spotit
YOUR SECURITY & NETWORK LAYER

How to prepare for growing cyber threats in healthcare

Frederik Rasschaert – Gert Tilburgs

Our identity

Our vision, strategy and focus

- Independent. Belgian. Privately owned
- Value driven. Quality and Expertise
- Niche player in networking and cyber security
- Your strategic partner
- Academy for raising talent

Big enough to deliver, small enough to care.

spotit

challenges in healthcare

Open Environment.

Changing Personnel & shifts.
Doctors/ freelancers with own devices & will.

Tight Budget.

Limited resources

Highly targeted.

Sensitive & Private Data.

Strict Regulations & Compliance.

(Outdated) IoT Devices.

Critical Infrastructure.

Together we can

Open Environment.

Changing Personnel & shifts. Doctors/ freelancers with own devices & will.

Enable technology to maximize value

Tight Budget.

Limited resources

Strategic architectures

Highly targeted.

Sensitive & Private Data.

Tailored MDR and SOC services

Strict Regulations & Compliance.

Expert department on GRC

(Outdated) IoT Devices.

Critical Infrastructure.

Expert department on (I) OT

Insights in attack trends

Sources

- Health ISAC 2025 Annual Threat Report
- Enisa threat landscape 2024
- Unit 42 Incident Response Report 2024
- Threat exposure Brucon 2024: inside the biggest hacks and facts of the past year
- CyberArk Identity Security Threat Landscape Report 2024
- Rapid7 2024 attack intelligence report
- Unit42 Attack Surface Threat Report
- Unit42 Cloud Threat Report volume7
- Bitsight Technologies Executive Report |report-2023-10-20
- Talos IR trends Q3 2024
- Verizon data breach report 2024

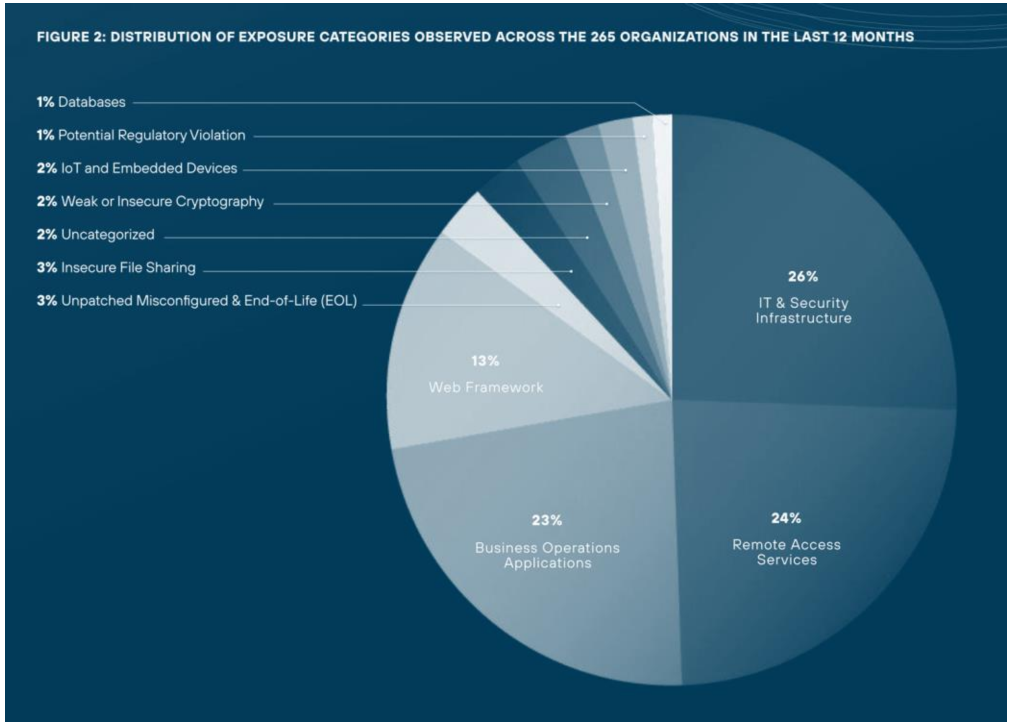
Attack Surface

Attack surface | Insights

73% of high-risk exposures originate in 3 main categories.

- IT & Security Infra
- Remote Access Services
- Business applications

FIGURE 2: DISTRIBUTION OF EXPOSURE CATEGORIES OBSERVED ACROSS THE 265 ORGANIZATIONS IN THE LAST 12 MONTHS



Key findings

26% of exposures involve critical IT and security infra!

Opportunities for lateral movement and data exfiltration are abundant.

Just three categories of exposures-IT and Networking Infrastructure, Business Operations Applications, and Remote Access Services-account for 73% of high-risk exposures across the organizations we studied and can be exploited for lateral movement and data exfiltration.

Critical IT and security services are dangerously exposed to the internet.

Over 26% of exposures involve critical IT and security infrastructure, opening doors to opportunistic attacks. These include vulnerabilities in application-layer protocols like SNMP, NetBIOS, PPTP, and internet-accessible administrative login pages of routers, firewalls, VPNs, and other core networking and security appliances.

Attack surface | Iomt | ISAC

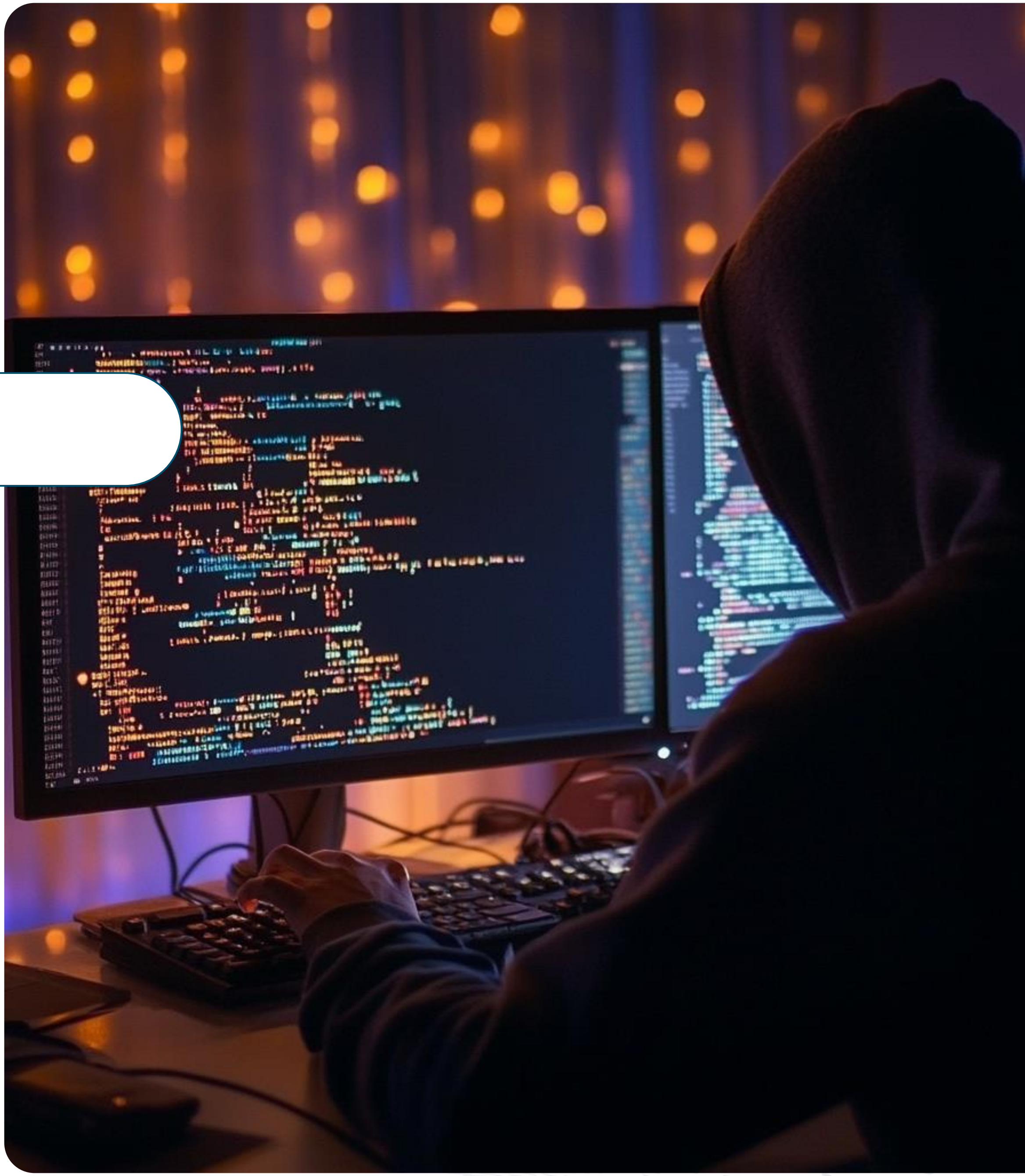
- Unsupported windows xp and windows 7 continue to be used in healthcare.
- As is windows 10 which goes end of support in 2025.
- Wannacry is the ninth most common vulnerability found on medical devices!
- The global state of internet of healthcare things identified 5100 publicly exposed DICOM servers!

→ Remote access services.

→ IT infrastructure.

→ Security holes in Business applications.

Spotit offensive security trends



Red Team assessments.
Without any information, credentials or devices.

56%

- → Lots of impact, compromised servers, devices, accounts.
- → Domain admin privileges

44%

- → Lots of impact, compromised servers, devices, accounts.
- → Access to sensitive data.
- → No domain admin privileges due to attack stop (point taken/ budget).

= 100% success ratio!

How attackers get in?

Ways to get in | Learned from Incident Response

- Credentials (MFA)!!!
- Phishing/ Social Engineering.
- Vulnerabilities.

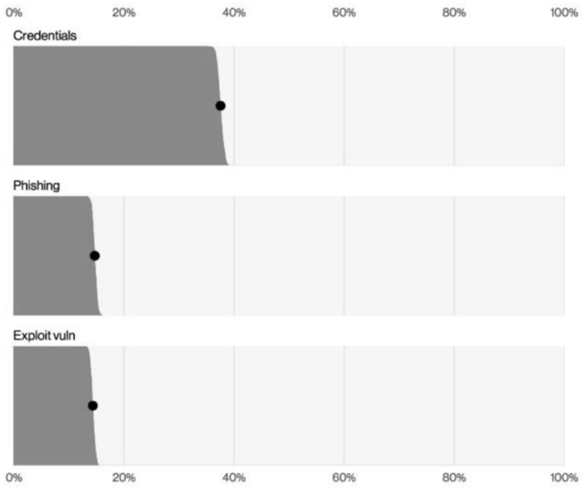
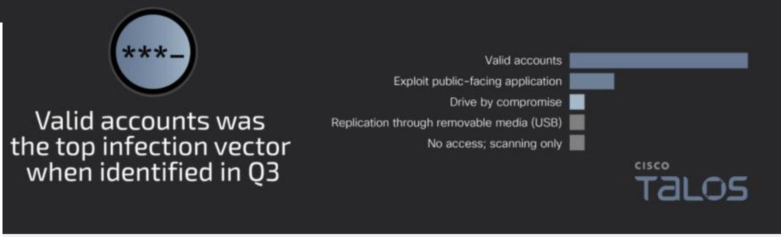


Figure 1. Select ways-in enumerations in non-Error, non-Misuse breaches (n=6,963)

Our ways-in analysis witnessed a substantial growth of attacks involving the exploitation of vulnerabilities as the critical path to initiate a breach when compared to previous years. It almost tripled (180% increase) from last year, which will come as no surprise to anyone who has been following the effect of MOVEit and similar zero-day vulnerabilities. These attacks were primarily leveraged by Ransomware and other Extortion-related threat actors. As one might imagine, the main vector for those initial entry points was Web applications.

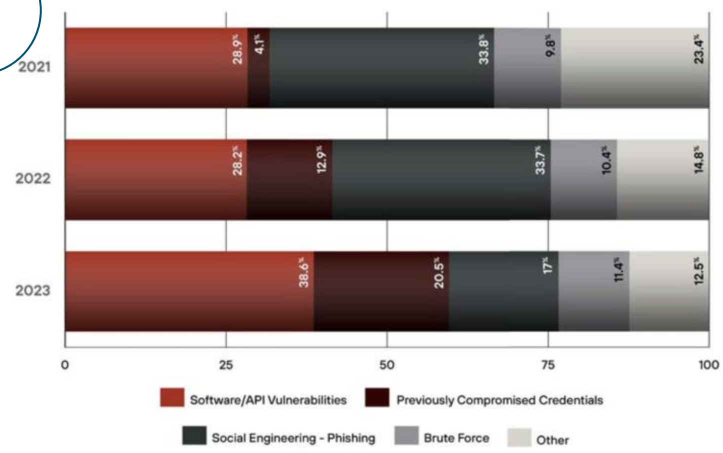
Initial access

For the fourth consecutive time in over a year, the most observed means of gaining initial access was the use of valid accounts, accounting for 66 percent of engagements when initial access could be determined. This is a *slight* increase compared to the previous quarter (60 percent). Additionally, 20 percent of engagements featured adversaries exploiting or leveraging vulnerable and public-facing applications for initial access.



Valid accounts was the top infection vector when identified in Q3

ure 6. Top 4 initial access vectors from Unit 42 incident response cases in 2023



Social Engineering | Health ISAC

Most reported in health care:

Help desk teams are targeted using social engineering attacks

- Impersonate leadership or others in an effort to increase authenticity.

TOAD (Telephone-Oriented Attack Delivery)

- Phishing mails including phone numbers to elicit voice communications.

Spam-bomb social engineering

- Add victim’s email to legitimate spam sites to bomb the victim with spam.
- Then call to offer tech support and request remote assistance .

Notable Vulnerabilities in healthcare attacks | ISAC

Vulnerabilities and Exposures

Health-ISAC shares threat bulletins as it receives information about pressing vulnerabilities. In 2024, Health-ISAC's Threat Operations Center shared 861 Targeted Alerts to member and non-member organizations in the health sector. Targeted Alerts warn organizations of high risks specific to their network-including things like vulnerable servers, cybercriminals selling access to their networks, stolen intellectual property, and compromised credentials. The top five vulnerabilities by targeted alert volume are as follows:

Vulnerabilities and Exposures	Targeted Alerts Distributed
Remote Desktop Protocol (RDP) Exposure	105
Ivanti Connect Secure Authentication Bypass Vulnerability (CVE-2023-46805, CVE-2024-21887)	57
Fortinet FortiOS Vulnerability (CVE-2024-21762)	56
MOVEit Transfer Authentication Bypass (CVE-2024-5806)	46
Check Point (CVE-2024-24919)	27

Spotit offensive security trends

Infrastructure pentest – 100% hit ratio

External

- 63% | High risk issues exposed & Risk on compromised network/ account.
- 37% | Enriched with social engineering to expose high risks (when it was in scope)/ found lower risk issues.

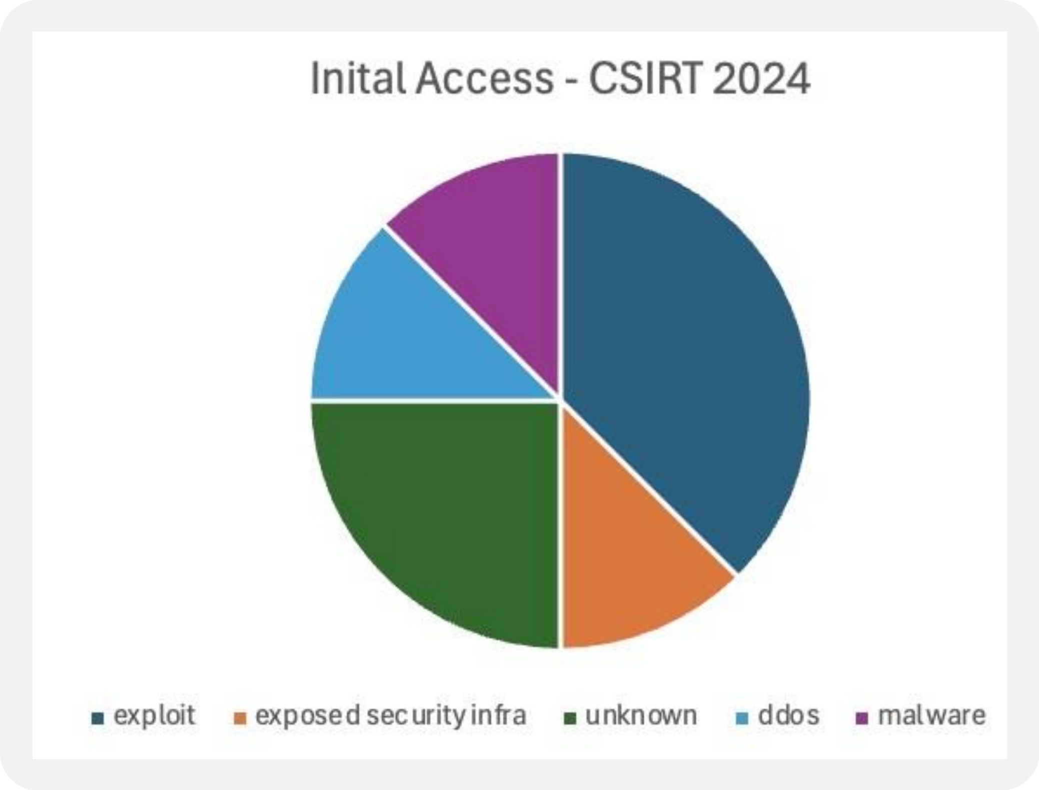
Internal

- 90% success rate on obtaining domain admin privileges.
- 10% aim for domain admin privileges out of scope.

Social Engineering | Always a hit.

- Often combined with infra pentest/ red teaming.
- Spear phishing (we target 1 person); takes 2-3 mails to obtain account access.
- Vishing | Using 1 phone call (average duration of 5-10min to have access to the account).
- Physical access; always backdoor device injected (AP, 4G, USB, ...).

