Changing Security Defense Strategies in a Borderless World

Stew Wolfe, CISSP, CISM, CISA

Cisco Global Security Services

HIMSS

CENTRAL & SOUTHERN OHIO Chapter

Considerations for Security Strategy

Changing Business Models

Dynamic Threat Landscape

Complexity and Fragmentation

Resource & Talent Shortage

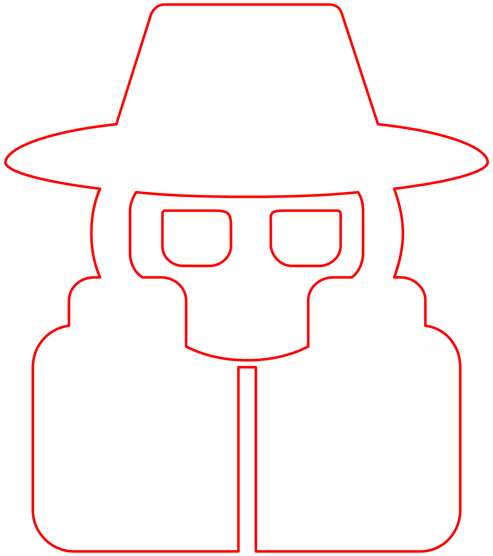
82% Realize They Need an Integrated Security Architecture

Source: ESG Cybersecurity Sentiment Findings 2016

20%

That’s the average functionality used of the security tools you own (and pay maintenance on each year)

Industrial Hackers Are Making Big Money with Innovative Tactics



Global Cybercrime
Market $450B–$1T

Is Ethical Hacking still effective?

Infrastructure

Building Out of Digital Economy on Fragile Infrastructure

Fragile, insecure infrastructure will not securely support the next-generation economy

Average time devices run known vulnerabilities

Top Cyber Challenges

- Protect from insider attacks
- Protect from unauthorized access to critical apps
- Establish best practices in architecture security
- Efficiently operate existing security infrastructure

What Mature Cyber Looks Like

- Overall focus on cyber program maturity (CMMI)
- Equal Focus on Operational Maturity and compliance
- Analytics, SOC vs MDR
- Plan for Segmentation

Top Causes of Breaches

- Weak security framework
- Open to privilege escalation
- Unmonitored new attack surface
- Lack of coordination between IR and third party risk

We need to work SMARTER not HARDER

Profile of a Cloud Optimized Organization

Multicloud Adoption

84%

Expect to choose from multiple cloud providers

Containers

66%

Believe Containers are important to their Cloud Strategy

Microservices

79%

Develop application using Microservices

DevOps

80%

Use DevOps practices

Governance

82%

Have robust cloud governance policies in place

Cloud IoT Apps

62%

Have adopted cloud based IoT applications and of those 53% in a private cloud environment

Cloud Security Apps

40%

Use cloud delivered management of security devices, located on or off-premises

Source: IDC InfoBrief, sponsored by Cisco, Cloud Going Mainstream. All Are Trying, Some Are Benefiting; Few Are Maximizing Value. September 2016

