cisco Connect

When the Network Meets Security

Håkan Nohre

Cisco EMEA Cyber Security

28 years, 1 month, 24 days, 3 hours

Dec 2, 2025 A.D

Megatrends that have already Impacted Cyber Security

"Internet is going dark"

Internet of Everything

Cloud Adoption

Megatrend #1 .... AI

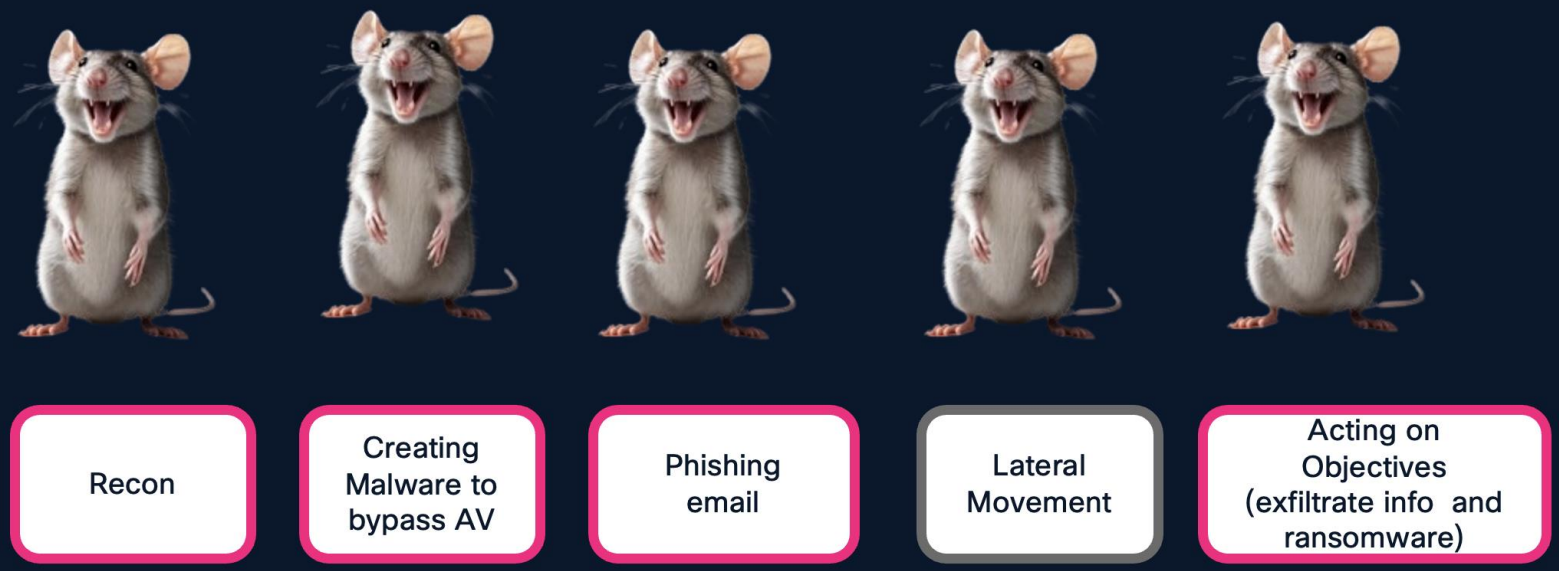
- **AI helping the attackers**
- AI changing network traffic
- AI helping the defenders
- Securing AI

