

CISCO *Live!*

ALL IN

#CiscoLive



The bridge to possible

Cyber Defense with a Tactical Security Mission Task

Kyu Lee, CyberSecurity Solutions Architect

BRKSEC-2087



#CiscoLive



Agenda

- Introduction
- Threat Mitigation Strategy
- MITRE ATT&K Use Case
- Platform Drill Down
- Cisco Security Reference Architecture
- Conclusion

Introduction



Kyu Lee: kylee2@cisco.com

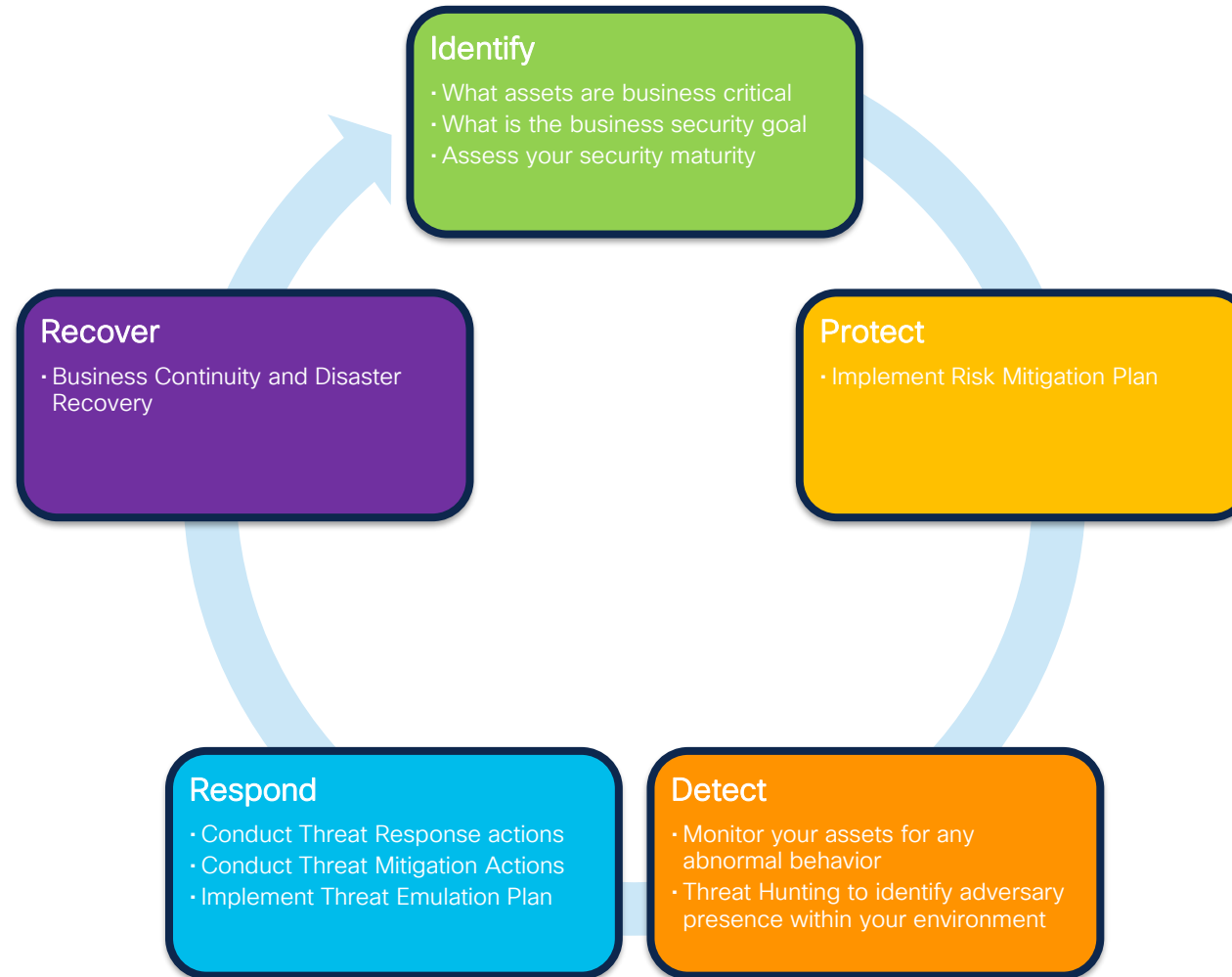
 www.linkedin.com/in/kyu-lee-cisco/

- Cyber Technical Solutions Architect
- Cyber Operations Officer in US ARMY
- GCIA, GNFA, GPEN, and GCPN
- 6 years @ Cisco
- Spent half of life in South Korea, and another half in U.S
- Wife to Cyber Threat Investigator, and Mom to 2 Boys


Threat Mitigation Strategy



Cyber Security Lifecycle



NSA's Top 10 Cybersecurity Mitigation Strategies

- | | | | |
|---|--|---|---|
| 1. Update and Upgrade Software Immediately |  Identify |  Protect | |
| 2. Defend Privileges and Accounts |  Identify |  Protect | |
| 3. Enforce Signed Software Execution Policies |  Protect |  Detect | |
| 4. Exercise a System Recovery Plan |  Identify |  Respond |  Recover |
| 5. Actively Manage Systems and Configurations |  Identify |  Protect | |
| 6. Continuously Hunt for Network Intrusions |  Detect |  Respond |  Recover |
| 7. Leverage Modern Hardware Security Features |  Identify |  Protect | |
| 8. Segregate Networks Using Application-Aware Defenses .. |  Protect |  Detect | |
| 9. Integrate Threat Reputation Services |  Protect |  Detect | |
| 10. Transition to Multi-Factor Authentication |  Identify |  Protect | |

NSA's Top 10 Cybersecurity Mitigation Strategies

Update and Upgrade Software Immediately

- Critical Asset Inventory
- Continuous Asset Vulnerability Scanning
 - Example: Qualys, RAPID7, Tenable
- Monitoring the software update requirement
- Patch Testing

Defend Privileges and Accounts

- Role-Based Access (RBAC)
- Network Segmentation Security

Enforce Signed Software Execution Policies

- Application Whitelisting
- Have a Good Software baseline to compare to
- Vulnerability and System Process Monitoring is still essential on signed software
 - Example: SolarWinds, Log4j

Exercise a System Recovery Plan

- Save the known good (previous) configuration
- Test the backup before implementation
- Segregate Backup Data

Actively Manage Systems and Configurations

- Inventory of network devices and software
- Identify and Remove stealth or unneeded hardware or software

Continuously Hunt for Network Intrusions

- Continuous Threat Monitoring and Proactive Threat Hunting
- Have SIEM or SOAR tools available that can ingest and correlate all the logs of threat evidences

Leverage Modern Hardware Security Features

- Monitor End of Life or End of Support devices and Schedule a hardware refresh
 - Those EoL or EoS does not get software patch release or support

