls  
Proxies  
DHCP  
Active Directory  
ETA

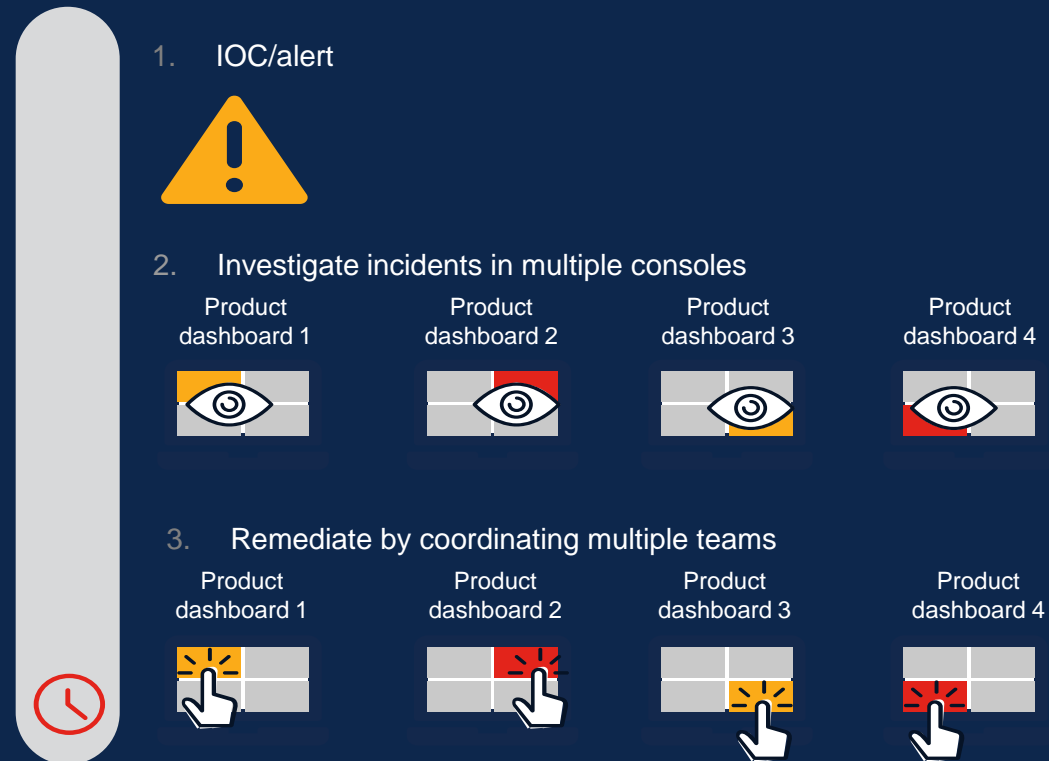
# Ransomware campaigns are *multi-vector*





# Siloed Detection & Response

Without XDR: xx minutes



# Simplify with Cisco XDR



# Correlation with attack chaining

- Alerts from XDR and integrated products are correlated prior to becoming XDR incidents.
- Alerts with common indicators are combined into attack chains.
- New alerts are also appended to incidents as they occur over time.
- Analysts can also link incidents together for manual correlation.

← Incidents

924

Incident Reported ▾

Attack Chain: "Mult..."

View Investigation

Reported by [Cisco Secure Cloud Analytics \(cisco-explorcorp-earth\)](#) on 2023-05-10T18:07:19.009Z - 5

BG RG

[Linked Incidents](#)