Good guy

Bad Guy

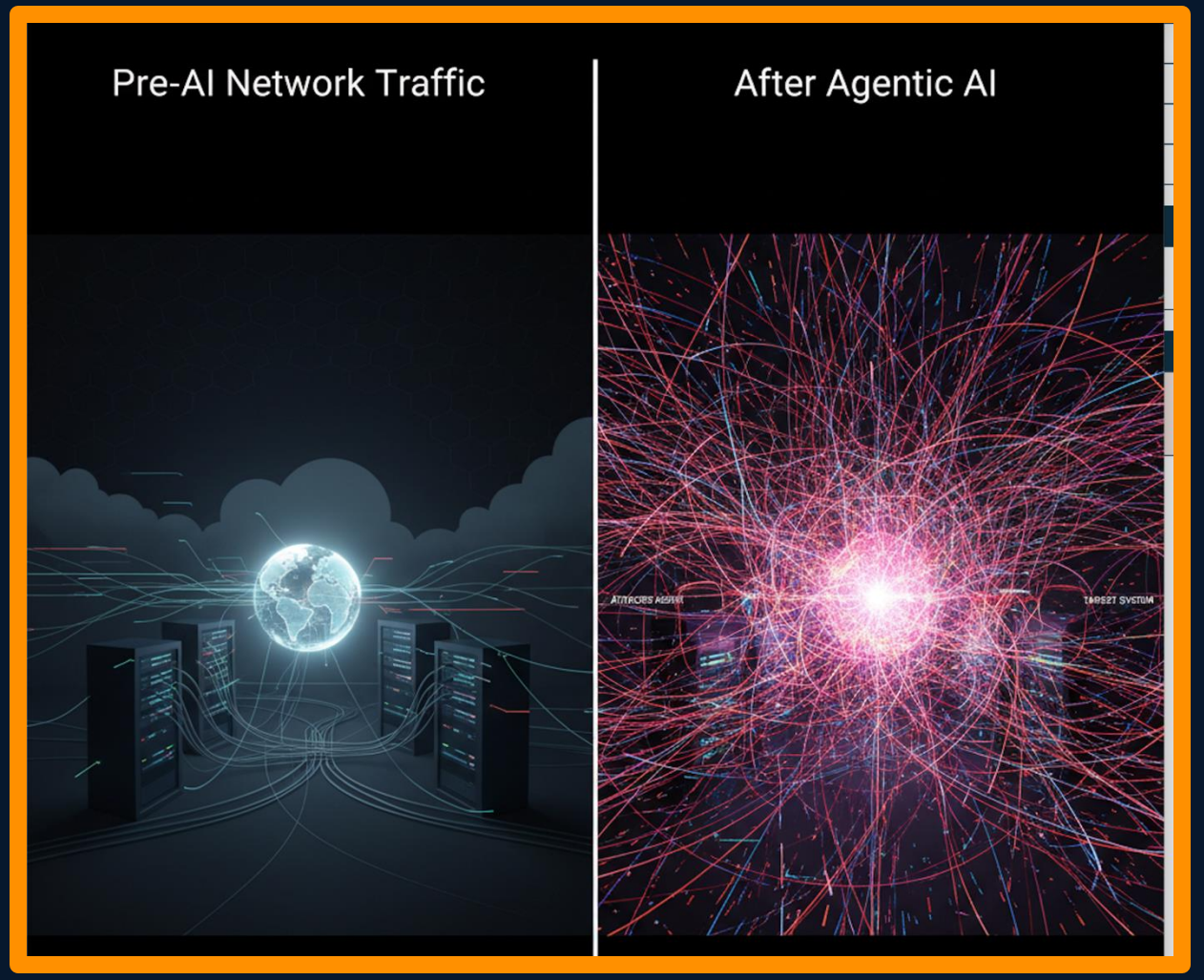
Megatrend #1 .... AI

- **AI helping the attackers**
- AI changing network traffic
- AI helping the defenders
- Securing AI



Megatrend #1 .... AI

- AI helping the attackers
- AI changing network traffic
- AI helping the defenders
- Securing AI



The Network – Our Office

Would you consider the printer a juicy target?

The Network – Manufacturing

The Network (Healthcare Region)....

Our Applications

Applications have changed from Old School Monolithic...

...to Microservices inside Kubernetes Clusters

”Our critical applications now live in a black box where we have no visibility”

Chief Network and Security Architect, Enterprise Bank

The Network Meets Security

- What is on the network?
- How does it behave?
- Enforce Zero Trust
- Observe and Remediate

The Network Meets Security

- **What is on the network?**
- How does it behave?
- Enforce Zero Trust
- Observe and Remediate

Does an IP address identify security objects?

