



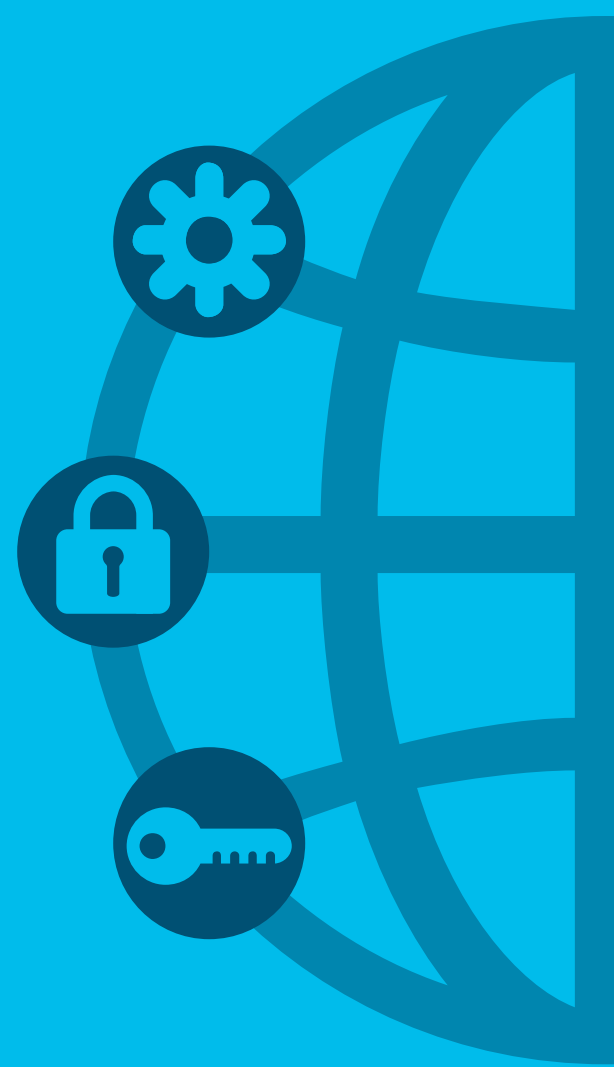
Cisco DC Security Architecture

Bing Reaport

Cybersecurity Sales Specialist

M: +639992217765

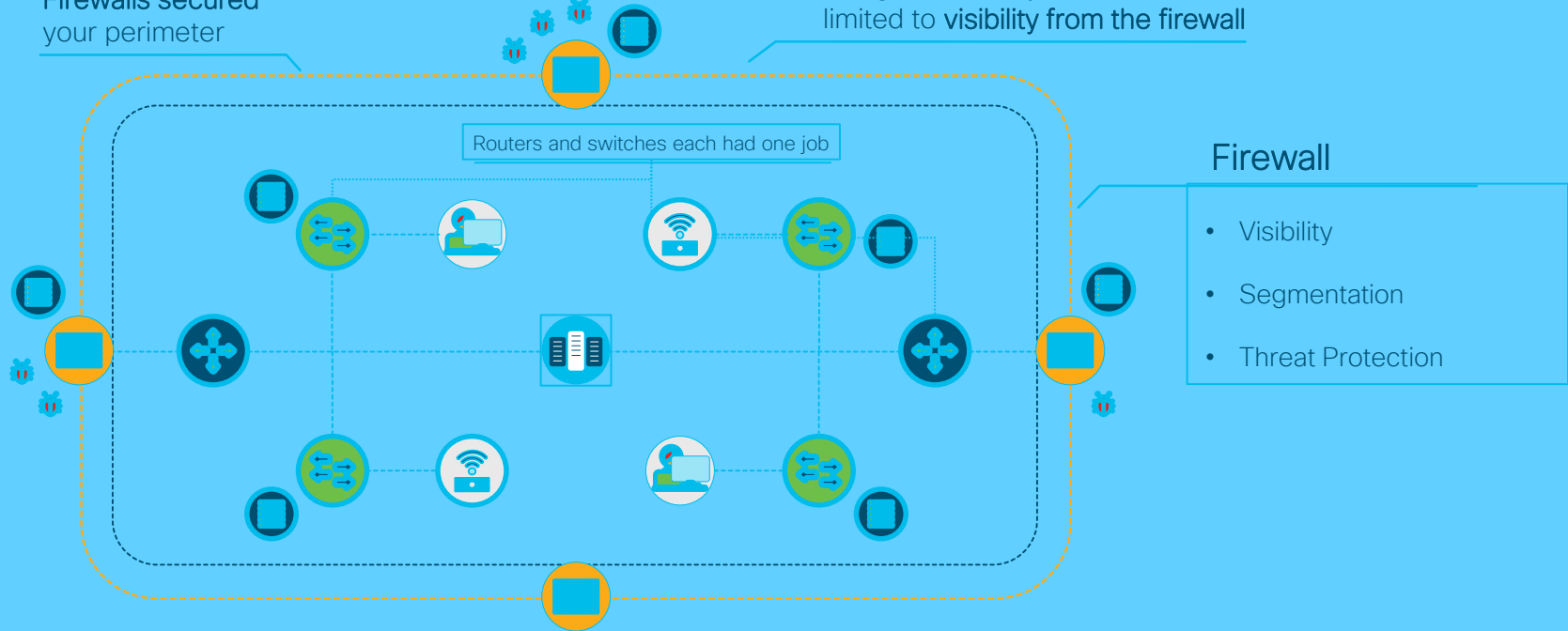
E: ereaport@cisco.com



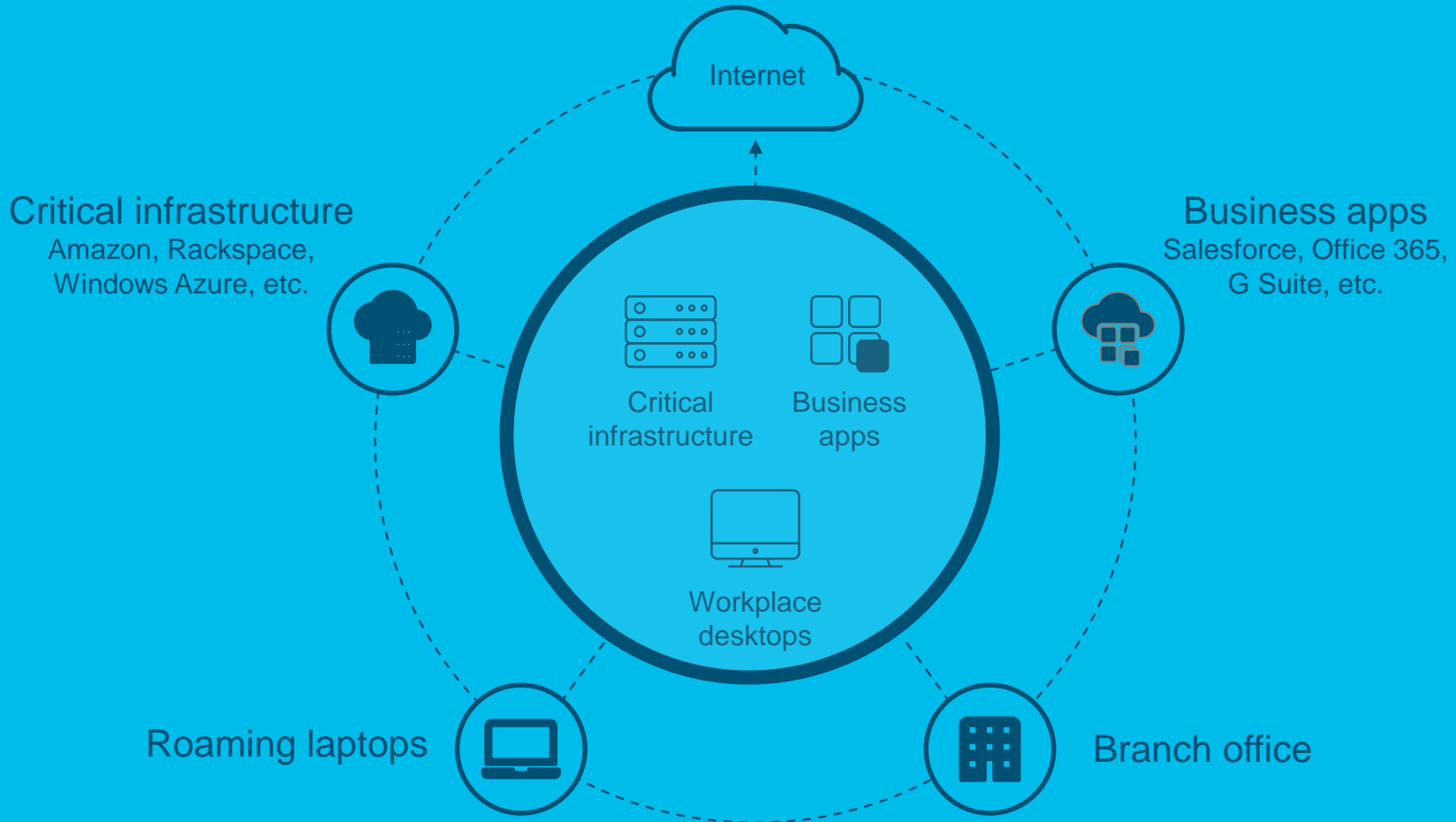
Yesterday's network security was about the perimeter