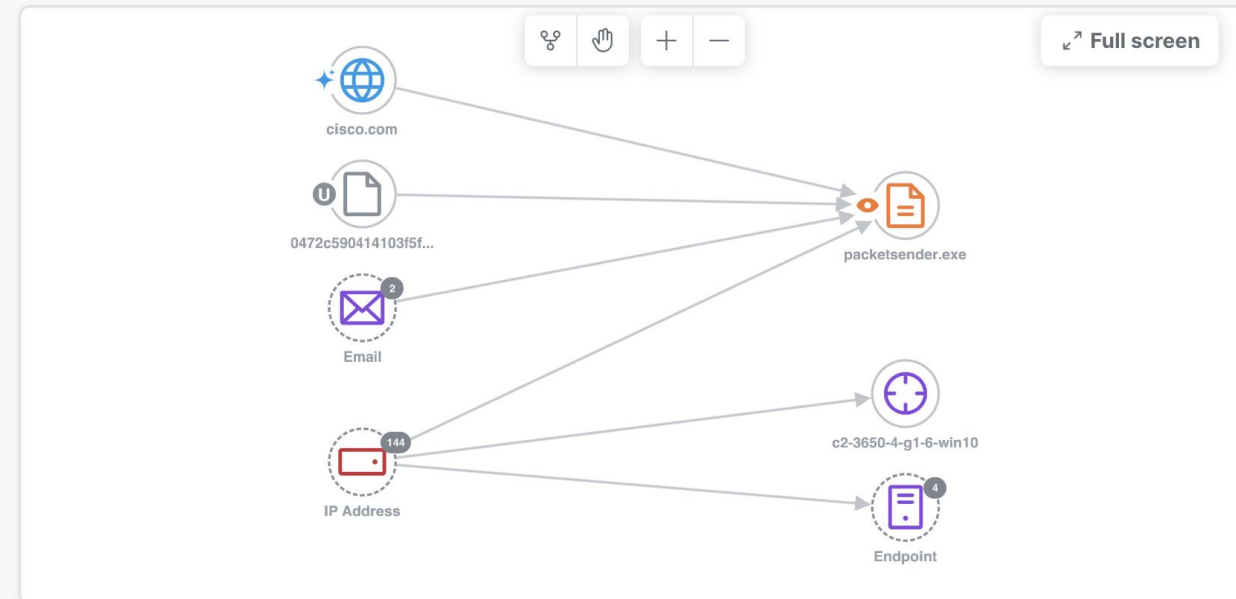
Persistence and Command and Control events have been identified by Cisco XDR Analytics for atl-t... [View Long Description](#)

Overview

Detection

Response

Worklog



8 Assets

[View all](#)

TOP ACTIVE

i-06c189f...	361 events
ip-10-90-...	106 events
i-075b9fe...	106 events
atl-tme-c...	102 events

144 Observables

[View all](#)

TOP ACTIVE

61.177.1...	47,406 events
61.177.1...	12,992 events
61.177.17...	6,568 events
198.51.10...	409 events

21 Indicators

[View all](#)

TOP ACTIVE

Cisco Secure Network A...	10 events
<b>Port Scan</b>	
Cisco Secure Cloud Analy...	5 events
<b>Confirmed Threat Ind...</b>	
Cisco Secure Cloud Analy...	5 events
<b>Confirmed Threat Wa...</b>	

# XDR Response playbooks

- Bring the ability to take immediate response actions into the incident manager.
- Powered by out of the box XDR Automation workflows.
- Broken down into four stages:



Identify



Contain



Eradicate



Recover

## Identify Affected Hosts

Add Note

Add note with summary of findings on the investigations of hosts found with ...

## Contain Incident: Overview

Add Note

Overview of how to contain Indicators of Compromise to stop the spread of ...

## Contain Incident: Assets

Select

Use asset-based containment to stop the spread of malicious activity.

This automation workflow will network isolate/quarantine all selected assets on your integrated Endpoint Detection & Response solutions. After clicking Execute, you will be able to choose all or a subset of assets associated with this incident. Please make sure you have done proper identification before executing the workflow.

## Contain Incident: IPs

Add Note

Contain IP indicators of compromise to stop the spread of malicious activity

## Contain Incident: Domains

Select

Contain domain indicators of compromise to stop the spread of malicious act...

This automation workflow blocks the selected domain names on your integrated network policy enforcement solutions. After clicking Execute, you will be able to choose all or a subset of domains associated with this incident. Make sure you have done proper identification before executing the workflow.

Back

Go to Eradication →

 **SECURE**