Segregate Networks Using Application-Aware Defenses

- Identity and Segregate business critical assets
- Gain Visibility into all application conversations
- Prevent Attacker's lateral movement by Implementing Segmentation with least privilege communication

Integrate Threat Reputation Services

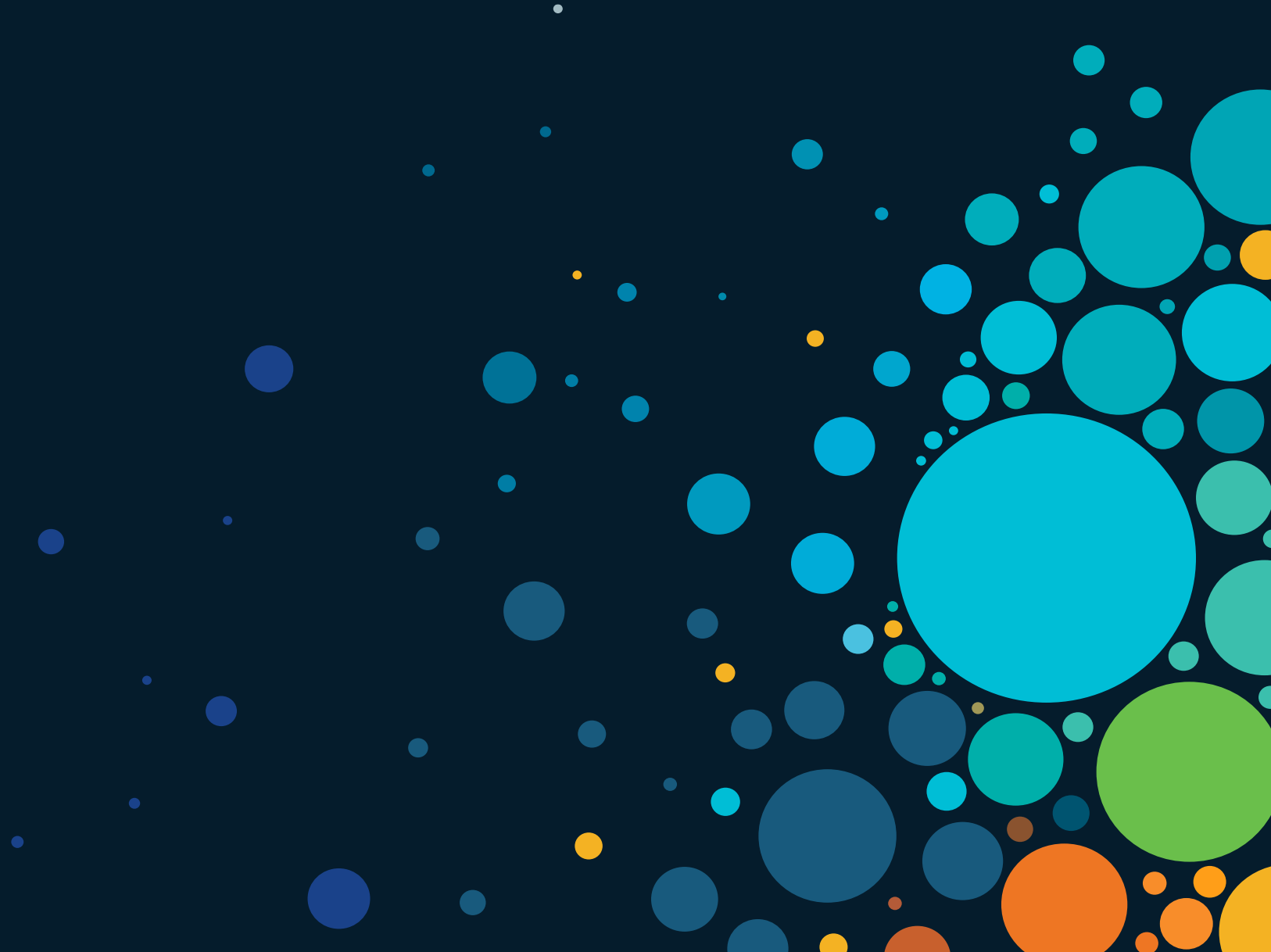
Open Source:

- Talos: [LINK](#)
- VirusTotal: [LINK](#)
- Hybrid-Analysis: [LINK](#)
- SANS Internet Storm: [LINK](#)
- URL Scan: [LINK](#)
- MITRE ATT&CK: [LINK](#)

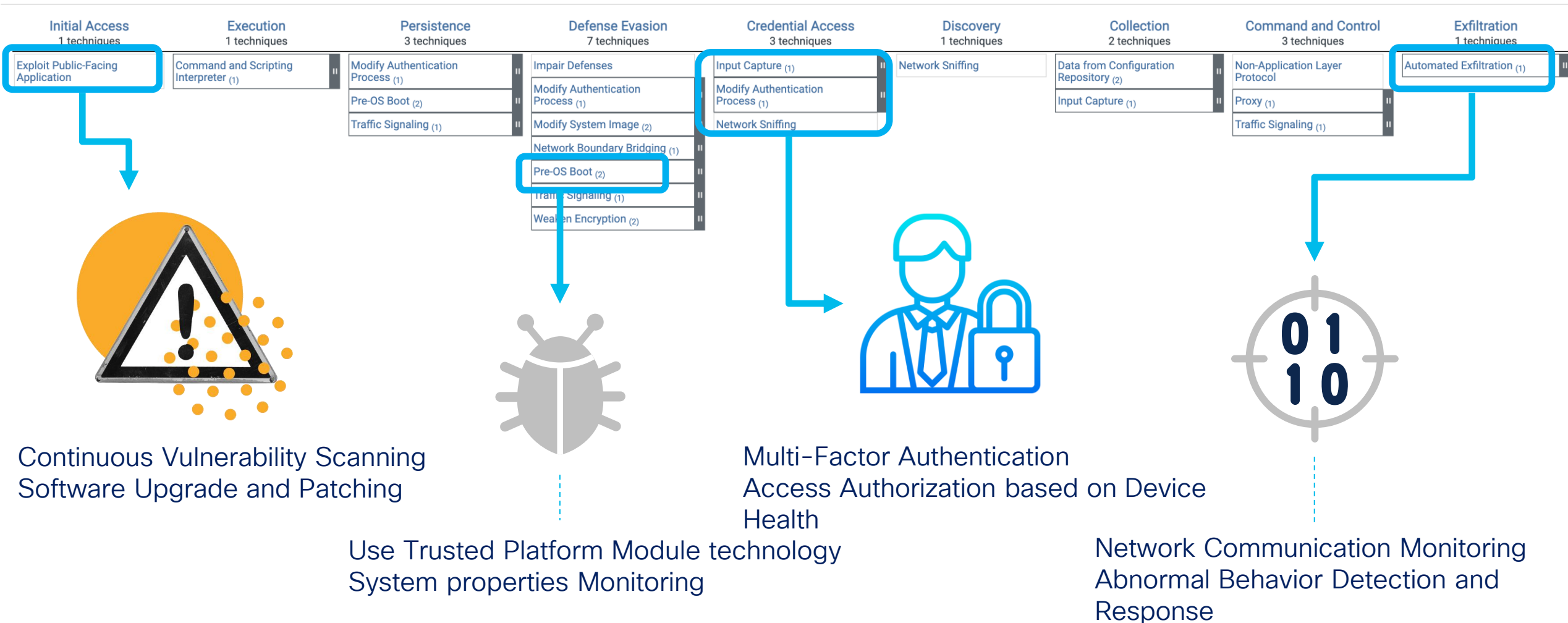
Transition to Multi-Factor Authentication