Spotit CSIRT | Numbers



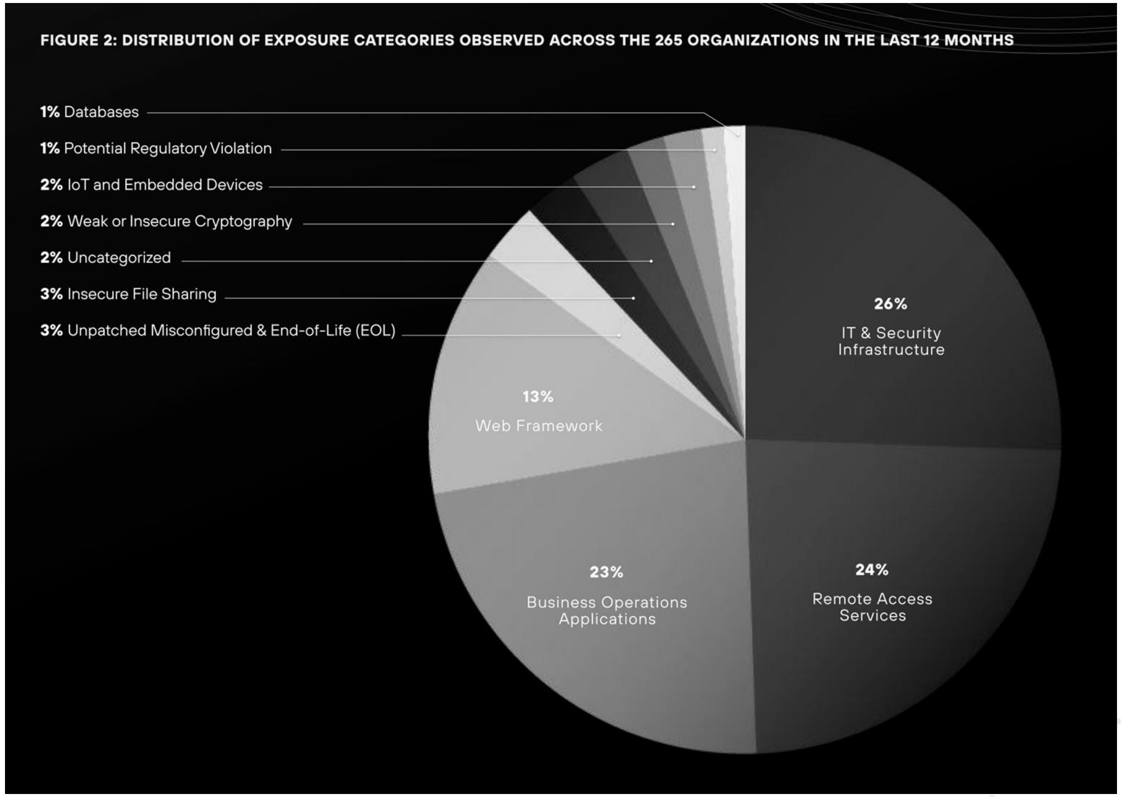


FIGURE 2: DISTRIBUTION OF EXPOSURE CATEGORIES OBSERVED ACROSS THE 265 ORGANIZATIONS IN THE LAST 12 MONTHS

Initial Recovery: 1-2 weeks before go live of most critical applications.

Types and volumes of attacks

Types and volumes of attacks | Incident Reponse Reports

- DDoS.
- Ransomware.
- Exploits (Third-Party).
- Human Element.

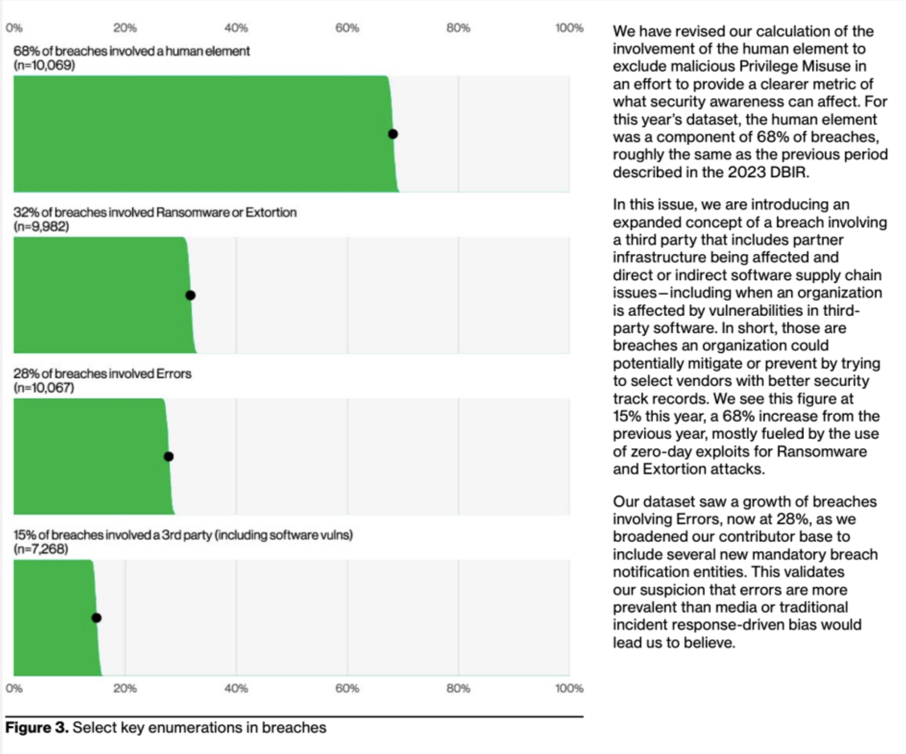


Figure 3. Select key enumerations in breaches

We have revised our calculation of the involvement of the human element to exclude malicious Privilege Misuse in an effort to provide a clearer metric of what security awareness can affect. For this year's dataset, the human element was a component of 68% of breaches, roughly the same as the previous period described in the 2023 DBIR.

In this issue, we are introducing an expanded concept of a breach involving a third party that includes partner infrastructure being affected and direct or indirect software supply chain issues—including when an organization is affected by vulnerabilities in third-party software. In short, those are breaches an organization could potentially mitigate or prevent by trying to select vendors with better security track records. We see this figure at 15% this year, a 68% increase from the previous year, mostly fueled by the use of zero-day exploits for Ransomware and Extortion attacks.

Our dataset saw a growth of breaches involving Errors, now at 28%, as we broadened our contributor base to include several new mandatory breach notification entities. This validates our suspicion that errors are more prevalent than media or traditional incident response-driven bias would lead us to believe.

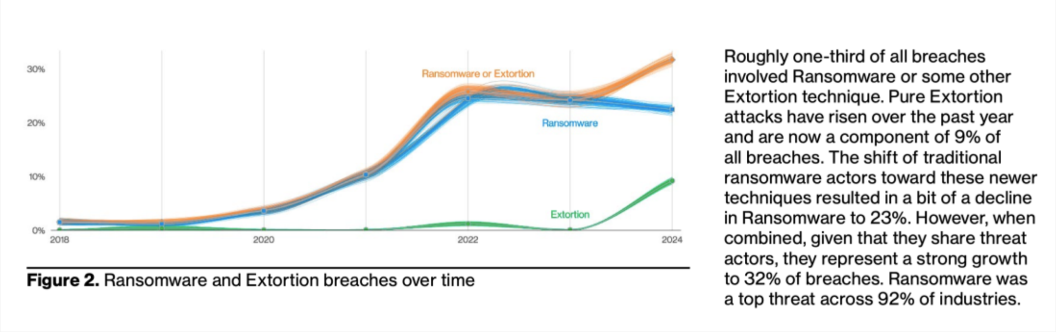


Figure 2. Ransomware and Extortion breaches over time

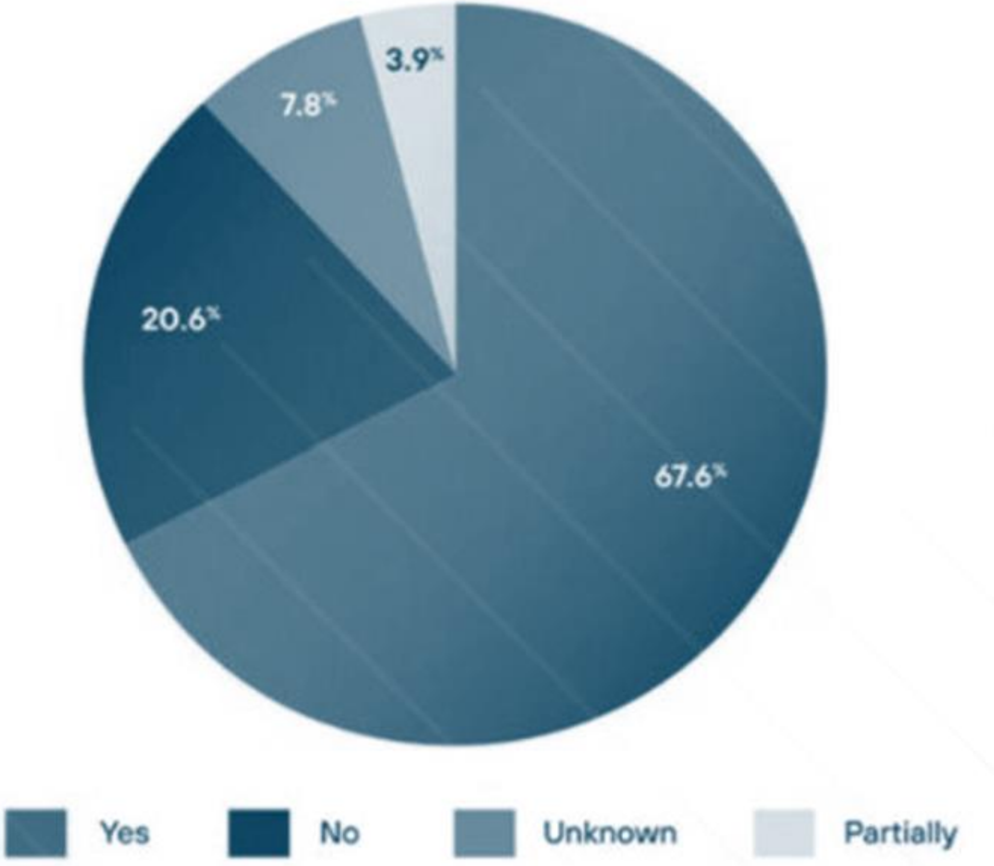
Roughly one-third of all breaches involved Ransomware or some other Extortion technique. Pure Extortion attacks have risen over the past year and are now a component of 9% of all breaches. The shift of traditional ransomware actors toward these newer techniques resulted in a bit of a decline in Ransomware to 23%. However, when combined, given that they share threat actors, they represent a strong growth to 32% of breaches. Ransomware was a top threat across 92% of industries.

Survey Findings

Top 5 Healthcare Attack Types

*Health sector security professionals reported Top Five Cyber Threats facing their organizations in **2024** as follows*

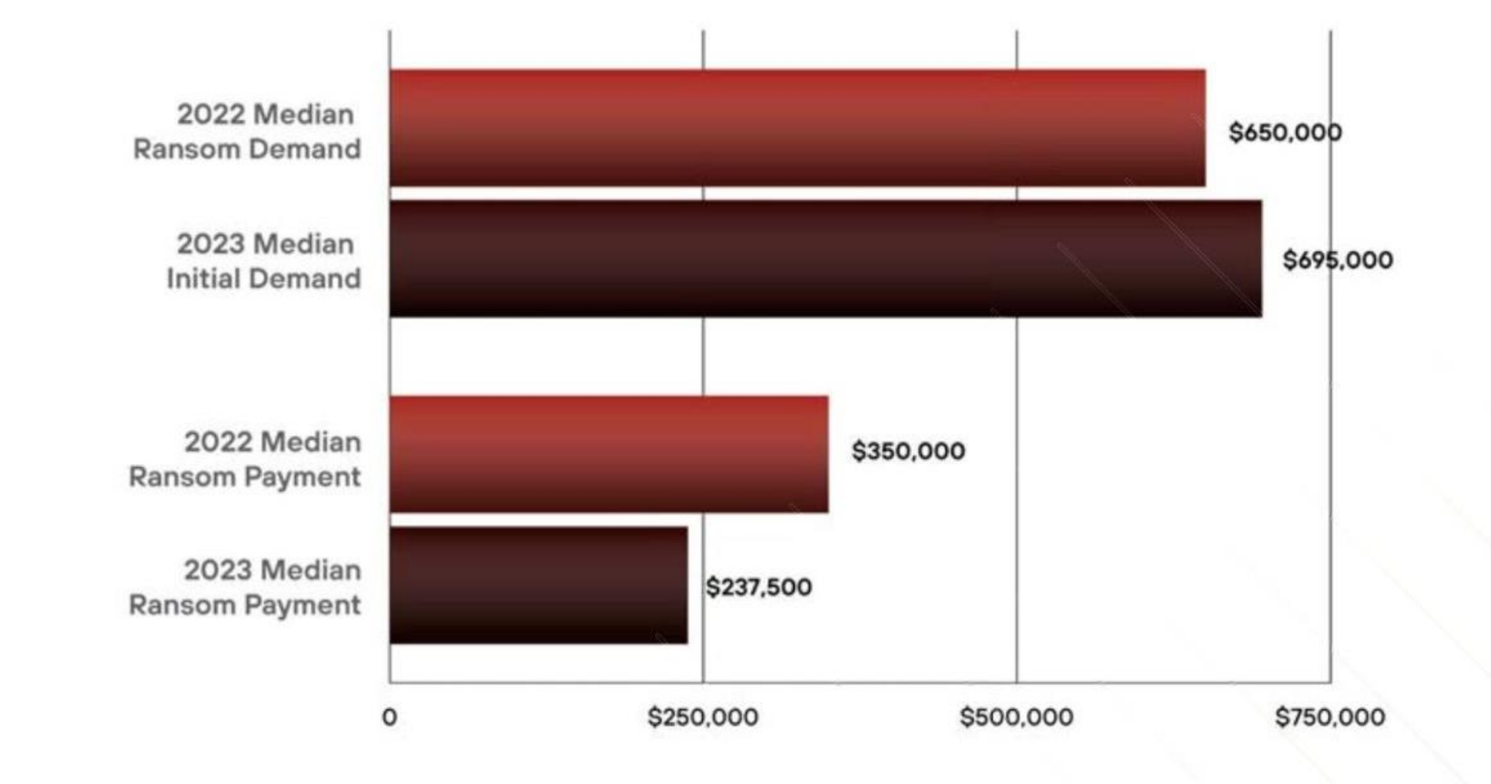
- Ransomware.
- Phishing.
- Compromised Credentials.
- Third-Party Credentials.
- Data Breaches.



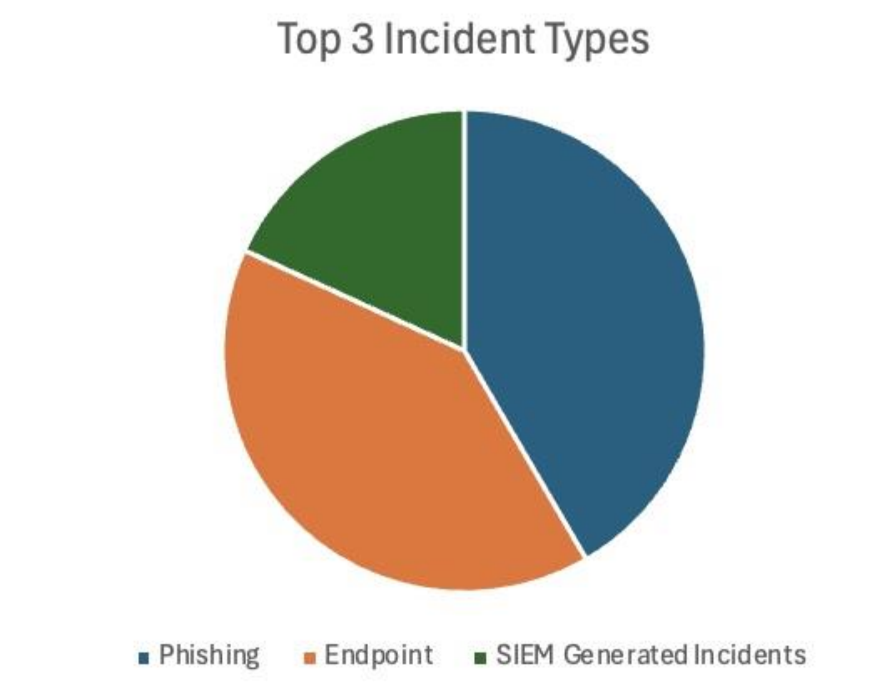
Do attackers keep their promises once they have been paid?

While in general it is best not to make payments in response to extortion, in cases where payment was made, we observed that attackers kept their promises more often than not.

Decrease in median ransom payment from 2022 to 2023



Spotit SOC numbers | Attack Types



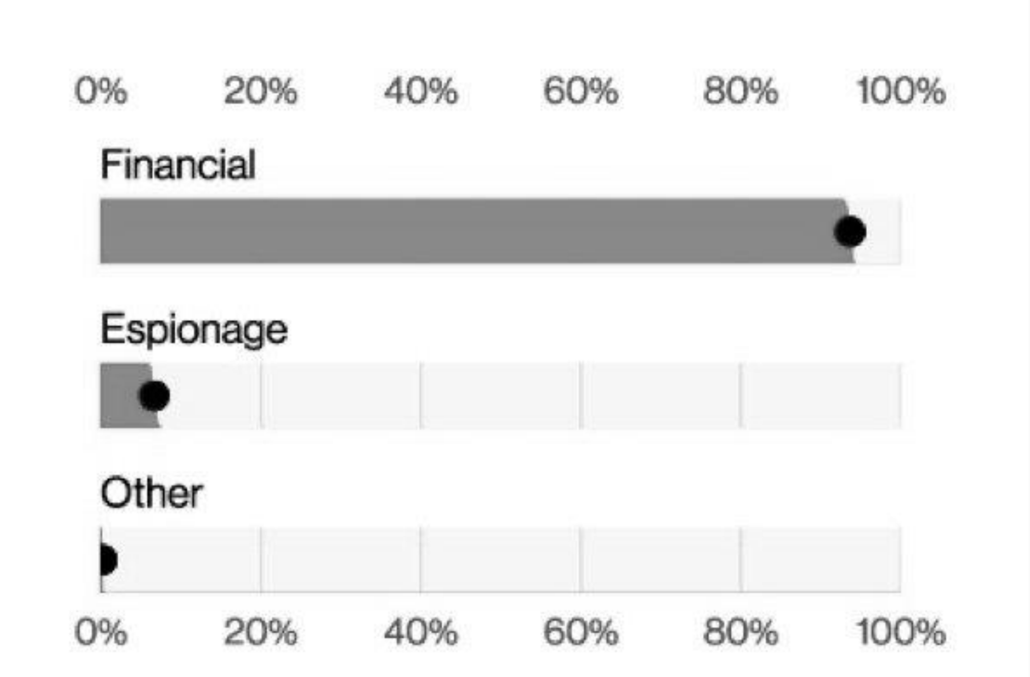
Endpoint (malware, ransomware).