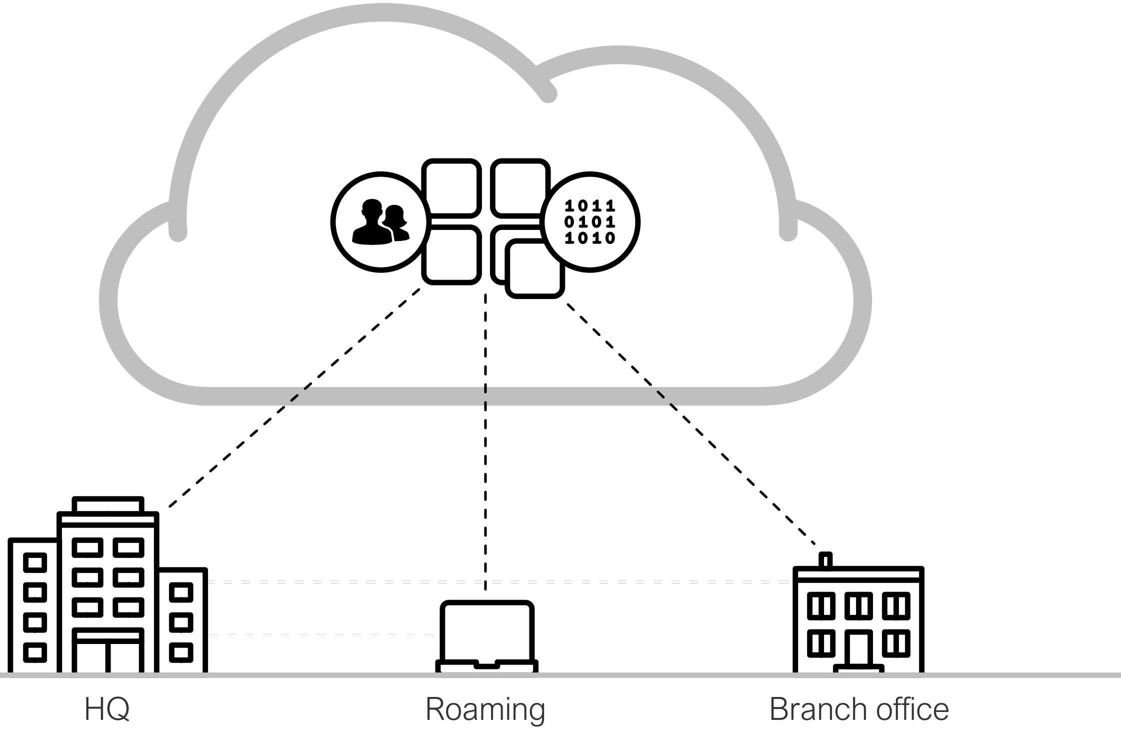
What’s changed

Apps, data, and identities move to the cloud

Business drives use of cloud apps and collaboration is easier

No longer need VPN to get work done

Branch offices have direct internet access



Secure Internet Gateways

- Visibility / Enforcement – User request patterns, reputational scores/statistics
- Port/protocol protection
- Proxy file inspection
- Shadow IT discovery

DNS & IP layer enforcement

Umbrella uses DNS to stop threats over all ports and protocols – even direct-to-IP connections. Stop malware before it reaches your endpoints or network.

Intelligent proxy

Instead of proxying all web traffic, Umbrella routes requests to risky domains for deeper URL and file inspection. Effectively protect without delay or performance impact.

Command & control callback blocking

Even if devices become infected in other ways, Umbrella prevents connections to attacker's servers. Stop data exfiltration and execution of ransomware encryption.

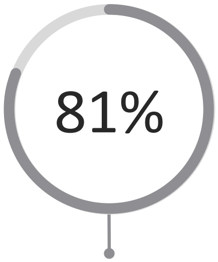
A Cloud Access Security Broker (CASB) addresses customers’ most critical cloud security use cases

Discover and Control

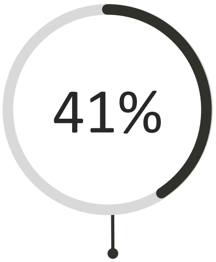
- Compromised Accounts
- Insider Threats
- Data Exposures and Leakages
- Privacy and Compliance Violations
- Cloud Malware
- Shadow IT/OAuth Discovery and Control

- User and Entity Behavior Analytics
- Cloud Data Loss Prevention (DLP)
- Apps Firewall

