Miben több a jövő hálózata?

Berényi Áron, Ács György
Cisco Systems

2018. április 5.

Rövid Történet

1969: ARPANET is commissioned by the DoD for research into networking. The first node (a mainframe computer) is at the University of California Los Angeles (UCLA) Network Measurements Center. The next three nodes consisted of Stanford Research Institute (SRI), the University of California Santa Barbara (UCSB), and the University of Utah. The first router is an Information Message Processor (IMP), a Honeywell 516 mini-computer with 12K of memory

1971: Fifteen nodes (23 hosts) are on the ARPANET

1982: ARPA establishes TCP/IP as the protocol suite for the ARPANET. This leads to one of the first definitions of an "Internet" as a connected set of networks that use TCP/IP.

1984: The Domain Name System (DNS) is introduced with RFC 920.

1984: The number of hosts on the Internet breaks 1000.

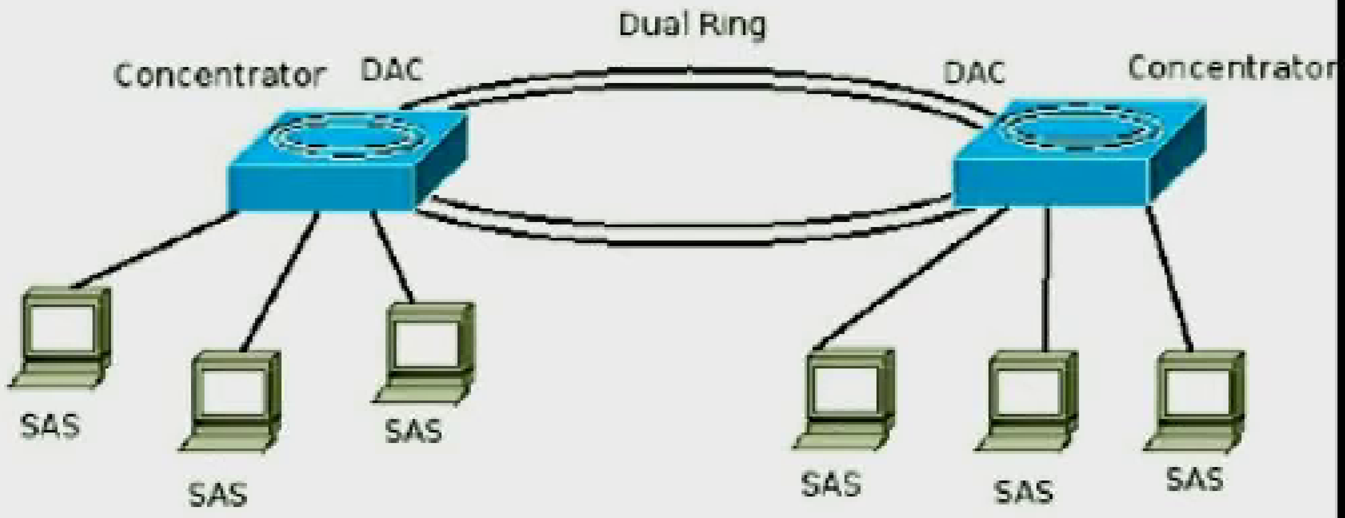
1984: Cisco Systems was founded in December 1984 by Leonard Bosack and Sandy Lerner, two Stanford University computer scientists, who pioneered the concept of a local area network (LAN) being used to connect geographically disparate computers over a multiprotocol router system.

Rövid Történet

1987: The number of hosts on the Internet breaks 10,000.
1989: *Cuckoo's Egg*, written by Clifford Stoll, tells the real-life tale of a German cracker group that infiltrated numerous U.S. facilities.
1992: The number of hosts on the Internet breaks 1,000,000.
1993: The U.S. White House comes online with www.whitehouse.gov. President Bill Clinton:president@whitehouse.gov and Vice President Al Gore:vicepresident@whitehouse.gov.
1994: Shopping on the Internet begins.
1994: Pizza from Pizza Hut can be ordered using the World Wide Web.
1997: The number of hosts on the Internet breaks 19,000,000. The Internet is a dynamic environment.
IPv4, and its 4.3 billion possible addresses, was introduced in 1983
31 January 2011: IPv4 address exhaustion, 14 September 2012 for Europe, 24 September 2015 for North America

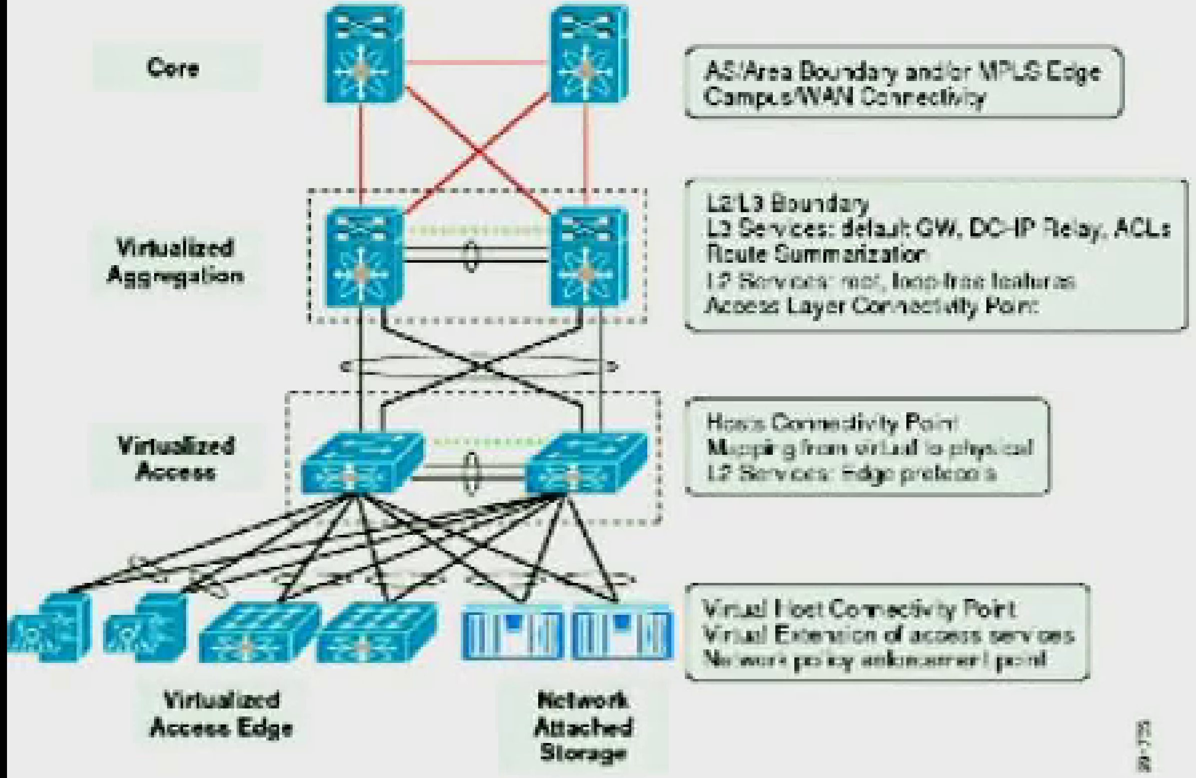
Hálózatok fejlődése

Token Ring, FDDI



Hálózatok fejlődése

3 Tier Ethernet



AS/Area Boundary and/or MPLS Edge
Campus/WAN Connectivity

L2/L3 Boundary
L3 Services: default GW, DHCP Relay, ACLs
Route Summarization
L2 Services: mct, loop-free features
Access Layer Connectivity Point

Hosts Connectivity Point
Mapping from virtual to physical
L2 Services: Edge protocols

Virtual Host Connectivity Point
Virtual Extension of access services
Network policy enforcement point