Phishing.

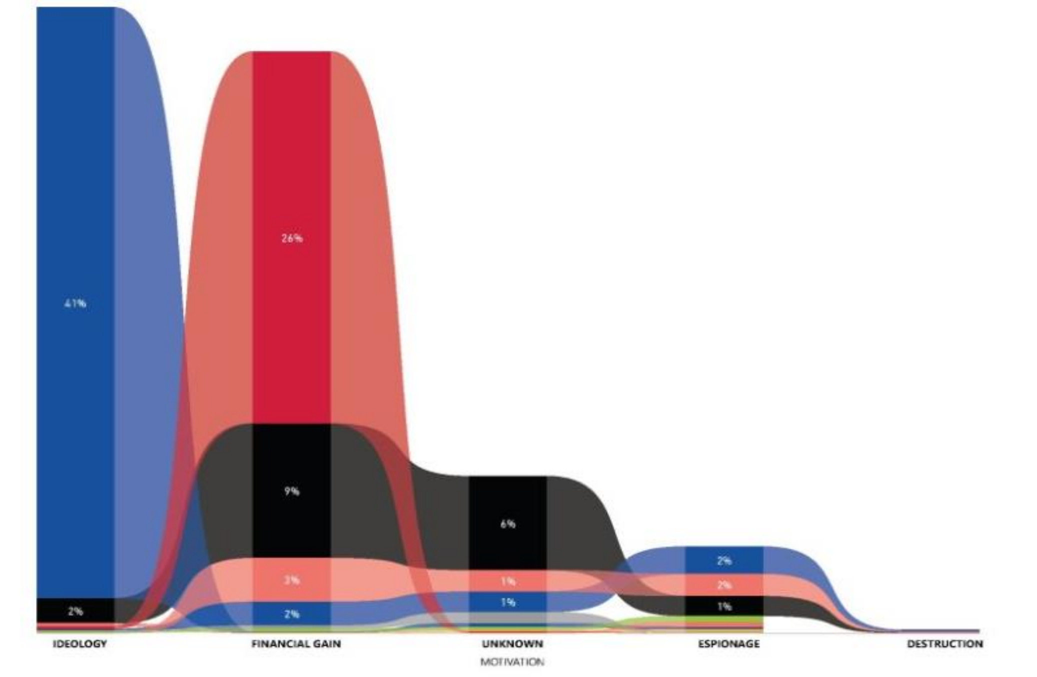
Compromised Credentials.

Victims

Victims and impact | Motives



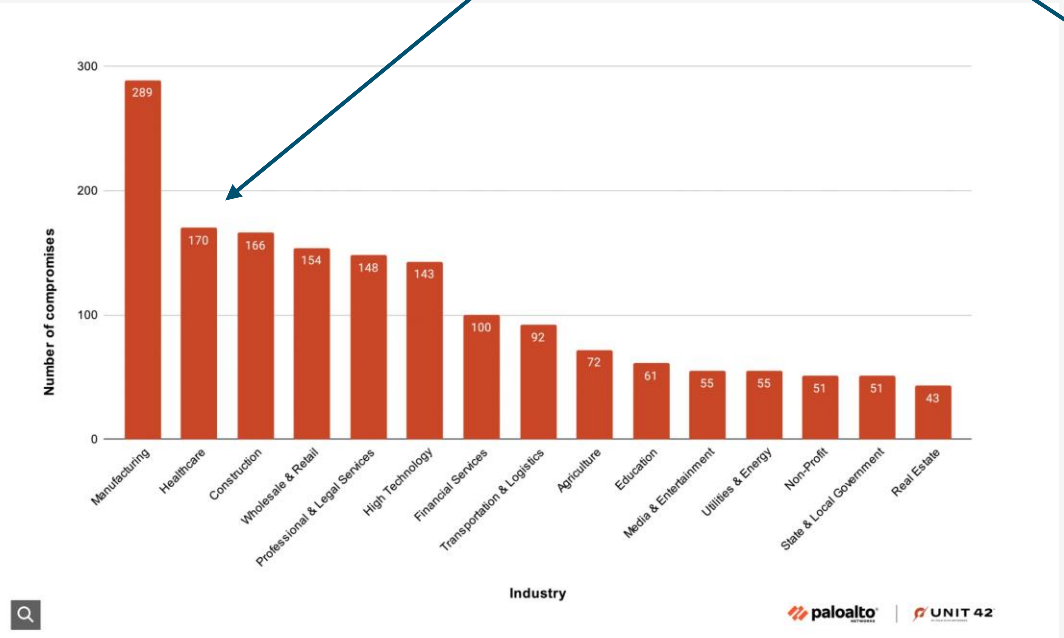
Threat actors' motives in breaches (n=5,632).

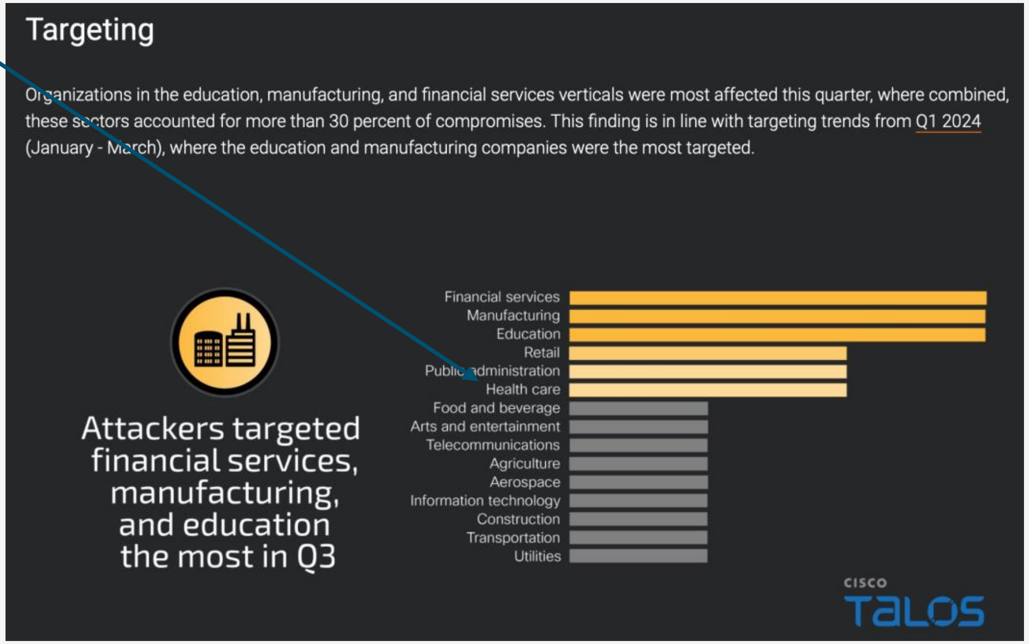


Motivation of threat actors per threat category.

Victims and impact | Targeting

healthcare



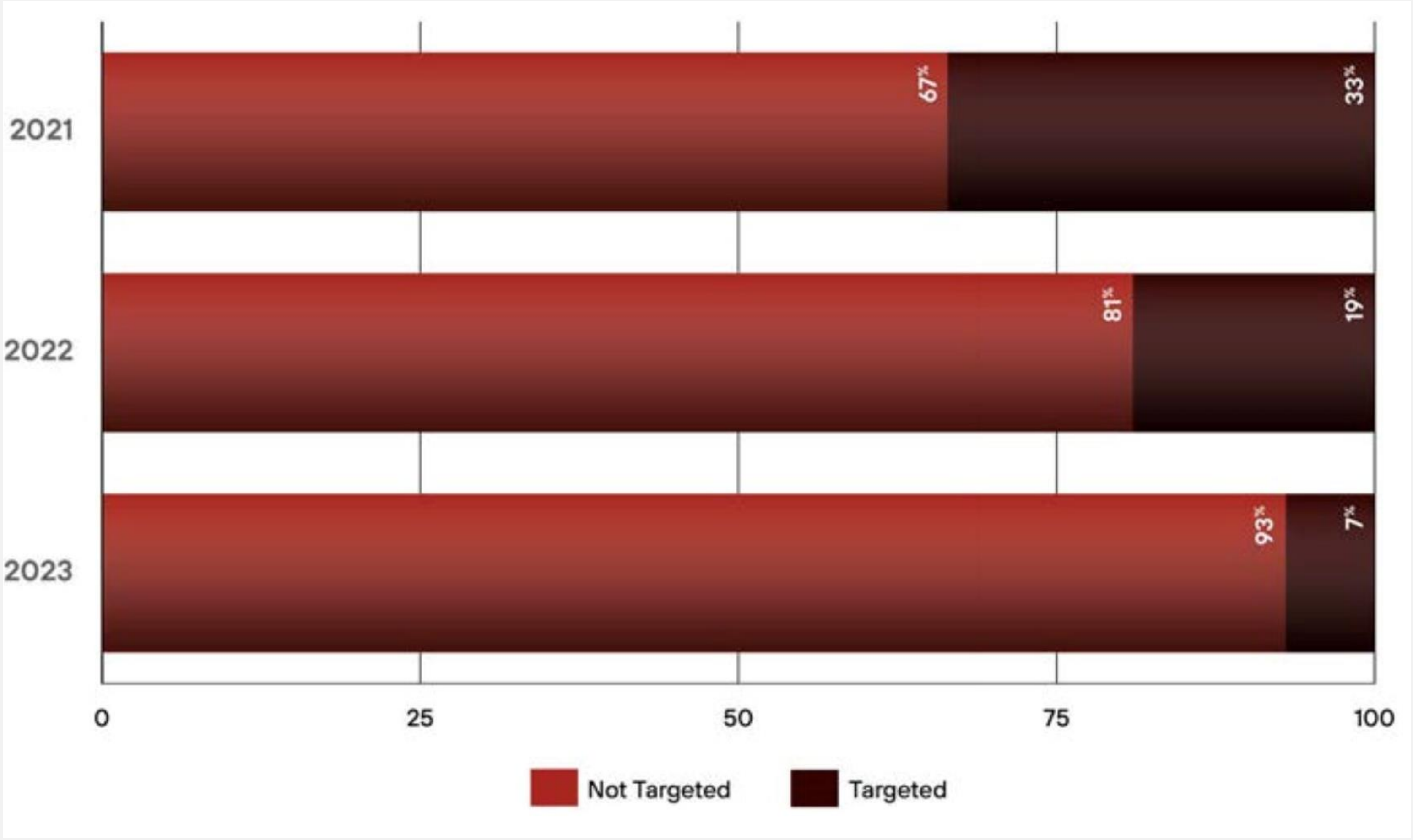


Targeting

Organizations in the education, manufacturing, and financial services verticals were most affected this quarter, where combined, these sectors accounted for more than 30 percent of compromises. This finding is in line with targeting trends from Q1 2024 (January - March), where the education and manufacturing companies were the most targeted.

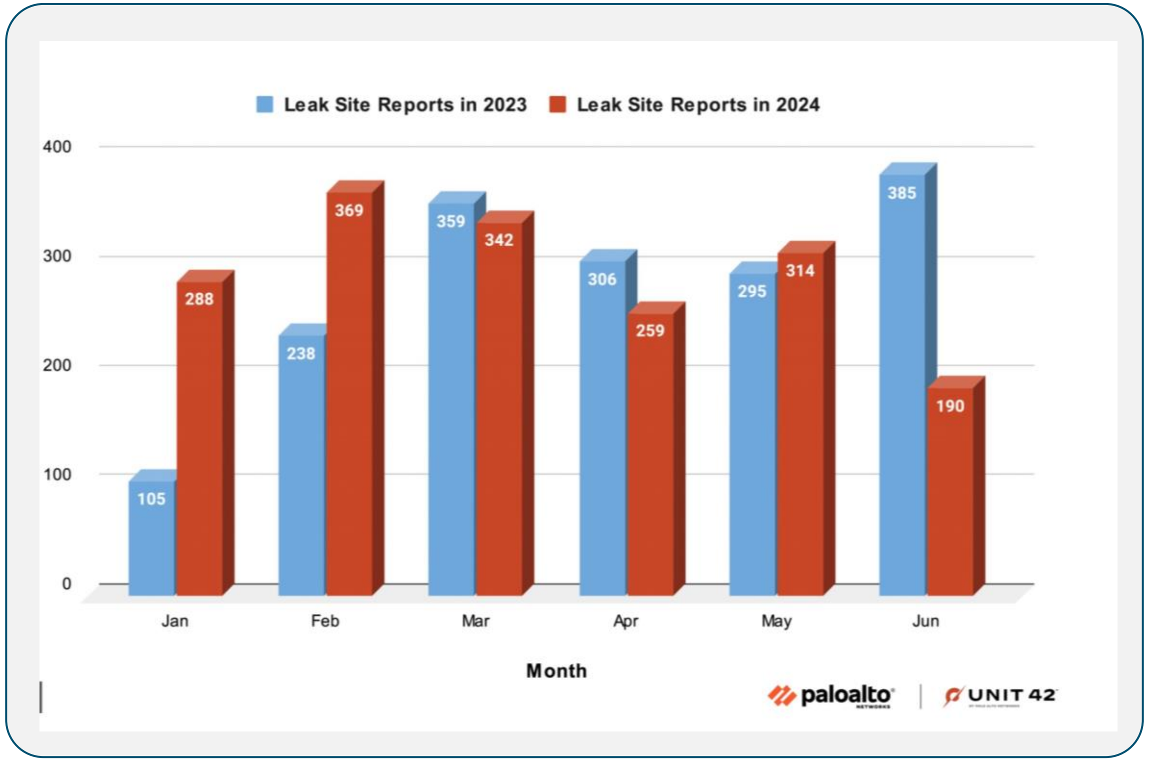
Attackers targeted financial services, manufacturing, and education the most in Q3

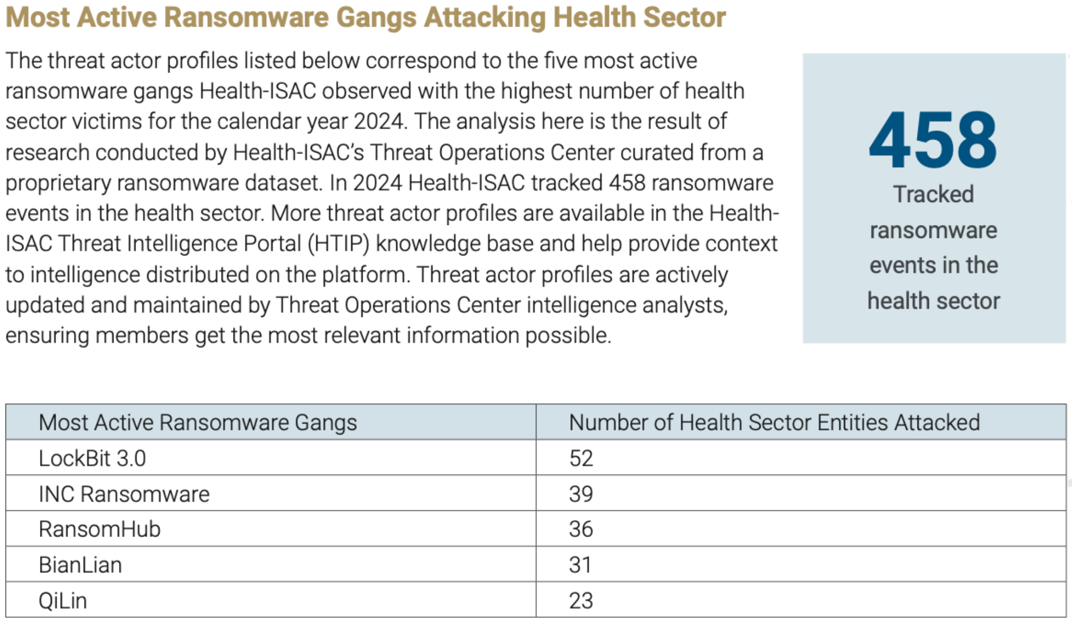
Non-targeted data theft dominated in 2023



Victims and impact | Arrest

We observed a notable decrease in ransomware leak site reports in June of 2024. Significant decreases in activity on the LockBit and 8Base leak sites largely accounted for this drop.





Most Active Ransomware Gangs Attacking Health Sector

The threat actor profiles listed below correspond to the five most active ransomware gangs Health-ISAC observed with the highest number of health sector victims for the calendar year 2024. The analysis here is the result of research conducted by Health-ISAC's Threat Operations Center curated from a proprietary ransomware dataset. In 2024 Health-ISAC tracked 458 ransomware events in the health sector. More threat actor profiles are available in the Health-ISAC Threat Intelligence Portal (HTIP) knowledge base and help provide context to intelligence distributed on the platform. Threat actor profiles are actively updated and maintained by Threat Operations Center intelligence analysts, ensuring members get the most relevant information possible.