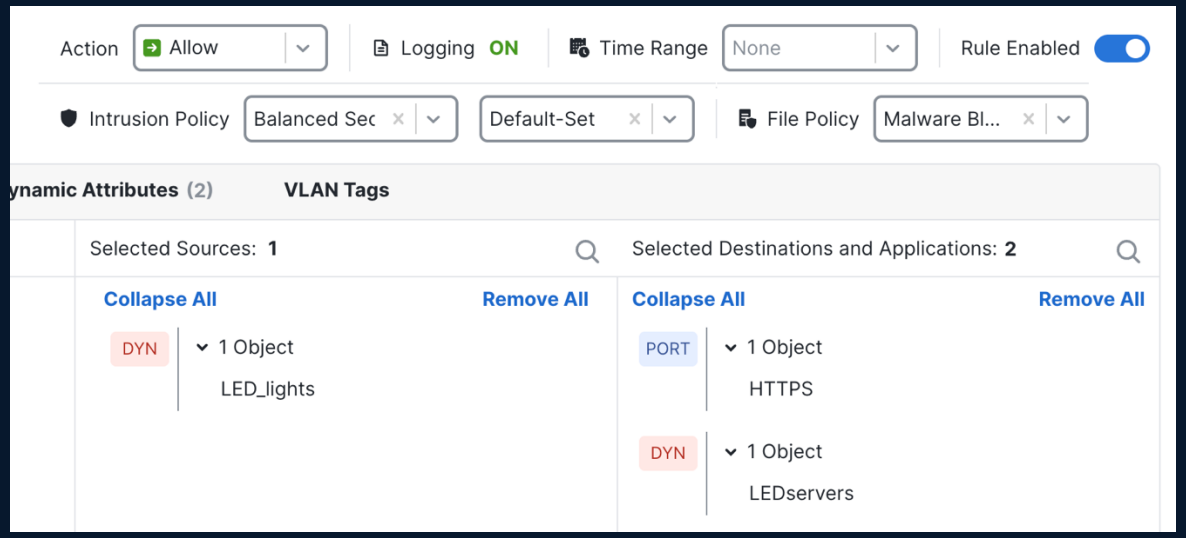
```
access-list ACL_SECURE_NET permit tcp 192.168.10.0 0.0.0.255 host 10.1.1.5 eq 80
access-list ACL_SECURE_NET permit tcp 192.168.20.0 0.0.0.255 host 10.1.1.5 eq 443
access-list ACL_SECURE_NET deny ip 192.168.30.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list ACL_SECURE_NET permit udp host 172.16.5.1 any eq 53
access-list ACL_SECURE_NET deny tcp any host 10.1.1.10 range 21 23
access-list ACL_SECURE_NET permit tcp 10.0.0.0 0.255.255.255 host 10.1.2.2 eq 3389
access-list ACL_SECURE_NET deny icmp any any echo
access-list ACL_SECURE_NET permit ip 172.16.0.0 0.0.255.255 10.1.1.0 0.0.0.255 established
access-list ACL_SECURE_NET permit udp 192.168.50.0 0.0.0.255 host 10.1.1.20 eq 161
access-list ACL_SECURE_NET deny tcp any host 10.1.1.30 eq 22
access-list ACL_SECURE_NET permit tcp host 172.16.100.1 host 10.1.1.40 eq 8443
access-list ACL_SECURE_NET permit ip host 192.168.1.1 host 10.1.1.50
access-list ACL_SECURE_NET deny ip any any log
```