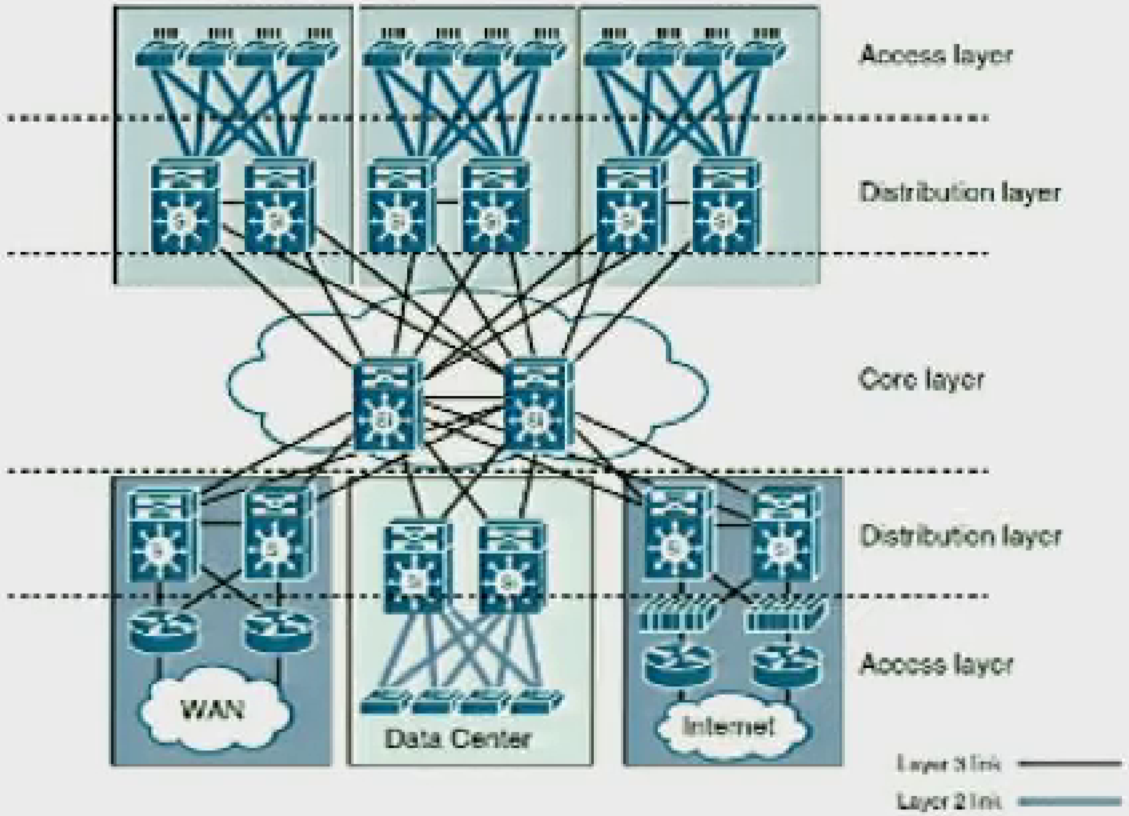


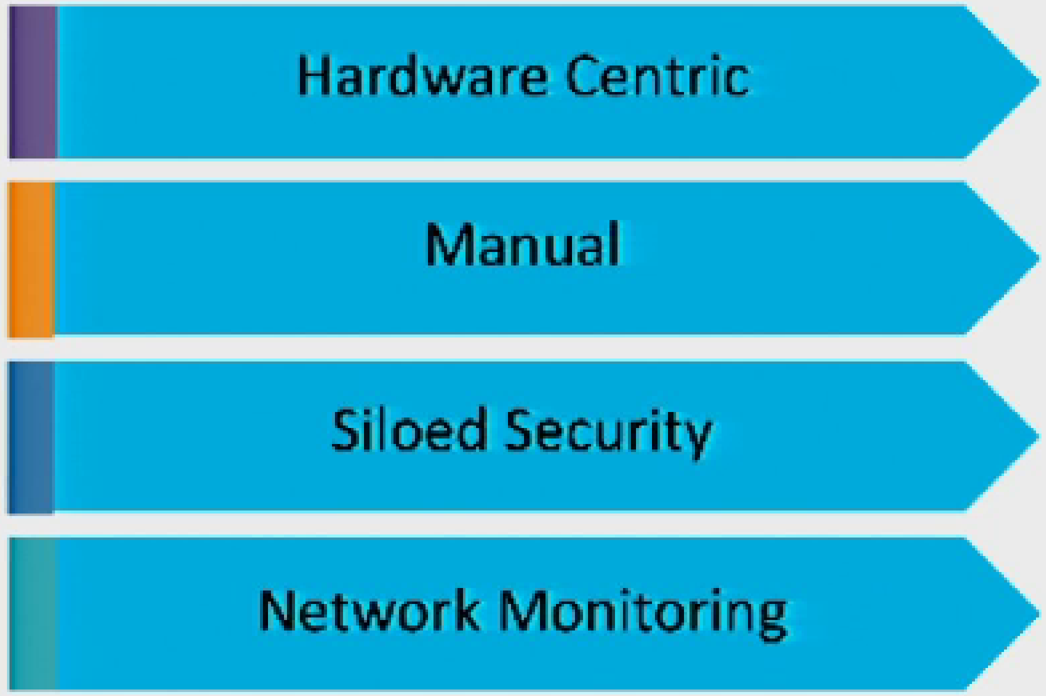
Figure 3-3 *Typical Modular Enterprise Campus Architecture*

Cisco újragondolja a hálózatokat (ismét ☺)

Traditional Network

You Need a Network that Drives your Digital Business

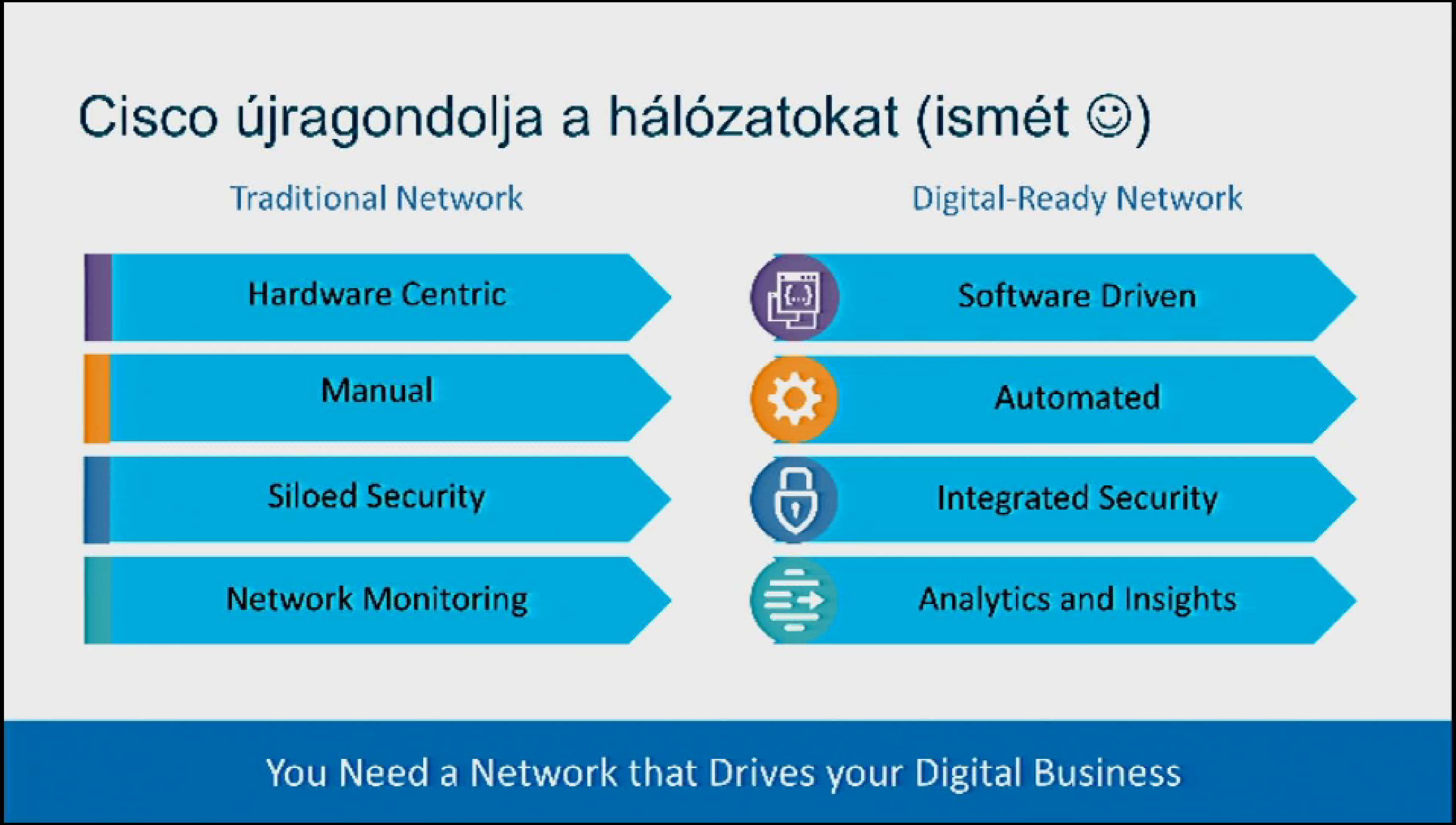
Cisco újragondolja a hálózatokat (ismét ☺)



Traditional Network

- Hardware Centric
- Manual
- Siloed Security
- Network Monitoring

You Need a Network that Drives your Digital Business



Cisco újragondolja a hálózatokat (ismét ☺)

Traditional Network	Digital-Ready Network
Hardware Centric	Software Driven
Manual	Automated
Siloed Security	Integrated Security
Network Monitoring	Analytics and Insights

