Interní bezpečnost IT systémů podle DORA: Minimalizace rizik spojených s lidským faktorem

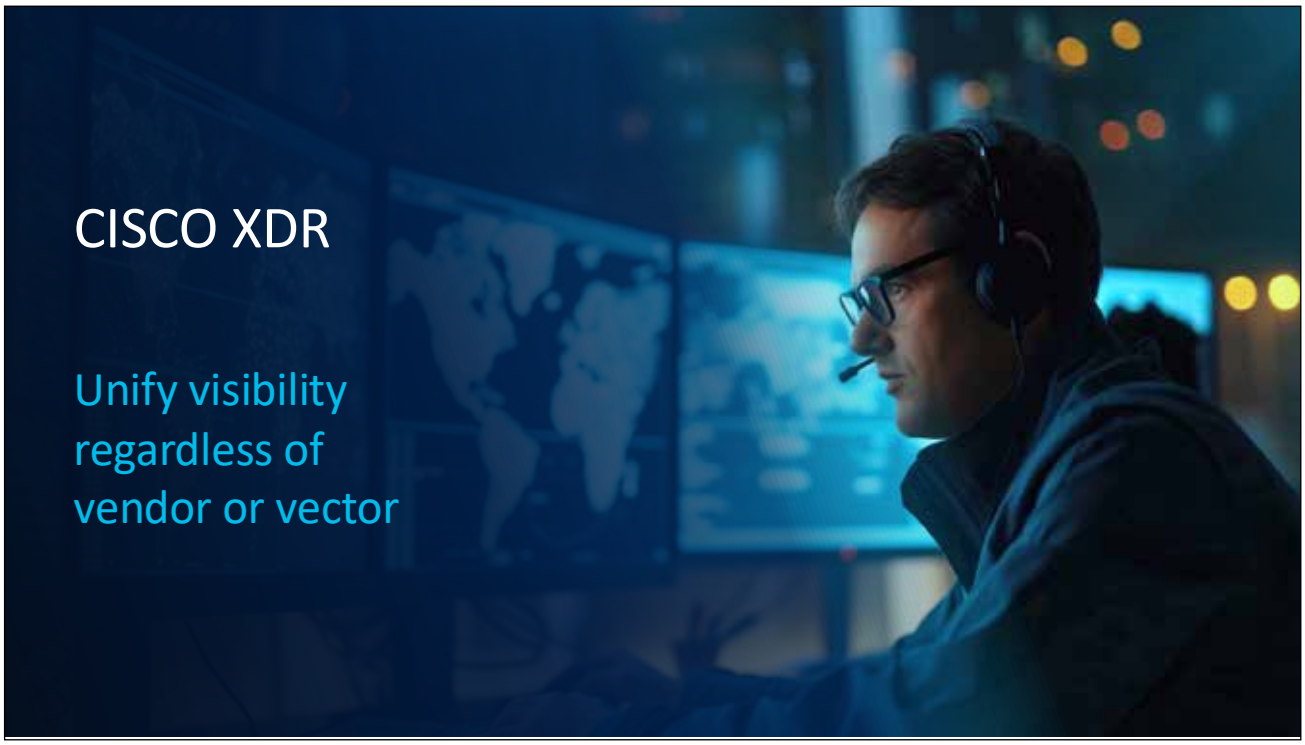
14.10.2025

Milan Habrcetl, Account Executive Security
mhabrcet@cisco.com

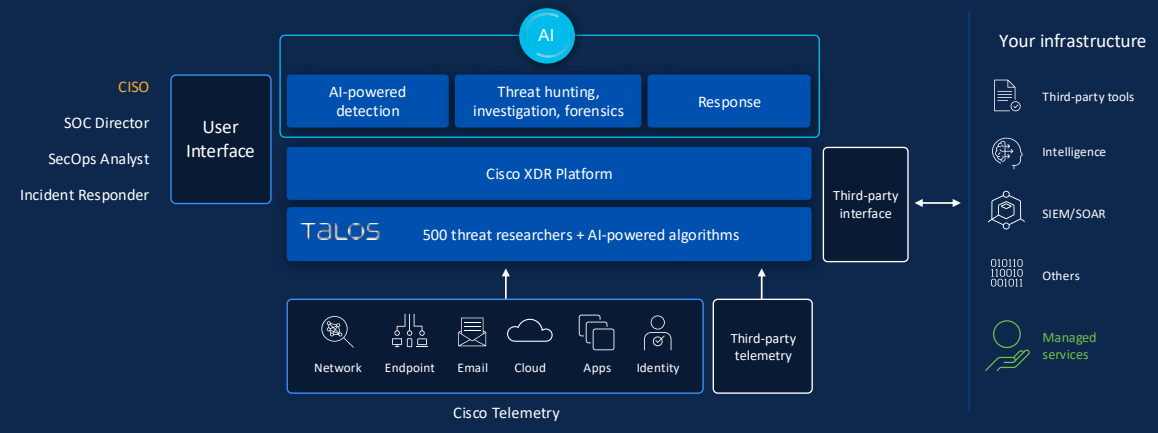
Jak může Cisco pomoci s DORA compliance

DORA pilíře

Řízení rizik ICT	Hlášení incidentů ICT	Testování digitální provozní odolnosti	Řízení rizik třetích stran v oblasti ICT	Sdílení informací
1.	2.	3.	4.	5.
Vedoucí pracovníci finančních subjektů musí definovat, provádět a dohlížet na strategie rizik ICT a zajistit dodržování předpisů DORA a osobní odpovědnost.	Finanční subjekty musí monitorovat, klasifikovat a hlásit incidenty ICT a podávat podrobné zprávy o kritických případech.	Podporuje bezpečný přístup třetích stran, posouzení rizik a průběžné monitorování aktivit poskytovatelů.	DORA klade důraz na řízení rizik třetích stran a vyžaduje, aby finanční subjekty zajistily, že poskytovatelé ICT splňují přísné standardy.	Finanční subjekty se musí učit z incidentů v oblasti ICT a mohou dobrovolně sdílet informace o hrozbách a zároveň chránit citlivá data.
Cisco XDR, Secure Network Analytics, DUO, Secure Access, Secure Firewall	Cisco XDR, Secure Network Analytics, Talos Incident Response	Cisco XDR, Secure Network Analytics, Secure Access, Secure Firewall, Talos Incident Response	Cisco XDR, Secure Network Analytics, DUO, Secure Access	Cisco XDR, Secure Access
Pomáhá organizacím identifikovat, monitorovat a zmírňovat rizika ICT pomocí Integrovaných bezpečnostních řešení.	Usnadňuje rychlou detekci, klasifikaci a zefektivněné hlášení incidentů ICT příslušným úřadům.	Umožňuje komplexní testování systémů za účelem posouzení zranitelností a posílení provozní odolnosti.	Podporuje bezpečný přístup třetích stran, posouzení rizik a průběžné monitorování aktivit poskytovatelů.	Podporuje bezpečnou spolupráci a efektivní sdílení údajů o shodě s předpisy.