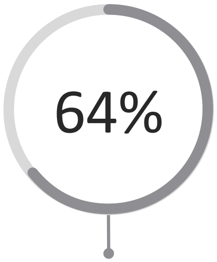
New threat landscape



of organizations have been victims of a cyber attack

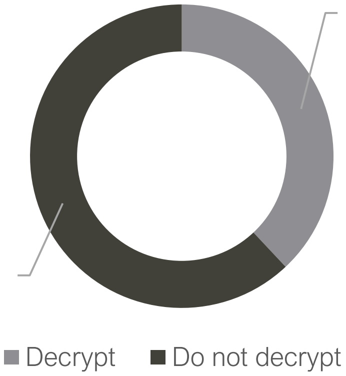


of attackers used encryption to evade detection



cannot detect malicious content in encrypted traffic

Organizations are at risk



New attack vectors

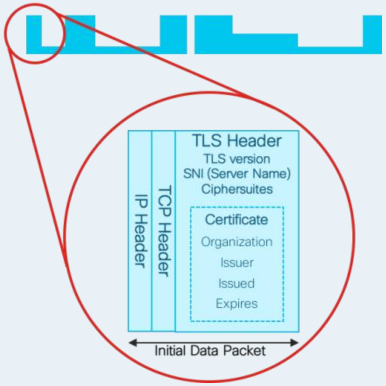
- Employees browsing over HTTPS: Malware infection, covert channel with command and control server, data exfiltration
- Employees on internal network connecting to DMZ servers: Lateral propagation of encrypted threats

Source: Ponemon Report, 2016

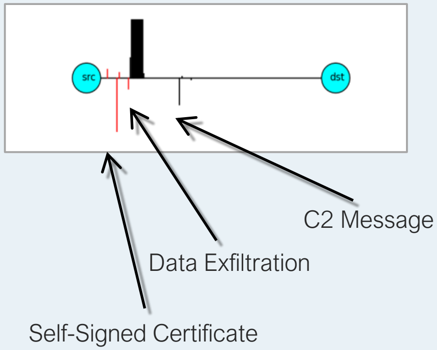
How can we inspect encrypted traffic?