You Need a Network that Drives your Digital Business

Az következő generációs hálózat

The New Network

Constantly Learning

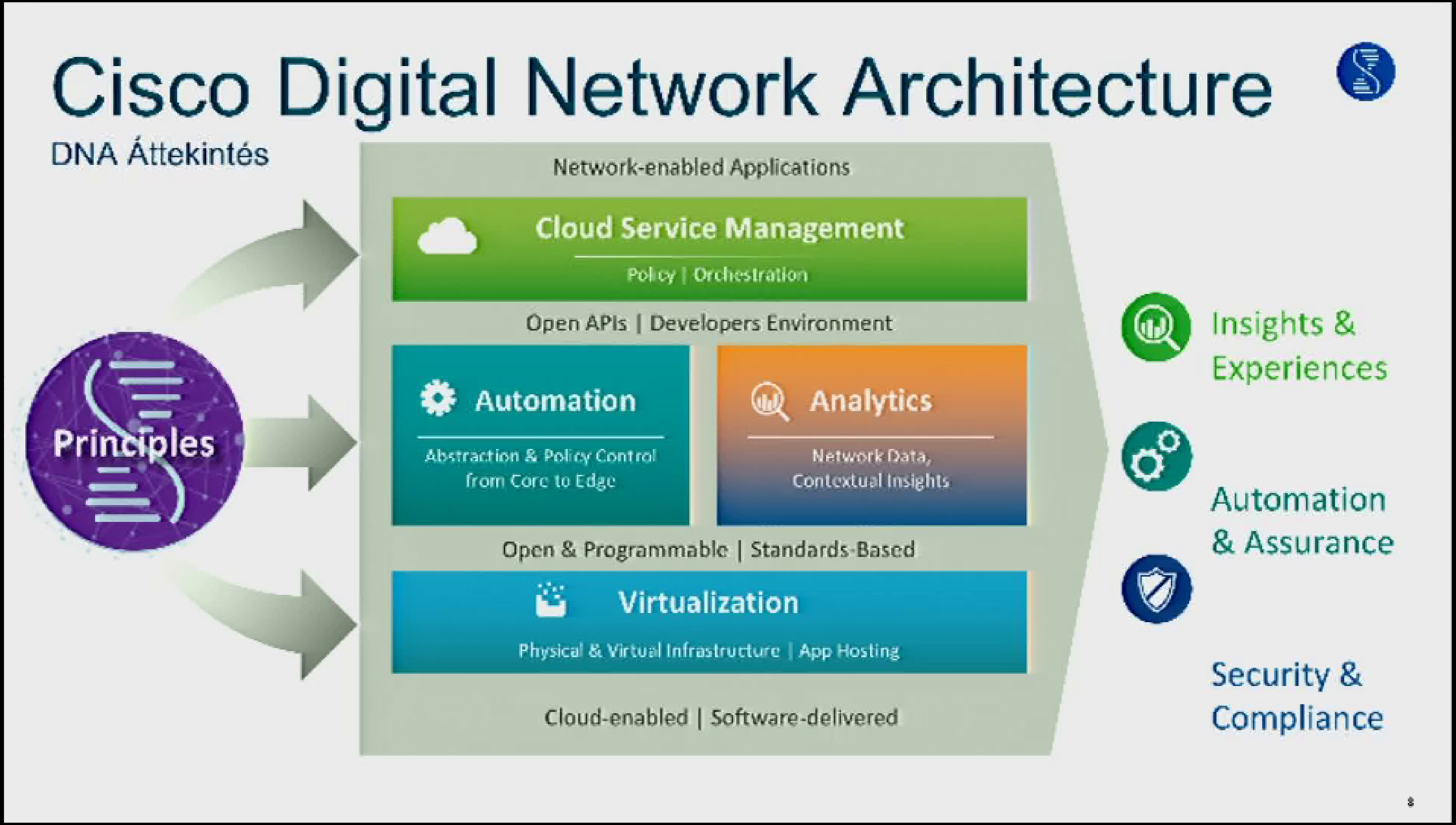
Support 100X new devices, apps, users

Constantly Adapting

Respond Instantly to business demands with limited staff and budget

Constantly Protecting

See and predict issues and threats and respond fast



Cisco Digital Network Architecture

DNA Áttekintés

Principles

Network-enabled Applications

Cloud Service Management

Policy | Orchestration

Open APIs | Developers Environment

Automation

Abstraction & Policy Control from Core to Edge

Analytics

Network Data, Contextual Insights

Open & Programmable | Standards-Based

Virtualization

Physical & Virtual Infrastructure | App Hosting

Cloud-enabled | Software-delivered

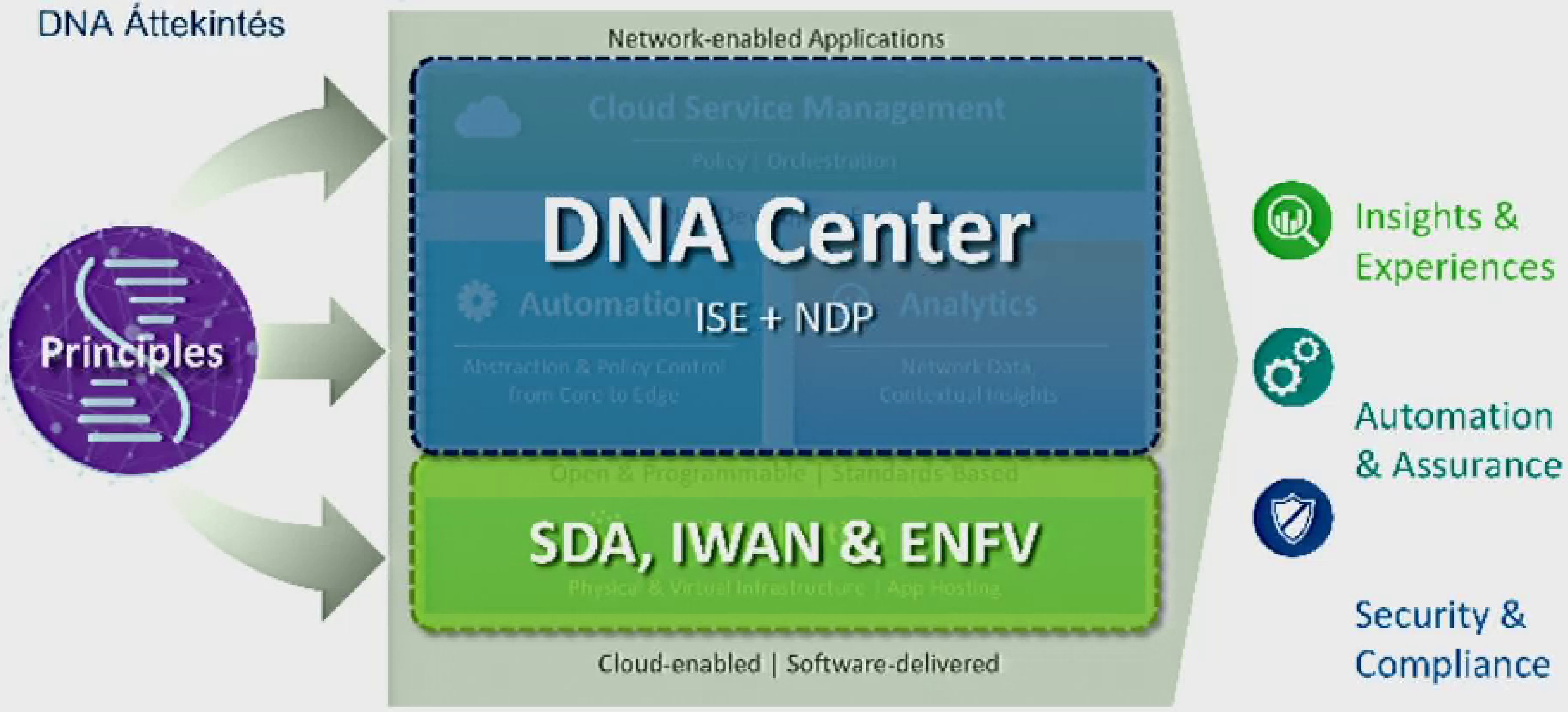
Insights & Experiences

Automation & Assurance

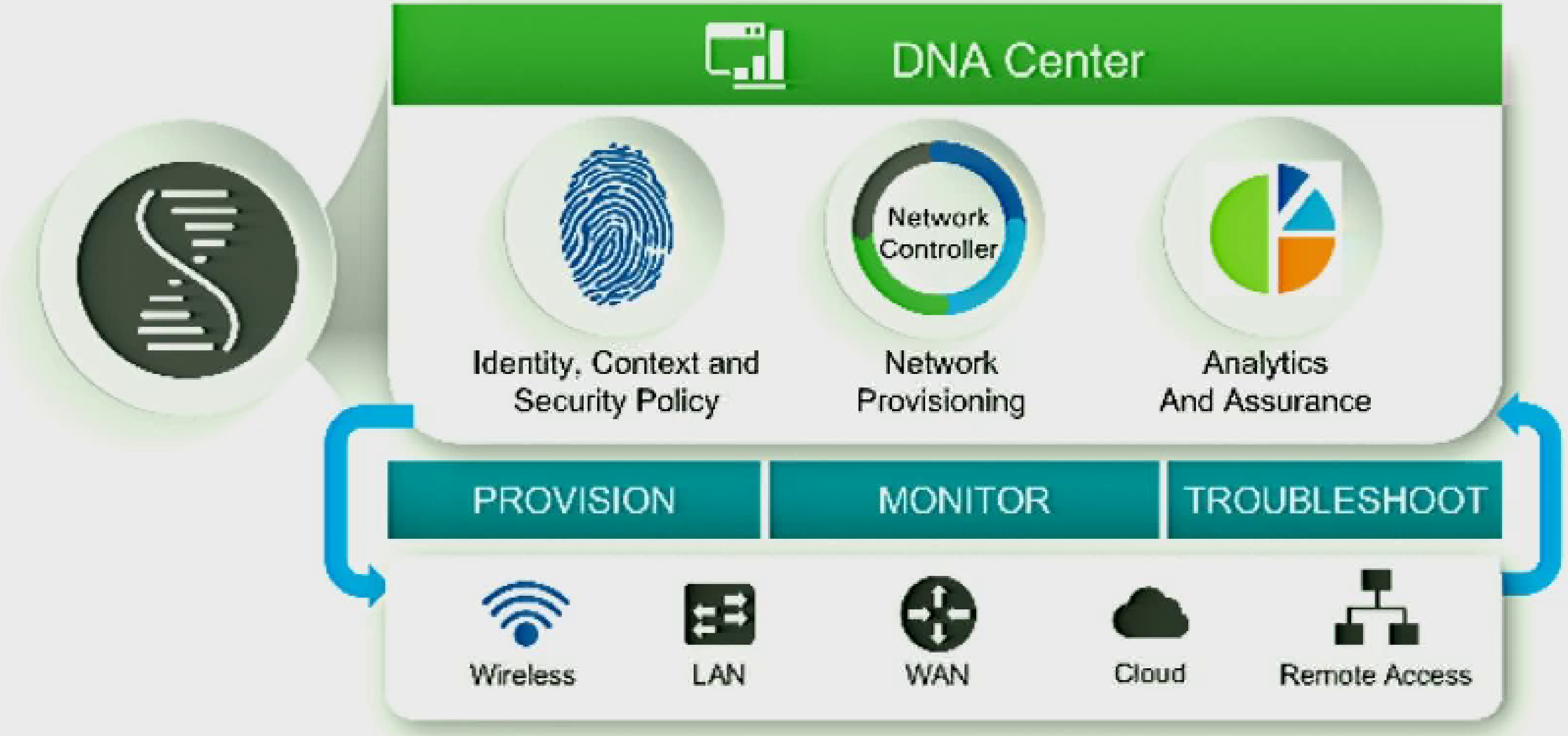
Security & Compliance

Cisco Digital Network Architecture

DNA Áttekintés


Principles
Network-enabled Applications
Cloud Service Management
Policy | Orchestration
DNA Center
Automation
ISE + NDP
Analytics
Abstraction & Policy Control from Core to Edge
Network Data, Contextual Insights
Open & Programmable | Standards-Based
SDA, IWAN & ENFV
Physical & Virtual Infrastructure | App Hosting
Cloud-enabled | Software-delivered
Insights & Experiences
Automation & Assurance
Security & Compliance

Cisco DNA Center



DNA Center

Network Controller

Identity, Context and Security Policy

Network Provisioning

Analytics And Assurance

PROVISION

MONITOR

TROUBLESHOOT

Wireless

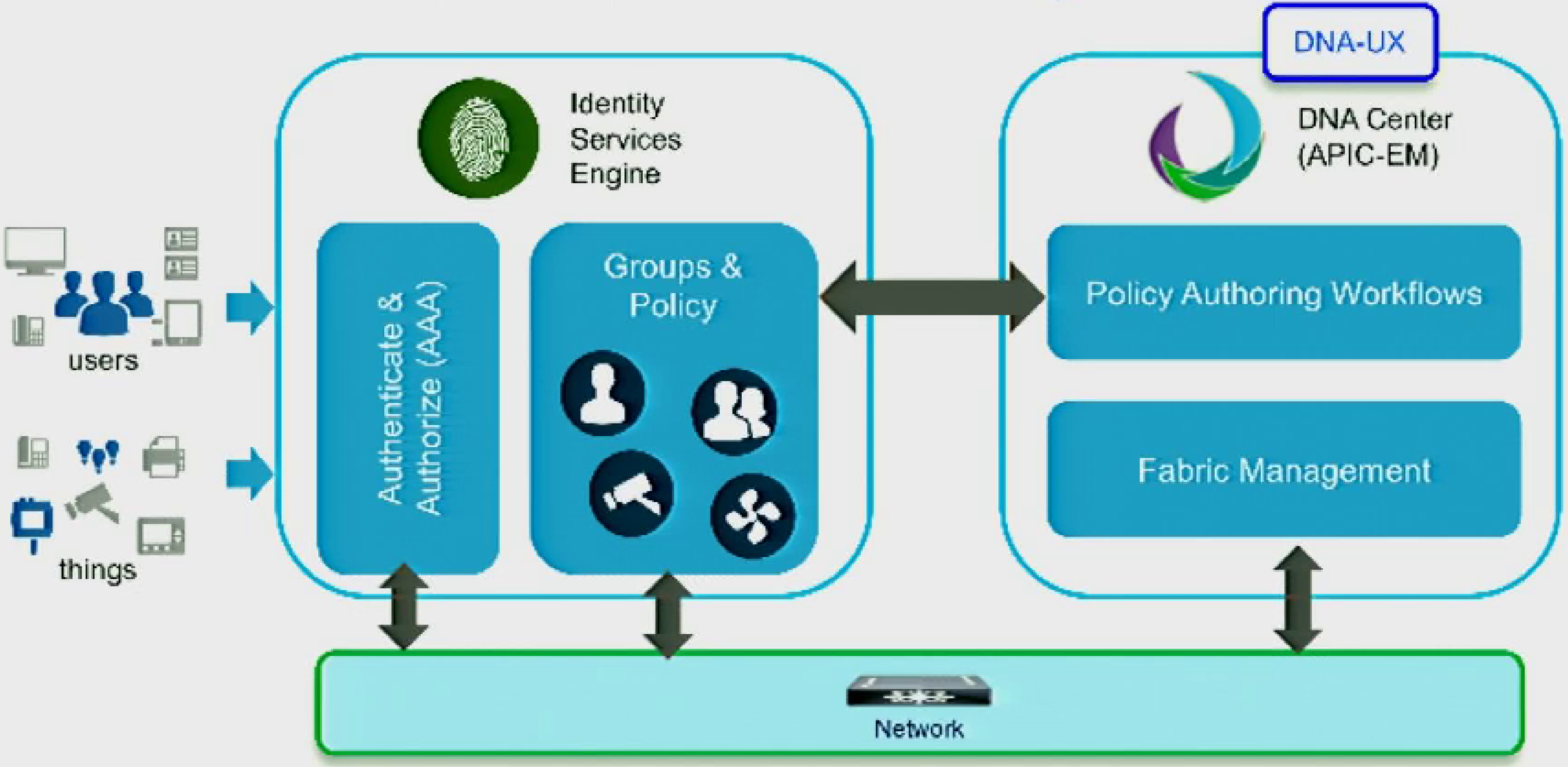
LAN

WAN

Cloud

Remote Access

ISE DNA Center integráció



DNA-UX

Identity Services Engine

Authenticate & Authorize (AAA)

Groups & Policy

DNA Center (APIC-EM)