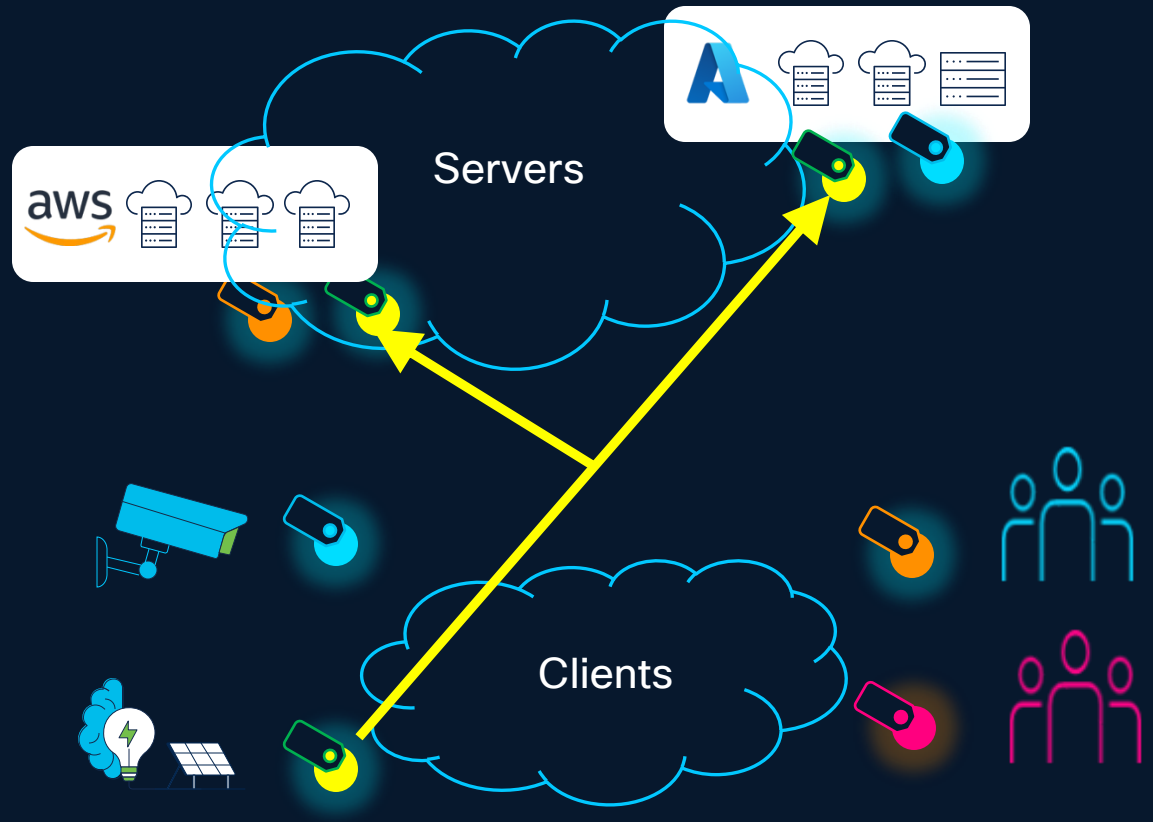
Policy rules with IP addresses?

- Difficult to maintain!
- Changes in the network mean changes in the ruleset
- New Security rules mean changes in the network
- IP addresses in the cloud are ephemeral! (temporary)

Security Groups: Rules without IP addresses

- No need to change rule with changing IP addresses!





The Network Meets Security

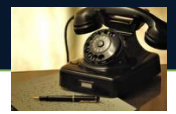
- What is on the network?
- **How does it behave?**
- Enforce Zero Trust
- Observe and Remediate

How can Network Telemetry Help?

David

Alice, his teenage daughter

Analogy with a Phone Bill



TELEPHONE USAGE CHARGES

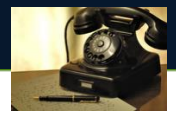
Charges Billed to **BRAHM, LAURENCE** **AUTHCODE**

DATE	TIME	PLACE		NUMBER	MIN	CHARGE
21-AUG-2005	09:35	ELKHORN	NE	4025531620	0.4	0.02
22-AUG-2005	09:41	MISSOULA	MT	4069283507	6.8	0.37
23-AUG-2005	09:48	GRASS VLY	CA	5302614689	1.0	0.06
24-AUG-2005	14:12	LARAMIE	WY	3073426413	2.4	0.13
27-AUG-2005	14:17	GREELEY	CO	9703306310	1.0	0.06
09-SEP-2005	14:22	SPOKANE	WA	5098381370	2.7	0.15
20-SEP-2005	14:25	FLAGSTAFF	AZ	9287143707	0.4	0.02
		CC		**8431464613**		
DATE	**TIME**	**PLACE**		**NUMBER**	**MIN**	**CHARGE**
28-AUG-2005	15:12	CHEYENNE	WY	3078218059	1.0	0.94
28-AUG-2005	15:22	PORTLAND	OR	5038256809	0.0	0.78
29-AUG-2005	15:23	FRESNO	CA	5592337953	1.0	0.12
15-SEP-2005	09:52	FT COLLINS	CO	9704745937	4.0	0.25
19-SEP-2005	16:25	HILLSBORO	OR	5035475794	2.0	0.90
		DT		**5037256659**		
DATE	**TIME**	**PLACE**		**NUMBER**	**MIN**	**CHARGE**
22-AUG-2005	10:47	EUGENE	OR	5413461656	0.6	0.03
26-AUG-2005	13:51	PORTLAND	OR	5037253694	0.7	0.00
01-SEP-2005	11:44	CORVALLIS	OR	5419375496	0.4	0.02
16-SEP-2005	09:39	ASHLAND	OR	5415526749	0.4	0.02
				TOTAL	24.8	3.87

New boyfriend...