Initial Data Packet

Make the most of the unencrypted fields



Sequence of Packet Lengths and Times



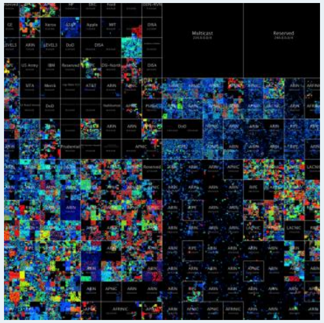
C2 Message

Data Exfiltration

Self-Signed Certificate

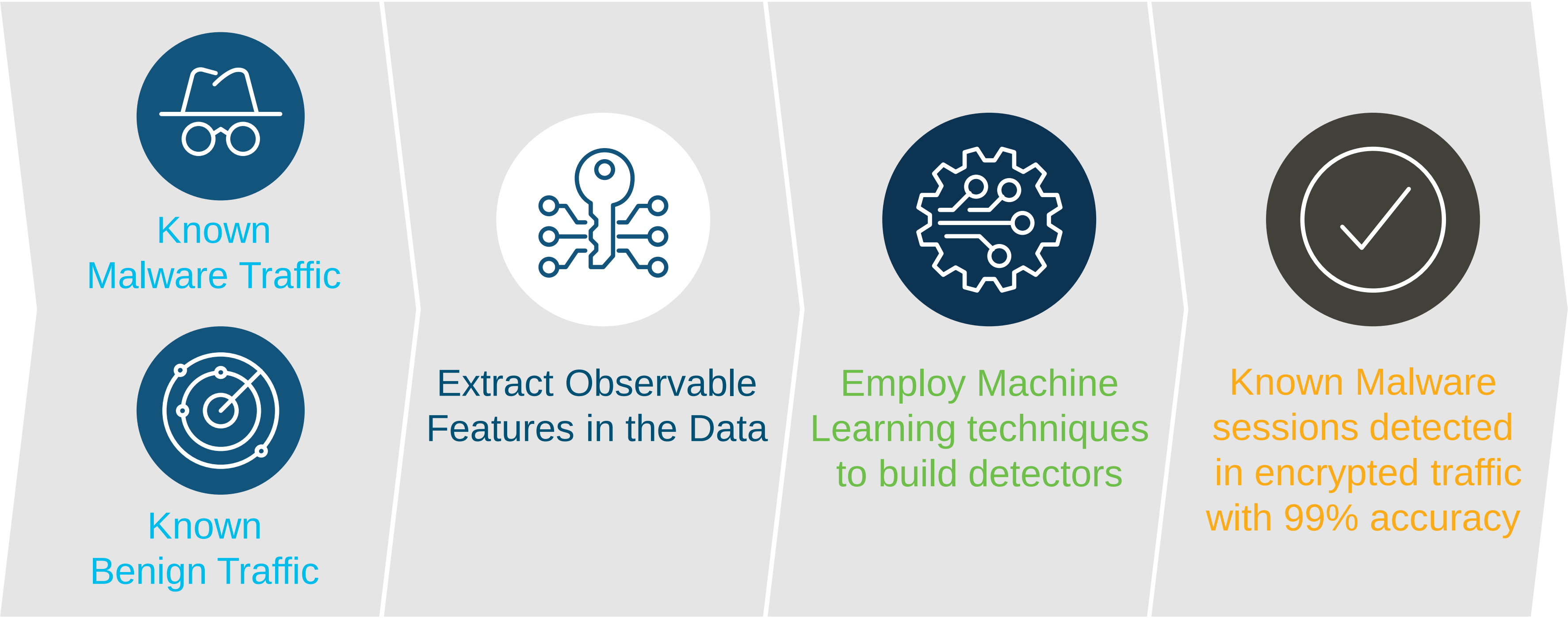
Threat Intelligence map

Who’s who of the Internet’s dark side



Broad behavioral information about the servers on the Internet.

Encrypted Traffic Analytics (ETA)