Policy Authoring Workflows

Fabric Management

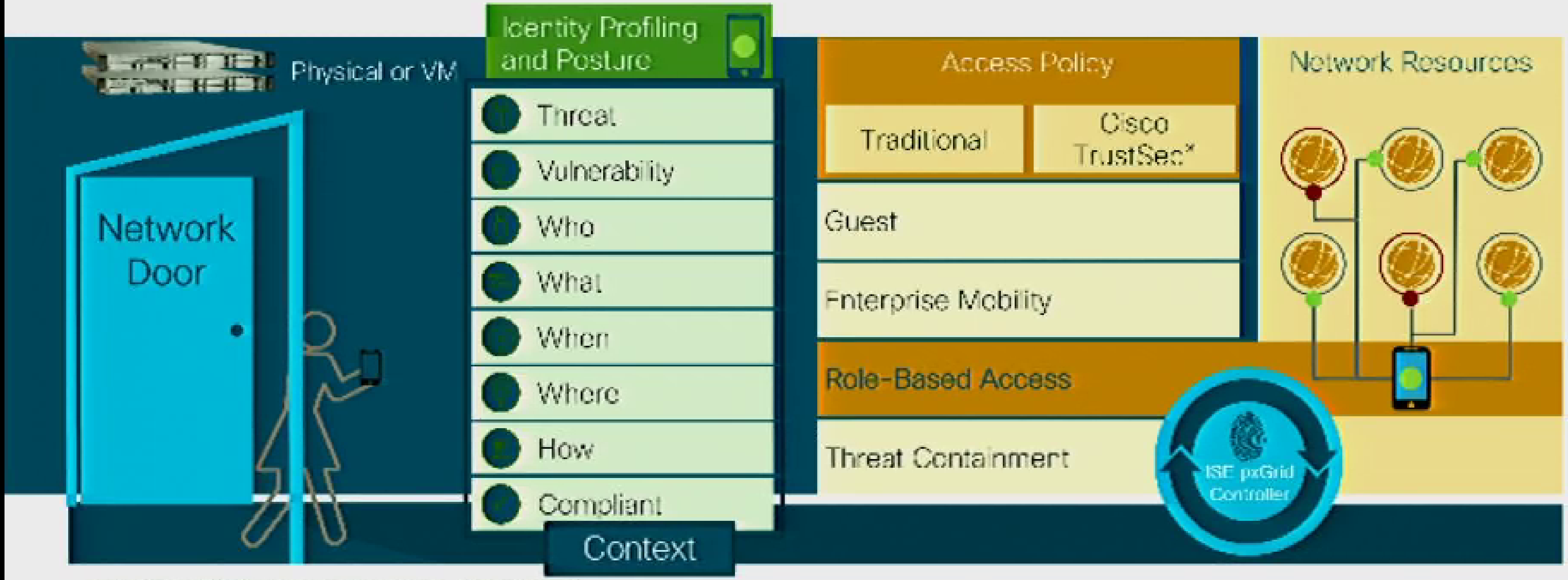
users

things

Network

Kontext és az Identity Services Engine (ISE)

A centralized security solution that automates context-aware access to network resources and shares contextual data



Physical or VM

Network Door

Identity Profiling and Posture

Threat

Vulnerability

Who

What

When

Where

How

Compliant

Context

Access Policy

Traditional

Cisco TrustSec*

Guest

Enterprise Mobility

Role-Based Access

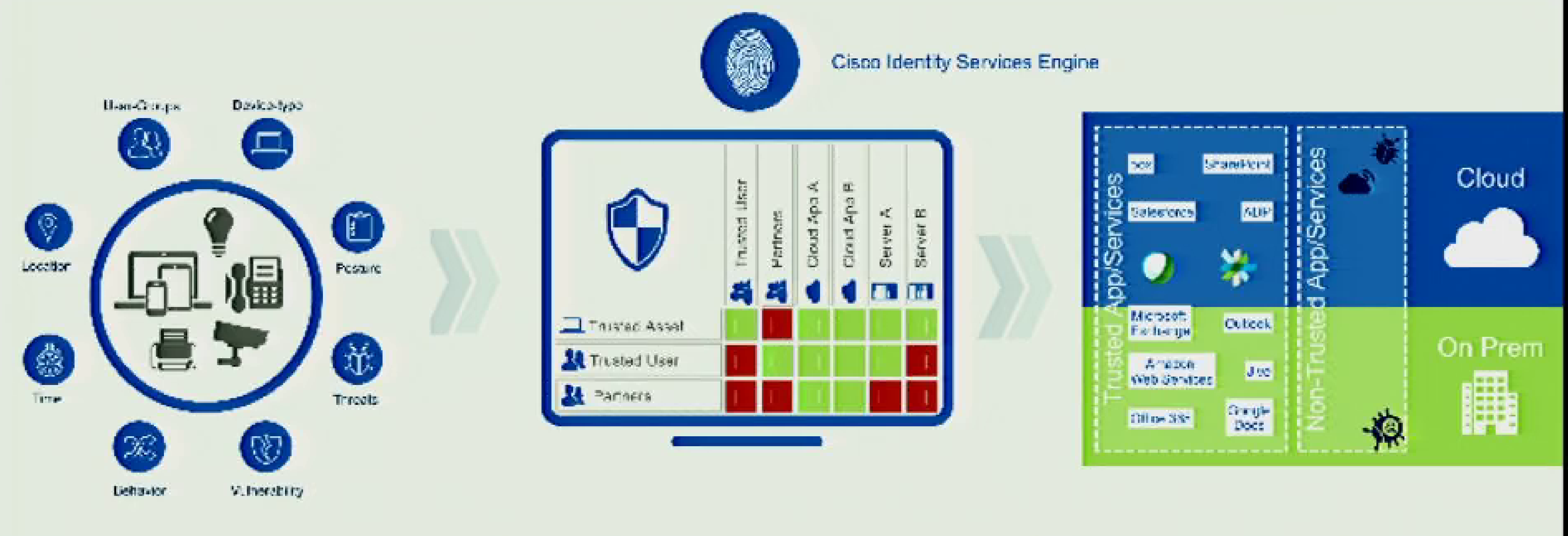
Threat Containment

Network Resources

ISE pxGrid Controller

Managing Policy Based on ‘Trust’

Connecting Trusted Users and Devices to Trusted Services



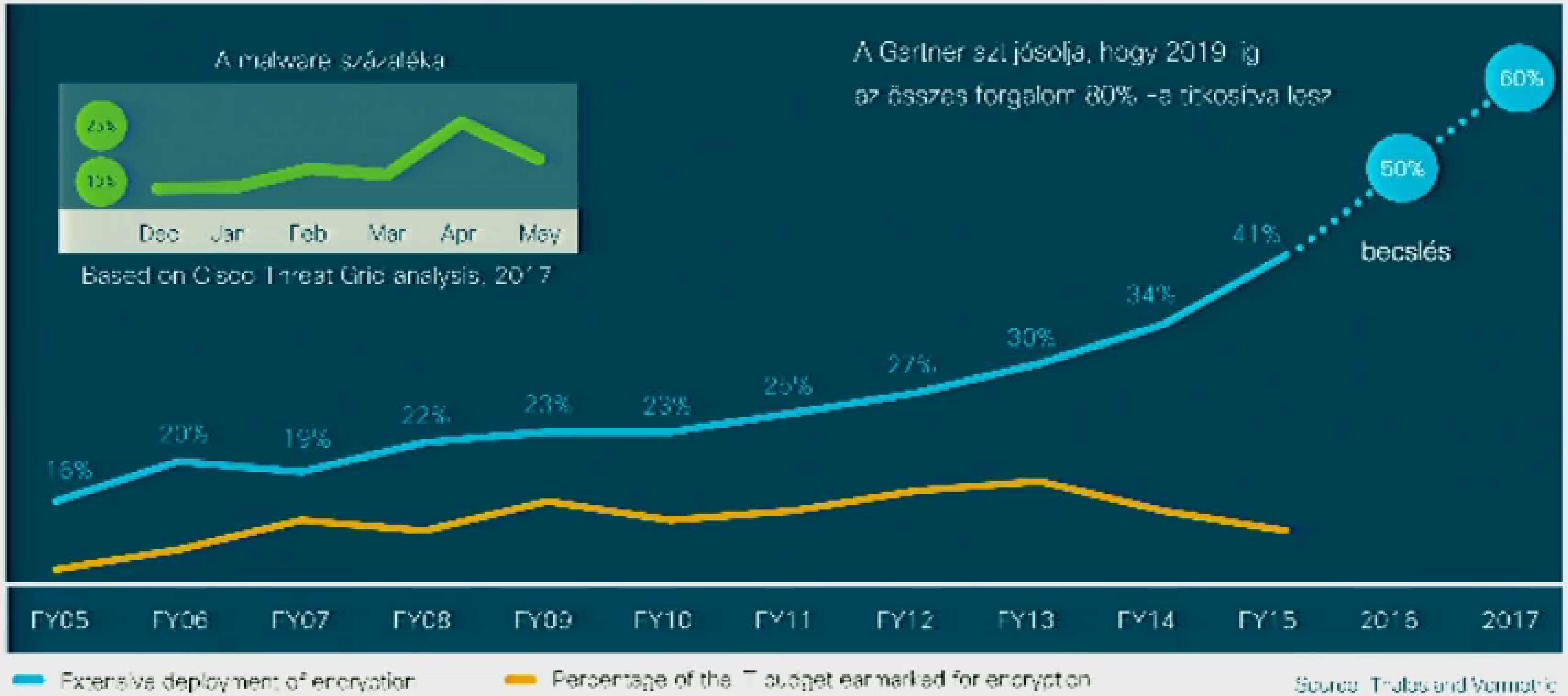
	Trusted User	Partners	Cloud App A	Cloud App B	Server A	Server B
Trusted Asset	🟩	🟥	🟩	🟩	🟩	🟩
Trusted User	🟥	🟩	🟩	🟩	🟩	🟥
Partners	🟥	🟥	🟩	🟩	🟥	🟥