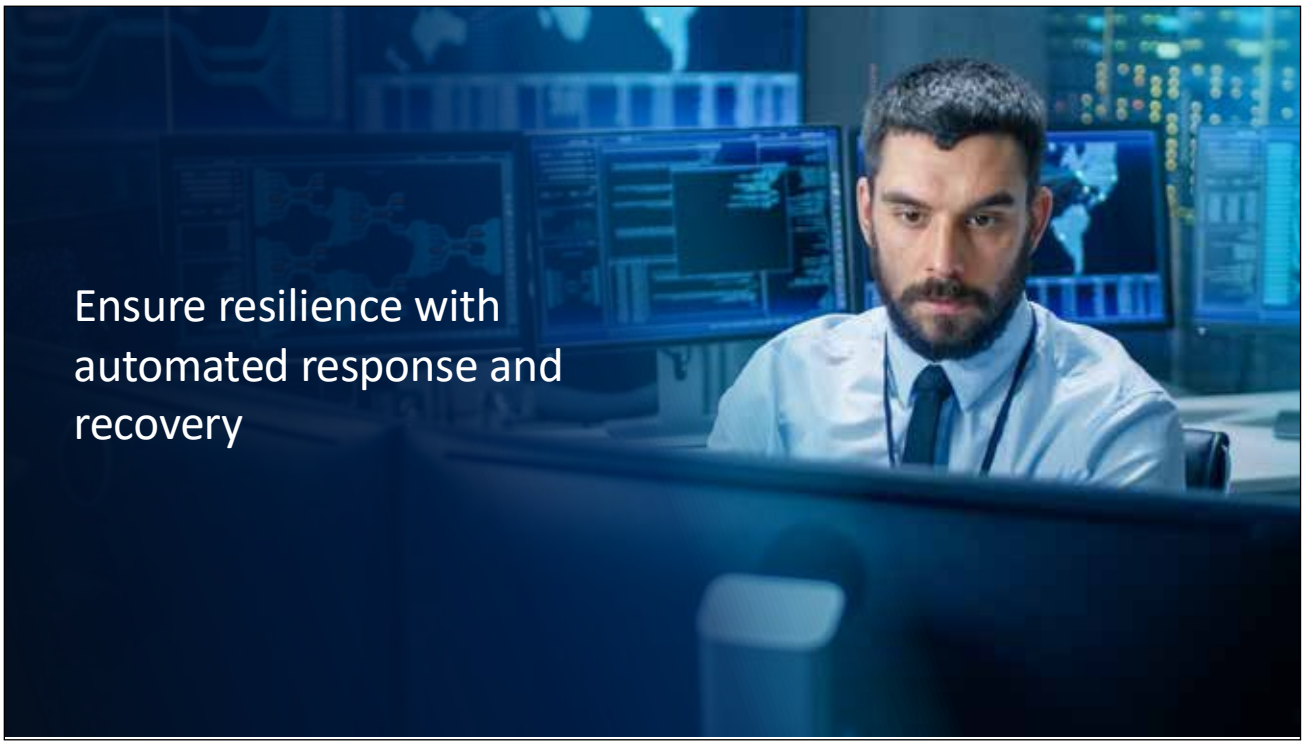
Complexity, simplified with an AI–first XDR



Power of data
Multi-vector detection with unmatched data across humans, machines, and services

Power of analytics
Clear prioritization with behavioral analytics and identity first platform

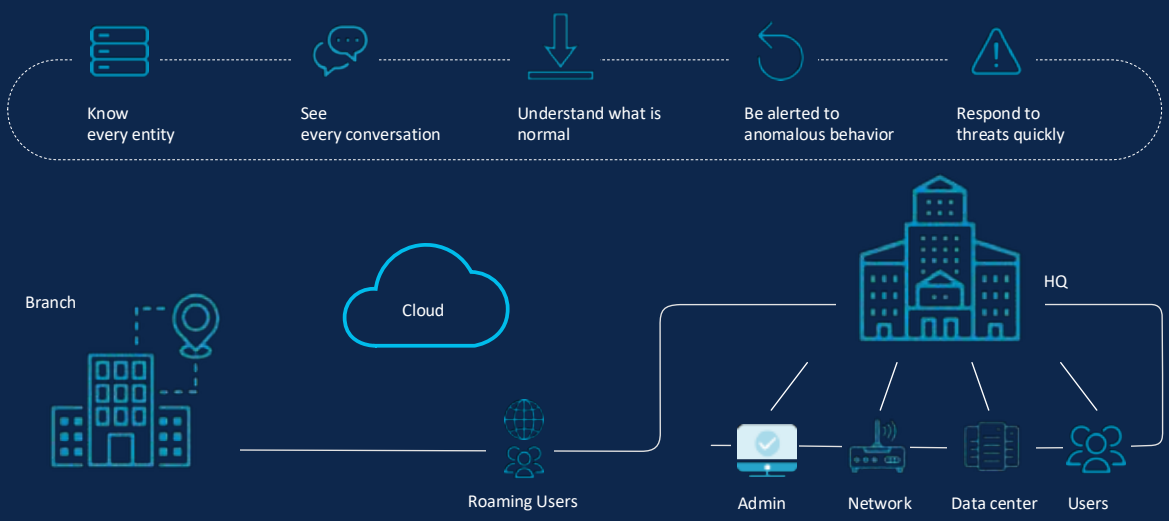
Power of AI
Automated playbooks and response guidance accelerated with Generative AI assistant