X

Analogy with a Phone Bill



TELEPHONE USAGE CHARGES

Charges Billed to **BRAHM, LAURENCE** **AUTHCODE**

DATE	TIME	PLACE		NUMBER	MIN	CHARGE
21-AUG-2005	09:35	ELKHORN	NE	4025531620	0.4	0.02
22-AUG-2005	09:41	MISSOULA	MT	4069283507	6.8	0.37
23-AUG-2005	09:48	GRASS VLY	CA	5302614689	1.0	0.06
24-AUG-2005	14:12	LARAMIE	WY	3073426413	2.4	0.13
27-AUG-2005	14:17	GREELEY	CO	9703306310	1.0	0.06
09-SEP-2005	14:22	SPOKANE	WA	5098381370	2.7	0.15
20-SEP-2005	14:25	FLAGSTAFF	AZ	9287143707	0.4	0.02
		CC		**8431464613**		
DATE	**TIME**	**PLACE**		**NUMBER**	**MIN**	**CHARGE**
28-AUG-2005	15:12	CHEYENNE	WY	3078218059	1.0	0.94
28-AUG-2005	15:22	PORTLAND	OR	5038256809	0.0	0.78
29-AUG-2005	15:23	FRESNO	CA	5592337953	1.0	0.12
15-SEP-2005	09:52	FT COLLINS	CO	9704745937	4.0	0.25
19-SEP-2005	16:25	HILLSBORO	OR	5035475794	2.0	0.90
		DT		**5037256659**		
DATE	**TIME**	**PLACE**		**NUMBER**	**MIN**	**CHARGE**
22-AUG-2005	10:47	EUGENE	OR	5413461656	0.6	0.03
26-AUG-2005	13:51	PORTLAND	OR	5037253694	0.7	0.00
01-SEP-2005	11:44	CORVALLIS	OR	5419375496	0.4	0.02
16-SEP-2005	09:39	ASHLAND	OR	5415526749	0.4	0.02
				TOTAL	24.8	3.87

You Ditched him!

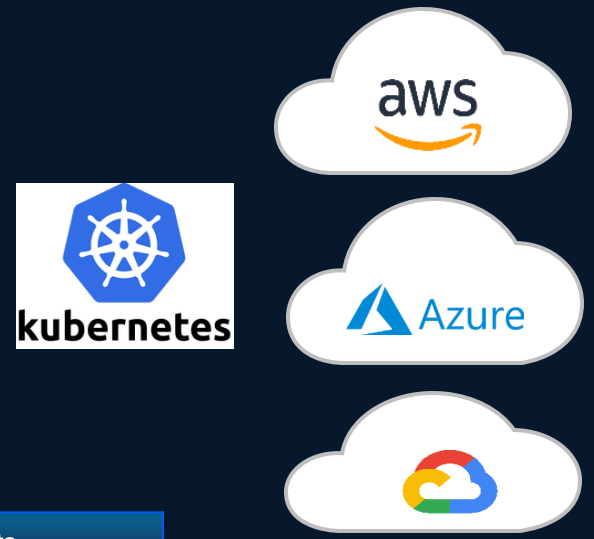
X

Netflow (and flows from cloud infra)

Switches

Routers

Firewalls



TELEPHONE USAGE CHARGES

Charges Billed to **BRAHM, LAURENCE** **AUTHCODE**

DATE	TIME	PLACE		NUMBER	MIN	CHARGE
21-AUG-2005	09:35	ELKHORN	NE	4025531620	0.4	0.02
22-AUG-2005	09:41	MISSOULA	MT	4069283507	6.8	0.37
23-AUG-2005	09:48	GRASS VLY	CA	5302614689	1.0	0.06
24-AUG-2005	14:12	LARAMIE	WY	3073426413	2.4	0.13
27-AUG-2005	14:17	GREELEY	CO	9703306310	1.0	0.06
09-SEP-2005	14:22	SPOKANE	WA	5098381370	2.7	0.15
20-SEP-2005	14:25	FLAGSTAFF	AZ	9287143707	0.4	0.02
		CC		8431464613		