Improved Visibility and Decision

Software-Defined Segmentation, Service Access and Entitlement

Location-Free App/Service Access

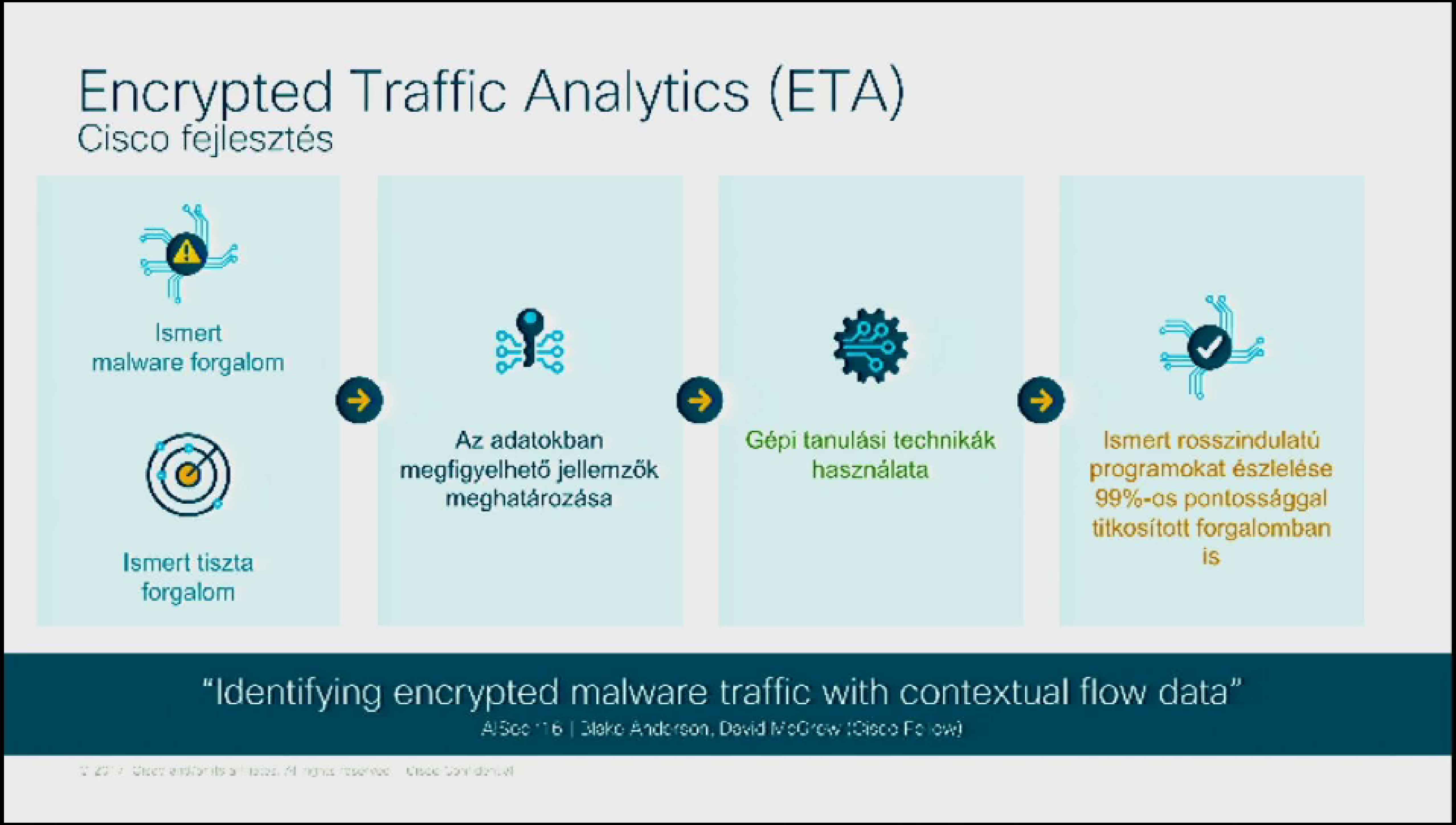
A titkosítás megváltoztatja a fenyegetési megközelítést



Based on Cisco Threat Grid analysis, 2017

A Gartner azt jósolja, hogy 2019-ig az összes forgalom 80%-a titkosítva lesz

Source: Thales and Vormetric



Encrypted Traffic Analytics (ETA)

Cisco fejlesztés

Ismert malware forgalom

Ismert tiszta forgalom

→

Az adatokban megfigyelhető jellemzők meghatározása

→

Gépi tanulási technikák használata

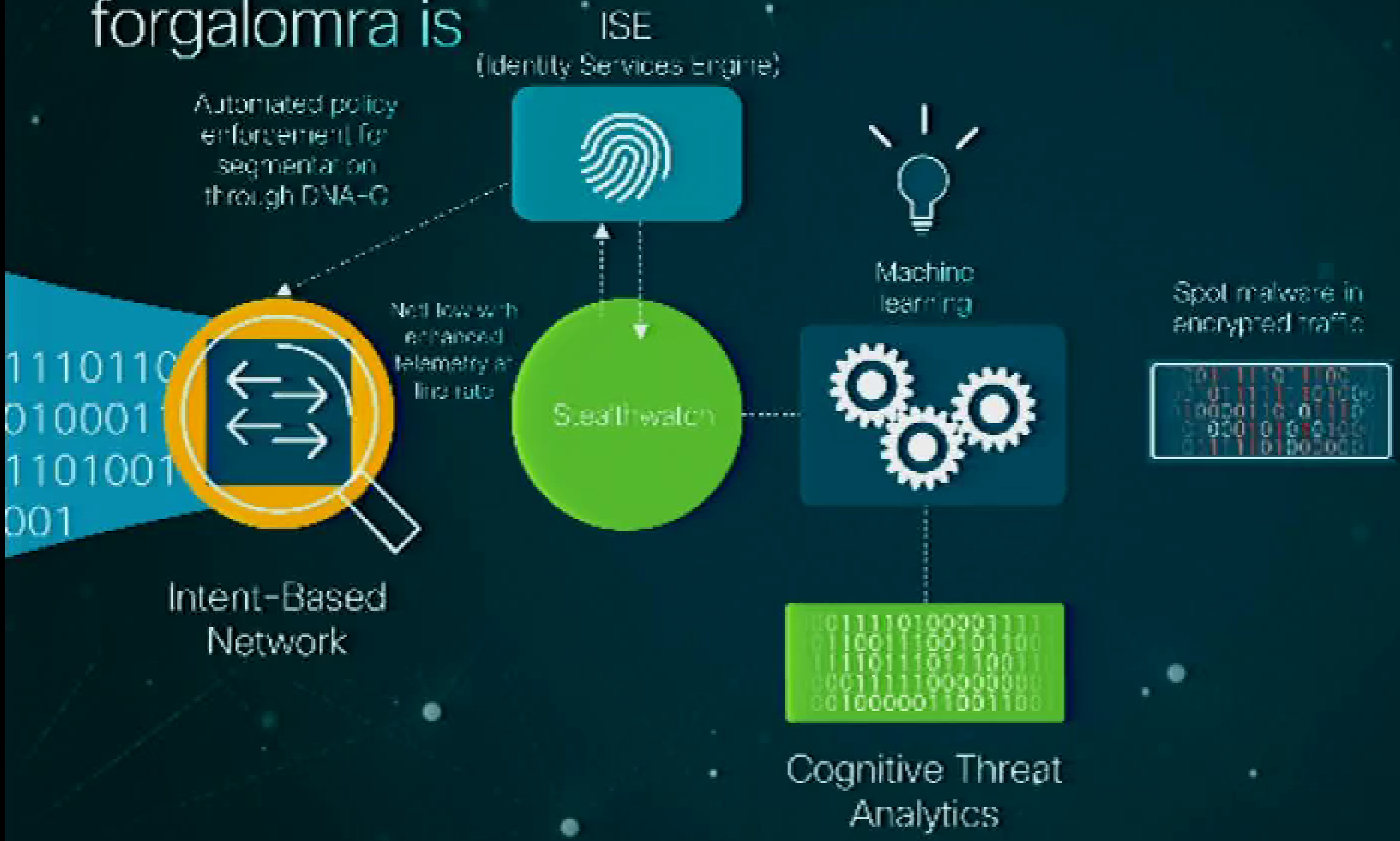
→

Ismert rosszindulatú programokat észlelése 99%-os pontossággal titkosított forgalomban is

"Identifying encrypted malware traffic with contextual flow data"

AISec '16 | Blake Anderson, David McGrew (Cisco Fellow)

Lássuk és cselekedjünk veszély esetén – most a titkosított forgalomra is


ISE
(Identity Services Engine)
Automated policy enforcement for segmentation through DNA-C
NetFlow with enhanced telemetry at line rate
Stealthwatch
Machine learning
Spot malware in encrypted traffic
Intent-Based Network
Cognitive Threat Analytics

99.9%
Threat Detection Accuracy*

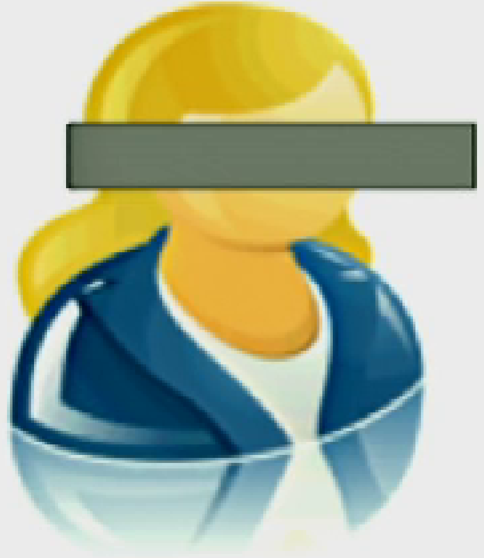
0.01%
False Positives*

*Source: Identifying Encrypted Malware Traffic with Contextual Flow Data, Oct 2016

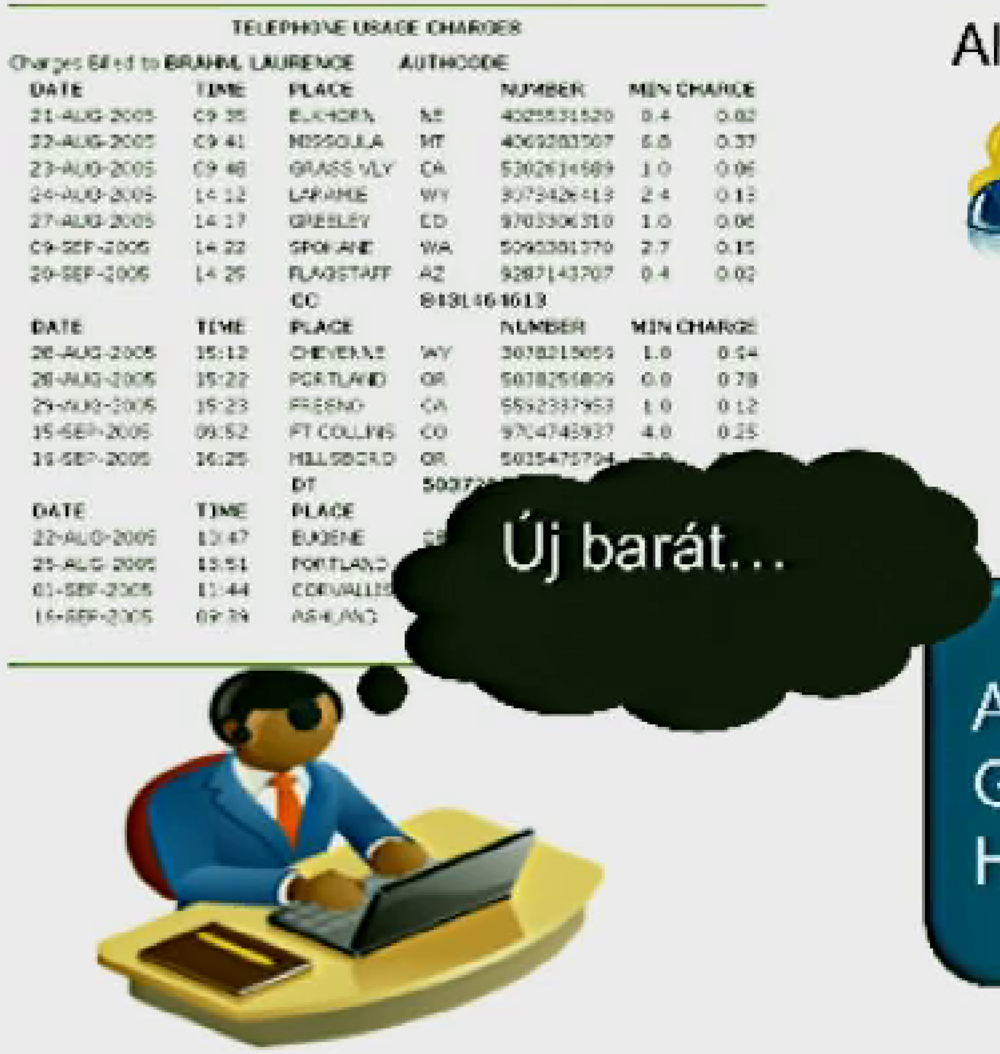
Ahol a ”Telemetria” segíthet…

A barátom: David

Alice,
David tini lánya



Analógia a telefon számlával



TELEPHONE USAGE CHARGES

Charges Billed to BRAHM, LAURENCE AUTHCODE

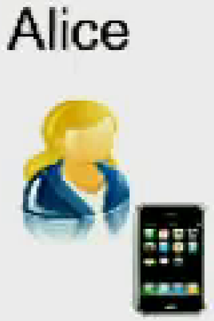
DATE	TIME	PLACE		NUMBER	MIN	CHARGE
21-AUG-2005	09:35	ELKHORN	NE	4025531520	0.4	0.02
22-AUG-2005	09:41	MISSOULA	MT	4069283507	6.8	0.37
23-AUG-2005	09:48	GRASS VLY	CA	5302614589	1.0	0.06
24-AUG-2005	14:12	LARAMIE	WY	3079426413	2.4	0.13
27-AUG-2005	14:17	GREELEY	CO	9703306310	1.0	0.06
09-SEP-2005	14:22	SPOKANE	WA	5096381370	2.7	0.15
20-SEP-2005	14:25	FLAGSTAFF	AZ	9287143707	0.4	0.02