- Biometric verification
- SMS Token Authenticator
- Hardware Token Authentication
 - Example: Common Access Card (CAC), YubiKey
- Software Token Authentication
 - Authentication Application Example: Duo Mobile, Google Authenticator

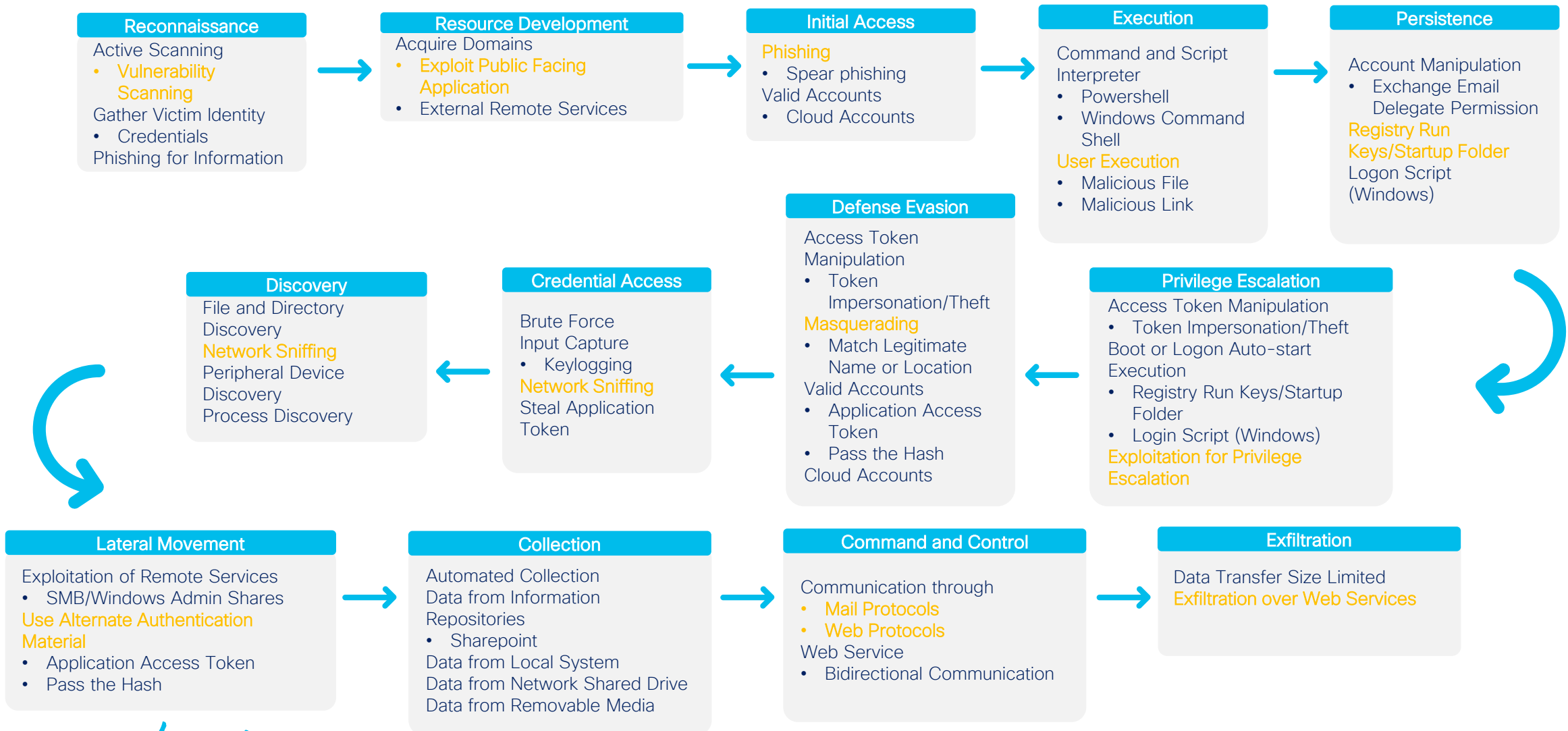
MITRE ATT&CK® Use Case



MITRE ATT&CK® Use Case - Data Exfiltration

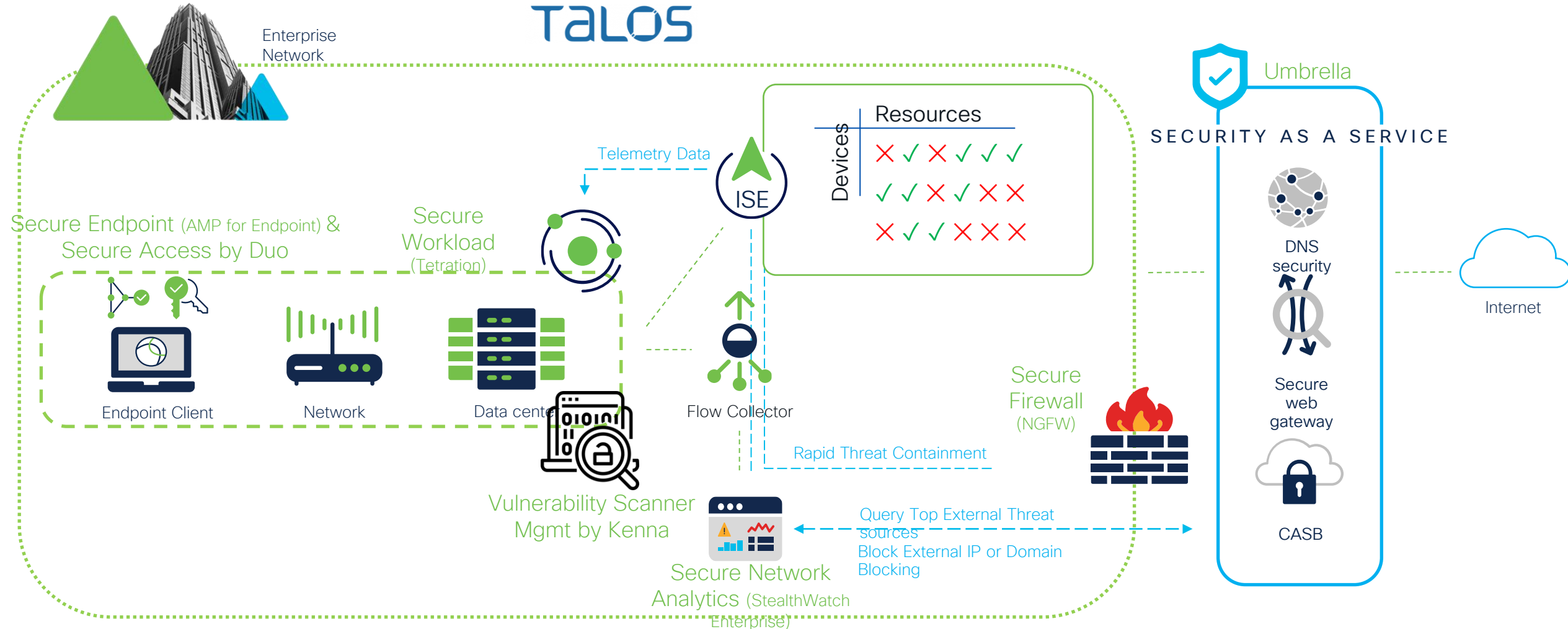


MITRE ATT&CK® Use Case – APT28



Cisco Security Summary: Data Exfiltration

TALOS

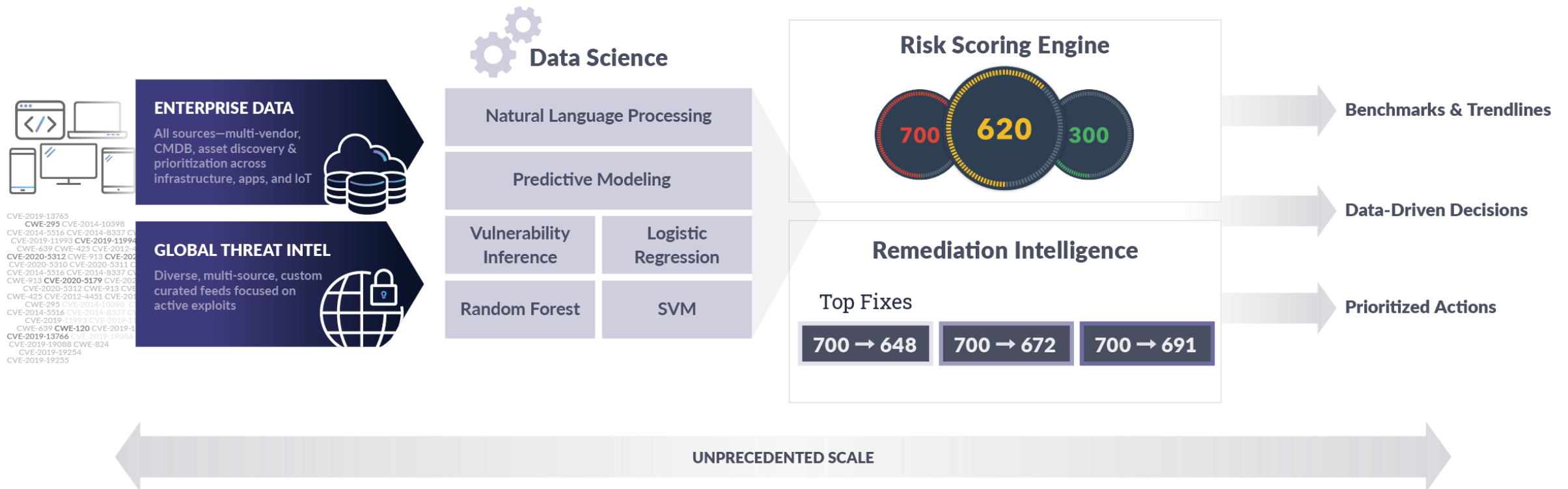


Platform Drill Down

Vulnerability Management



Vulnerability Scanner Manager: How Kenna Works



Access Control



Secure Access by Duo: Attributes



Mobile Devices

- Corp managed asset status
- Biometrics (Touch/Face) status
- Screen lock status
- OS condition (tampered) status
- Encryption status
- Platform type
- Device OS type
- Device OS version
- Device owner
- Duo Mobile version