Firewalls secured your perimeter

Knowing what's on your network was limited to **visibility from the firewall**



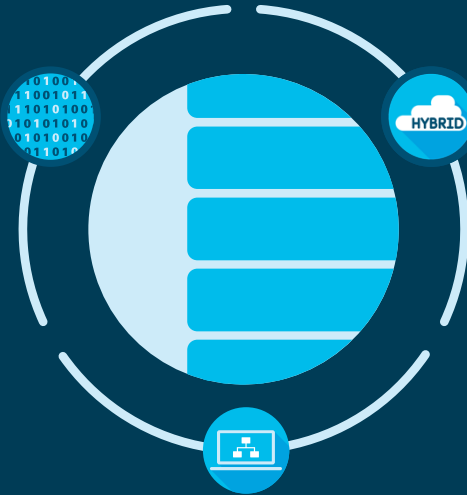
The way we work has changed



The Modern Data Center is Incredibly Complex

Big and Fast Data

Virtualization
Expanded attack surface
Increase in east-west traffic



Hybrid Cloud

Multi cloud orchestration
Workload portability
Zero trust model

Application Architecture

Continuous development | Micro Services | APIs



Network Challenges

- Outage/degraded service
- Insufficient visibility into the network, workload, application
- Rising security breaches and destruction of service (DeOS) attacks
- Increasing regulatory compliance requirements and audits
- Rising ACL/FW rule complexity and administration burden

- Not enough threat **visibility** in the network, workloads, applications
- Inconsistent policies across workloads
- Too many point security vendors
- Hackers are more sophisticated
- Attack surface is too broad



Security Challenges

Securing networks is a challenge that intensifies when networking and security technologies are decoupled

Networking



Complex system integration

takes too much time and leaves room for error

Security



Piecemeal security solutions

complicate the network and let threats slip through

Infrastructure



Difficult infrastructure choices

create a dilemma between performance and security

Digitization complicates visibility

Market demands have taken the network beyond your perimeter

More IoT devices
connect everyday

Over 20B connected "things"
will be in use by 2020

Users work anywhere
across many devices

By 2020, 2/3rds of all IP traffic will
come from wireless and mobile
devices



Threats are more
numerous and complex

Companies experienced a 27.4%
average increase in security
breaches in 2017

Threats are using encryption
to evade detection

3X increase in encrypted
communication from malware in a
12-month period

Effective security depends on total visibility



KNOW
every host



SEE
every conversation



Understand what
is **NORMAL**



Be alerted to
CHANGE



Respond to
THREATS quickly

Branch



Cloud

Roaming Users



Network



HQ

Users



Data Center



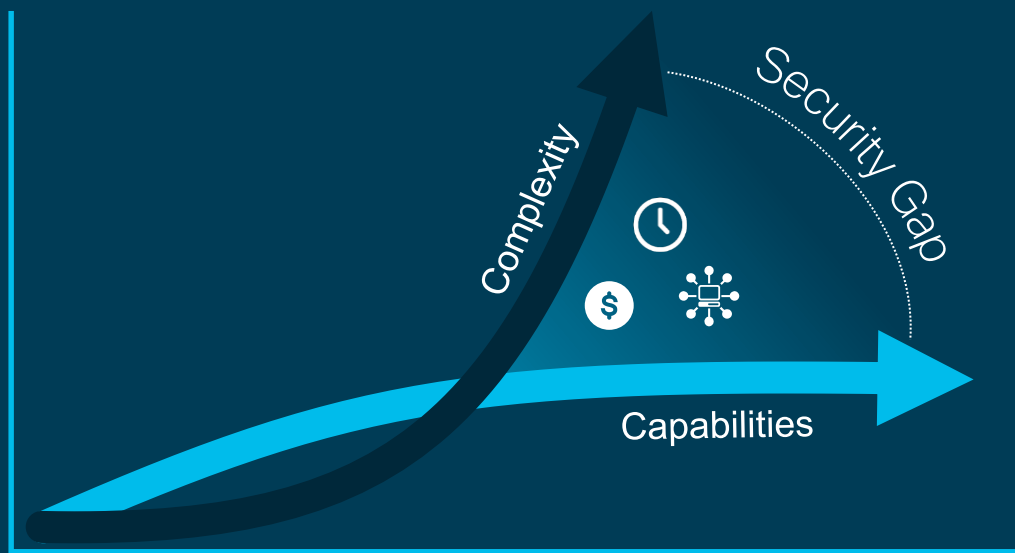
Admin



The Existing Security Stack...



Adding point solutions adds complexity and can make you less secure



55% Of customers rely on more than 5 vendors to secure their network¹

54% Of legitimate security alerts are not remediated due to lack of integrated defense systems²

100 days Industry average to detect a common threats³

¹ [Cisco 2017 Annual Cybersecurity Report](#)

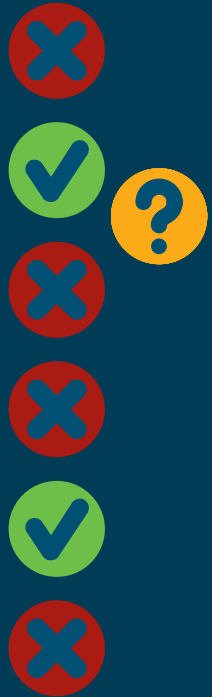
² [Cisco 2017 Annual Cybersecurity Report](#)

³ [Cisco 2016 Mid-Year Cybersecurity Report](#)



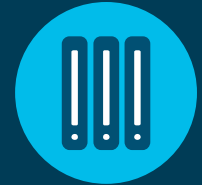
Customer

Threat Intelligence



Customer

Internal Monitoring



Threat Intelligence



Customer



Internal Monitoring



Cisco Data Center Security



Visibility "See Everything"

Complete visibility of users, devices, networks, applications, workloads and processes



Segmentation "Reduce the Attack Surface"

Prevent attackers from moving laterally east-west with application whitelisting and micro-segmentation



Threat Protection "Stop the Breach"

Quickly detect, block, and respond to attacks before hackers can steal data or disrupt operations