DATE			IN CHARGE
28-AUG-2		1.0	0.94
28-AUG-2		0.0	0.78
29-AUG-2		1.0	0.12
15-SEP-2		4.0	0.25
19-SEP-2		2.0	0.90

DATE			IN CHARGE
22-AUG-2		0.6	0.03
26-AUG-2		0.7	0.00
01-SEP-2		0.4	0.02
16-SEP-2		0.4	0.02
		4.8	3.87

Flow Information	Packets
DESTINATION ADDRESS	172.168.134.2
SOURCE PORT	47321
DESTINATION PORT	443
INTERFACE	Gi0/0/0
IP TOS	0x00
IP PROTOCOL	6
NEXT HOP	172.168.25.1
TCP FLAGS	0x1A
SOURCE SGT	100
:	:
APPLICATION NAME	NBAR SECURE-HTTP

EDR meets NDR: Cisco Network Visibility Module (NVM)

Cisco Secure Client (NVM Module)

Start Time*
End Time*
Source IP*
Source Port*
Destination IP*
Destination Port*
Bytes Sent*
Bytes Received*
Packet Count*
(derived)
Protocol*

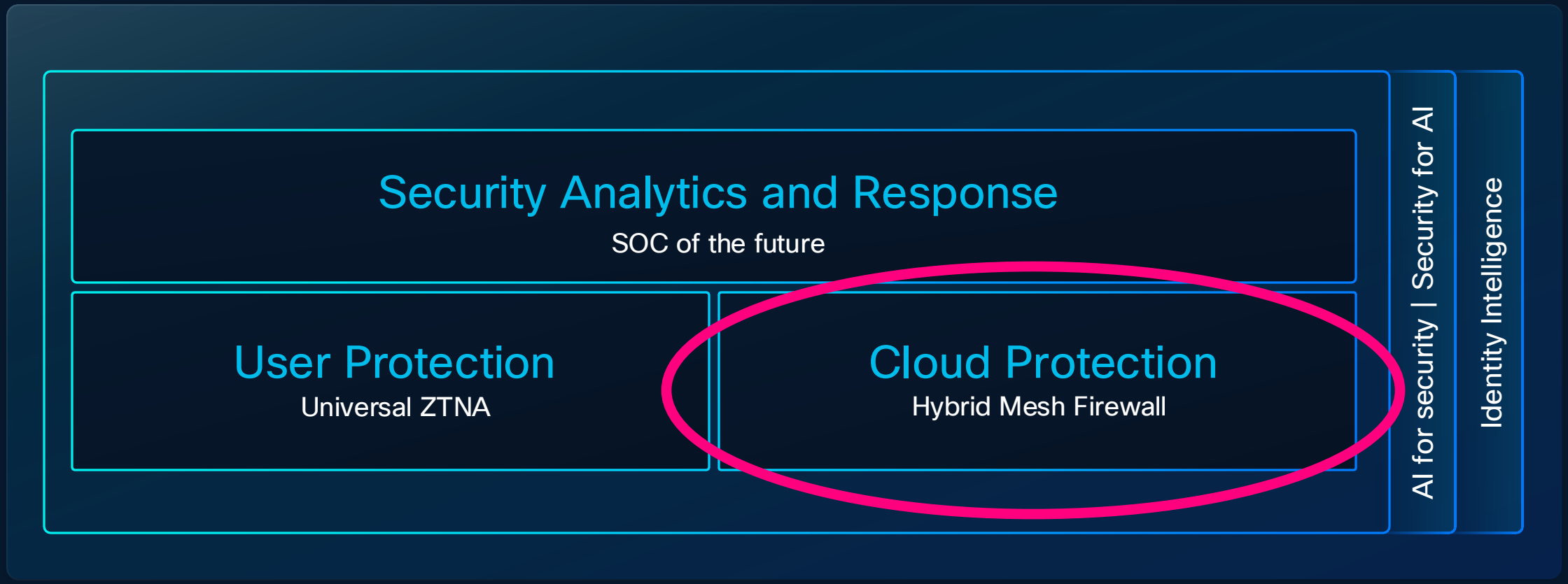
Interface Info UID
Interface Index
Interface Type
Interface Name
Interface Details List
Interface Mac Addr.
UDID
User
User Account Type
Agent Version
Virtual Station Name
OS Name
OS Version
OS Edition
System Manufacturer
System Type