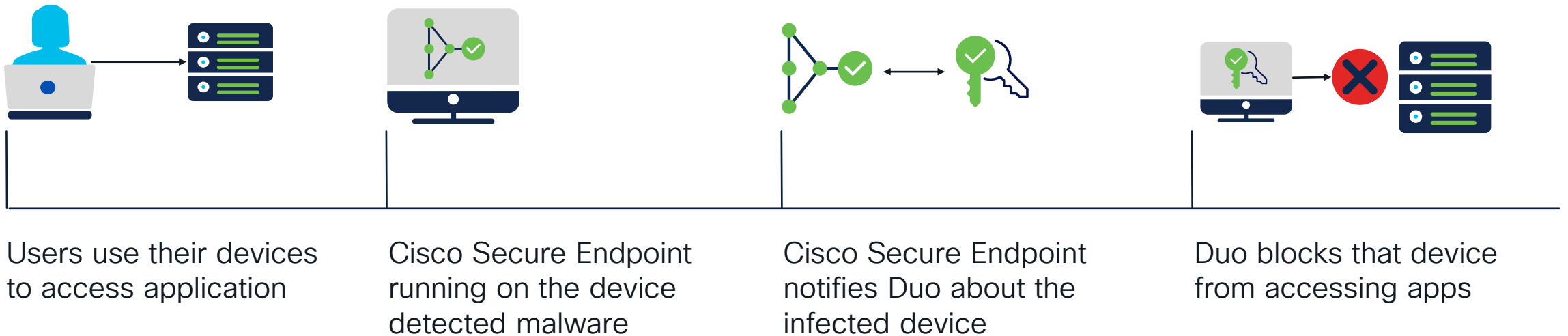


Laptops / Desktops

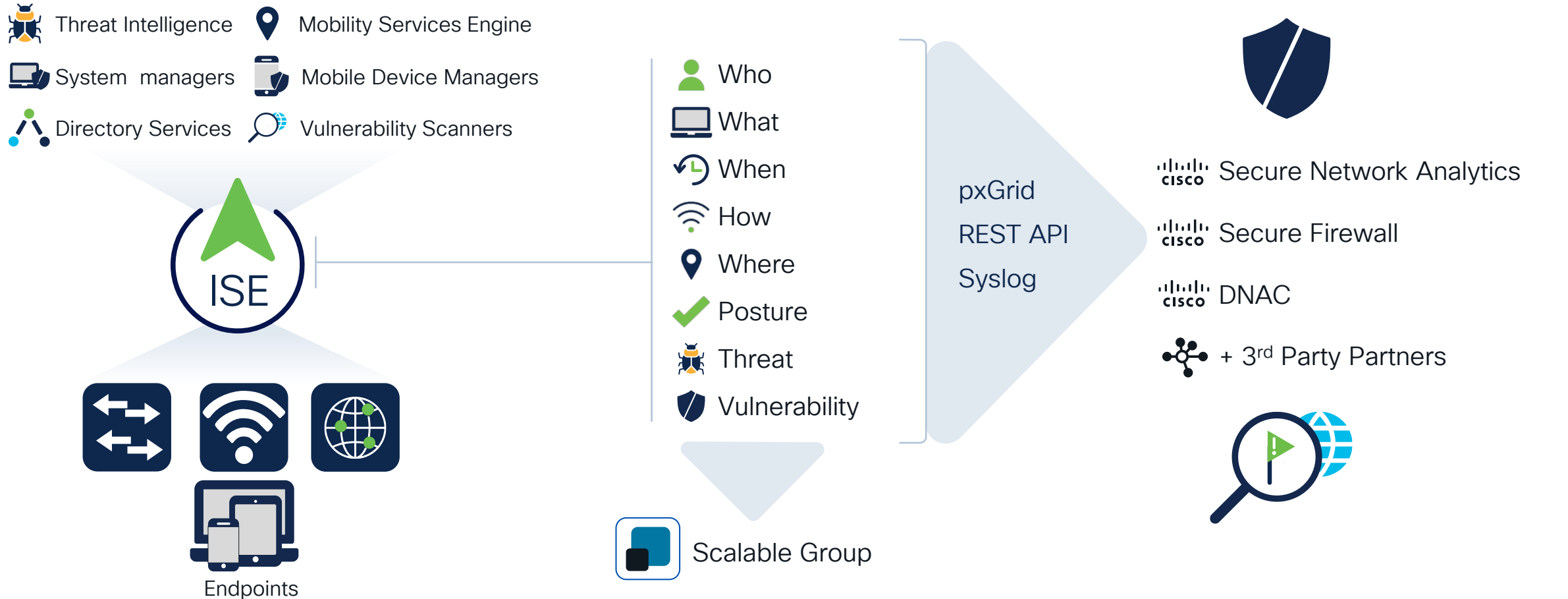
- Disk encryption
- Firewall enabled
- Device password
- OS patch level (Win 10)
- Third party agents
- Corp managed asset status*
- OS type & versions
- Browser type & versions
- Flash & Java plugins versions
- OS, browser and plugins status



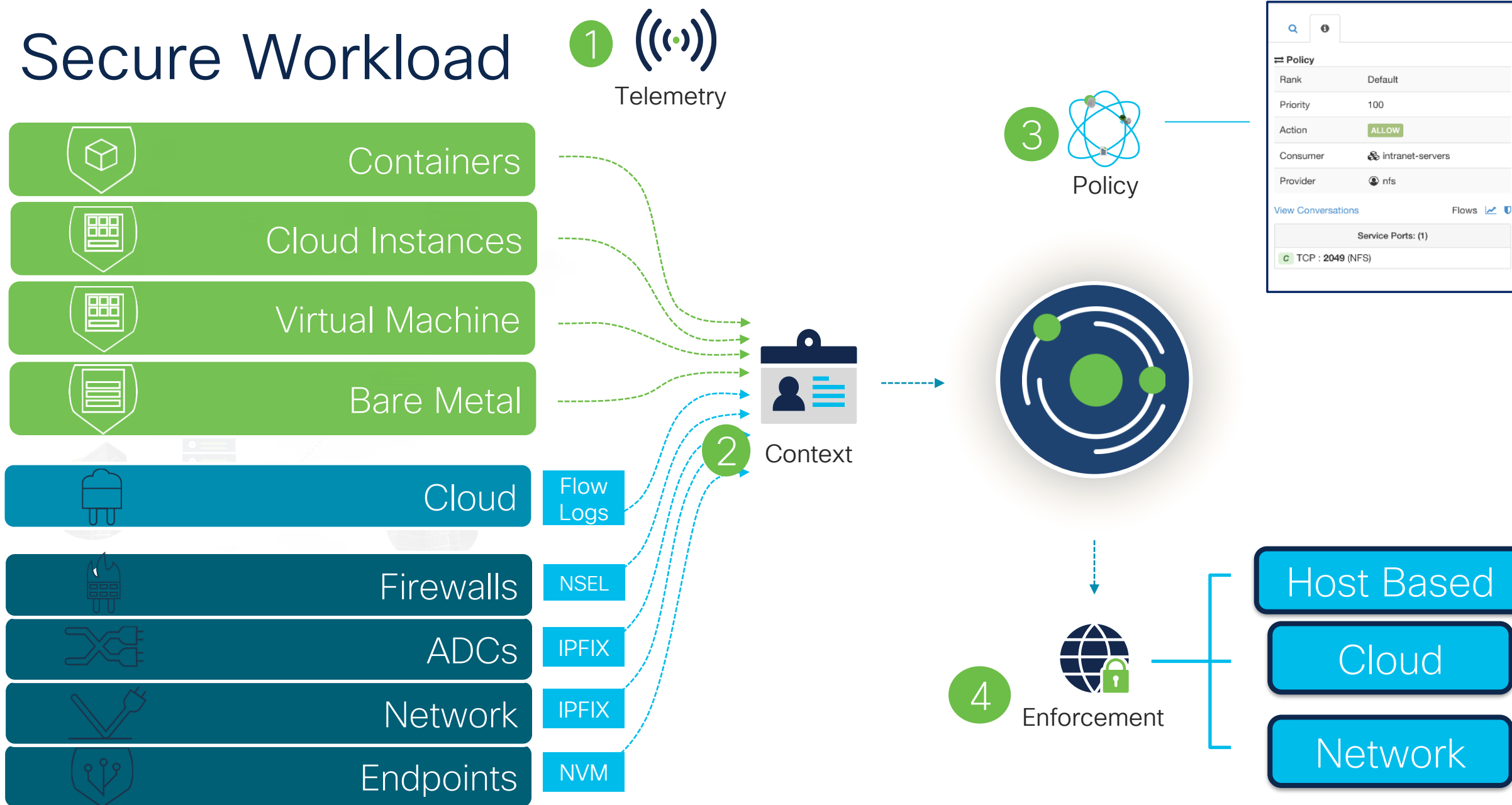
Secure Access by Continuous Endpoint Inspection