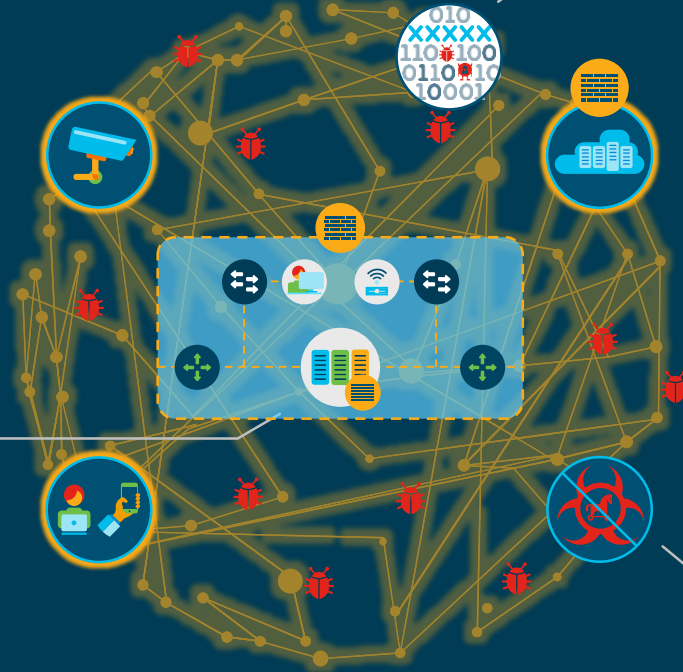
The Solution: Network + Security

Enlist the Rest of your Network for Security

Detect threats everywhere

See and analyze all traffic across the extended network

Typical Network:
<10 firewalls
<100 routers
<1000 switches



Fortify the Security

Posture

Strategically place next-gen security gateways for more effective protection

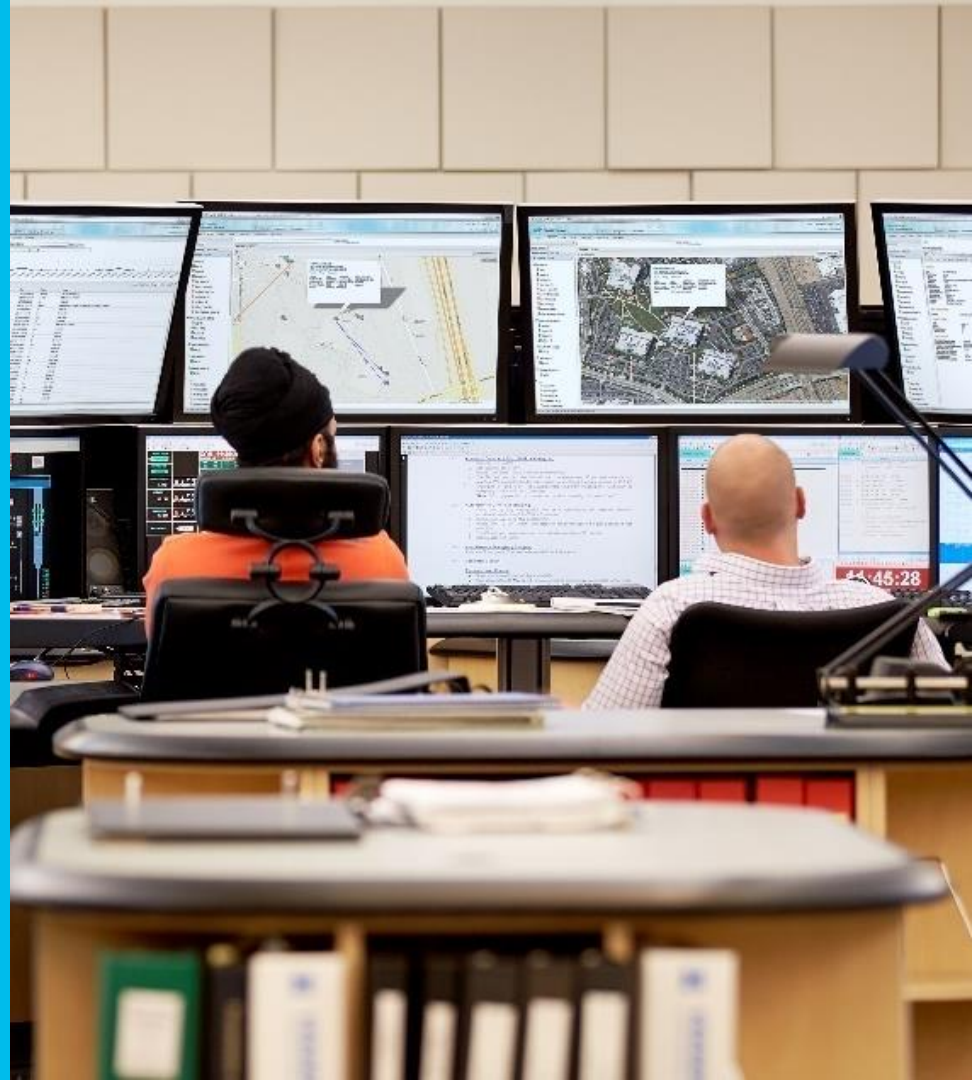
Contain and isolate threats

Dynamically enforce software-defined segmentation based on business roles

Without straining the network

Effective security doesn't...

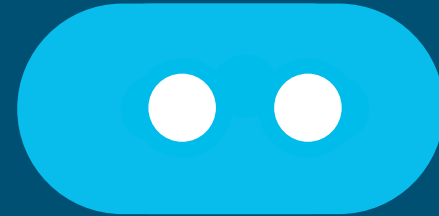
- Impede performance
- Add complexity
- Create blind spots



Cisco network telemetry for security awareness



A powerful information source for every network conversation



A critical tool to identify a security breach

Network Flows Highlight Malicious Behavior

Is our security posture effective?



Threat



Detection

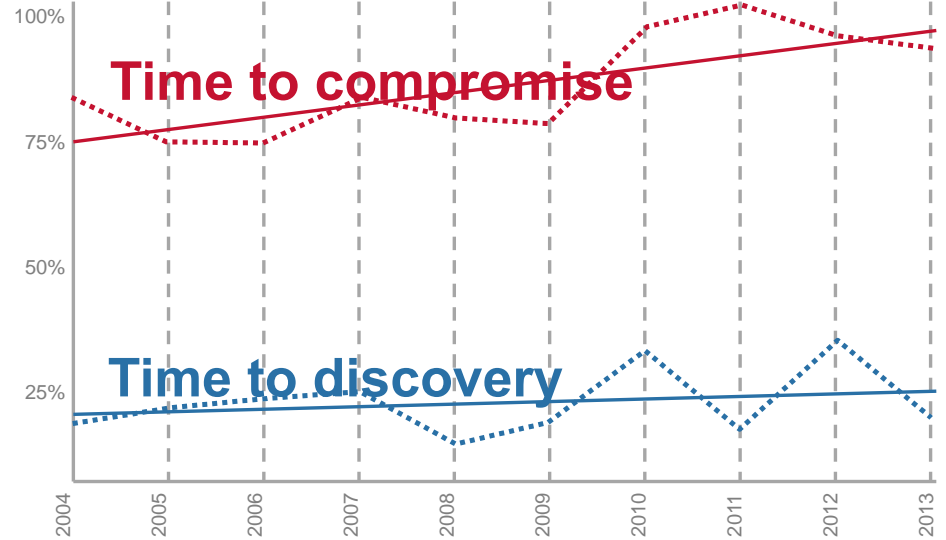


Response

Industry Result



Percent of breaches where time to compromise (orange)/
time to discovery (blue) was days or less



Source: Verizon 2014 Data Breach Investigations Report

Cisco Security Strategy

Intelligence

Best of breed
Portfolio

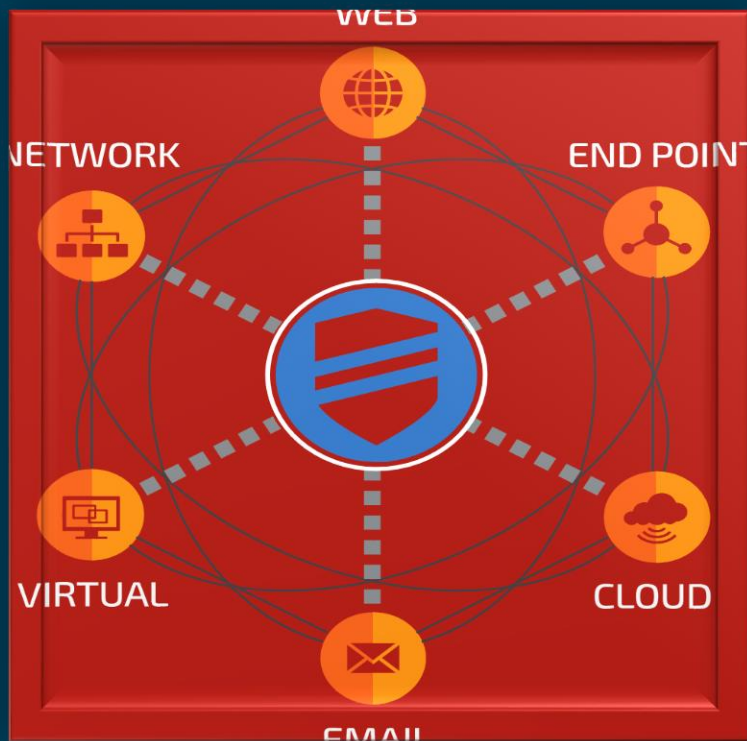


Integrated
Architecture

Cisco's Integrated Security Portfolio



MULTI-TIERED DEFENSE





Cloud to Core Coverage

- **WEB:** Reputation, URL Filtering, AVC
- **END POINT:** Software – ClamAV, Razorback, Moflow
- **CLOUD:** FireAMP & ClamAV detection content
- **EMAIL:** Reputation, AntiSpam, Outbreak Filters
- **NETWORK:** Snort Subscription Rule Set, VDB – FireSIGHT Updates & Content, SEU/SRU Product Detection & Prevention Content
- Global Threat Intelligence Updates

Cisco Security: Power of a Comprehensive Architecture







Network

-  Next-Generation Firewall
-  NGIPS
-  Segmentation
-  Web Security
-  Network Access Control
-  Security Analytics







Endpoint

-  Endpoint Detection and Response
-  DNS-layer Roaming Protection
-  Mobile Security
-  VPN Secure Access



Cloud

-  Security Internet Gateway
-  Public Cloud Security
-  Workload Security
-  Cloud Access Security
-  Email Security
-  Virtual Network Security