Known
Malware Traffic

Known
Benign Traffic

Extract Observable
Features in the Data

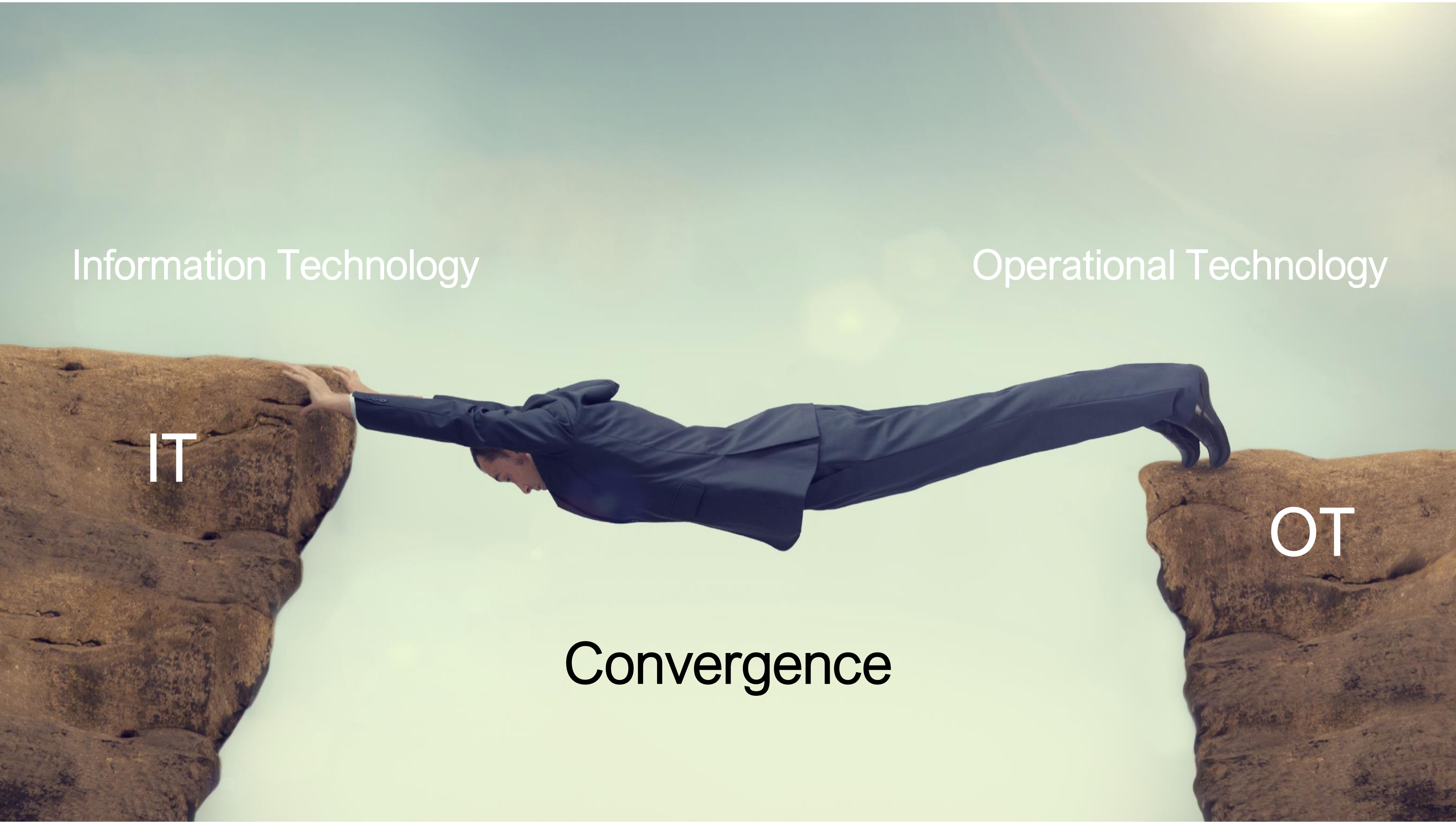
Employ Machine
Learning techniques
to build detectors

Known Malware
sessions detected
in encrypted traffic
with 99% accuracy

“Identifying Encrypted Malware Traffic with Contextual Flow Data”

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

Tools That Enable Security Segmentation



1K 1M 1B 10B

50B

CONNECTED THINGS

Projection:
IoT devices accounts for **83%** of all Internet connections by

2020

- 90% of world’s data created in the last 2 years
- By 2020, 40% of data will come from sensors