458
Tracked ransomware events in the health sector

Most Active Ransomware Gangs	Number of Health Sector Entities Attacked
LockBit 3.0	52
INC Ransomware	39
RansomHub	36
BianLian	31
QiLin	23

Wrap up

Healthcare sector is a prime target for cyberattacks

3 reasons why

Valuable data.

Critical systems.

Underinvestment in security

*Healthcare organizations are a gold mine for cybercriminals engaged in identity theft, insurance fraud, or the sale of data on the dark web.

How they get in? wrap up

Most frequent attack vectors

- Social Engineering.
- Vulnerability exploits.
- Credentials / Lacking MFA.

In relation to attack surface

Vulnerabilities exploited on

- Exposed IT infrastructure.
- Remote access service.

Credentials / MFA lacking on

- Exposed IT infrastructure.
- Remote access services.
- Business applications.

Nearly 75% of exposed attack surface consist of:

→ Lack of firewalls. Inadequate network controls.

→ Poor authentication.

> You don’t need eyes to see, you need vision.

By Maxi Jazz (Faithless)

Cisco Security for Healthcare

Addressing Key Threats in Healthcare

Gert Tilburgs – Systems Engineer Security @ Cisco

Health sector

RECAP

Cybercriminals Exploit Healthcare Vulnerabilities: Key Threats & Defense Strategies

- Phishing.
- Insider threats.
- Medical device vulnerabilities.
- Ransomware.

Use Case 1: Insider Threats

Malicious endpoint on network

Phishing email

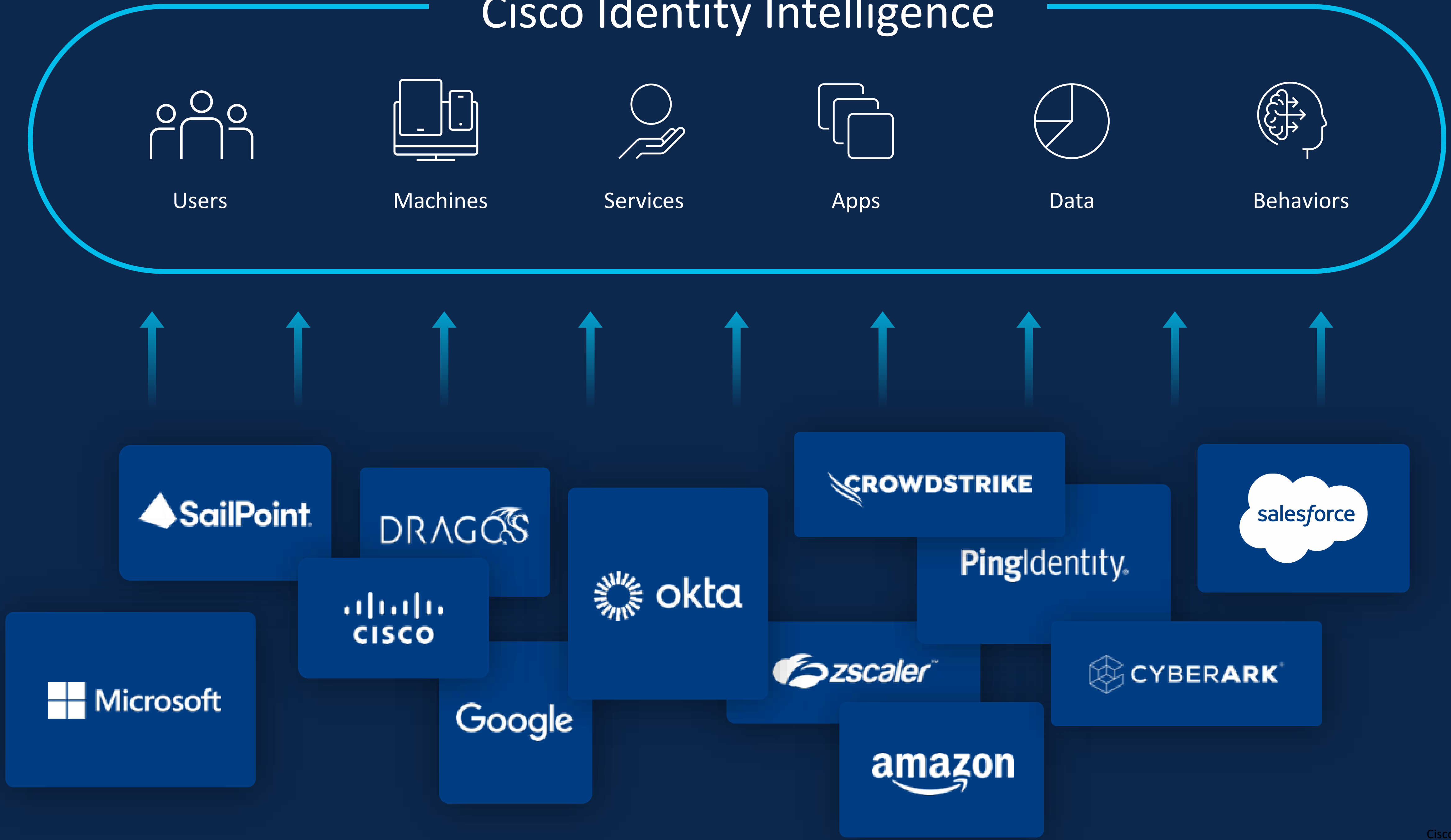
MFA attack

Social Engineering

Malicious website

Stolen credentials

Cisco Identity Intelligence



Users

Machines

Services

Apps

Data

Behaviors

Cisco Identity Intelligence

User 360 View

The user details is known as the “user 360 view”

A true look at the user’s identity related security, activity, posture and other important properties.

Activity Flow

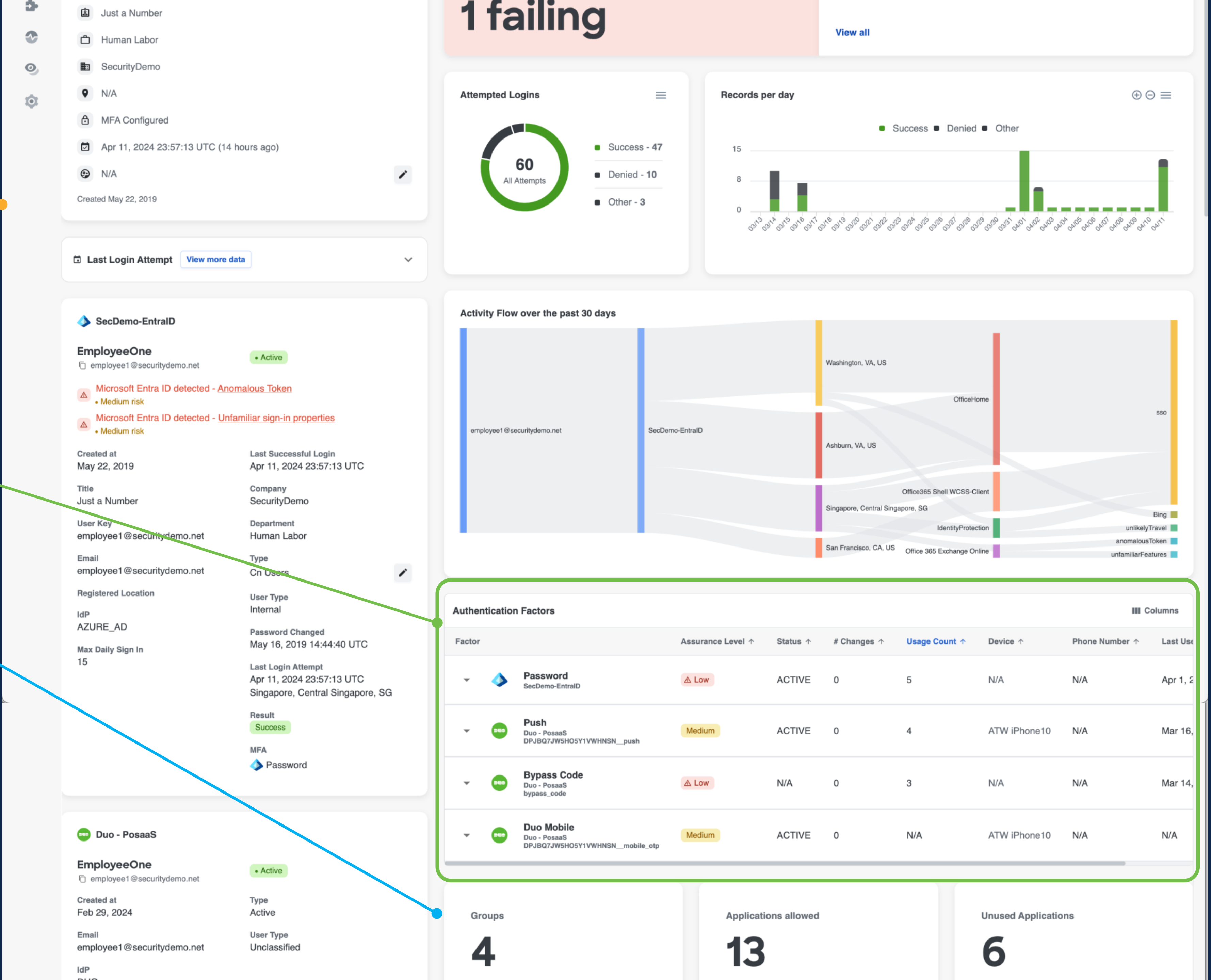
Combined view of the user's activity patterns. Easily spot when deviations have occurred

Combined Auth Log

Combined view of the users authentications and factors across all the integrated IdPs

Key Benefits

- Eliminate dormant accounts
- Highlight MFA gaps
- Reduce excessive admin privileges
- License Validation



Just a Number
Human Labor
SecurityDemo
N/A
MFA Configured
Apr 11, 2024 23:57:13 UTC (14 hours ago)
N/A
Created May 22, 2019

Last Login Attempt View more data

SecDemo-EntraID

EmployeeOne • Active
employee1@securitydemo.net

Microsoft Entra ID detected - Anomalous Token
• Medium risk

Microsoft Entra ID detected - Unfamiliar sign-in properties
• Medium risk

Created at: May 22, 2019
Last Successful Login: Apr 11, 2024 23:57:13 UTC
Title: Just a Number
Company: SecurityDemo
User Key: employee1@securitydemo.net
Department: Human Labor
Email: employee1@securitydemo.net
Type: Cn Users
Registered Location
User Type: Internal
IdP: AZURE_AD
Password Changed: May 16, 2019 14:44:40 UTC
Max Daily Sign In: 15
Last Login Attempt: Apr 11, 2024 23:57:13 UTC
Singapore, Central Singapore, SG
Result: Success
MFA: Password

Duo - PosaaS

EmployeeOne • Active
employee1@securitydemo.net

Created at: Feb 29, 2024
Type: Active
Email: employee1@securitydemo.net
User Type: Unclassified
IdP

1 failing

View all

Attempted Logins

60
All Attempts

- Success - 47
- Denied - 10
- Other - 3

Records per day

Activity Flow over the past 30 days

Authentication Factors

Columns

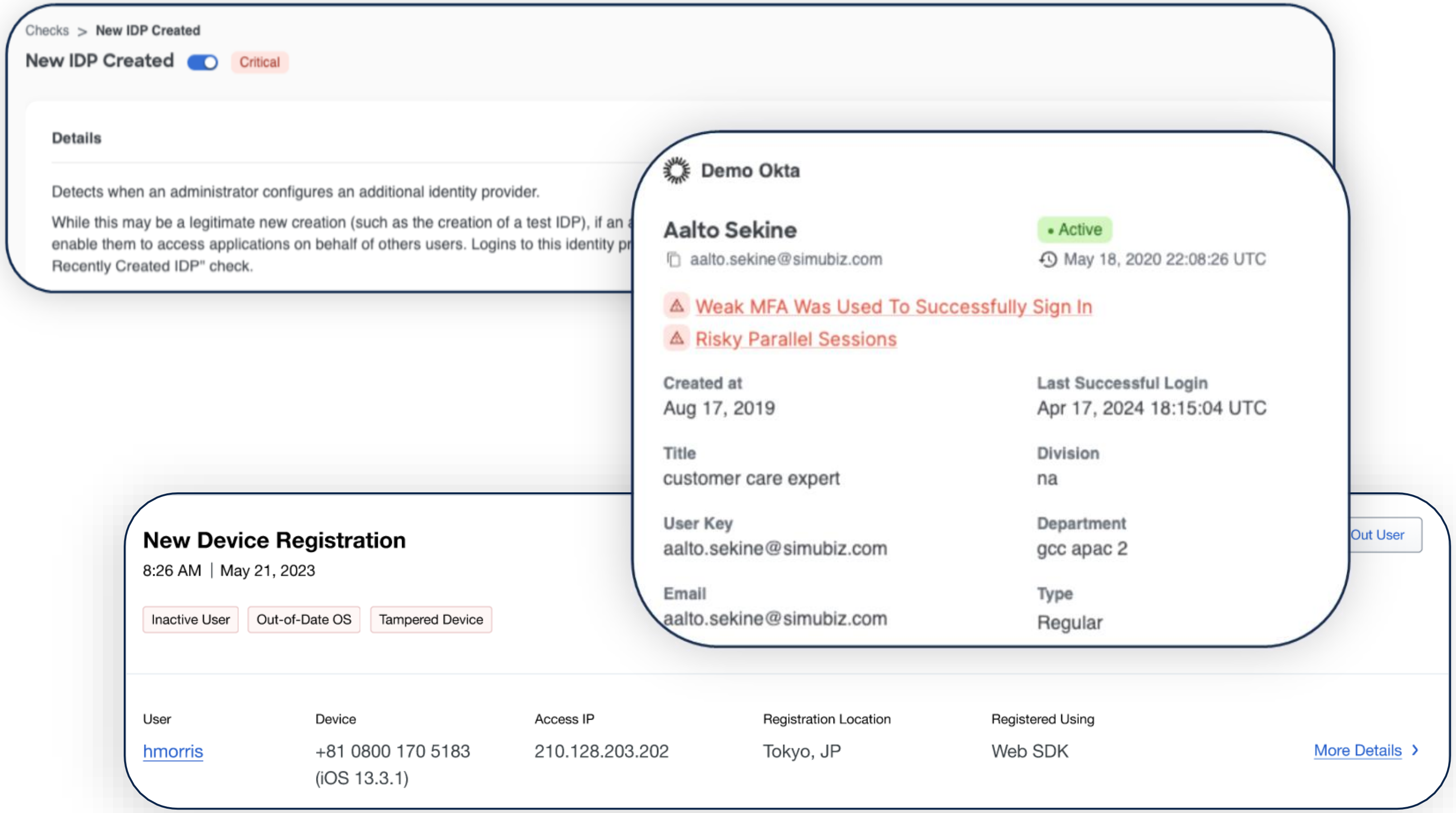
Factor	Assurance Level ↑	Status ↑	# Changes ↑	Usage Count ↑	Device ↑	Phone Number ↑	Last Use
Password SecDemo-EntraID	⚠ Low	ACTIVE	0	5	N/A	N/A	Apr 1, 2
Push Duo - PosaaS DPJBQ7JW5HO5Y1VWHNSN__push	Medium	ACTIVE	0	4	ATW iPhone10	N/A	Mar 16,
Bypass Code Duo - PosaaS bypass_code	⚠ Low	N/A	0	3	N/A	N/A	Mar 14,
Duo Mobile Duo - PosaaS DPJBQ7JW5HO5Y1VWHNSN__mobile_otp	Medium	ACTIVE	0	N/A	ATW iPhone10	N/A	N/A

Groups
4

Applications allowed
13

Unused Applications
6

Detect: Correlate identity data, detect attack patterns



Checks > New IDP Created

New IDP Created Critical

Details

Detects when an administrator configures an additional identity provider.

While this may be a legitimate new creation (such as the creation of a test IDP), if an
enable them to access applications on behalf of others users. Logins to this identity pr
Recently Created IDP" check.

Demo Okta

Aalto Sekine • Active

aalto.sekine@simubiz.com

May 18, 2020 22:08:26 UTC

⚠ Weak MFA Was Used To Successfully Sign In

⚠ Risky Parallel Sessions

Created at Aug 17, 2019	Last Successful Login Apr 17, 2024 18:15:04 UTC
Title customer care expert	Division na
User Key aalto.sekine@simubiz.com	Department gcc apac 2
Email aalto.sekine@simubiz.com	Type Regular

New Device Registration

8:26 AM | May 21, 2023

Inactive User | Out-of-Date OS | Tampered Device

User	Device	Access IP	Registration Location	Registered Using
hmorris	+81 0800 170 5183 (iOS 13.3.1)	210.128.203.202	Tokyo, JP	Web SDK

Threat Insights

Cross-platform identity context feeds dedicated threat detection engine that is optimized and managed by experts

Smart Detection

Leverage AI and ML to highlight anomalous and suspicious identity behavior

Coverage Mapping

Easily map threats to security frameworks like Mitre ATT&CK and CIS

Secure Any Corporate Application using DUO

Proprietary Apps (APIs)

C# · Java · python · node JS · Ruby

Microsoft Environments

Microsoft Forefront · Windows · Office 365 · Microsoft Active Directory Federation Services · Microsoft Active Directory · Outlook

Cloud Services

Active Directory Federation Services · Centrify · onelogin · okta · PingIdentity

Unix Devices (SSH Sessions)

FreeBSD · Linux · redhat · ubuntu

Internal Applications (VPNs)

OPENVPN · paloalto NETWORKS · Array NETWORKS · Check Point SOFTWARE TECHNOLOGIES LTD · Barracuda · f5 · FORTINET · cisco · JUNIPER NETWORKS

Cloud Applications

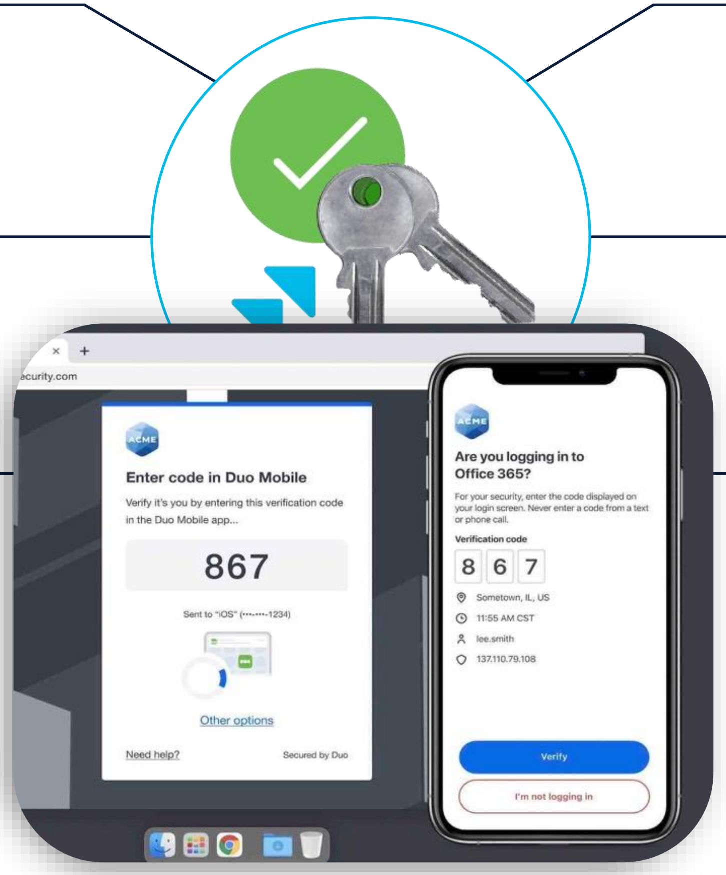
Dropbox · salesforce · Google Apps · workday · amazon web services · box · Office 365 · Cisco webex · slack

Web Applications

splunk> · Drupal · Atlassian Confluence · WordPress · Atlassian JIRA · Shibboleth

SAML 2.0 Applications

Google Apps · amazon web services · Office 365 · salesforce · box



Enter code in Duo Mobile

Verify it's you by entering this verification code in the Duo Mobile app...