Breach Readiness
and Response

Incident Response
Services

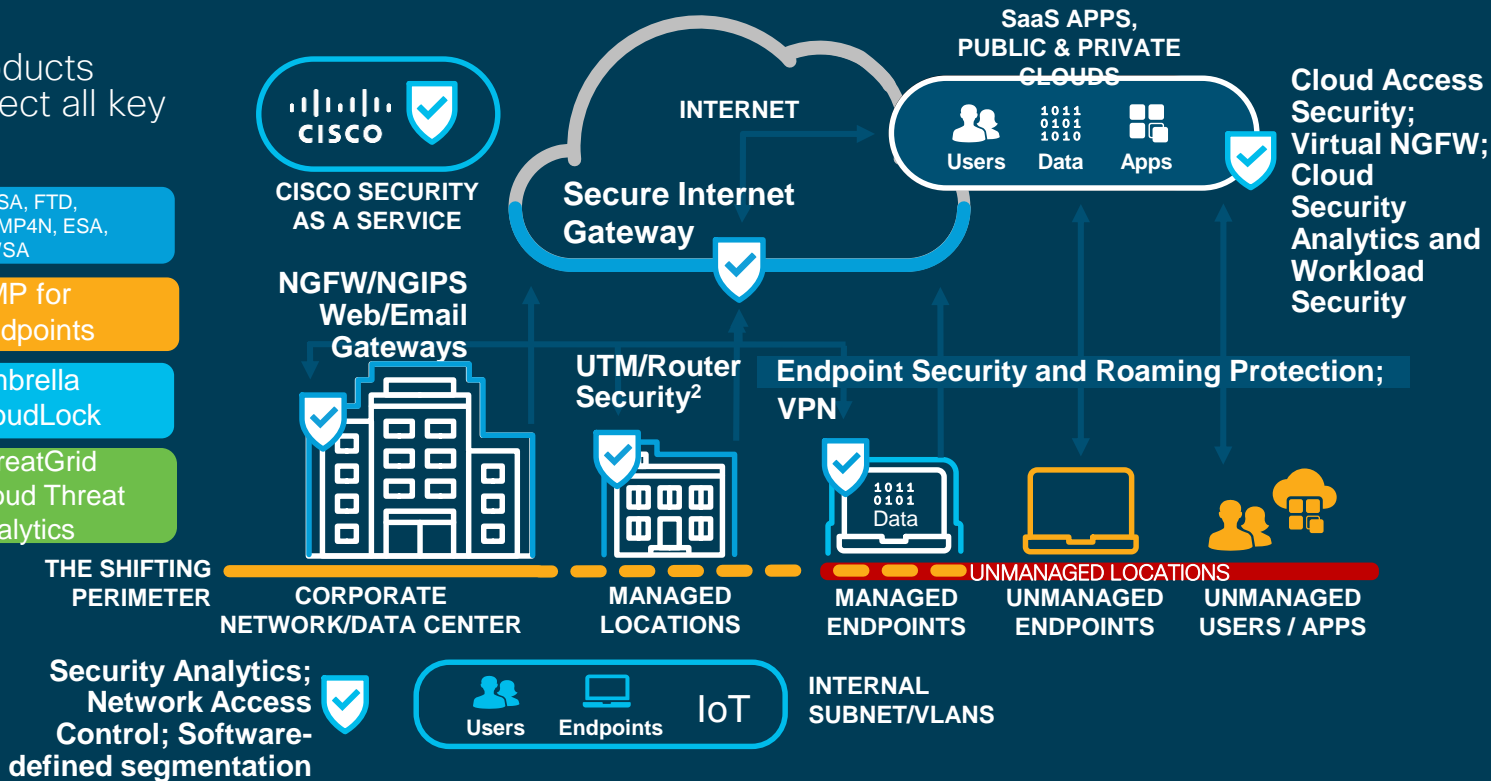
Segmentation
Services

Cisco Security Portfolio

Best of breed products integrated to protect all key vectors

Cloud-managed network security, cloud-managed UTM, Cloud Threat Analytics and Sandboxing, Cloud Email Security

Network Security	ASA, FTD, AMP4N, ESA, WSA
Endpoint Security	AMP for Endpoints
Cloud Security	Umbrella CloudLock
Security via the cloud	ThreatGrid Cloud Threat Analytics



1. Not the same as cloud security
2. ISR Firepower services



TALOS

PROTECTING YOUR NETWORK

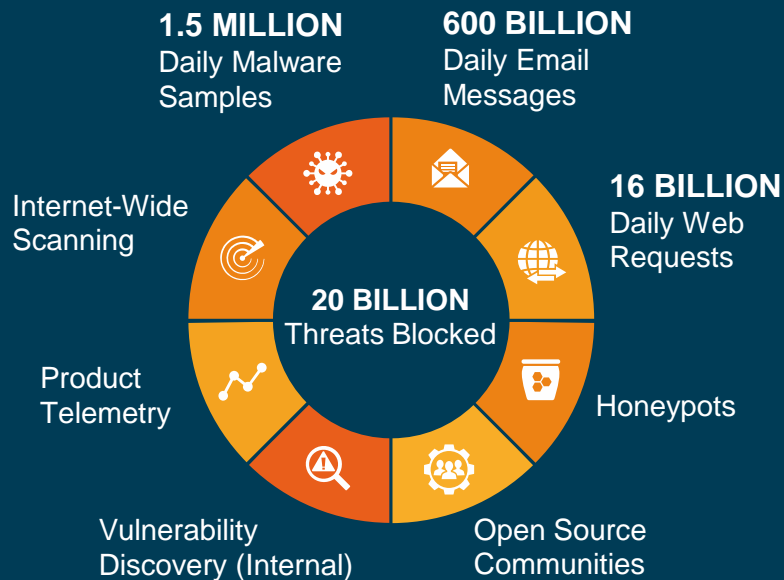


Industry-leading threat intelligence. The largest threat detection network in the world.

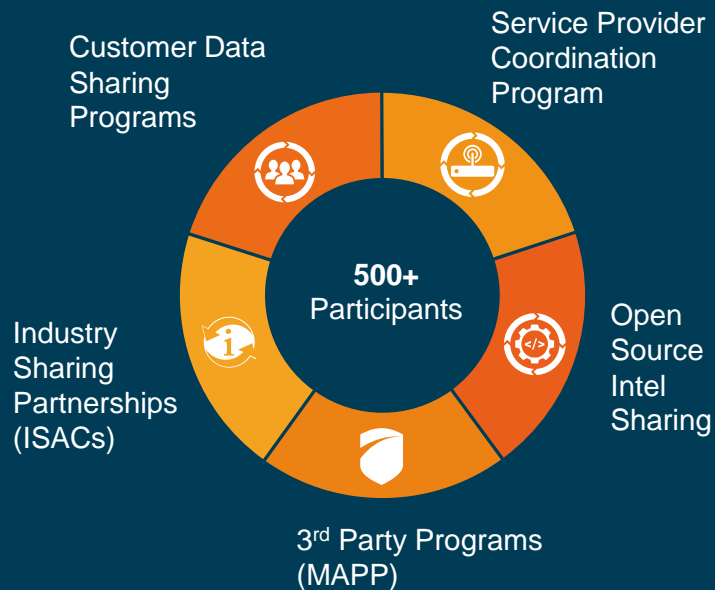
© 2016 Cisco and/or its affiliates. All rights reserved.

TALOS INTEL BREAKDOWN

THREAT INTEL



INTEL SHARING



250+
Full Time Threat Intel Researchers



MILLIONS
Of Telemetry Agents



4
Global Data Centers



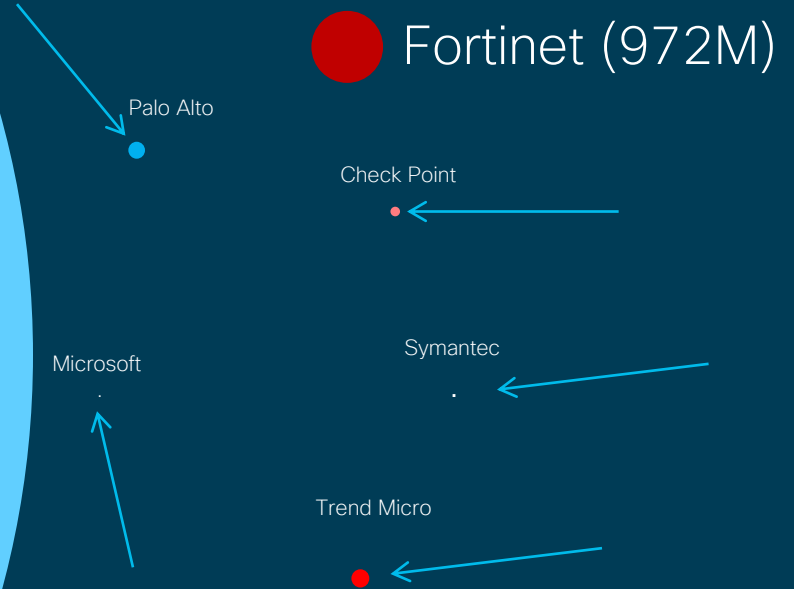
100+
Threat Intelligence Partners



1100+
Threat Traps

Threats blocked (daily)

TALOS
20,000,000,000



Unique malware samples (daily)