4 Billion
Connected People

25+ Million
Apps

25+ Billion
Embedded and Intelligent System

50 Trillion
GBs of Data

Source: Mario Morales, IDC

Connected Cities

1 Citizen Services

2 Citizen Engagement

3 Parking optimization

4 Incident management

5 Public safety

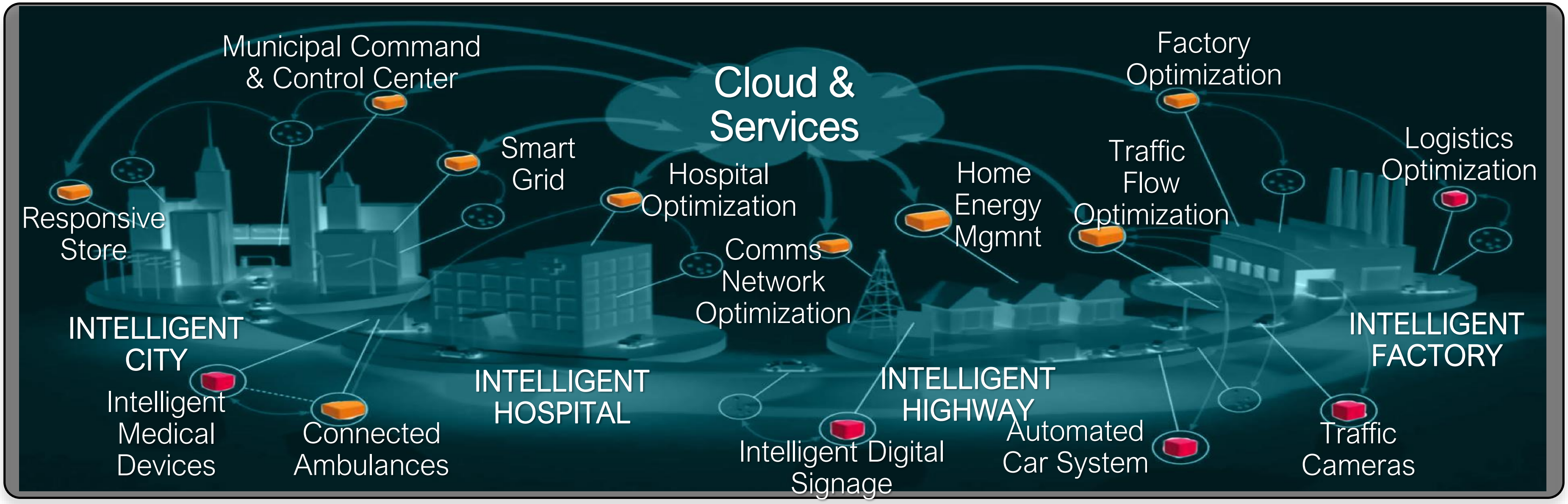
6 City lighting

7 Transportation

8 Sports & Entertainment

9 Education

10 Health & Wellness



Source: Intel

Securing the Internet of Everything

Organizations worldwide are becoming digital to capitalize on the unprecedented opportunity brought about by the next wave of the internet – the Internet of Everything (IoE). While creating incredible opportunity this transformation also presents new challenges.

CEO's Top Challenges

42%
Threat to data or physical security

38%
Inability of IT to keep pace with change

32%
Regulatory or compliance challenges

IoE Creates More Attack Vectors

Increased connectivity creates more attack vectors for bad actors to exploit. With such a dynamic threat landscape, security is constantly changing, increasingly complex, and critical to success.

65% of companies said they couldn’t stop the breach because it evaded their existing preventative measures.

55% of companies couldn’t identify where in their network the breach occurred.

33% of companies took more than 2 years to discover a breach occurred.

52% of companies said they lost reputation, brand image, and marketplace value due to a breach.

Isolate & Segment

Building Management Systems & Third Party Vendors

Isolate & Segment

Legacy Medical Devices

Segmentation Improves Patient Safety

Segmentation Slows IP Theft - Clinical Research

802.1x Network Access Control Profiling

- Profiling is:
  - Dynamic classification of every device that connects to network using the infrastructure.
  - Provides the context of "What" is connected independent of user identity for use in access policy decisions

PCs	Non-PCs				
	UPS	Phone	Printer	AP	Infra

- What Profiling is NOT:
  - An authentication mechanism.
  - An exact science for device classification

How Do you Profile?