867

Sent to "iOS" (•••-•••-1234)

Other options

Need help?

Secured by Duo

Are you logging in to Office 365?

For your security, enter the code displayed on your login screen. Never enter a code from a text or phone call.

Verification code

8 6 7

Sometown, IL, US

11:55 AM CST

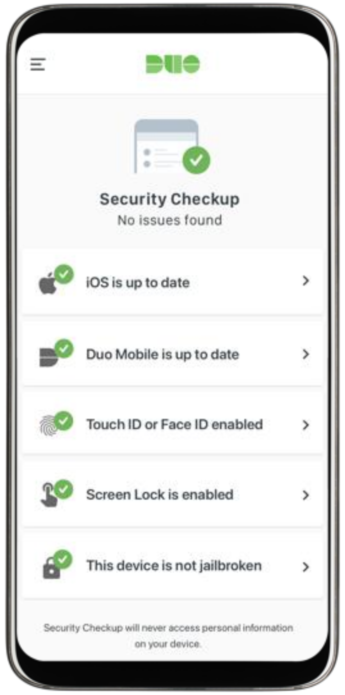
lee.smith

137.110.79.108

Integration documents are available at duo.com/docs

Protect your device

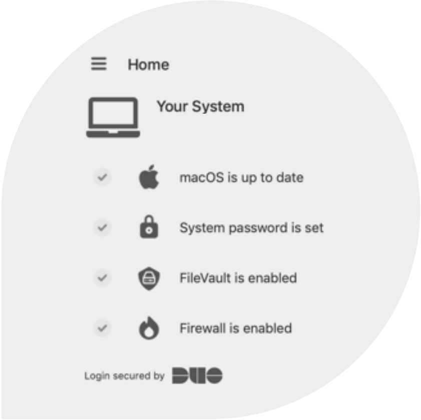
Establish device trust before granting access



Security Checkup
No issues found

- iOS is up to date
- Duo Mobile is up to date
- Touch ID or Face ID enabled
- Screen Lock is enabled
- This device is not jailbroken

Security Checkup will never access personal information on your device.



Home

Your System

- ✓ macOS is up to date
- ✓ System password is set
- ✓ FileVault is enabled
- ✓ Firewall is enabled

Login secured by DUO

Check Device Health

Assess Security Posture

Deny access to compromised or out of compliance devices

Guide Self-Remediation

Eliminate vulnerabilities and lower IT costs by empowering users to remediate their device

Verify Endpoint Trust

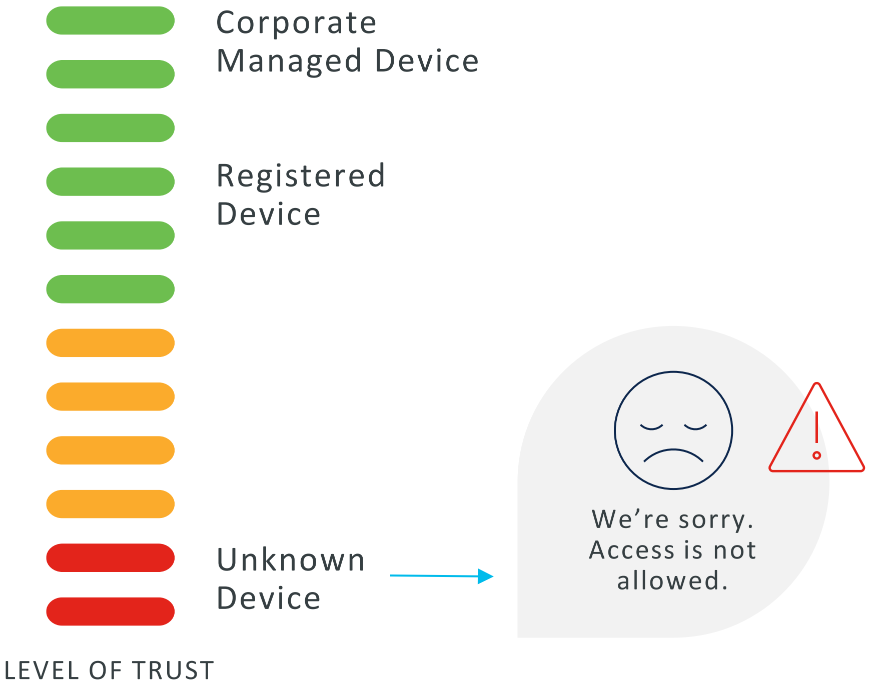
Block access from unmanaged and unknown devices

Provide Complete Visibility

Gain complete visibility into all laptops and mobile devices accessing your resources

Allow only Registered devices

Block attackers by only allowing registered and managed devices to gain access to corporate resources



Block Attackers

Only allow registered or managed devices to gain access to corporate apps and resources

Control Device Access

Give organizations control over which devices can access corporate apps and resources

Cover BYOD

Safely allow BYOD and 3rd party devices without requiring Mobile Device Management software

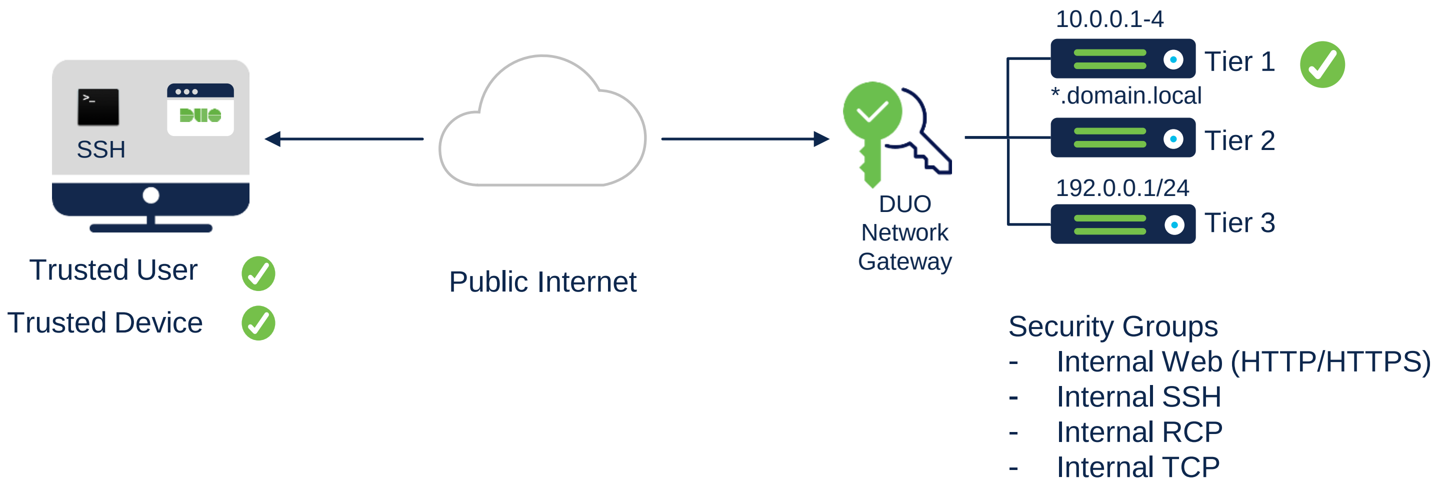
Mitigate Risk

When limited authenticator options are available

VPN-less access using Duo Network Gateway

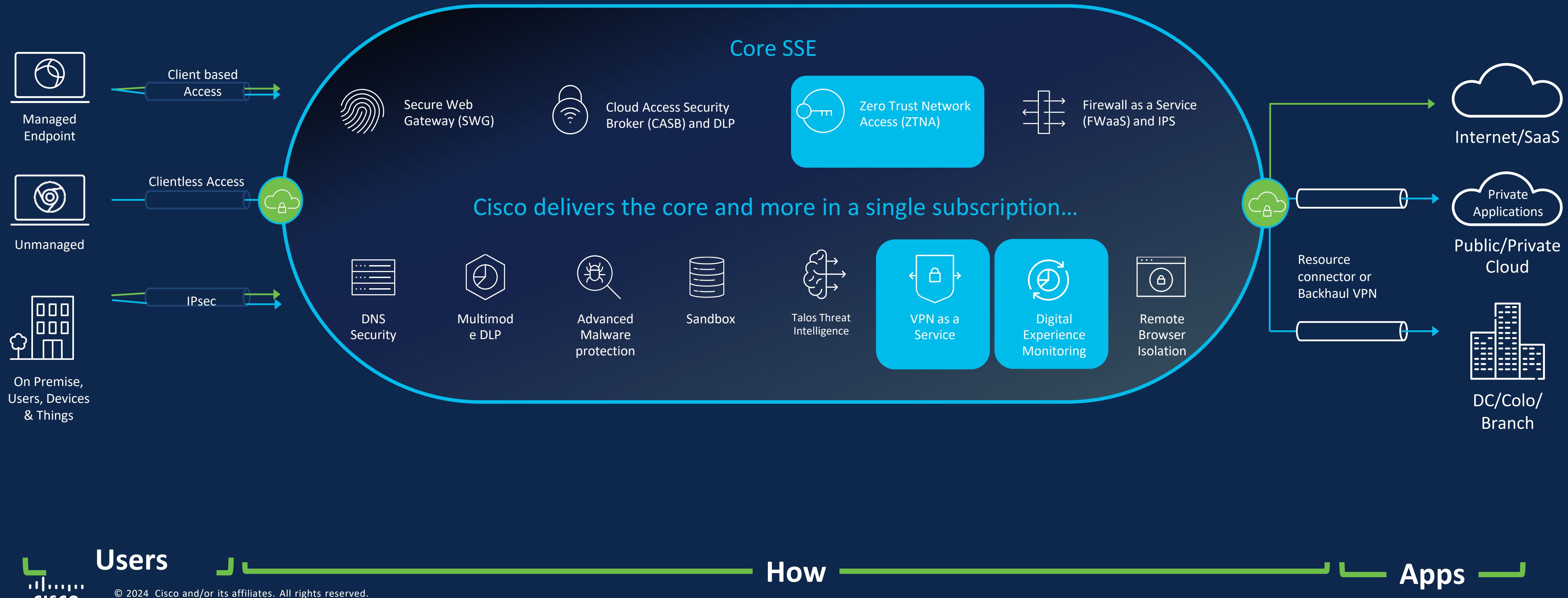
- ✓ Consistent user experience accessing apps regardless of network location
- ✓ Applies zero trust security principles, verifying every user (with MFA) and device before allowing access
- ✓ Does not allow full network access, only application or resource specific access (web apps, SSH, RDP, TCP, etc.).
- ✓ Supports managed and *unmanaged* devices (BYOD) with Granular Policies
- ✓ Enables agentless security posture checking of devices

Utilizes user and device context for proxying access to any application without full VPN



Cisco Secure Access

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

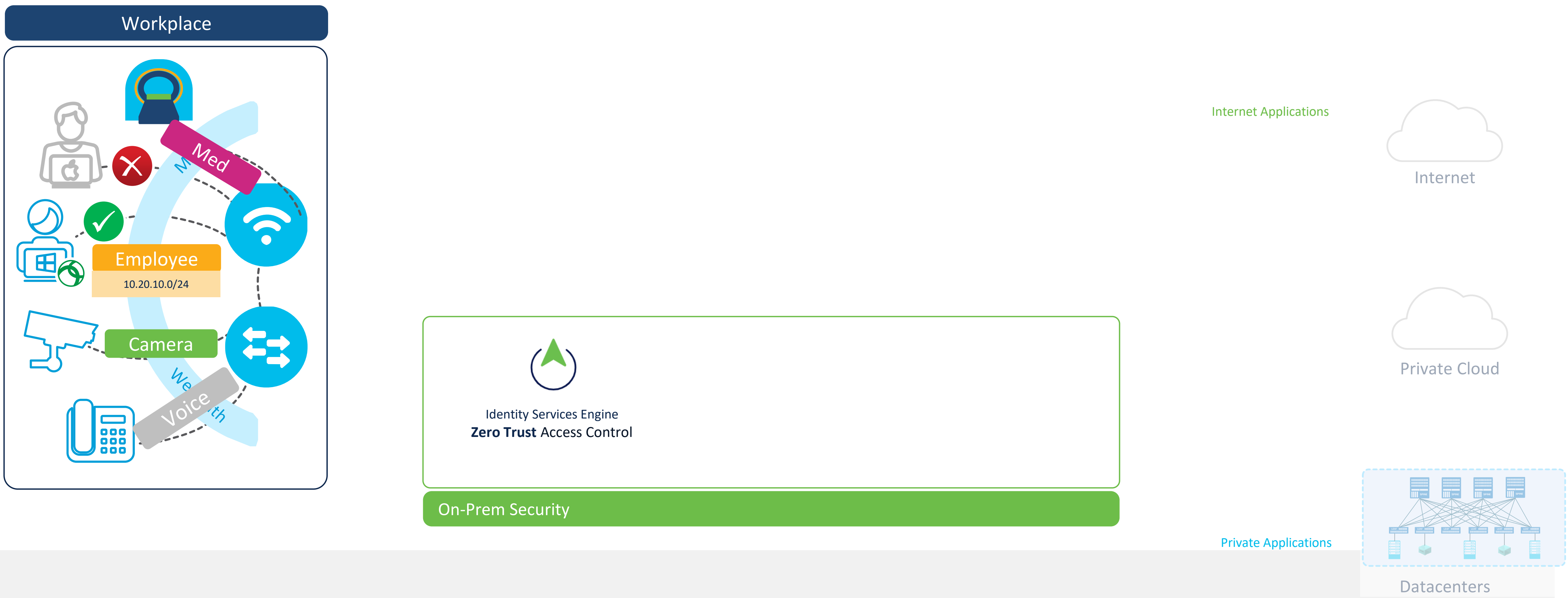


Managed Endpoint
Client based Access
Unmanaged
Clientless Access
On Premise, Users, Devices & Things
IPsec
Core SSE
Secure Web Gateway (SWG)
Cloud Access Security Broker (CASB) and DLP
Zero Trust Network Access (ZTNA)
Firewall as a Service (FWaaS) and IPS
Cisco delivers the core and more in a single subscription…
DNS Security
Multimod e DLP
Advanced Malware protection
Sandbox
Talos Threat Intelligence
VPN as a Service
Digital Experience Monitoring
Remote Browser Isolation
Resource connector or Backhaul VPN
Internet/SaaS
Private Applications
Public/Private Cloud
DC/Colo/ Branch
Users
How
Apps

Use Case 2: Vulnerabilities?