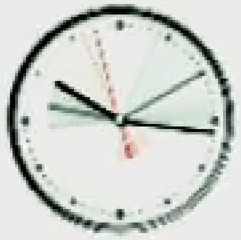
CC 8131464613

DATE	TIME	PLACE		NUMBER	MIN	CHARGE
26-AUG-2005	15:12	CHEYENNE	WY	3078215055	1.0	0.04
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
16-SEP-2005	16:25	HILLSBORO	OR	5035479794	[illegible]	[illegible]

DT 5037[illegible]

DATE	TIME	PLACE		NUMBER	MIN	CHARGE
22-AUG-2005	13:47	EUGENE	[illegible]	[illegible]	[illegible]	[illegible]
25-AUG-2005	13:51	PORTLAND	[illegible]	[illegible]	[illegible]	[illegible]
01-SEP-2005	11:44	CORVALLIS	[illegible]	[illegible]	[illegible]	[illegible]
16-SEP-2005	09:39	ASHLAND	[illegible]	[illegible]	[illegible]	[illegible]



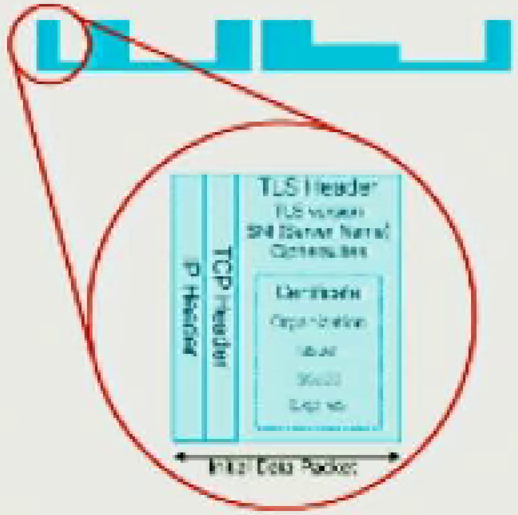


Alice hívásokat fogad és kezdeményez “B” felé
Gyakran, különböző időpontokban
Hosszú idejű hívások, 30 – 90 perc

Hogyan ellenőrizhetjük a titkosított forgalmat?

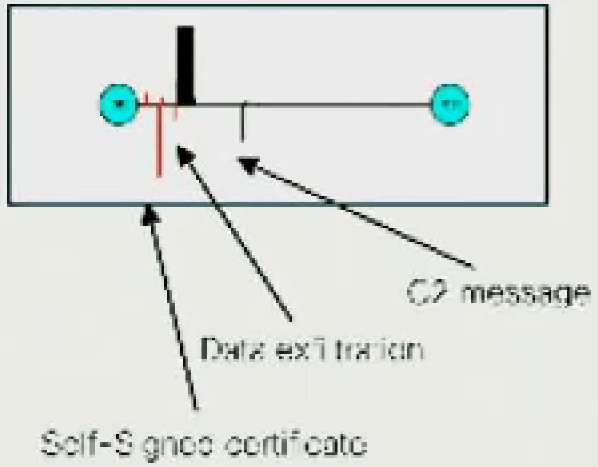
Initial Data Packet

Make the most of the unencrypted fields



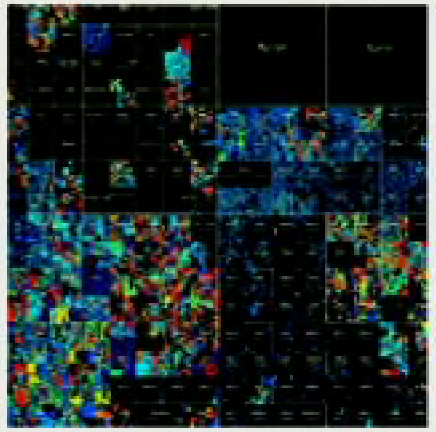
Sequence of Packet Lengths and Times

Identify the content type through the size and timing of packets



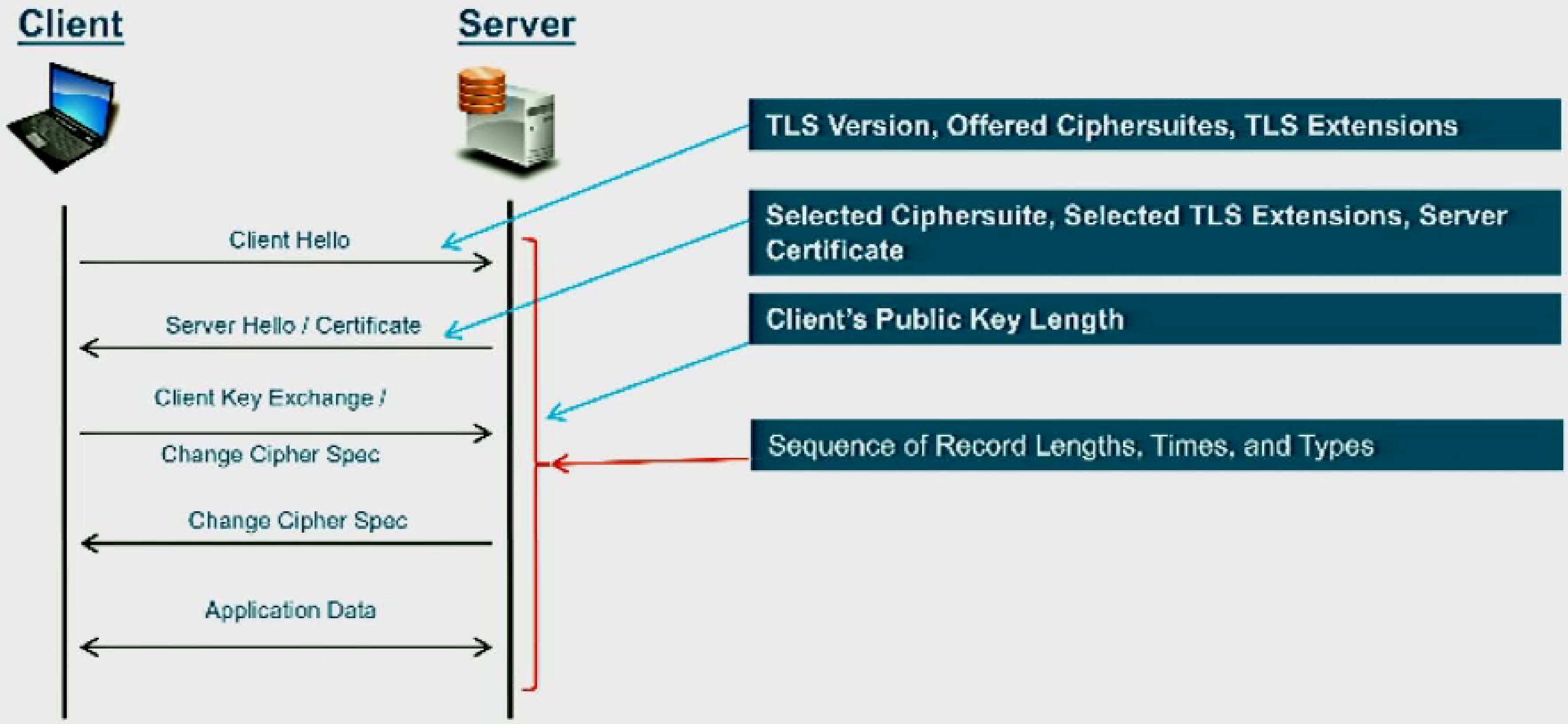
Threat Intelligence Map

Who's who of the Internet's dark side



Broad behavioral information about the servers on the Internet.

Initial Data Packet, IDP



Client

Server

Client Hello

Server Hello / Certificate

Client Key Exchange /

Change Cipher Spec

Change Cipher Spec

Application Data

TLS Version, Offered Ciphersuites, TLS Extensions

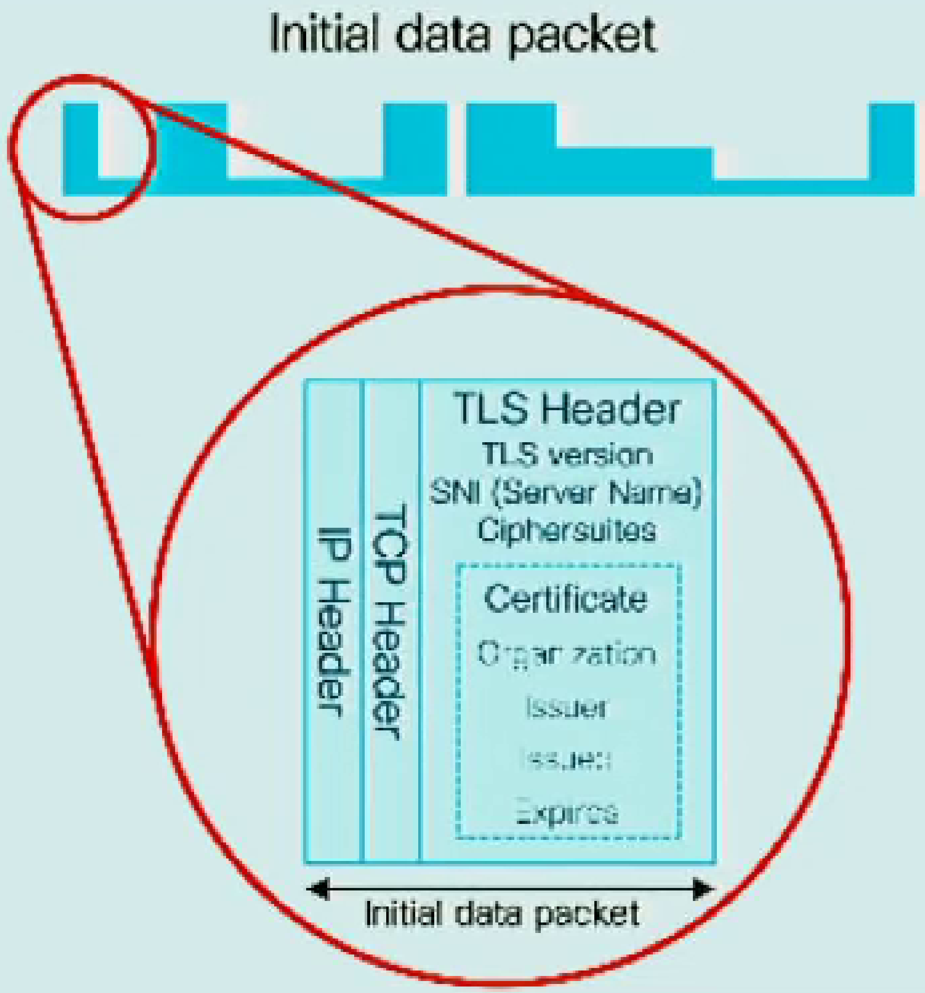
Selected Ciphersuite, Selected TLS Extensions, Server Certificate