TALOS
1,500,000

Microsoft

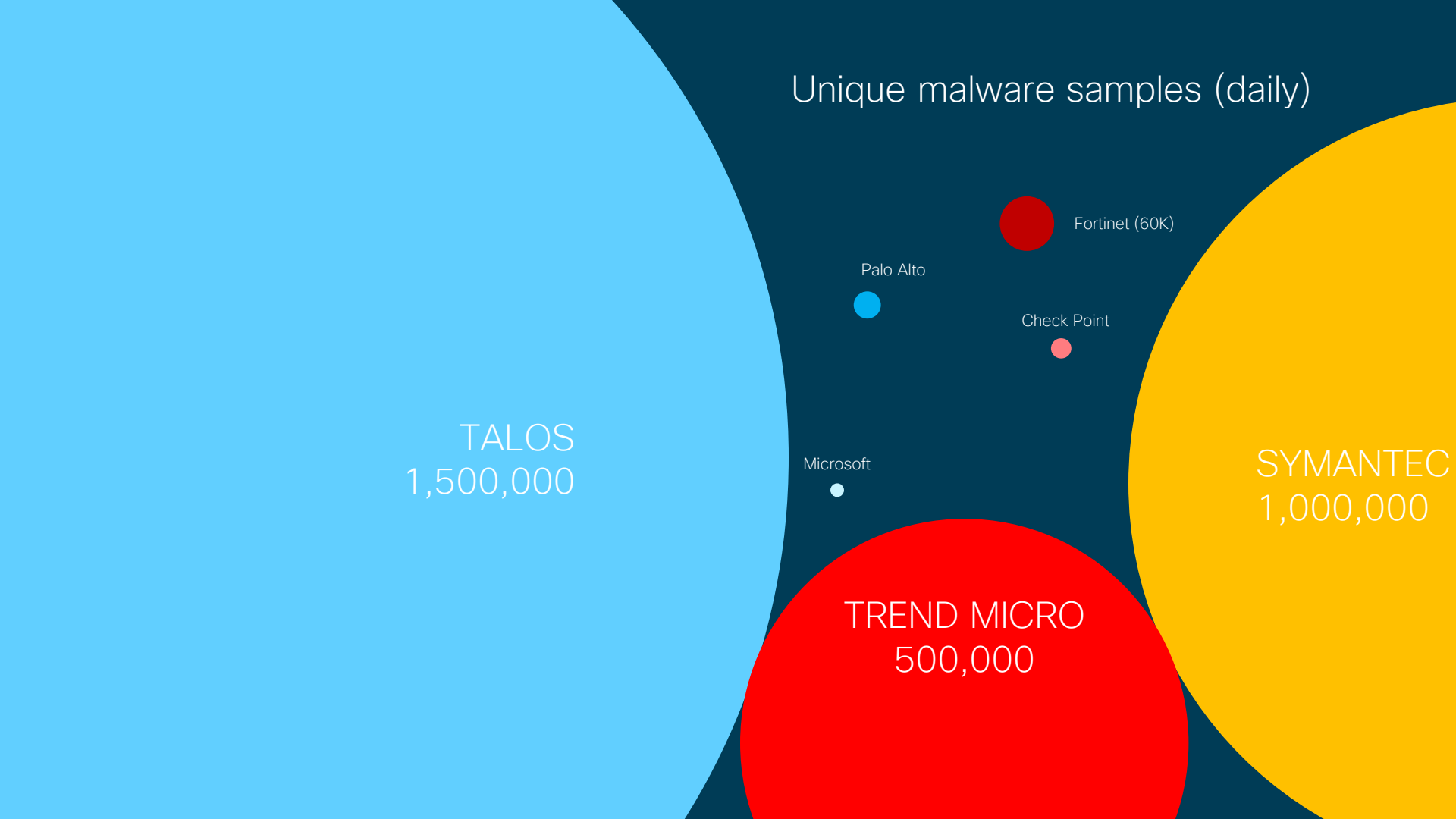
TREND MICRO
500,000

Palo Alto

Check Point

Fortinet (60K)

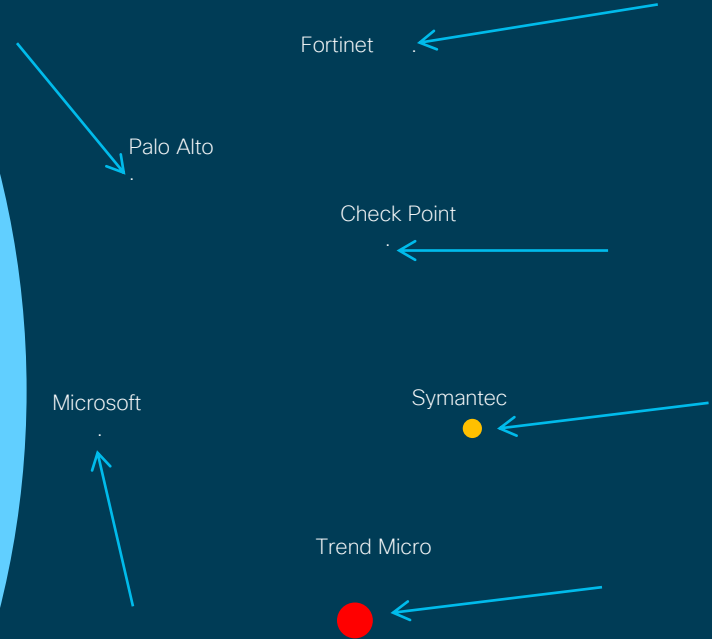
SYMANTEC
1,000,000



URLs processed (daily)

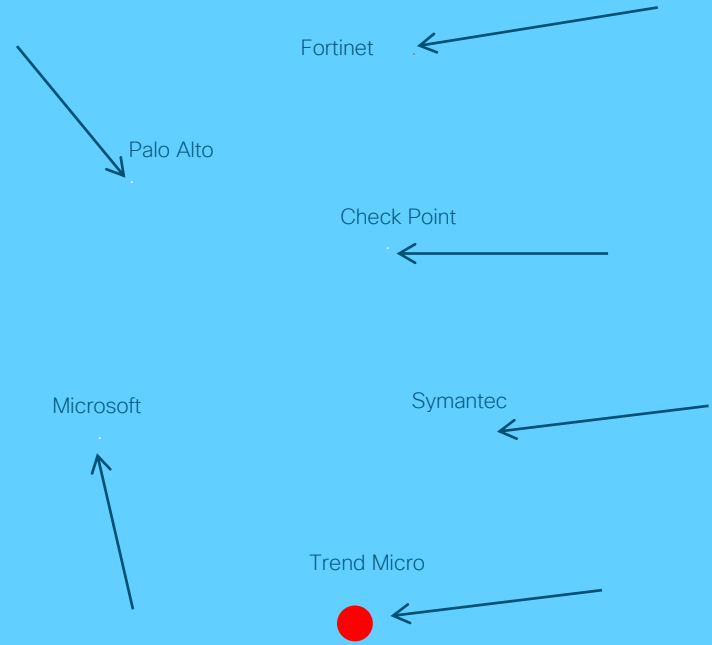


16,000,000,000

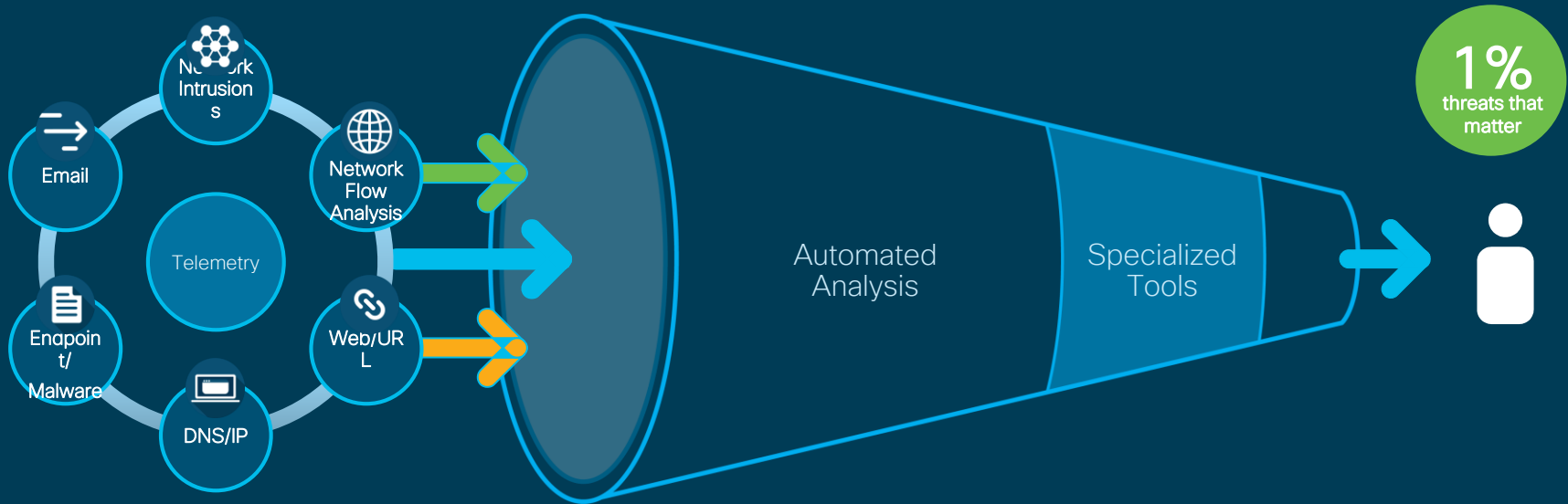


DNS entries processed (daily)