Process Account*
Process Account Type
Process ID
Process Name*
Process Hash*
Process Path
Process Args
Parent Process ID
Parent Process Account
Process Account
Parent Process Name*
Parent Process Hash*
Parent Process Path
Parent Process Args
Host Name
DNS Suffix
Module Name List
Module Hash List
Parent Process Name
Parent Process Hash

The Network Meets Security

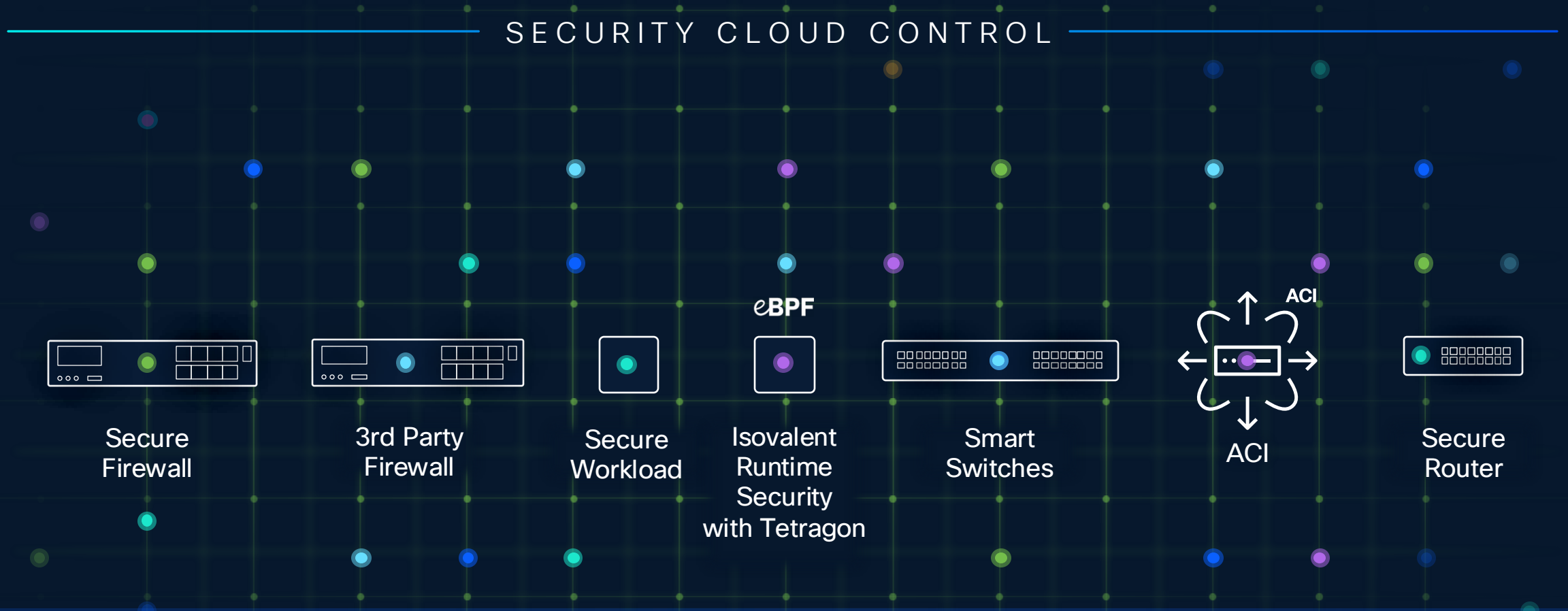
- What is on the network?
- How does it behave?
- **Enforce Zero Trust**
- Observe and Remediate

Cisco Security Cloud (Architecture)



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Hybrid Mesh Firewall



Write policy once, enforce across the mesh

Great Stuff, but many tools?