Client's Public Key Length

Sequence of Record Lengths, Times, and Types

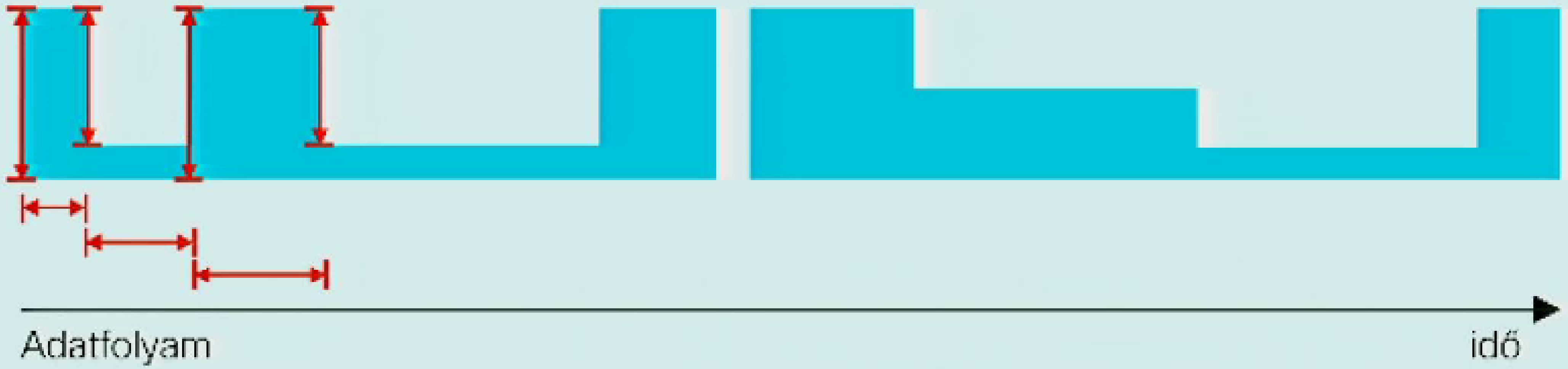
Initial Data Packet

- A HTTPS fejléc számos "információ-gazdag" mezőt tartalmaz
- A kiszolgáló neve domain információkat nyújt
- A kriptográfiai információk a kliens és a szerver viselkedését és az alkalmazások azonosságát jellemzik.
- A tanúsítványinformációk hasonlóak, mint a "whois" a domainre
- Sokkal többet lehet érteni, amikor az információkat összevonjuk a globális adatokkal



Sequence of packet lengths and times

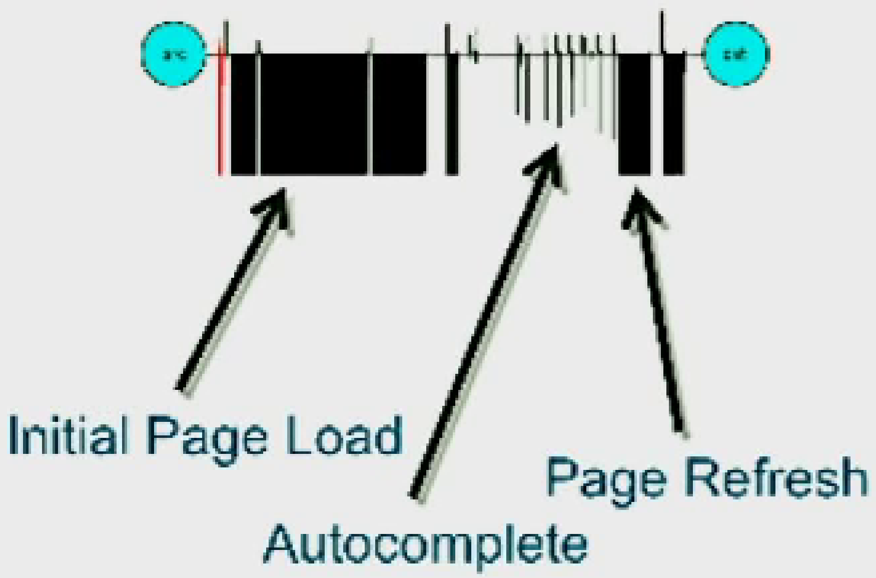
Sequence of packet lengths and times



- A csomagok mérete és időzítése lehetővé teszi számunkra, hogy megbecsüljük az adatok típusát a titkosított csatornán belül.
- Megkülönböztethetjük a video-, web-, API-hívásokat, hangokat és más adattípusokat egymástól, és jellemezhetjük az osztályon belüli forrást.