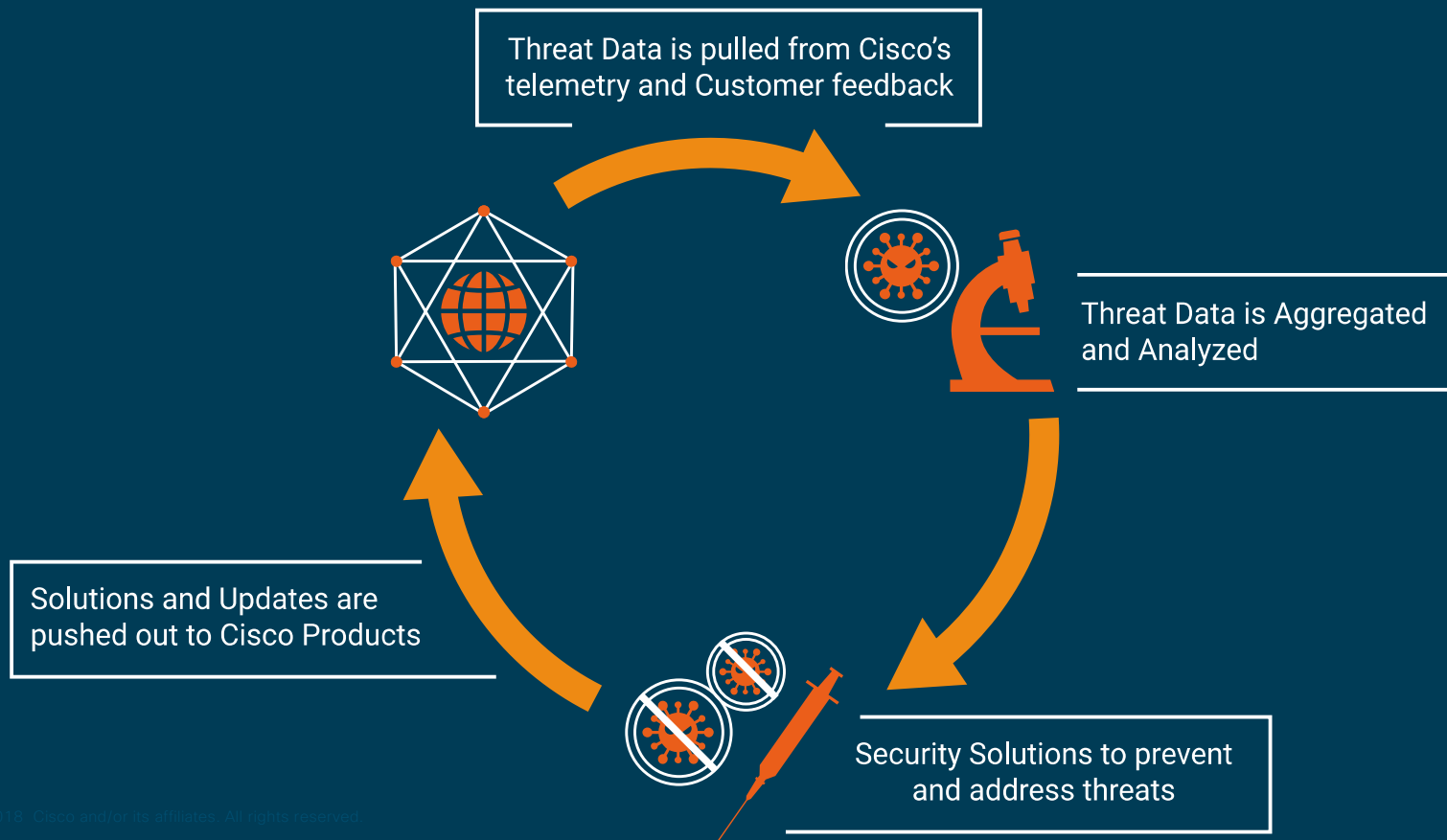
TALOS **OpenDNS**
150,000,000,000



How Talos Protects Customers



Threat Data Cycle





Cisco Secure DC Architecture

Network Security Control Challenges



Growing attack
Surface

- Businesses under attack: hacktivists, organized crime, and nation states



Dynamic threat
landscape

- Most organizations have highly-available, fast, flat, open networks
- Threats get into networks

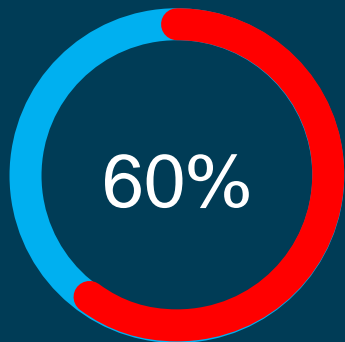


Complexity and
fragmentation

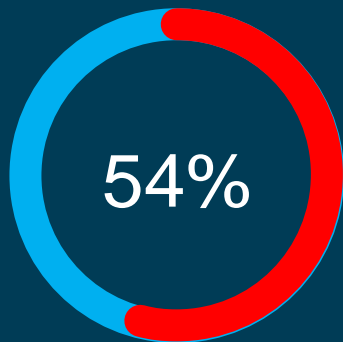
- Inside threats are hard to stop

Network Security Visibility Challenges

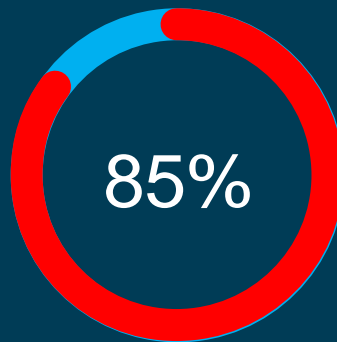
Undetected threats are effective



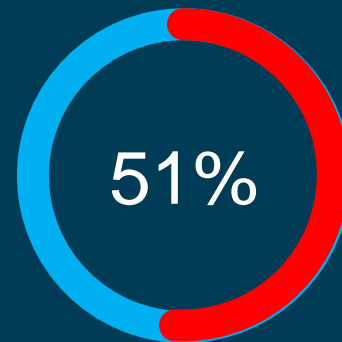
Data stolen
in hours



Breaches
undiscovered
for months



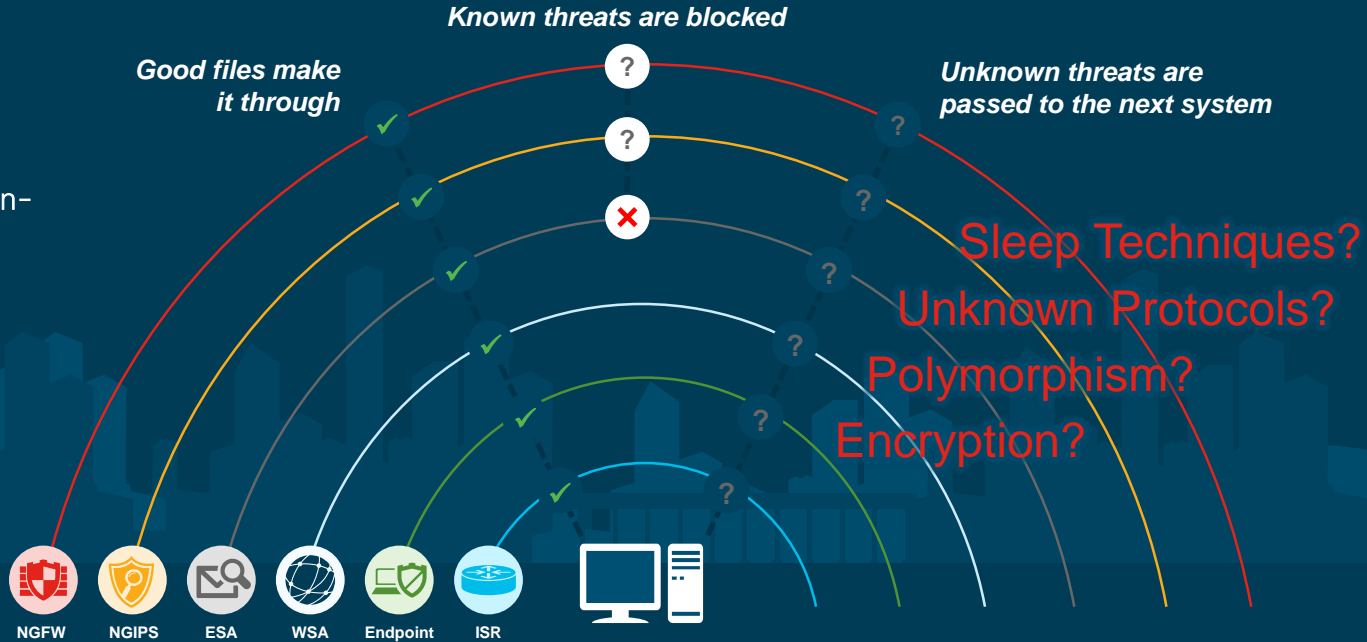
PoS intrusions
undiscovered
for weeks



Increase of
companies
losing \$10M

It's Impossible to Block 100% of Threats 100% of the Time

Current defense in-depth approach is built on binary detection



Single points of inspection have their limitations

Cisco Data Center Security



Visibility "See Everything"

Complete visibility of users, devices, networks, applications, workloads and processes



Segmentation "Reduce the Attack Surface"

Prevent attackers from moving laterally east-west with application whitelisting and micro-segmentation



Threat Protection "Stop the Breach"

Quickly detect, block, and respond to attacks before hackers can steal data or disrupt operations