Switch
Router
Firewalls
ASA
FTD

Data Center Micro-segmentation
Hyper shield
Secure Workload

AI Defense

XDR
email security
...more

Universal ZTNA

Identity Intelligence

Security Cloud Control: Management Consolidation

Security Cloud Control

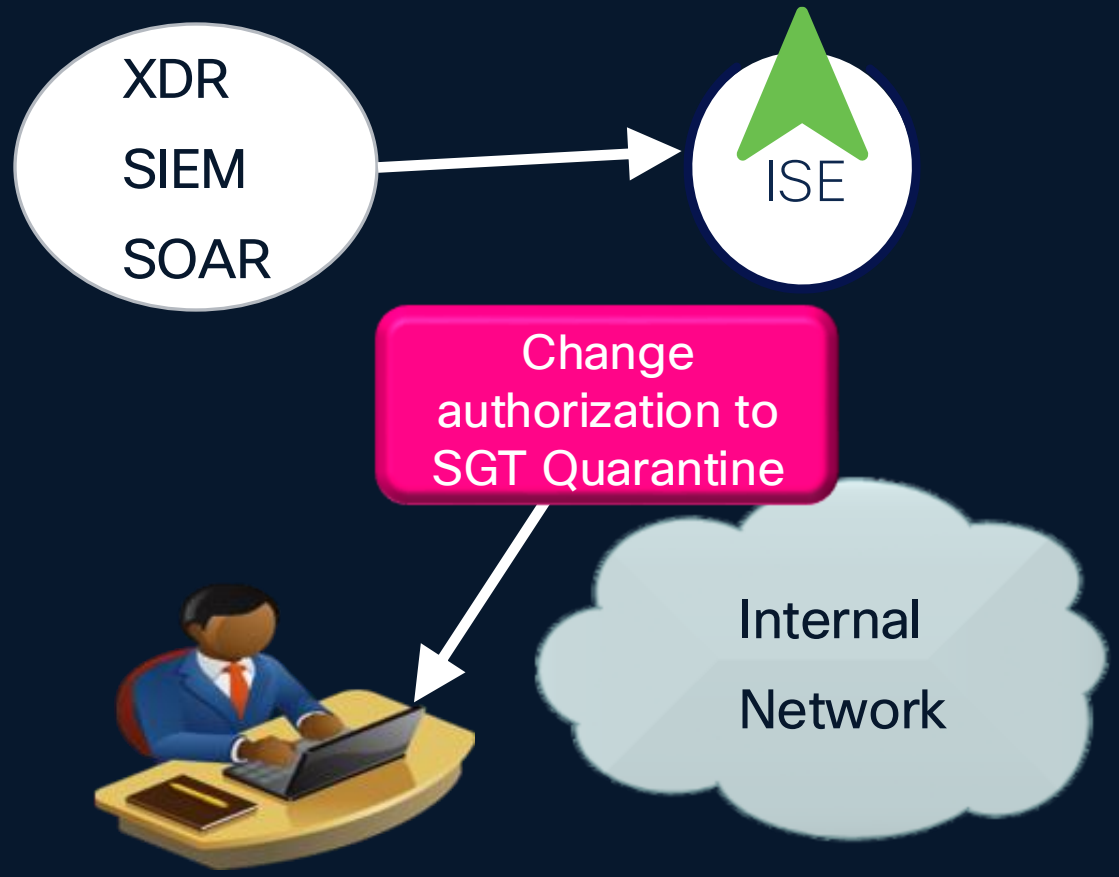
- One console https://security.cisco.com
- Multi-tenancy
- Common IDP and RBAC for all solutions
- Access to solutions via microapps or cross-launch
- Common services like Search and AI assistant across solutions
- Shared objects (like network objects) between solutions
- ISE pxGrid Cloud integration across solutions
- Identity Intelligence across solutions

The Network Meets Security

- What is on the network?
- How does it behave?
- Enforce Zero Trust
- **Observe and Remediate**

Network Remediation of Compromised Endpoints

- Change of Authorization to…
  - Network for forensics
  - Network for recovery
- Change
  - Security Group
  - VLAN
  - dACL



Call to Action

- The Network is often the only point for security enforcement
- Choice of enforcement points, price and performance
- Security Groups instead of IP addresses!
- Network Visibility to detect threats and to implement Zero Trust


CISCO