cisco

Cisco Secure Network Analytics

Secure Network Analytics



Cisco Secure Network Analytics

Use the network as a security sensor

Comprehensive visibility

Full network visibility with enriched contextual insight

Advanced threat detection

Multi-layered analytics for high-fidelity threat detection

Streamlined incident response

Automated response for rapid threat containment

Cisco Secure Access

Safer for everyone

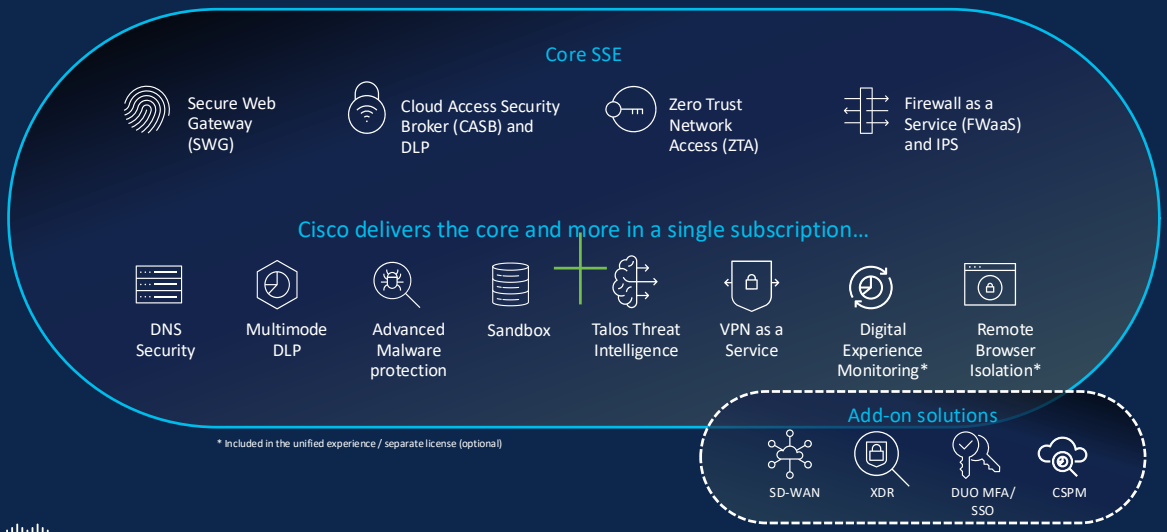
Modern Zero Trust Enforcement

Cisco Secure Access

Moderní přístup ochrany ICT pomocí konvergované cloudové služby postavené na principech Zero Trust

Cisco Secure Access

Go beyond core Secure Service Edge (SSE) to better connect and protect your business



Duo Identity & Access Management (IAM)