01



02

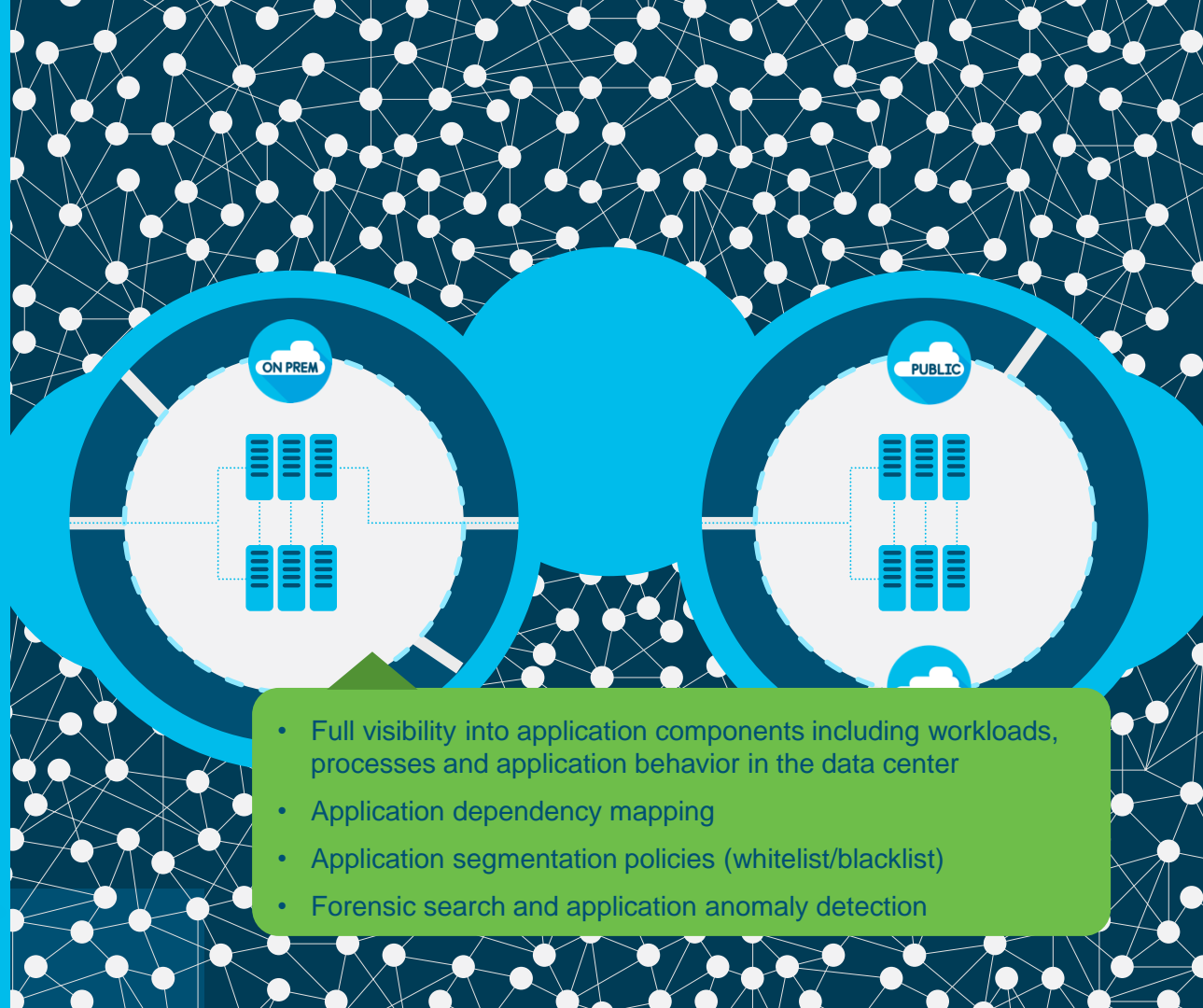


03



Visibility: See Application Components & their Behavior

Cisco Tetration



- Full visibility into application components including workloads, processes and application behavior in the data center
- Application dependency mapping
- Application segmentation policies (whitelist/blacklist)
- Forensic search and application anomaly detection

01



02

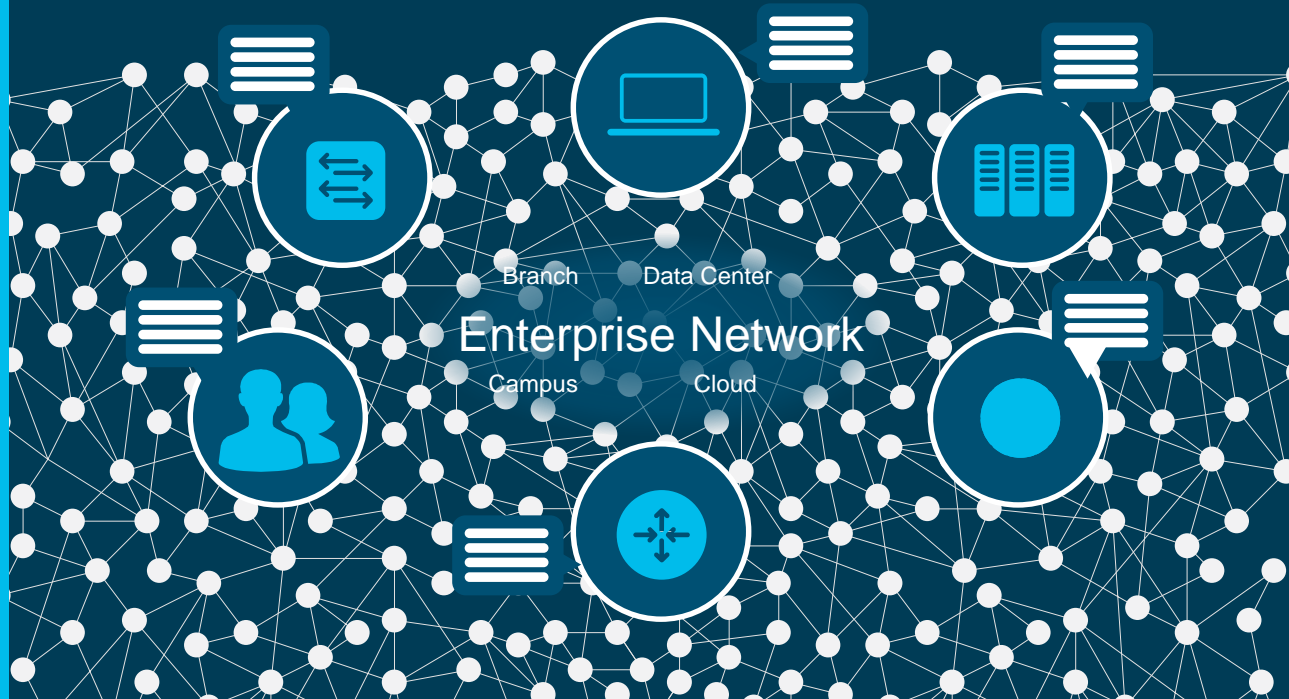
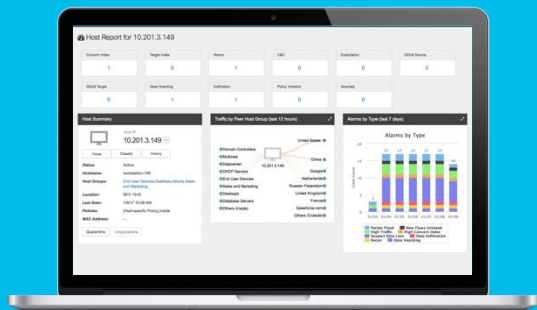


03



Visibility: See Across the Enterprise Network

Cisco Stealthwatch



- Enterprise-wide network visibility across users, hosts, networks, and infrastructure (switches, routers, firewalls, servers)
- Collects network flow and other data to provide network visibility for understanding network wide traffic and discover threats
- Real-time situational awareness of users, devices, and applications
- Network flow monitoring of policy violations validates enterprise-wide network access to facilitate compliance and segmentation requirements