Threat-centric Network Access Control

Segmentation & Inspection on the Network



Identity Services Engine

Policy Server for Network Access Control

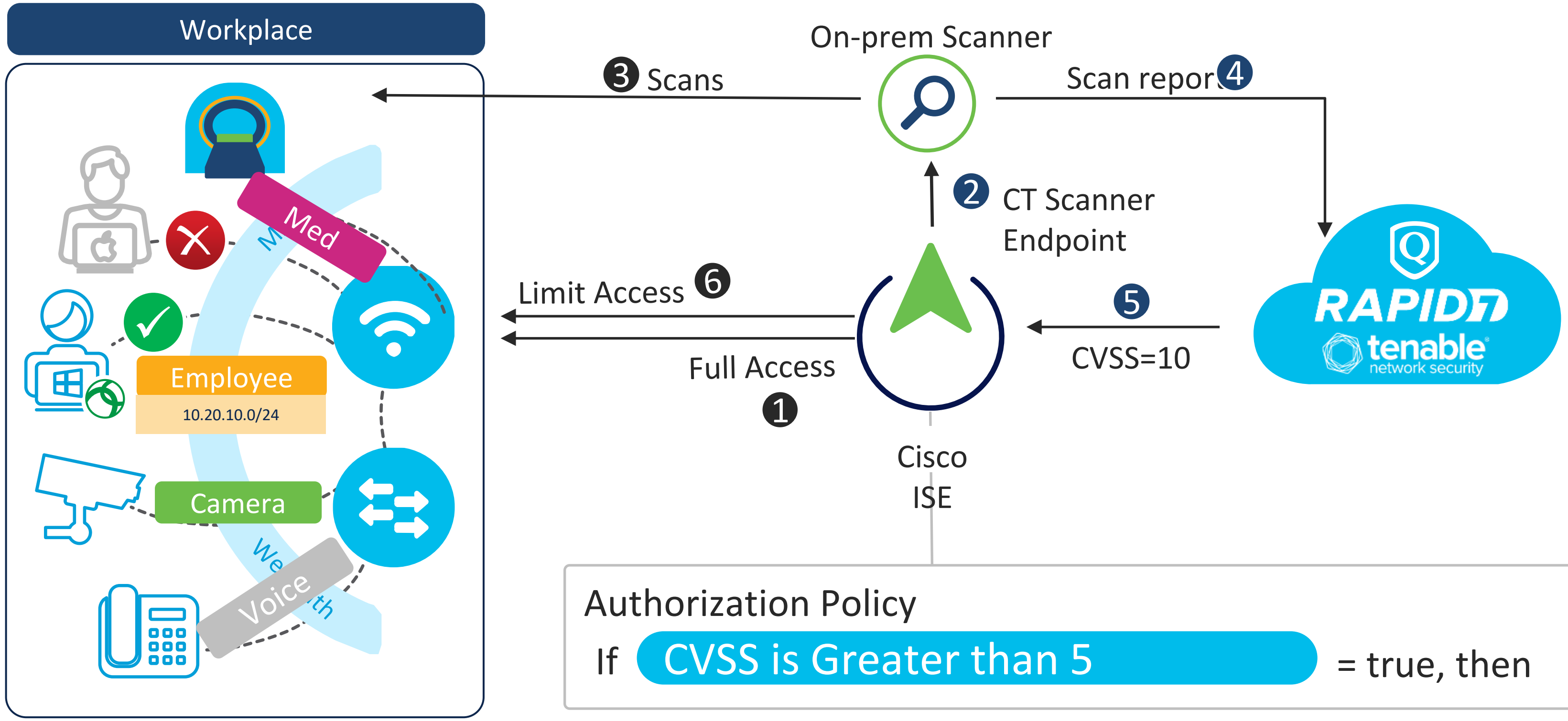
Authentication

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

Threat-centric Network Access Control

Segmentation based on CVSS Score

Shield Risk Scoring!



Workplace

Med

Employee

10.20.10.0/24

Camera

Voice

On-prem Scanner

3 Scans

Scan report 4

2 CT Scanner Endpoint

Limit Access 6

Full Access

1

5

CVSS=10

RAPID7

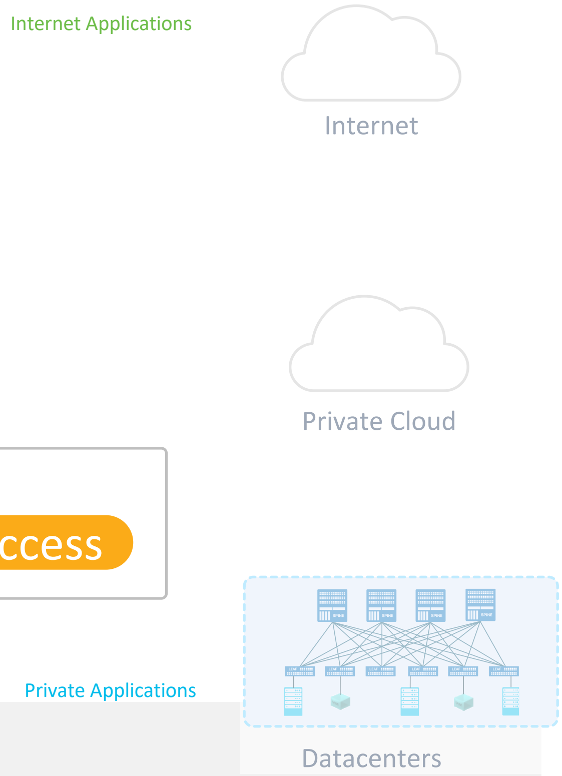
tenable network security

Cisco ISE

Authorization Policy

If CVSS is Greater than 5 = true, then Limit Access

CVSS: Common Vulnerability Scoring System



Identity Services Engine

Policy Server for Network Access Control

Context

Define network permission based on external context.

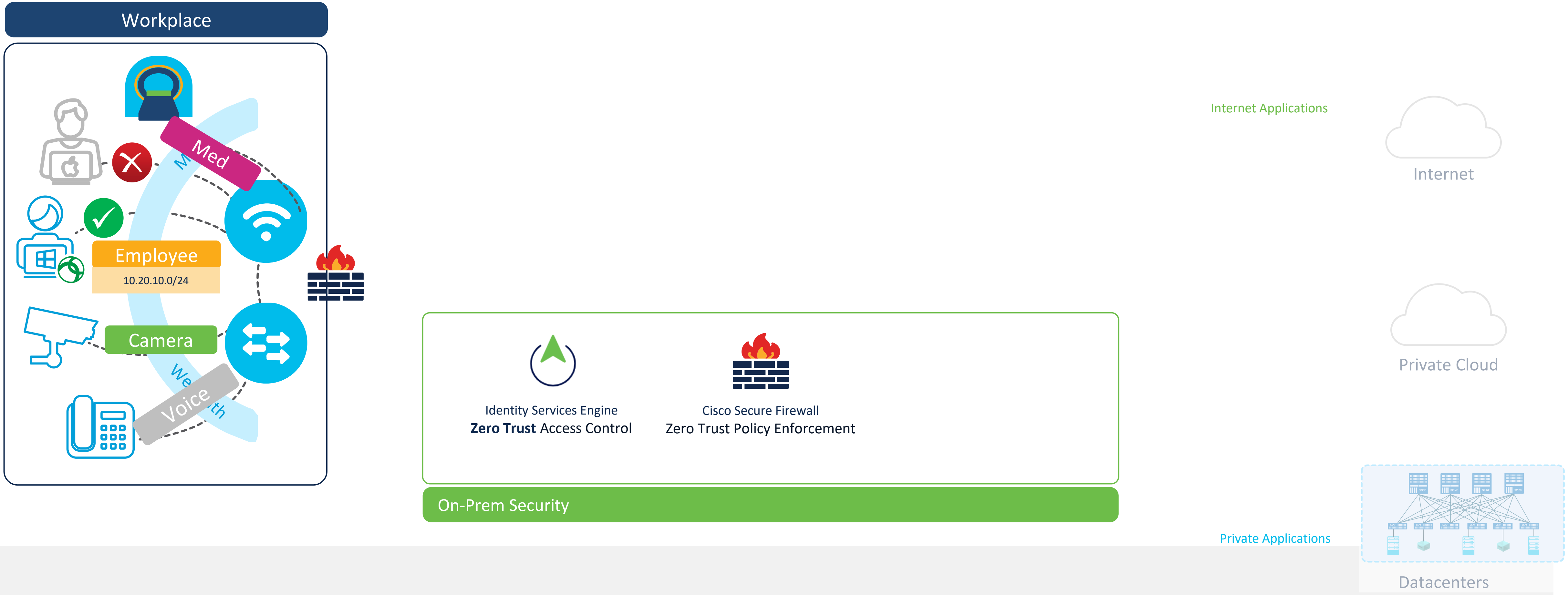
Authentication

802.1x & MAB

Limiting the network to Trusted devices only.

Inspecting for malicious intent

Intrusion Prevention System on Cisco FTD



Identity Services Engine

Policy Server for Network Access Control

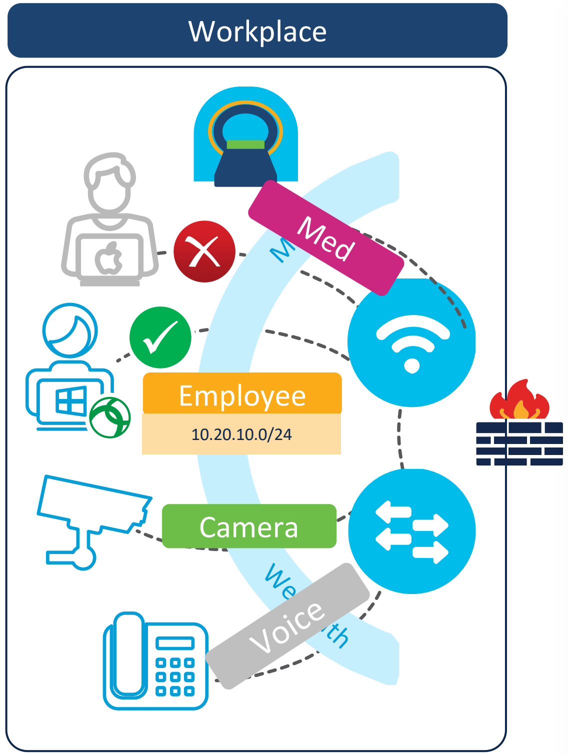
Authentication

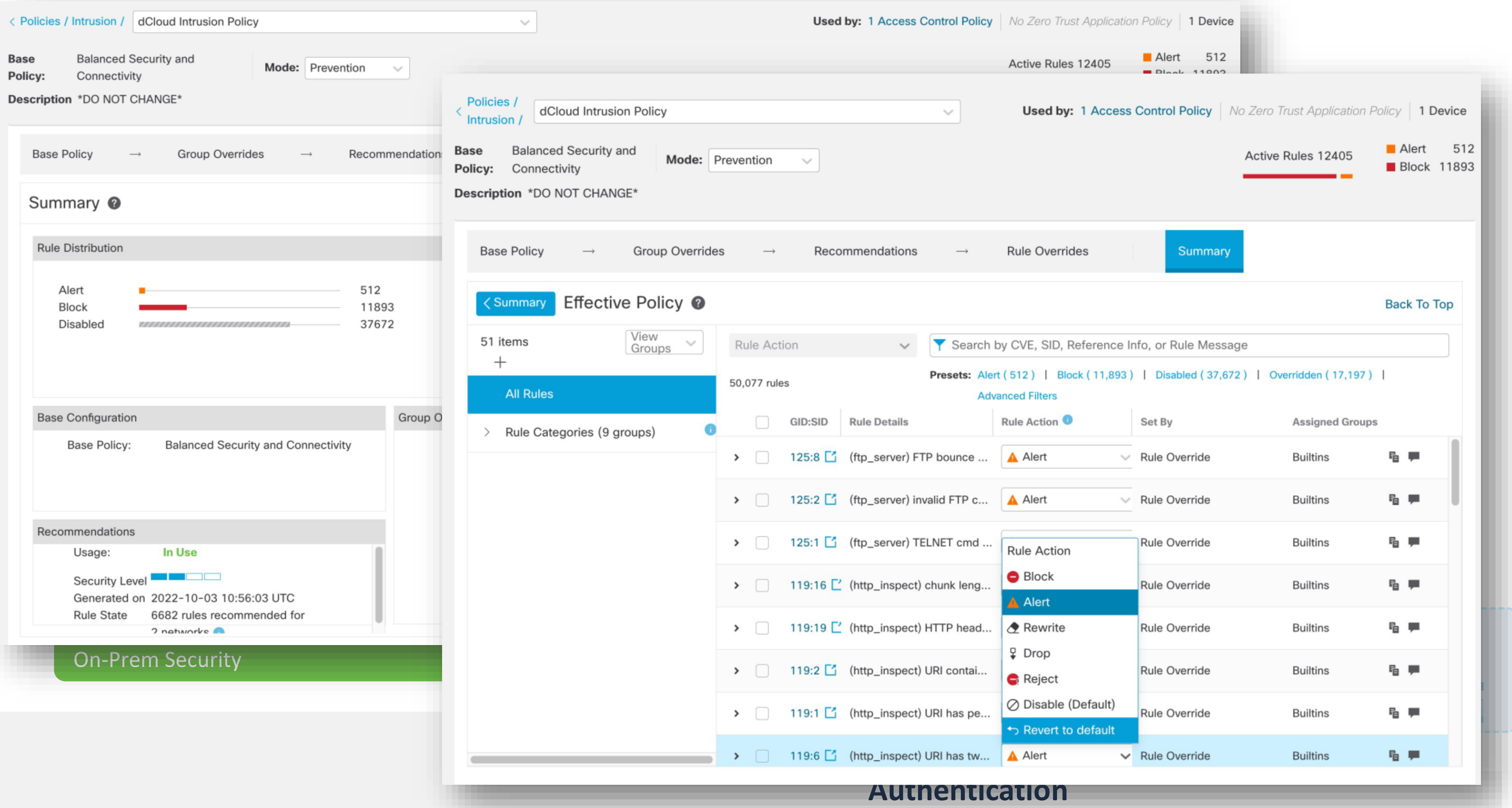
802.1x & MAB

Limiting the network to Trusted devices only.

Campus: Establishing & Enforcing Trust

Segmentation & Inspection on the Network





< Policies / Intrusion / dCloud Intrusion Policy

Used by: 1 Access Control Policy | No Zero Trust Application Policy | 1 Device

Base Policy: Balanced Security and Connectivity

Mode: Prevention

Description *DO NOT CHANGE*

Active Rules 12405 — Alert 512

Base Policy → Group Overrides → Recommendations

Summary

Rule Distribution

Alert	512
Block	11893
Disabled	37672

Base Configuration

Base Policy: Balanced Security and Connectivity

Group O

Recommendations

Usage: In Use

Security Level

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

Rule State 6682 rules recommended for 2 networks

< Policies / Intrusion / dCloud Intrusion Policy

Used by: 1 Access Control Policy | No Zero Trust Application Policy | 1 Device

Base Policy: Balanced Security and Connectivity

Mode: Prevention

Description *DO NOT CHANGE*

Active Rules 12405

Alert 512
Block 11893

Base Policy → Group Overrides → Recommendations → Rule Overrides | Summary

< Summary Effective Policy

Back To Top

51 items | View Groups

All Rules

Rule Categories (9 groups)

Rule Action | Search by CVE, SID, Reference Info, or Rule Message

50,077 rules

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

Advanced Filters

GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
125:8	(ftp_server) FTP bounce ...	Alert	Rule Override	Builtins
125:2	(ftp_server) invalid FTP c...	Alert	Rule Override	Builtins
125:1	(ftp_server) TELNET cmd ...		Rule Override	Builtins
119:16	(http_inspect) chunk leng...		Rule Override	Builtins
119:19	(http_inspect) HTTP head...		Rule Override	Builtins
119:2	(http_inspect) URI contai...		Rule Override	Builtins
119:1	(http_inspect) URI has pe...		Rule Override	Builtins
119:6	(http_inspect) URI has tw...	Alert	Rule Override	Builtins

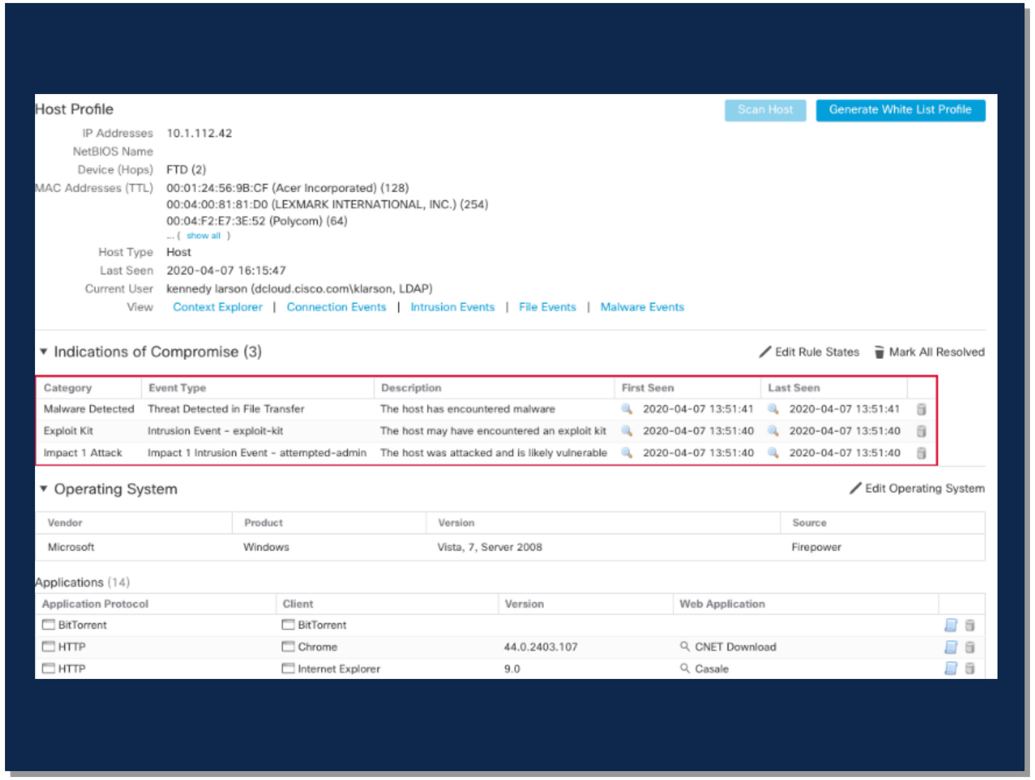
On-Prem Security

Identity Services Engine
Policy Server for Network Access Control

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

Correlate Host Profile and IPS

Drive impact analysis and rule recommendations



Host Profile

IP Addresses	10.1.112.42
NetBIOS Name	
Device (Hops)	FTD (2)
MAC Addresses (TTL)	00:01:24:56:9B:CF (Acer Incorporated) (128) 00:04:00:81:81:D0 (LEXMARK INTERNATIONAL, INC.) (254) 00:04:F2:E7:3E:52 (Polycom) (64) ... (show all)
Host Type	Host
Last Seen	2020-04-07 16:15:47
Current User	kennedy larson (dcloud.cisco.com\klarson, LDAP)
View	Context Explorer | Connection Events | Intrusion Events | File Events | Malware Events

▼ Indications of Compromise (3)

Category	Event Type	Description	First Seen	Last Seen
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2020-04-07 13:51:41	2020-04-07 13:51:41
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2020-04-07 13:51:40	2020-04-07 13:51:40
Impact 1 Attack	Impact 1 Intrusion Event - attempted-admin	The host was attacked and is likely vulnerable	2020-04-07 13:51:40	2020-04-07 13:51:40