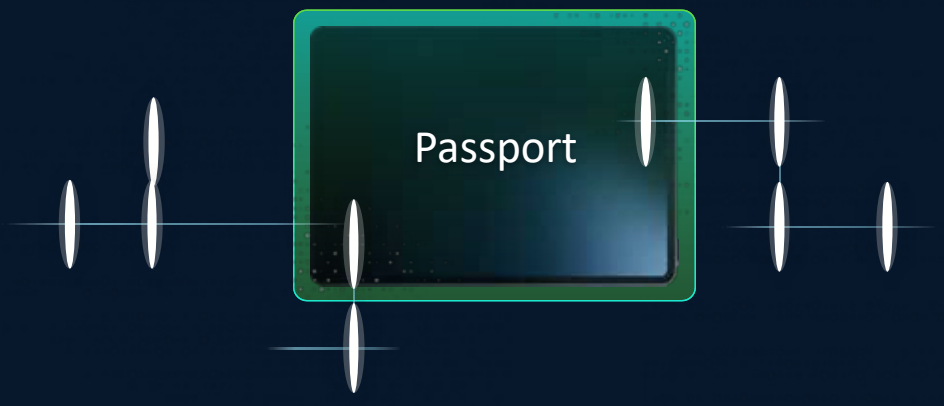
Duo IAM

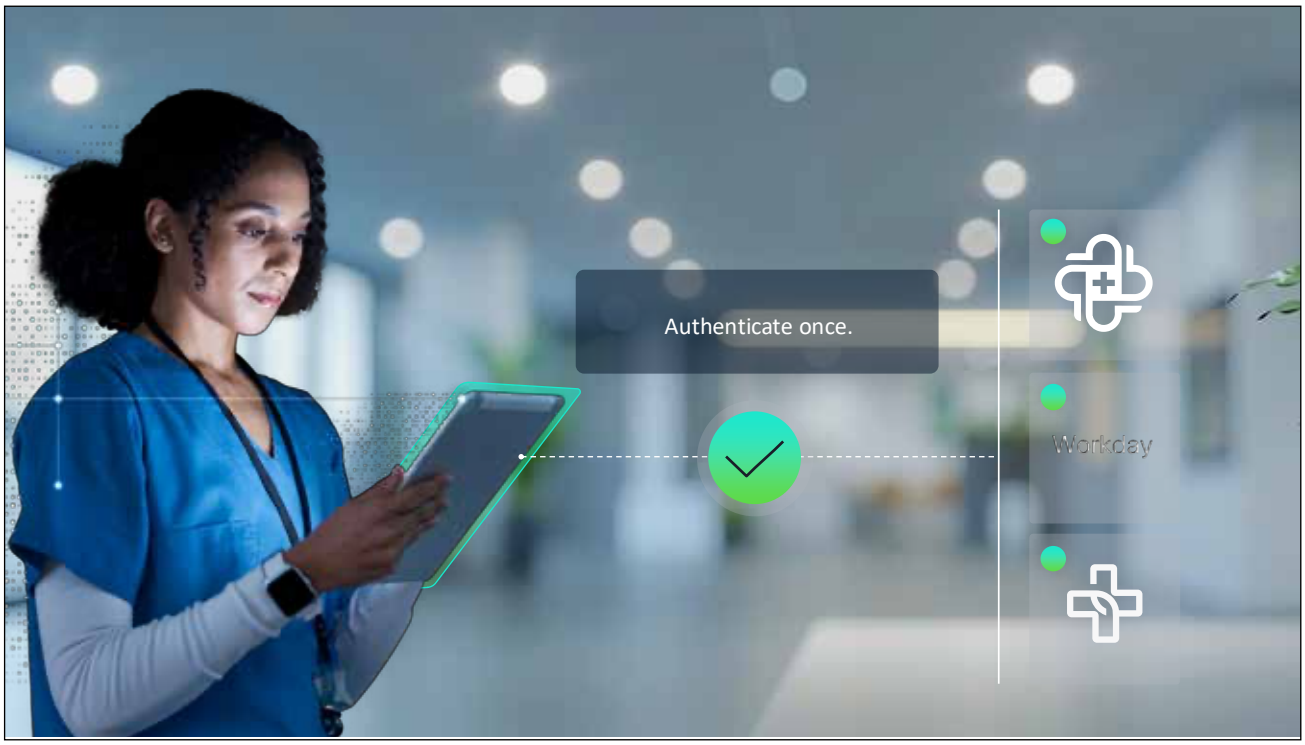
Security-First Identity

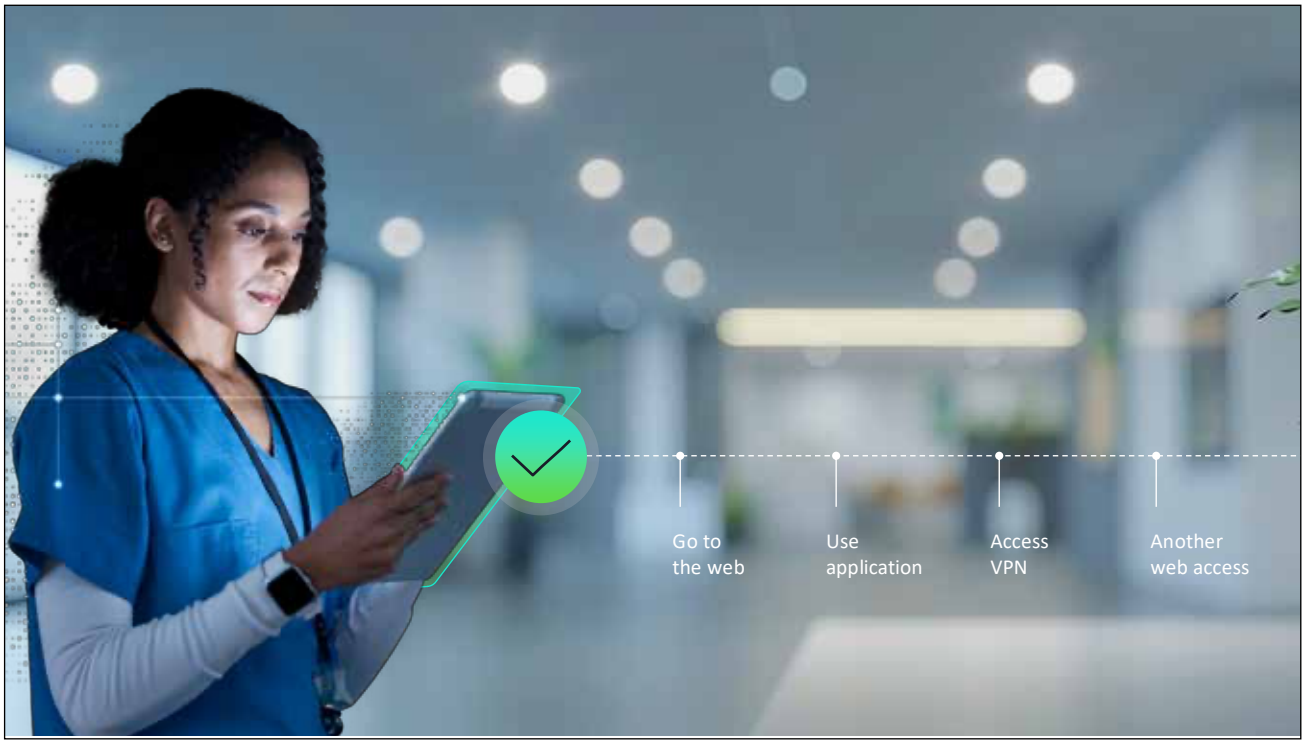
End to end phishing resistance

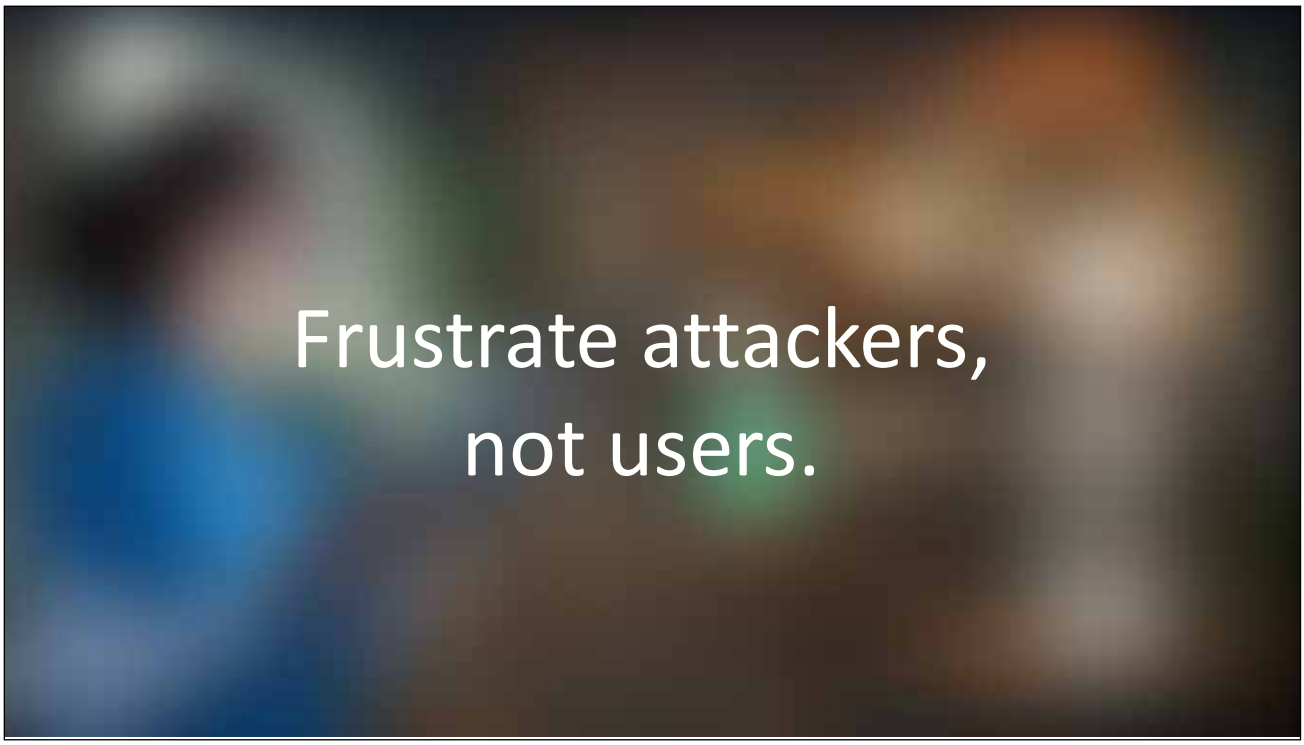
Unified Identity intelligence

World-class user experience




Authenticate once.
Workday


Go to
the web
Use
application
Access
VPN
Another
web access



Next-Generation Firewall

Price-performance leader

Inspected throughput
(4200, 3100, 1200 series)

Leader

The Forrester Wave ™
Enterprise Firewall Solutions Q4 2024

Cloud native

Encrypted traffic at scale

Perimeter and zone firewalling

Firewall price-performance leader

Top to bottom

Branch		Campus	Data center		Cloud
NEW				NEW	
					
200 Series	1200 Series	3100 Series	4200 Series	6100 Series	Public/Private