Identity Services Engine: Visibility & Access Control



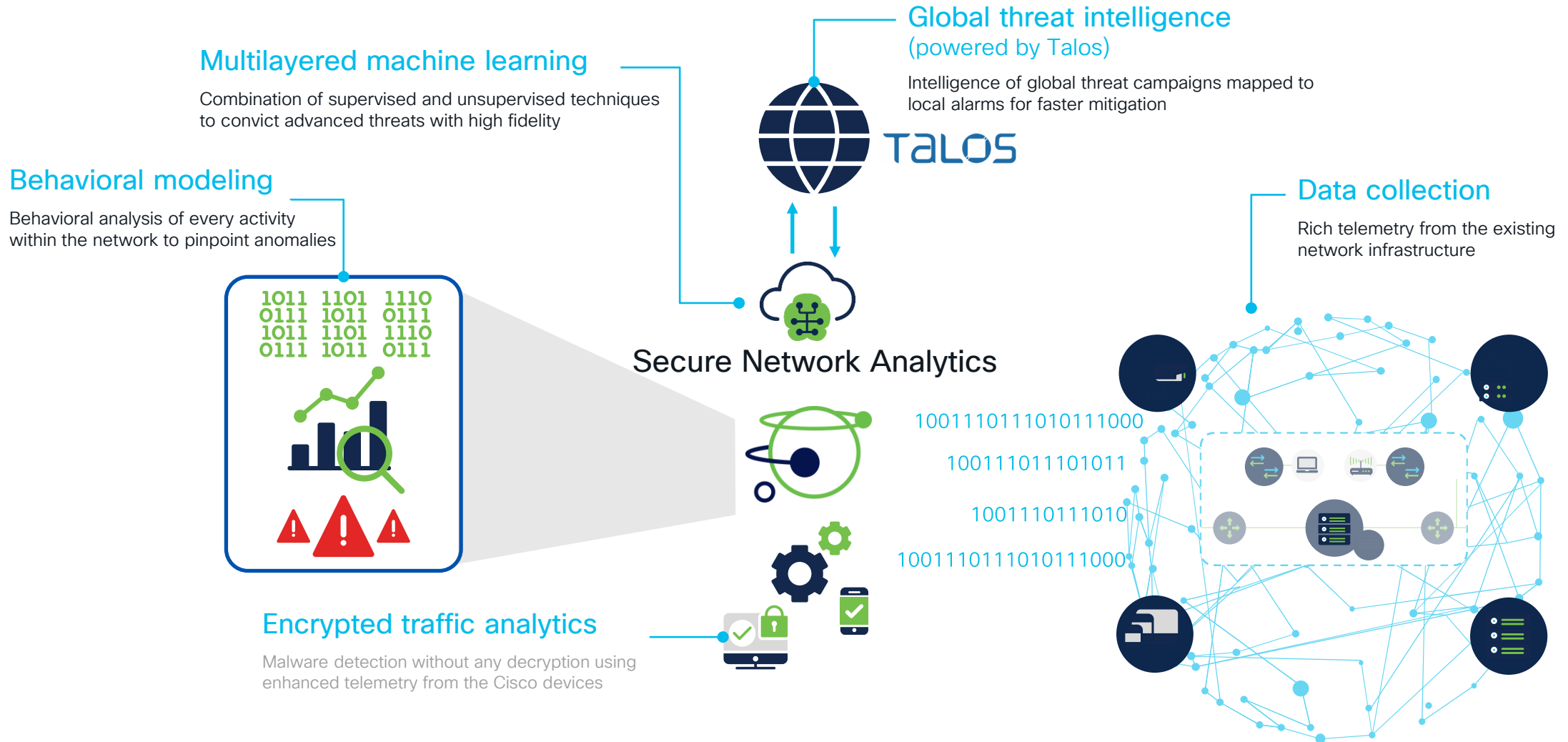
Secure Workload



Threat Detection and Response



Secure Network Analytics



Mapping to the MITRE ATT&CK Enterprise matrix

Initial Access

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Spearphishing Attachment
- Spearphishing Link
- Trusted Relationship
- Valid Accounts

Execution

- Dynamic Data Exchange
- Exploitation for Client Execution
- PowerShell
- Scheduled Task
- Windows Management
- Instrumentation
- Windows Remote Management

Exfiltration

- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Scheduled Transfer

Privilege Escalation

- Scheduled Task
- Valid Accounts

Defense Evasion

- BITS Jobs
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- Port Knocking
- Redundant Access
- SIP and Trust Provider Hijacking
- Valid Accounts
- Web Service

Credential Access

- Account Manipulation
- Brute Force
- Forced Authentication
- LLMNR/NBT-NS Poisoning and Relay
- Network Sniffing

Collection

- Data Staged
- Data from Information Repositories
- Data from Network Shared Drive
- Email Collection

Discovery

- Account Discovery
- Application Window Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Remote System Discovery
- System Information Discovery
- System Network Connections Discovery
- System Service Discovery

Lateral Movement

- Application Deployment Software
- Exploitation of Remote Services
- Remote Desktop Protocol
- Remote File Copy
- Remote Services
- Windows Admin Shares
- Windows Remote Management

Persistence

- Account Manipulation
- BITS Jobs
- External Remote Services
- Port Knocking
- Redundant Access
- SIP and Trust Provider Hijacking
- Scheduled Task
- Valid Accounts

Command and Control

- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Fallback Channels
- Multi-Stage Channels
- Multi-hop Proxy
- Multiband Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

Impact

- Network Denial of Service
- Resource Hijacking

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. 2163580 07/2020

To learn more about Stealthwatch, please visit cisco.com/go/stealthwatch
Sign up for a free 2-week visibility assessment [here](#)

Cisco Umbrella – DNS, CDFW, SWG

Add New Security Setting

Setting Name
New Security Setting

This security list is applied to:
DNS Policies

Copy From Existing
None

☐ Malware
Websites and other servers that host malicious software, drive-by downloads/exploits, mobile threats and more.

☒ Newly Seen Domains
Domains that have become active very recently. These are often used in new attacks.

☐ Command and Control Callbacks
Prevent compromised devices from communicating with attackers' infrastructure.

☐ Phishing Attacks
Fraudulent websites that aim to trick users into handing over personal or financial information.

☒ Dynamic DNS
Block sites that are hosting dynamic DNS content.