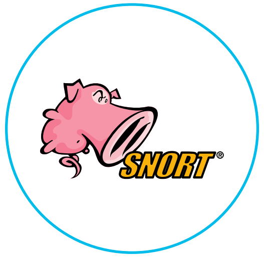
▼ Operating System

Vendor	Product	Version	Source
Microsoft	Windows	Vista, 7, Server 2008	Firepower

Applications (14)

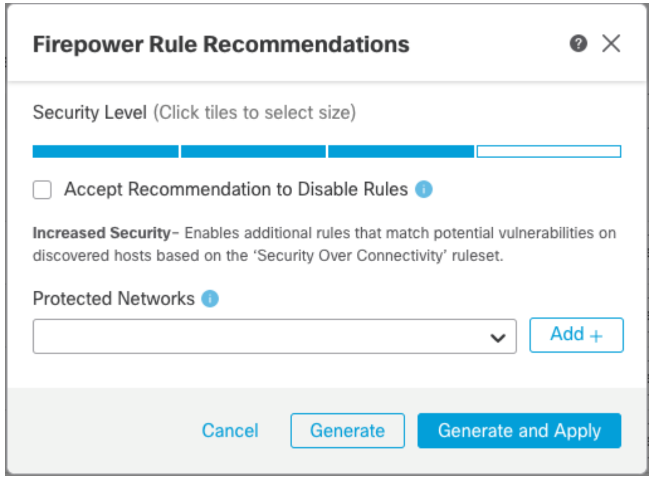
Application Protocol	Client	Version	Web Application
BitTorrent	BitTorrent		
HTTP	Chrome	44.0.2403.107	CNET Download
HTTP	Internet Explorer	9.0	Casale

+



=

Impact flag	Administrator action	Why
1 ⚑	Act immediately, Vulnerable	Event Corresponds to vulnerability mapped to host
2 ⚑	Investigate, Potentially Vulnerable	Relevant port open or protocol in use but no vuln mapped
3 ⚑	Good to know, Currently Not available	Relevant port not open or protocol not in use
4 ⚑	Good to know, Unknown Target	Monitored network but unknown host
0 ⚑	Good to know, Unknown Network	Unmonitored network



Firepower Rule Recommendations

Security Level (Click tiles to select size)

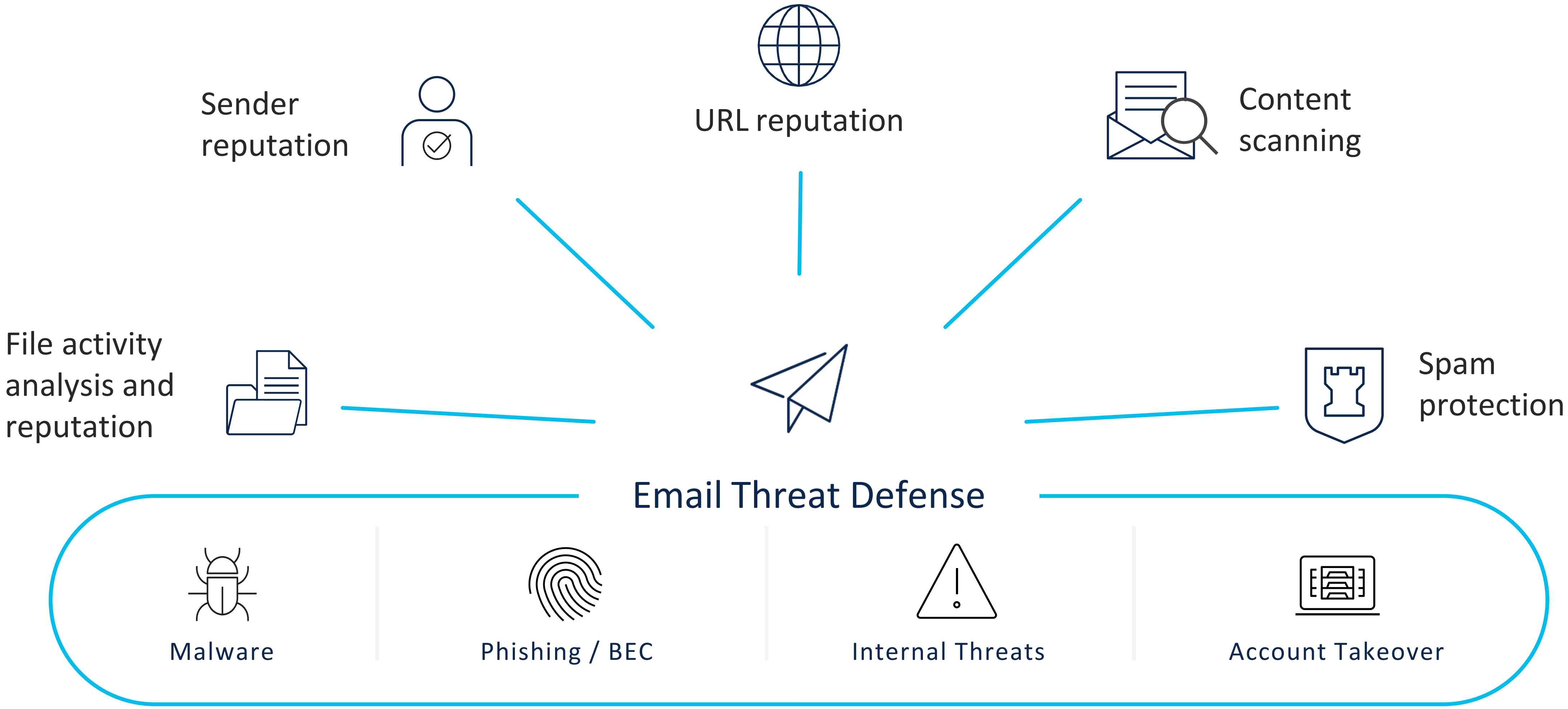
☐ Accept Recommendation to Disable Rules

Increased Security- Enables additional rules that match potential vulnerabilities on discovered hosts based on the 'Security Over Connectivity' ruleset.

Protected Networks

Use Case 3: Ransomware / Threat detection and Response

Comprehensive Email Protection



Sender reputation

URL reputation

Content scanning

File activity analysis and reputation

Spam protection

Email Threat Defense

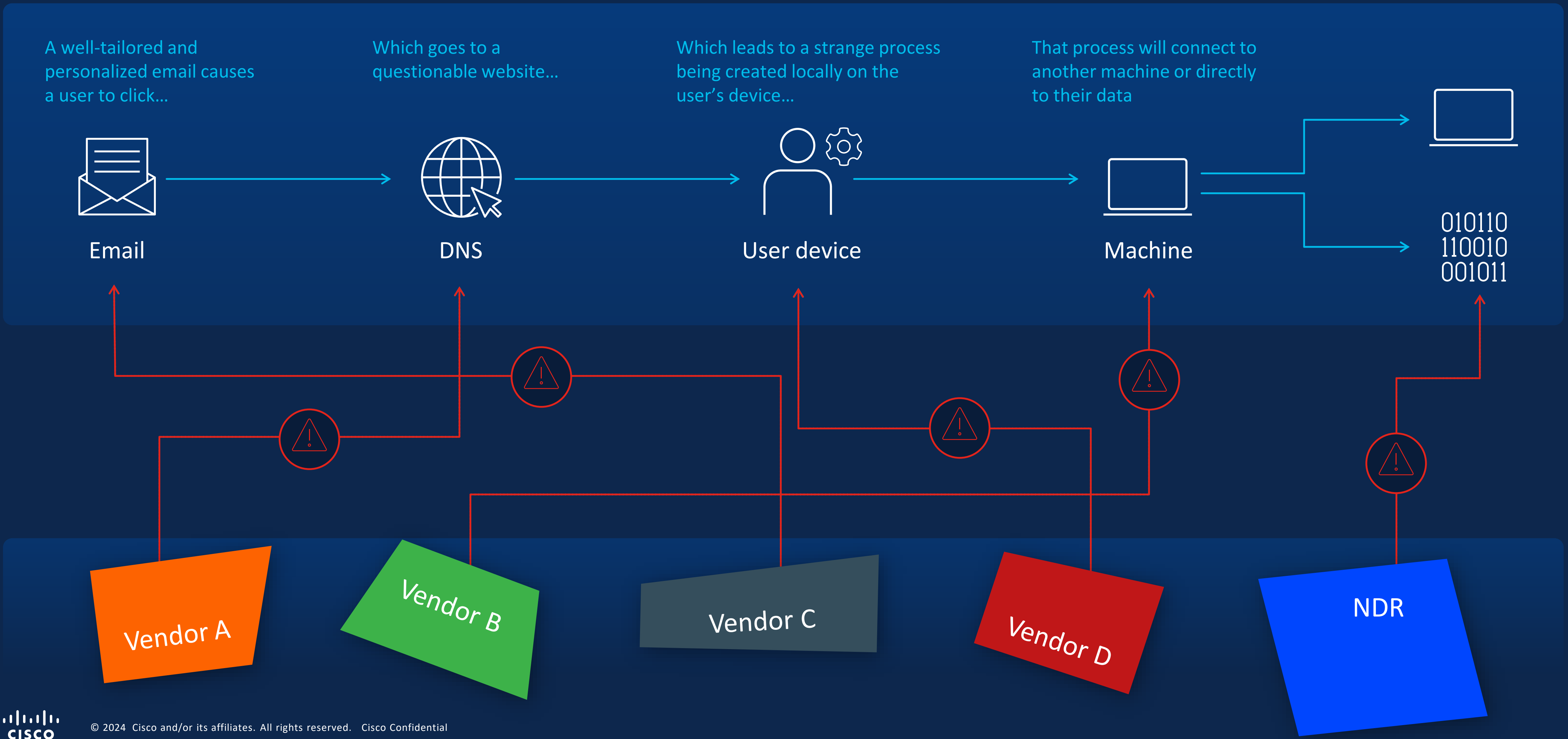
Malware

Phishing / BEC

Internal Threats

Account Takeover

Ransomware campaigns are *multi*-vector



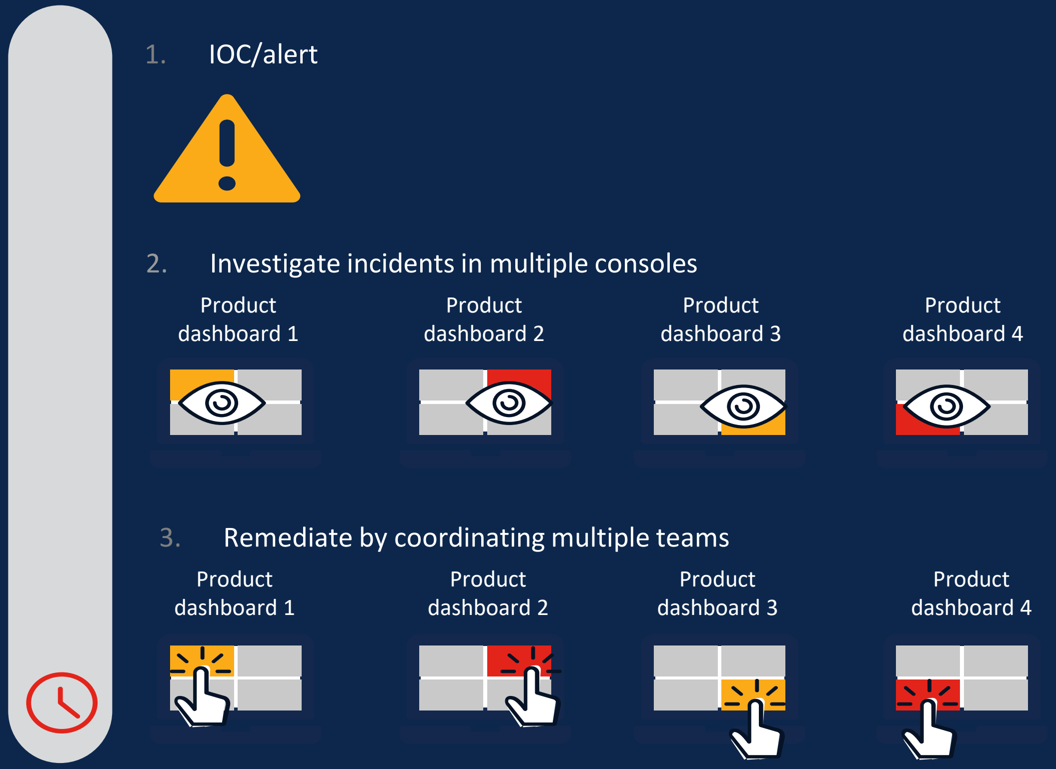
A well-tailored and personalized email causes a user to click…

Which goes to a questionable website…

Which leads to a strange process being created locally on the user's device…

That process will connect to another machine or directly to their data

Siloed Detection & Response



Without XDR: xx minutes

1. IOC/alert

2. Investigate incidents in multiple consoles

Product dashboard 1 | Product dashboard 2 | Product dashboard 3 | Product dashboard 4

3. Remediate by coordinating multiple teams

Product dashboard 1 | Product dashboard 2 | Product dashboard 3 | Product dashboard 4

Cisco XDR

Cisco & 3rd party

Network

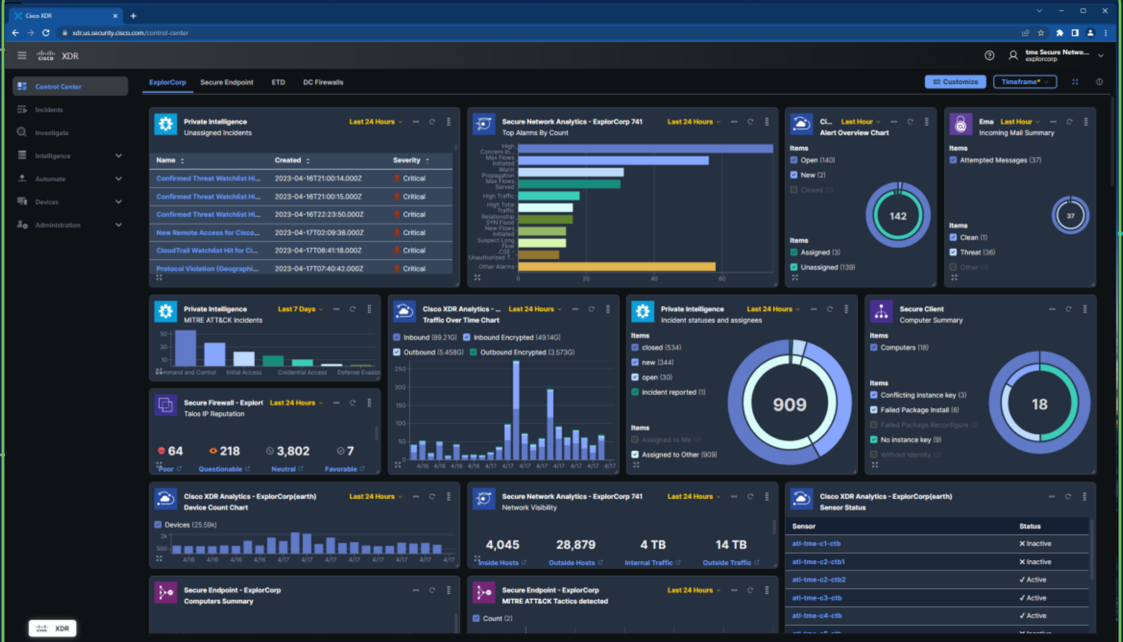
Endpoint

Email

Cloud

Applications

Identity



Name	Created	Severity
Confirmed Threat Watchlist Hi...	2023-04-16T21:00:14.000Z	Critical
Confirmed Threat Watchlist Hi...	2023-04-16T21:00:15.000Z	Critical
Confirmed Threat Watchlist Hi...	2023-04-16T22:23:50.000Z	Critical
New Remote Access for Cisco...	2023-04-17T02:09:38.000Z	Critical
CloudTrail Watchlist Hit for Ci...	2023-04-17T06:41:18.000Z	Critical
Protocol Violation (Geographi...	2023-04-17T07:40:42.000Z	Critical

Sensor	Status
atl-tme-c1-ctb	✕ Inactive
atl-tme-c2-ctb1	✕ Inactive
atl-tme-c2-ctb2	✓ Active
atl-tme-c3-ctb	✓ Active
atl-tme-c4-ctb	✓ Active