01



02



03

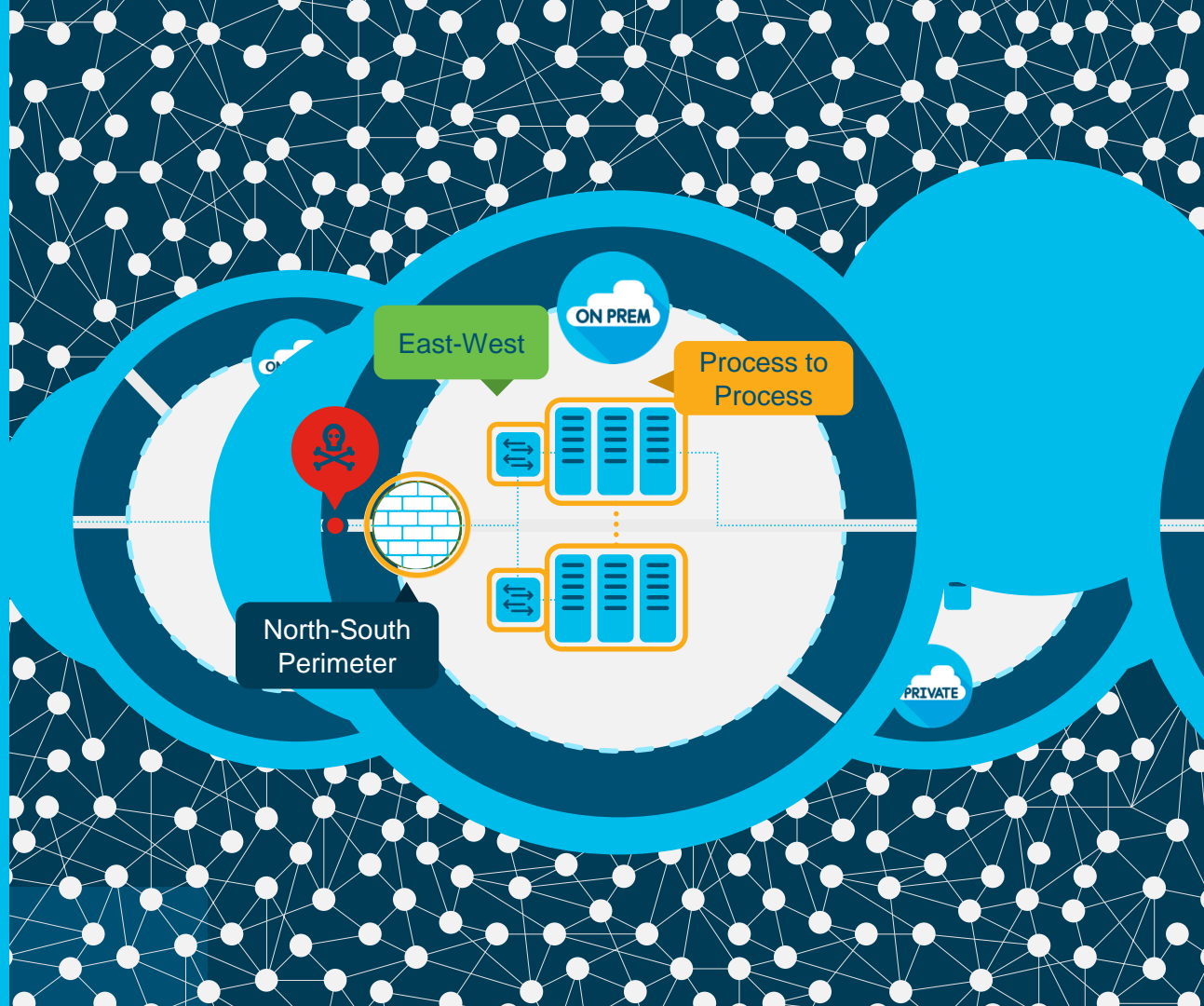


Segmentation: Reduce the Attack Surface

Cisco NGFW

Cisco ACI

Cisco Tetration



01



02



03

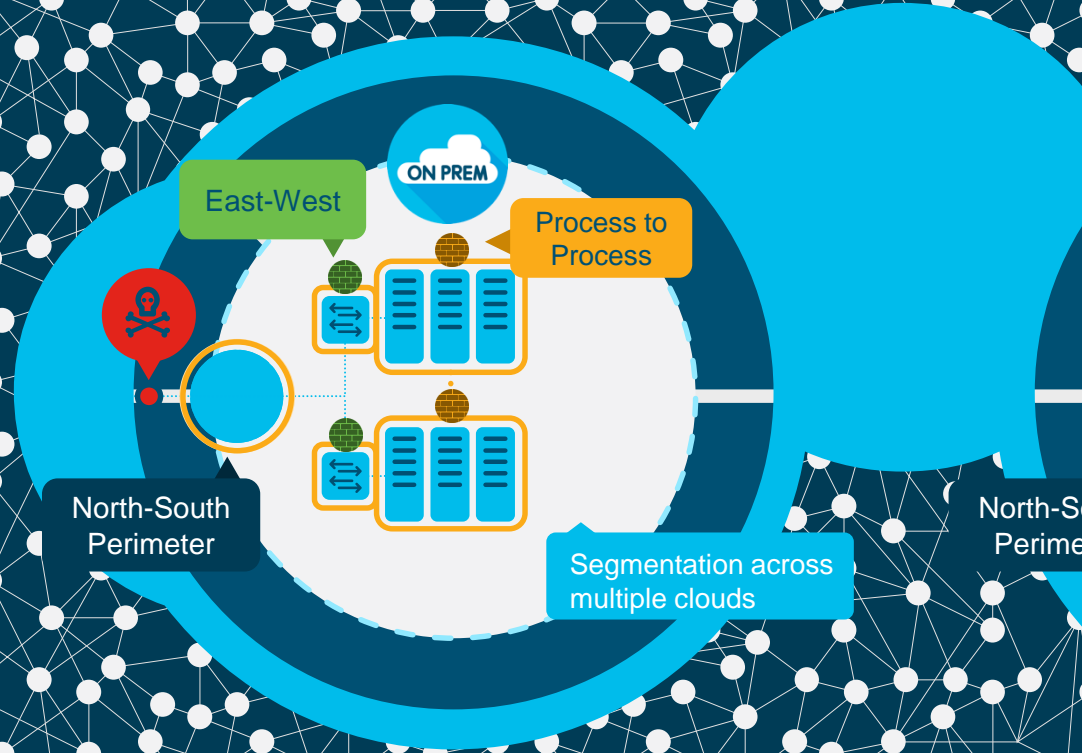


Segmentation: Reduce the Attack Surface

Cisco NGFW

Cisco ACI

Cisco Tetration



North-S
Perime

01



02



03



Threat Protection: Stop the Breach

By strategically deploying threat sensors north-south, east-west

Multi-Layered Threat Sensors

Quickly detect, block, and respond dynamically when threats arise to prevent breaches from impacting the business



Next-Gen IPS with AMP



Next-Gen Firewall with Radware DDoS



Next-Gen Firewall with AMP



Stealthwatch



Cisco ACI

Cisco Tetration

01



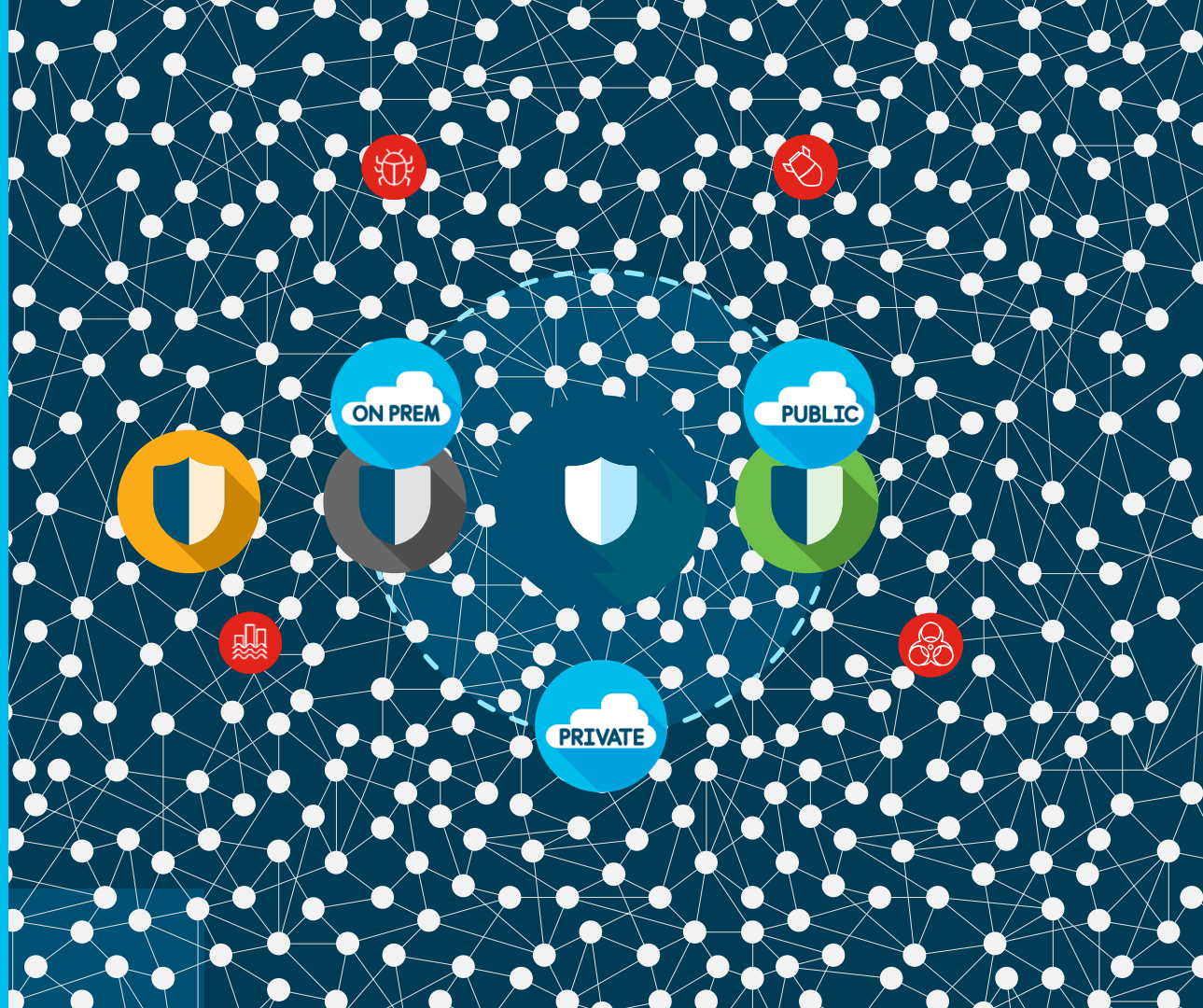
02



03



Protect the Workload Everywhere



AMP helps detect and mitigate threats that have evaded defenses



Make the unknown,
known



See once, block
everywhere



Accelerate security
response

Cisco Security Architecture: Security that works together



Threat Intelligence

- Threat Hunting and research
- Cross-portfolio notification

Event Data and Correlation

- Common view of threat information
- Dynamic, event-driven alarms

Policy Information

- Situational and contextual awareness
- See it once, block it everywhere

Contextual Information

- Applications, Operating Systems
- Who, What, When, How, Where