1 Model	6 Models	5 Models	3 Models	2 Models	20+ cloud variants
Firewalling + IPS	Firewalling + IPS	Firewalling + IPS	Firewalling + IPS	Firewalling + IPS	
Up to 1.5 Gbps	Up to 18 Gbps	Up to 45 Gbps	Up to 140 Gbps	Up to 400 Gbps	

Session ID: PSOSEC-1026

Cisco Encrypted Visibility Engine

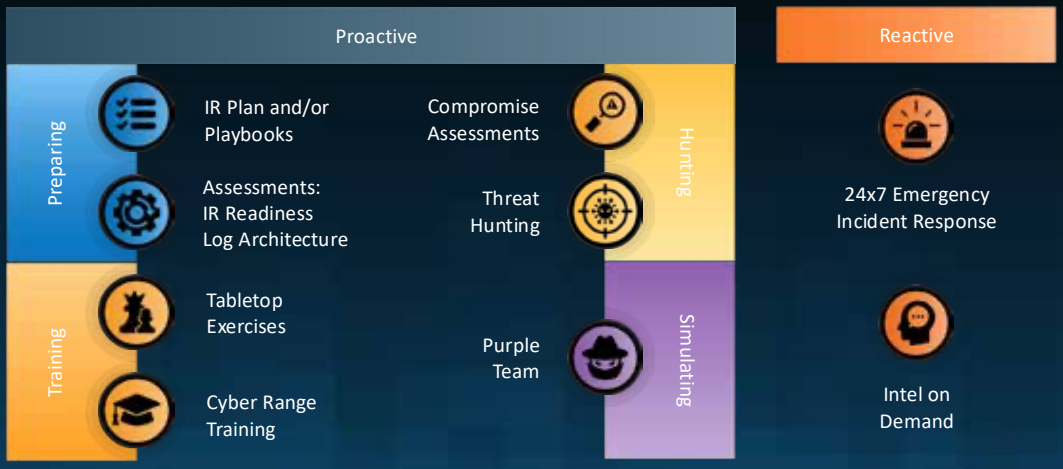
AI

Visibility to malicious flows in encrypted traffic without decryption

Machine learning (ML) technology	Processes 1 B+ TLS fingerprints	Processes 10 K+ malware samples daily

Talos Incident Response Retainer Services

Learn more at http://cs.co/TalosIRServiceDescription



Cisco DORA Advisory and Assessment Service

Security Architecture Assessment

- Know where you stand by discovering, prioritizing, and addressing shortcomings and gaps
- Understand your current level of security maturity in your ICT
- Know the gaps in your security architecture
- Understand where you can maximize your security investments

Threat Modeling

- Comprehend the threats your business faces and potential impacts
- Recognize the key functions and assets, and data to discern how these threats could affect important business services
- Know and understand mitigative and detective controls that are needed
- Establish necessary controls to mitigate them

Red Teaming Threat Simulation

- Know the real-world attack scenarios your business faces
- Know the effectiveness of your security control layers in preventing and limiting breaches
- Identify weaknesses to strategically prioritize future investments
- Strengthen internal security teams' response with insight gained