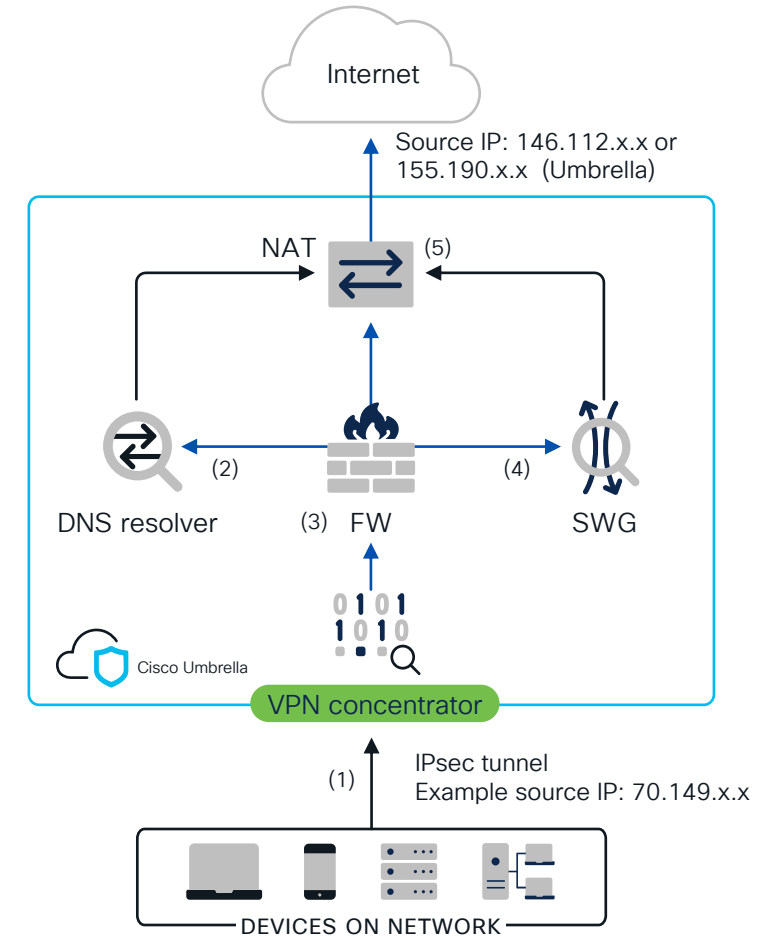
☒ Potentially Harmful Domains
Domains that exhibit suspicious behavior and may be part of an attack.

☒ DNS Tunneling VPN
VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer.

☒ Cryptomining
Cryptomining allows organizations to control cryptominer access to mining pools and web miners.

INTEGRATIONS

CANCEL SAVE



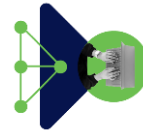
Endpoint Prevention, Detection & Response

Secure Endpoint: Prevent, Detect, Respond

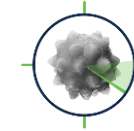
Threat Intelligence



Anti-Malware
Endpoint Detection & Response



Malware Analytics



PREVENT

DETECT

RESPOND

File Reputation	Network Flow Correlation	System Process Protection	Indications of Compromise	Global Threat Alerts	Retrospective Security
Signature-based Antivirus	Machine Learning	Exploit Prevention	Prevalence Analysis	SecureX Threat Hunting	Endpoint Isolation
File Grouping Engine	Ransomware Protection	Script Protection & Control	Vulnerable Surface Detection	API Integrations	Automated Actions & Orchestrator
	Behavior Protection		Orbital Advanced Search		Cross-Platform Response

Cisco Security Reference Architecture

Security Operations

SECURE X (XDR)

Managed Detection and Response Services

Threat Visibility & Hunting

Security, Orchestration, Automation and Response

Device Insights

Kenna Vuln Mgmt

Secure Cloud Insights

Incident Response and Remediation Services

3rd Party Integrations

User/Device Security

ZERO TRUST WORKFORCE

Adaptive MFA | Passwordless | Trust

Duo Secure Access | Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed



Cisco Secure Client

VPN

Posture

Telemetry

Threat

Query



ThousandEyes (Visibility)

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access Control | Managed Remote Access