Built on the Cisco security platform

Open and extensible

Clear prioritization

Automation and response guidance

Streamlined investigations

Your Infrastructure

3rd party tools

Intelligence

010110
110010
001011
Others

SIEM/SOAR

SecOps Analyst

CISO

Incident responder

Your SOC

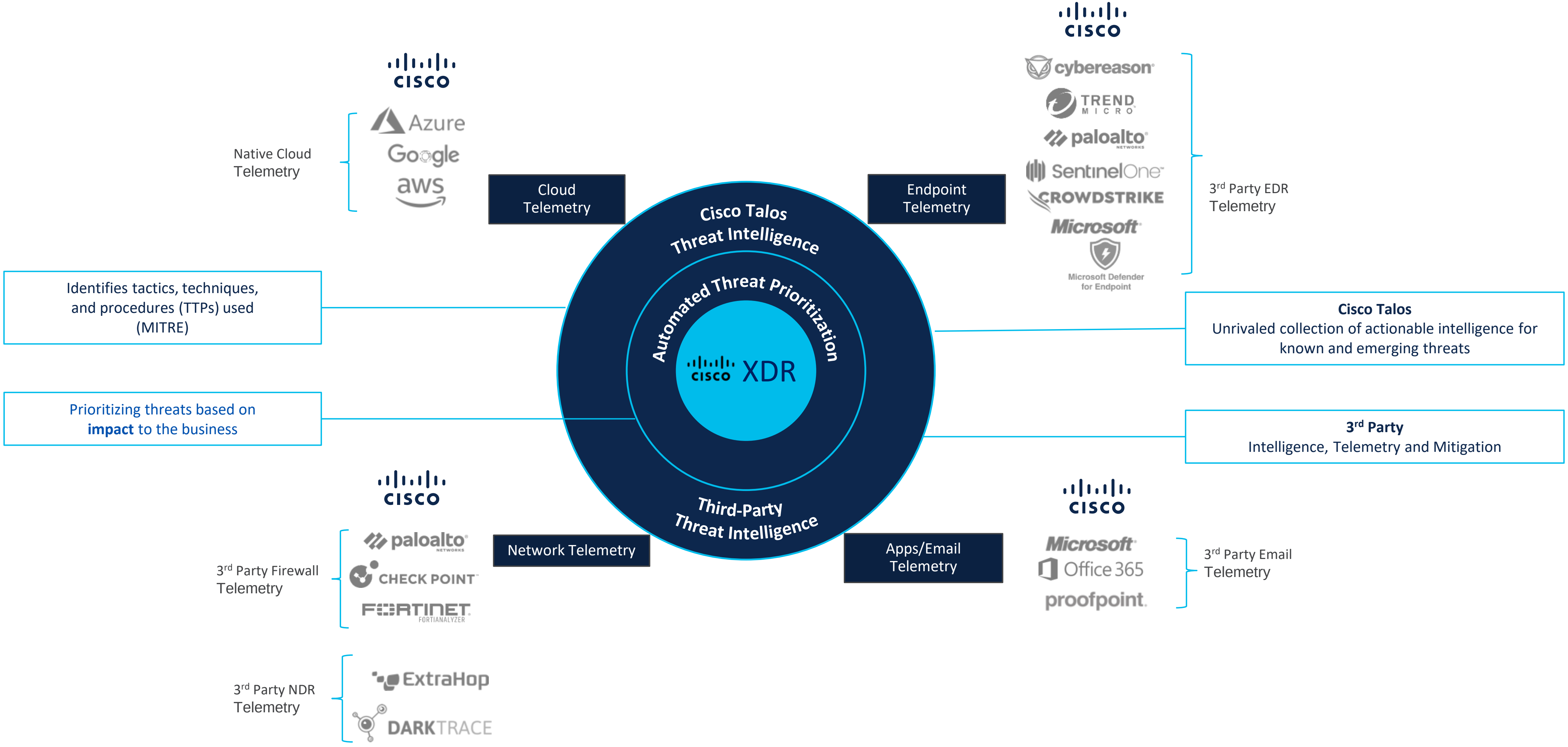
Detect sooner

Prioritize by impact

Speed up investigations

Accelerate response

Cisco XDR: Strategic integrations to deliver customer outcomes



Identifies tactics, techniques, and procedures (TTPs) used (MITRE)

Prioritizing threats based on **impact** to the business

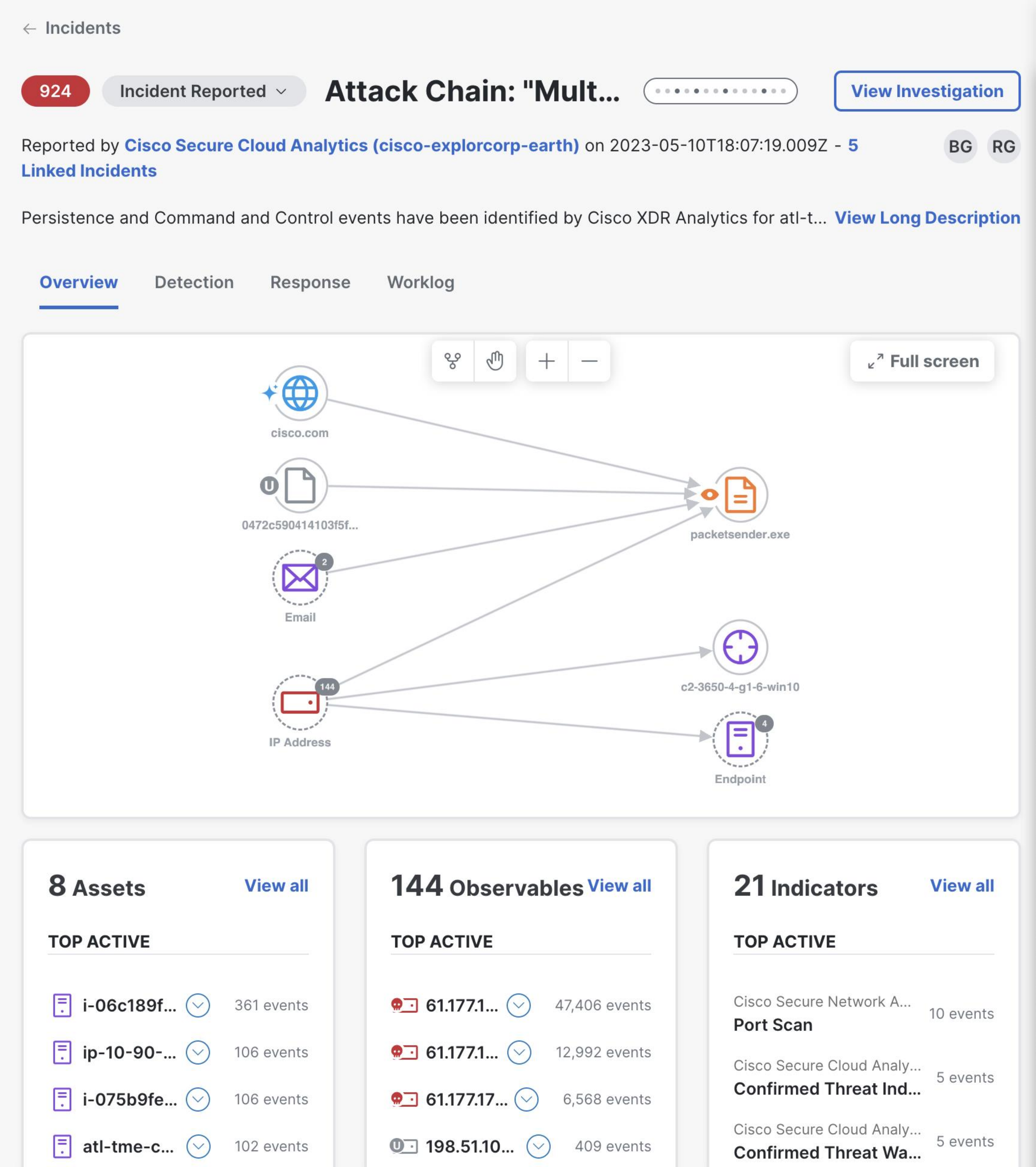
Cisco Talos
Unrivaled collection of actionable intelligence for known and emerging threats

3rd Party
Intelligence, Telemetry and Mitigation

cisco SECURE

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.



Attack Chain: "Mult...

Reported by Cisco Secure Cloud Analytics (cisco-explorcorp-earth) on 2023-05-10T18:07:19.009Z - 5 Linked Incidents

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

8 Assets

TOP ACTIVE

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

144 Observables

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

TOP ACTIVE

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

XDR Response playbooks

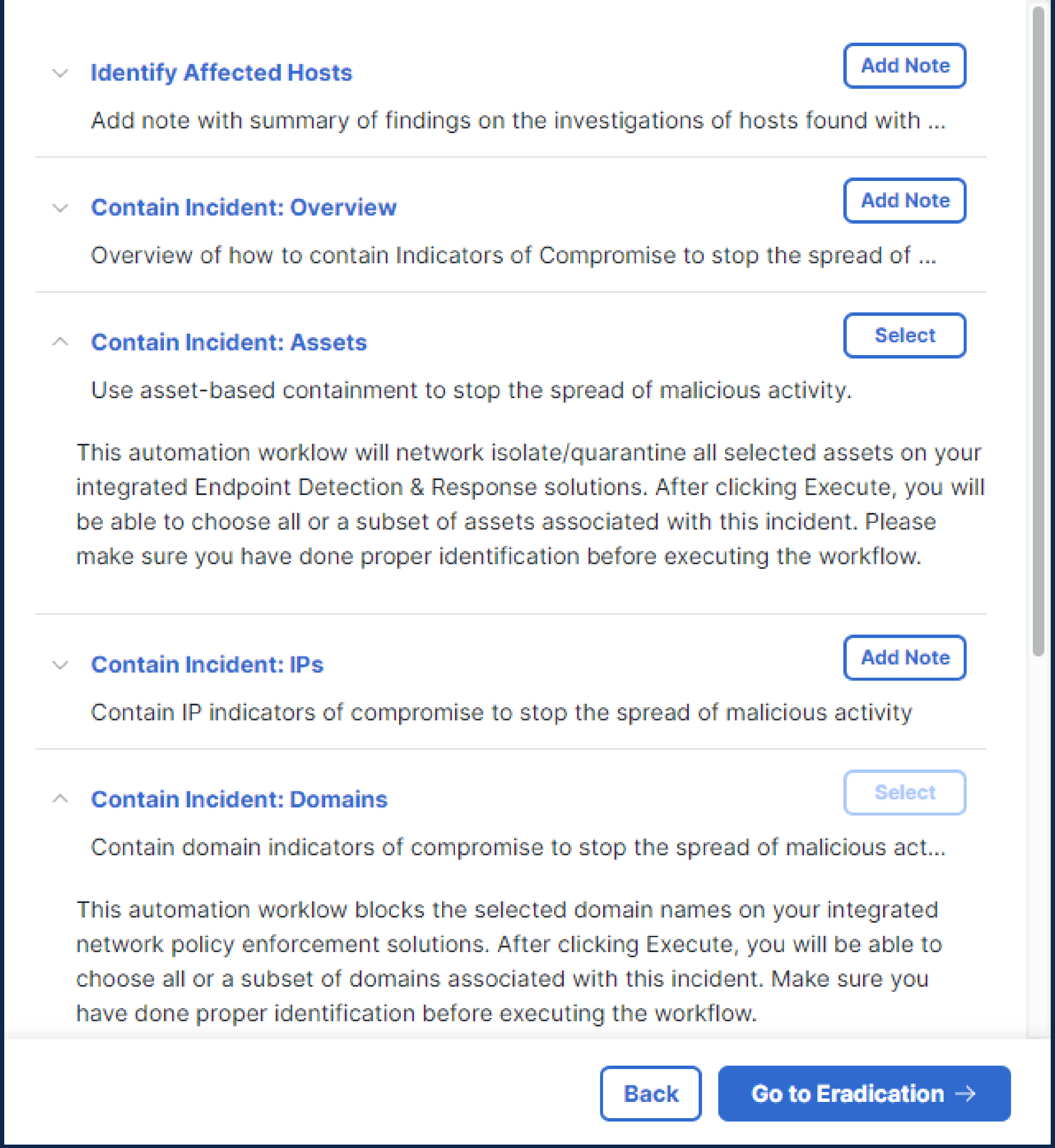
- Bring the ability to take immediate response actions into the incident manager.
- Powered by out of the box XDR Automation workflows.
- Broken down into four stages:

Identify

Contain

Eradicate

Recover



Identify Affected Hosts

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

Contain Incident: Overview

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

Contain Incident: Assets

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

This automation worklow 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

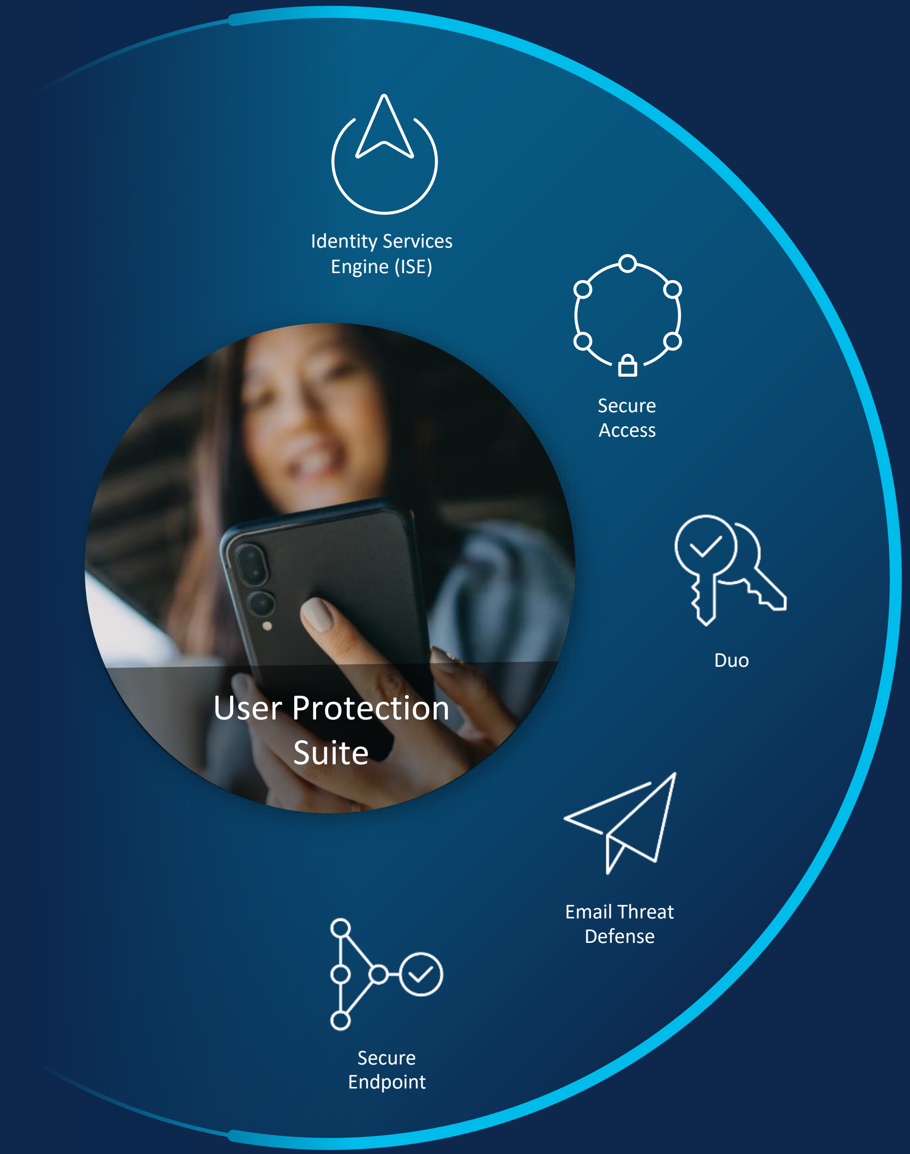
Contain IP indicators of compromise to stop the spread of malicious activity

Contain Incident: Domains

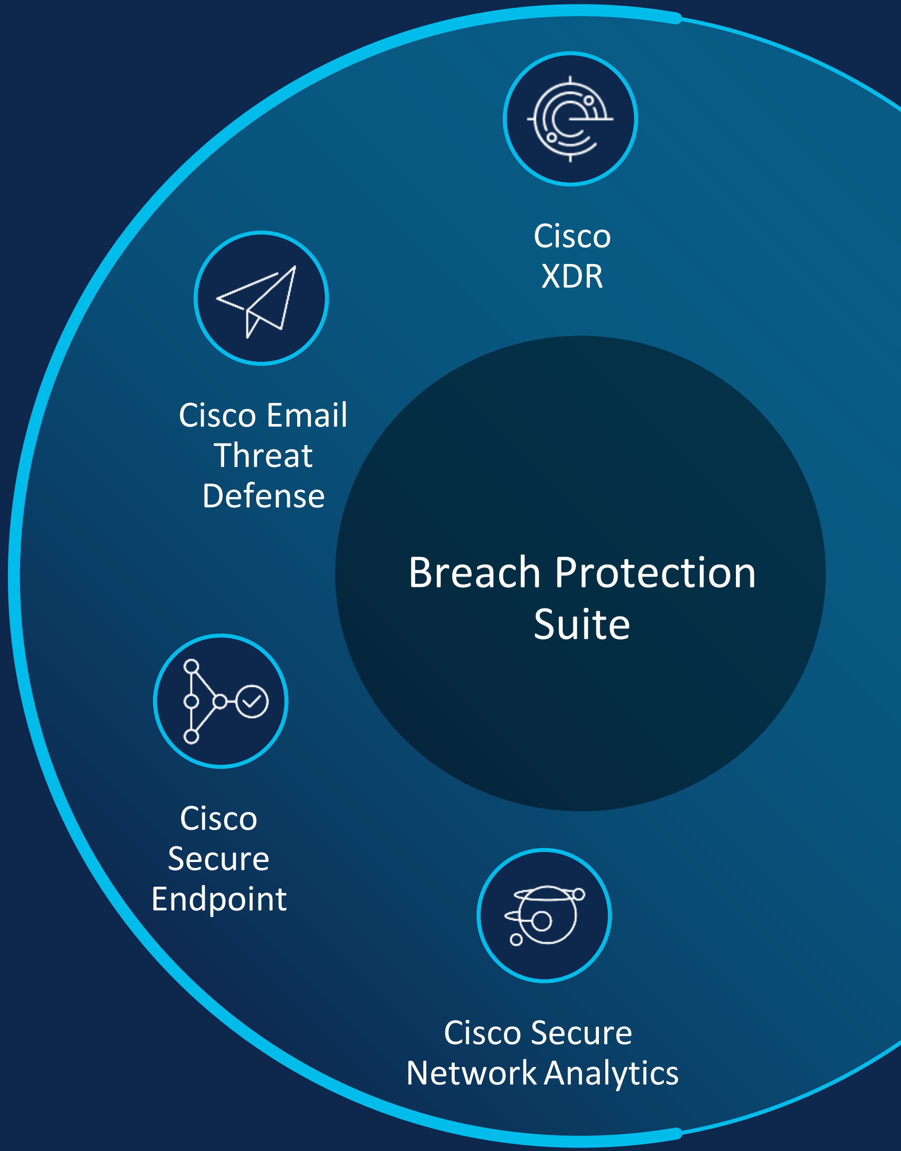
Contain domain indicators of compromise to stop the spread of malicious act...

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.

Too many products?



Cisco Security Suites to simplify security consumption & optimize product integrations.



Thank you!