Forgalmi viszonyok

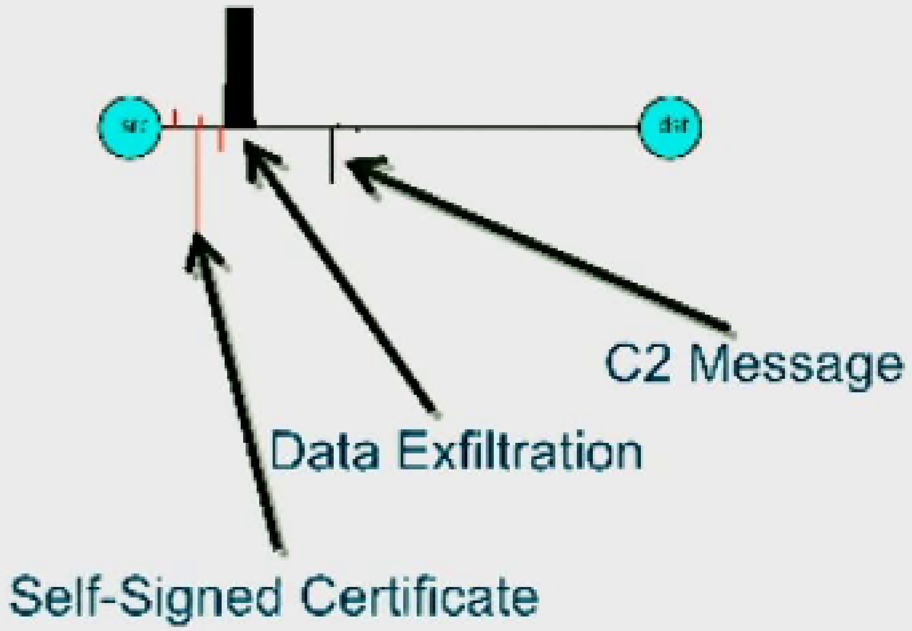
Google Search



Initial Page Load

Autocomplete

Page Refresh

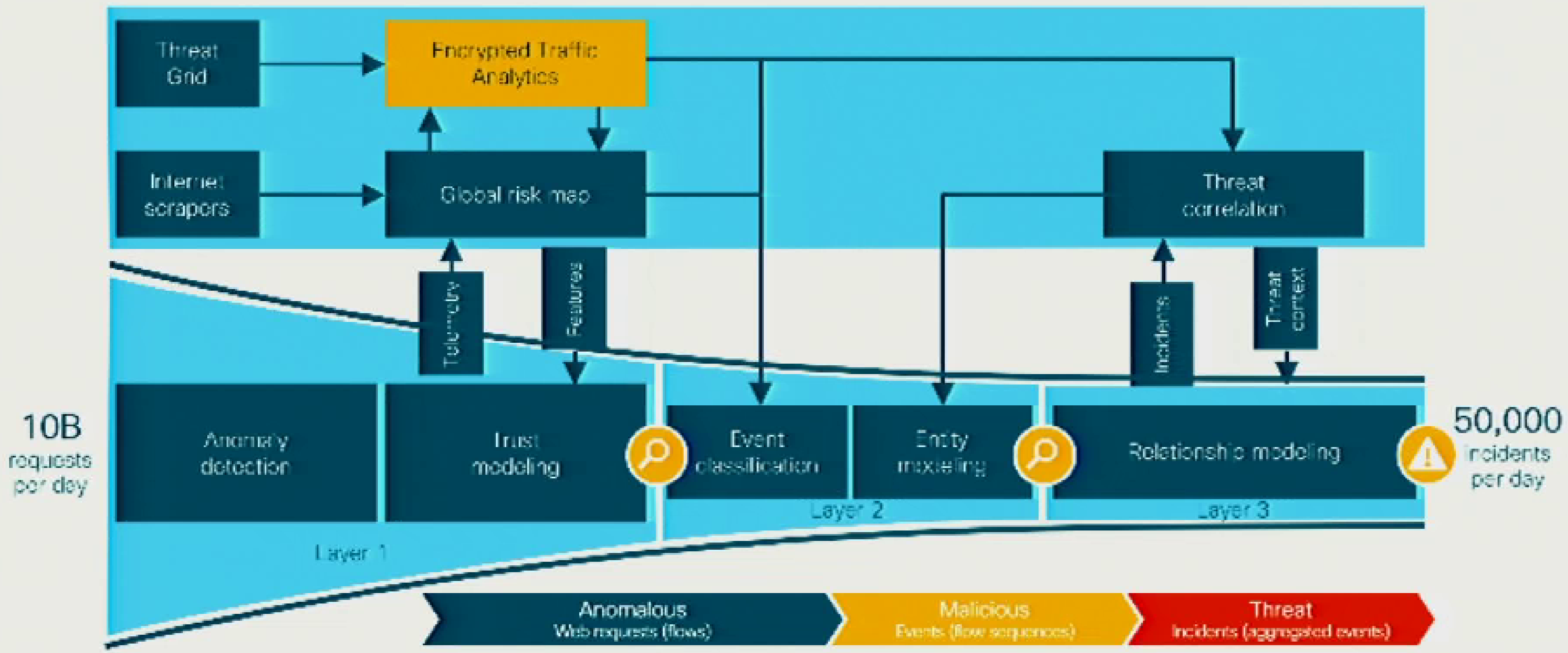


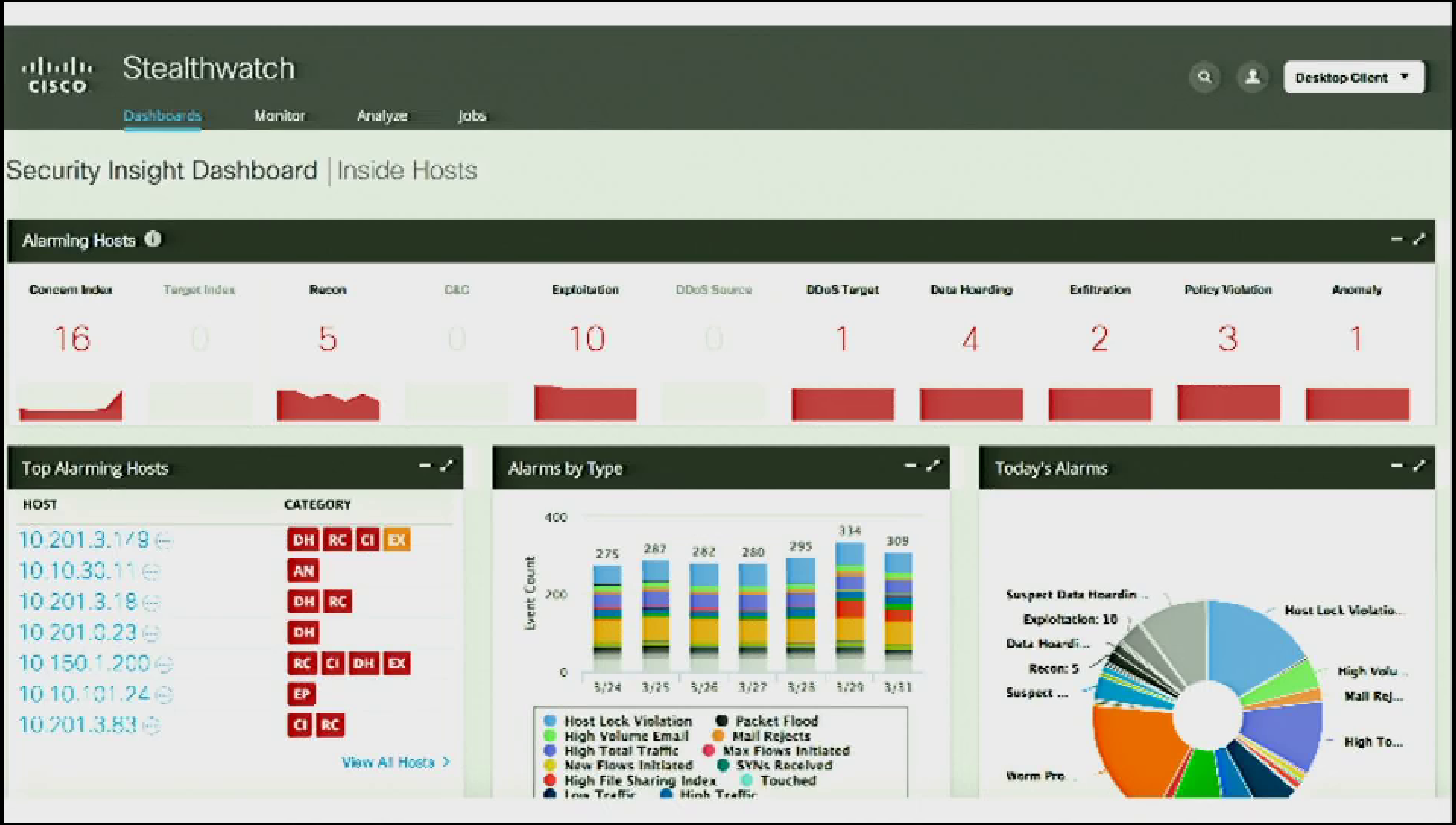
C2 Message

Data Exfiltration

Self-Signed Certificate

Kognitív analitikai többrétegű gépi tanulás





Security Insight Dashboard | Inside Hosts

Alarming Hosts

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
16	0	5	0	10	0	1	4	2	3	1

Top Alarming Hosts

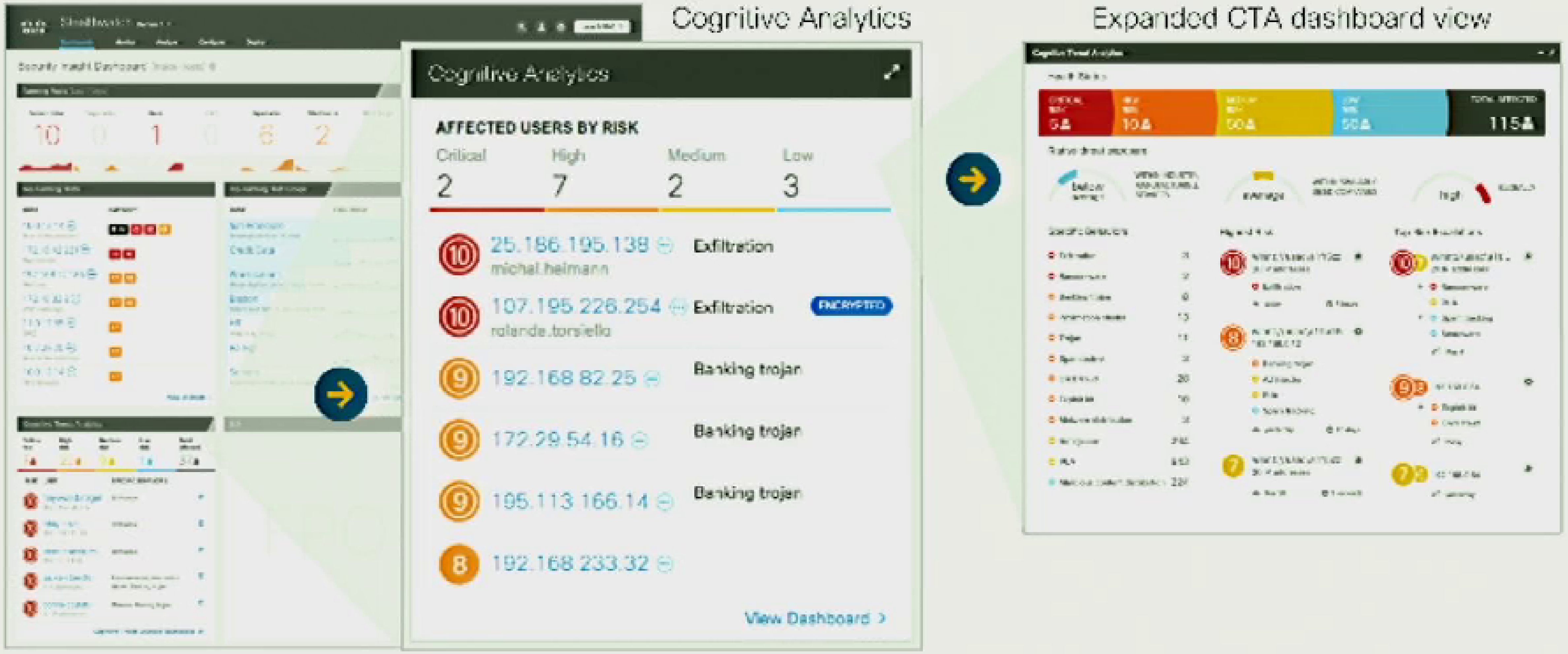
HOST	CATEGORY
10.201.3.179	DH RC CI EX
10.10.30.11	AN
10.201.3.18	DH RC
10.201.0.23	DH
10.150.1.200	RC CI DH EX
10.10.101.24	EP
10.201.3.83	CI RC

View All Hosts >

Alarms by Type

Today's Alarms

Titkosított kártevők észlelése



Cognitive Analytics

Expanded CTA dashboard view

Cognitive Analytics

AFFECTED USERS BY RISK

Critical	High	Medium	Low
2	7	2	3

10 25.186.195.138 michal.heimann Exfiltration

10 107.195.226.254 rolande.torsiello Exfiltration ENCRYPTED

9 192.168.82.25 Banking trojan

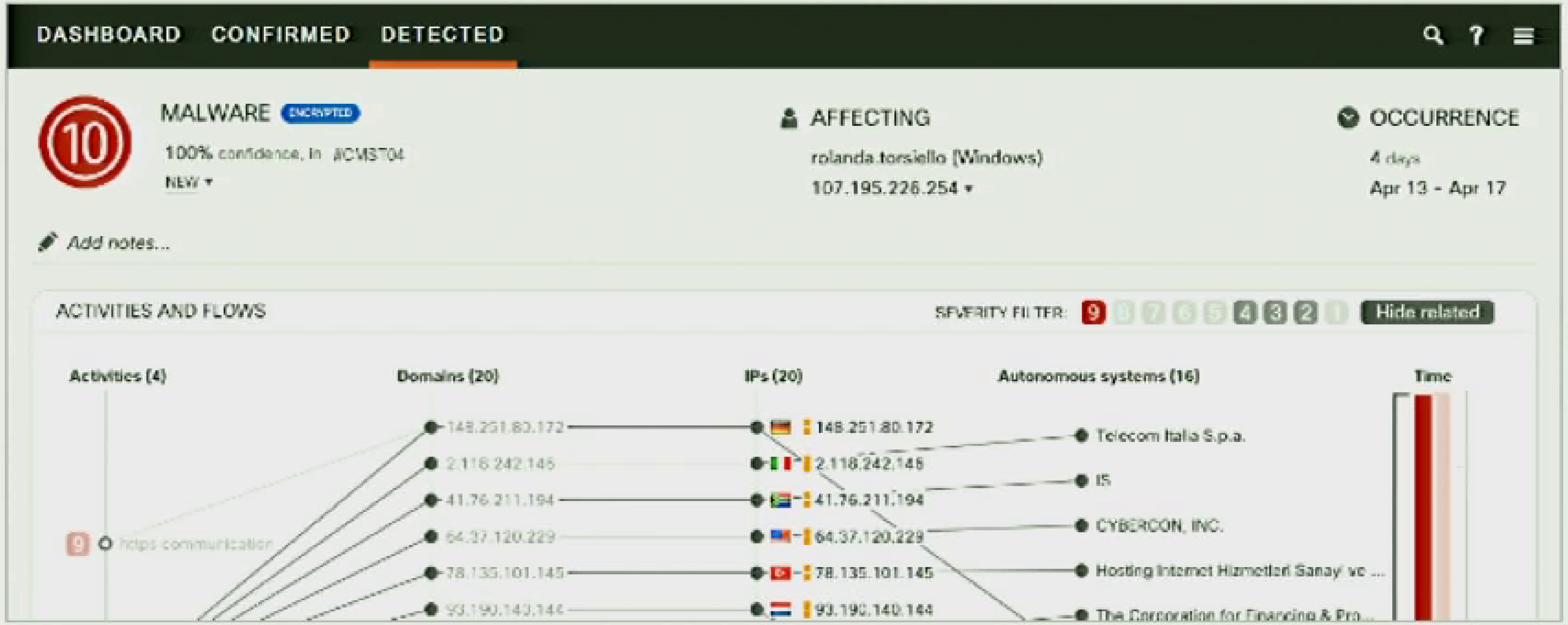
9 172.29.54.16 Banking trojan

9 195.113.166.14 Banking trojan

8 192.168.233.32

View Dashboard >

Titkosított rosszindulatú program észlelése: példa esemény



MALWARE

100% confidence, in #CMST04

NEW ▾

AFFECTING

rolanda.torsiello (Windows)

107.195.226.254 ▾

OCCURRENCE

4 days

Apr 13 - Apr 17

ACTIVITIES AND FLOWS

Activities (4)	Domains (20)	IPs (20)	Autonomous systems (16)	Time
	148.251.80.172	148.251.80.172	Telecom Italia S.p.a.	
	2.118.242.145	2.118.242.145	IS	
	41.76.211.194	41.76.211.194	CYBERCON, INC.	
9 https communication	64.37.120.229	64.37.120.229	Hosting Internet Hizmetleri Sanayi ve ...	
	78.135.101.145	78.135.101.145	The Corporation for Financing & Pro...	
	93.190.140.144	93.190.140.144		

Köszönjük!