Umbrella/Duo



ZTNA



DNS-layer security



Secure web gateway



L7 firewall + IPS



Cloud access security broker/shadow IT



RAaaS



SSL decryption



Remote browser isolation



Data loss prevention



Cloud malware detection

SDWAN

CISCO Meraki SDWAN

SDWAN by Viptela

Secure Firewall

ThousandEyes

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

CISCO Meraki SDWAN

SDWAN by Viptela

Secure Firewall

ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT



Industrial Router



Industrial Firewall



Industrial Switch/AP



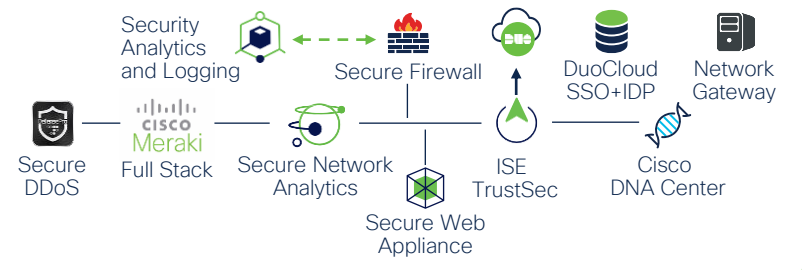
Cyber Vision



ISE TrustSec

ZERO TRUST WORKPLACE

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility



Application Security

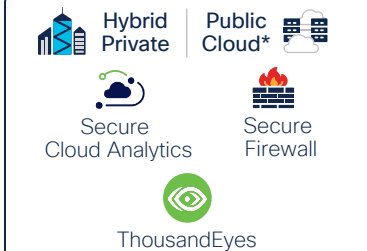
ZERO TRUST WORKLOAD

Policy | API Security
Application Segmentation
Run-time Application Security

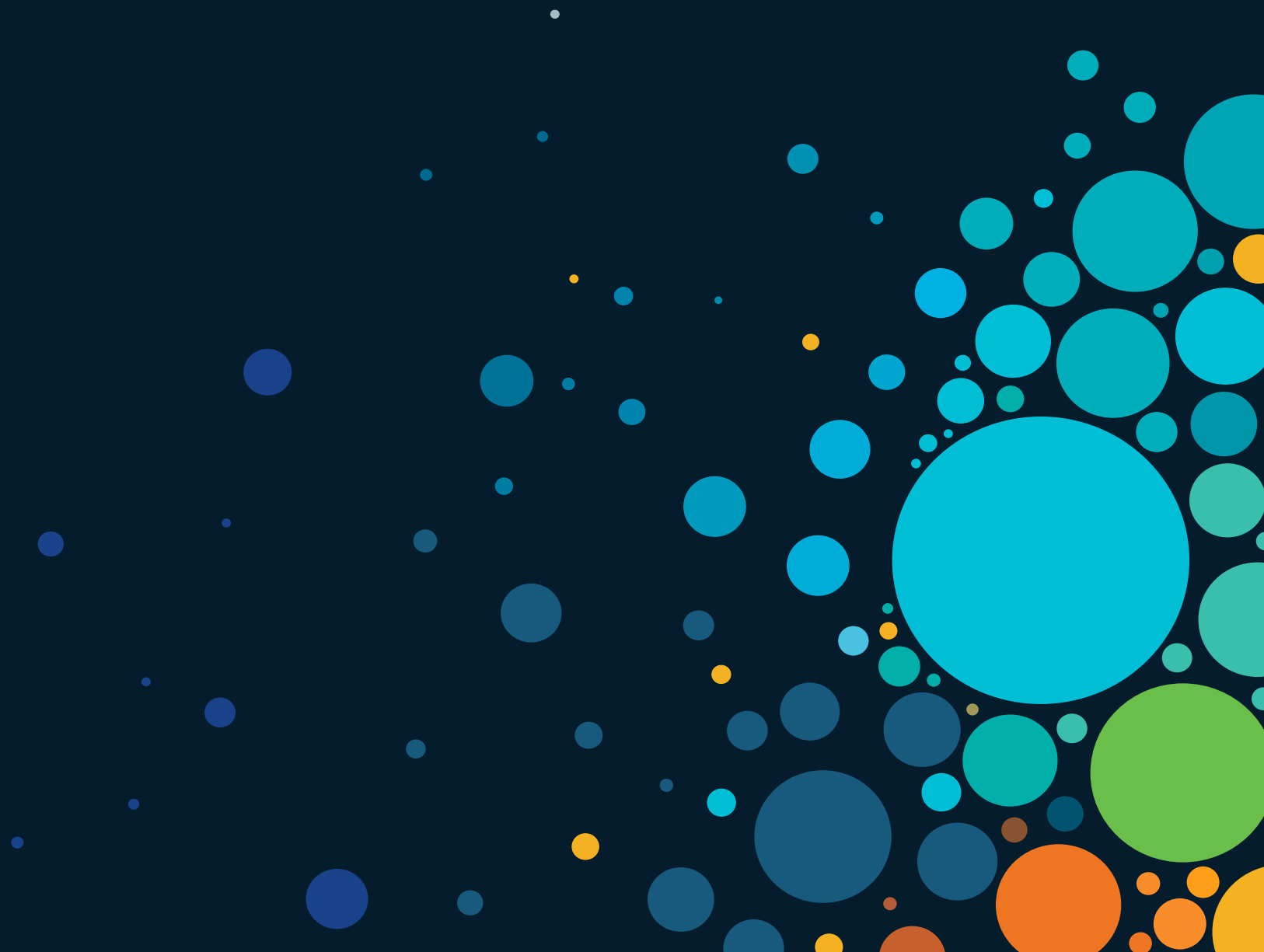
Application Security Stack



App Visibility | Detection | Response

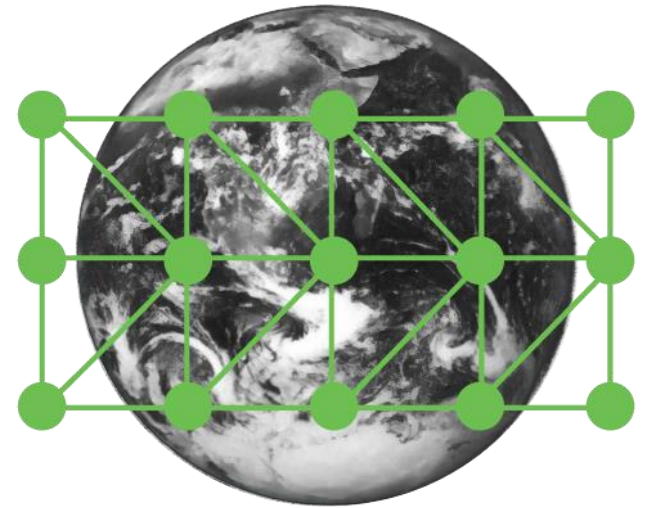


Conclusion



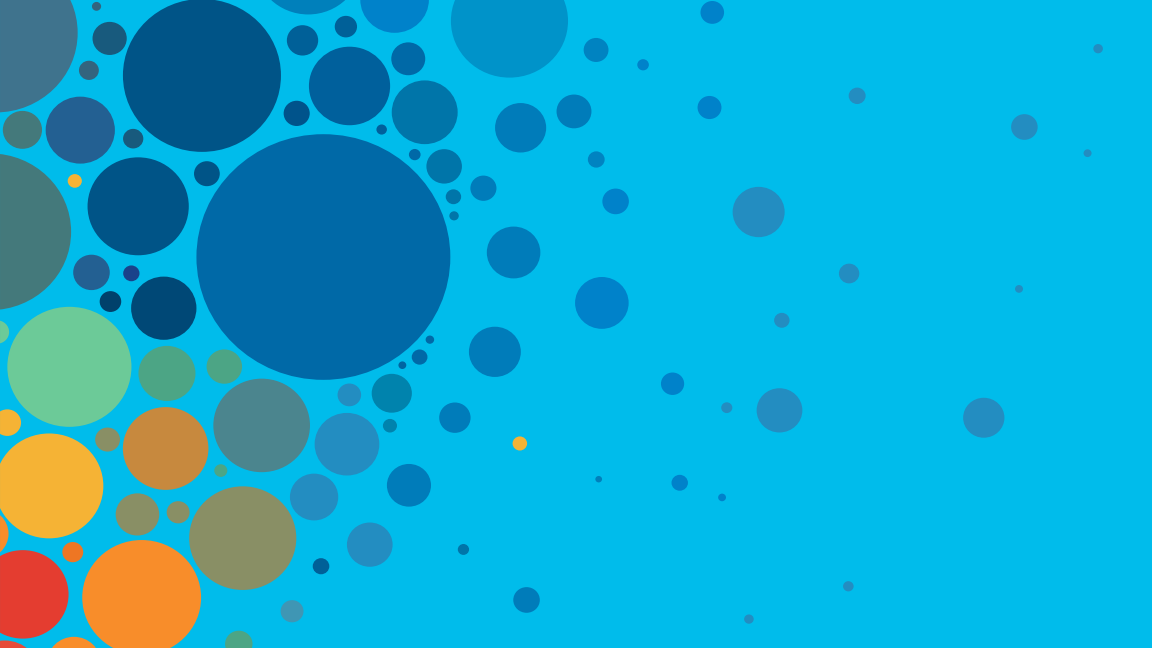
Wrap Up

- Track the inventory of your Business-Critical Assets
- Conduct scheduled Vulnerability Scanning, and Prioritize your business-critical asset for Vulnerability Patching
- Continuous Threat Monitoring and Proactive Threat Hunting using Threat Intelligence tools
- Build a strategy and Execute Network Segmentation – Least Privilege Access & Least Privilege Communication
- Segregate Backup Data
- Gain Visibility into your application and device communication within your network
- Use Modern Security Features for more detection, prevention, and faster response to Security Incidents
- Transition to Multi-Factor-Authentication



Resources

- NSA's Top 10 Cybersecurity Mitigation Strategies – [LINK](#)
- MITRE ATT&CK – [LINK](#)
- Kenna Security – [LINK](#)
- Secure Access by Duo – [LINK](#)
- Cisco Identity Services Engine – [LINK](#)
- Secure Workload – [LINK](#)
- Secure Network Analytics – [LINK](#)
 - MITRE ATT&CK Enterprise matrix – [LINK](#)
- Cisco Umbrella – [LINK](#)
- Secure Endpoint – [LINK](#)



Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



The bridge to possible

Thank you

CISCO *Live!*

ALL IN

#CiscoLive