Collection

NMAP AD NetFlow

HTTP SNMP LLDP

Radius DNS DHCP

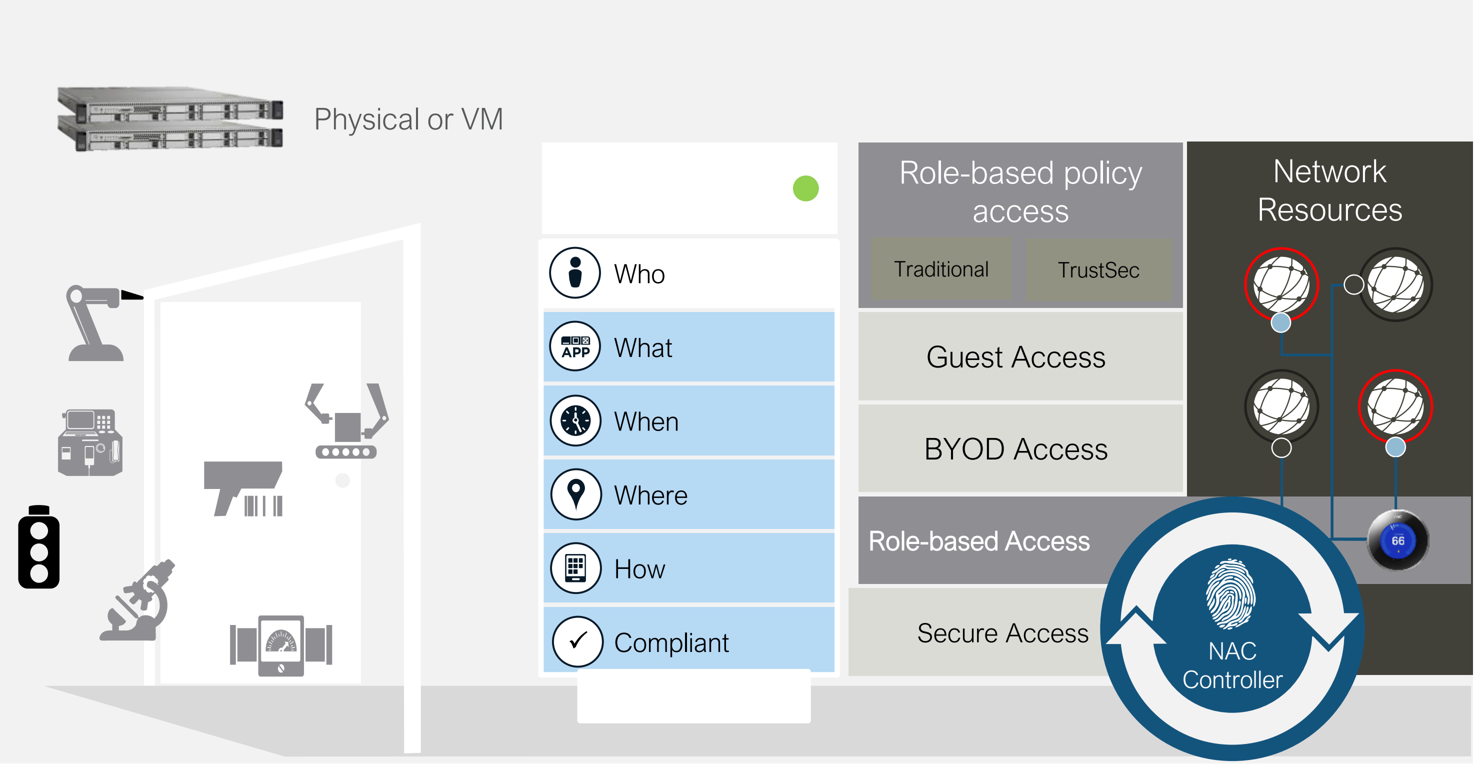
- Process of collecting data to be used for identifying devices
- Uses Probes for collecting device attributes

Classification

Classifies based on Device fingerprint

Network Access Control – Wired & Wireless

Applies Policy to Identity Context to Control Access



Today’s world of IoT and threats everywhere requires access control based context that comprises device type, user, time, location and many more attributes.

NAC uses the most advanced probes to identify device types and match them to policy. It can also enforce policy on wired devices without 802.1X agents.

NAC uses NGFW to apply different policies based on the context. NAC uses the network to control access to resources such as applications in a TrustSec or ACI data center.

Context Is Everything

IP Address: 192.168.2.101	Unknown	Infusion Pump	Known
Unknown		Vendor	
Unknown		Building-A Floor-1	
Unknown		10:30 AM EST on April 27	
Unknown		Wireless / Ethernet / Zigbee	
Unknown		No Threats / Vulnerabilities	

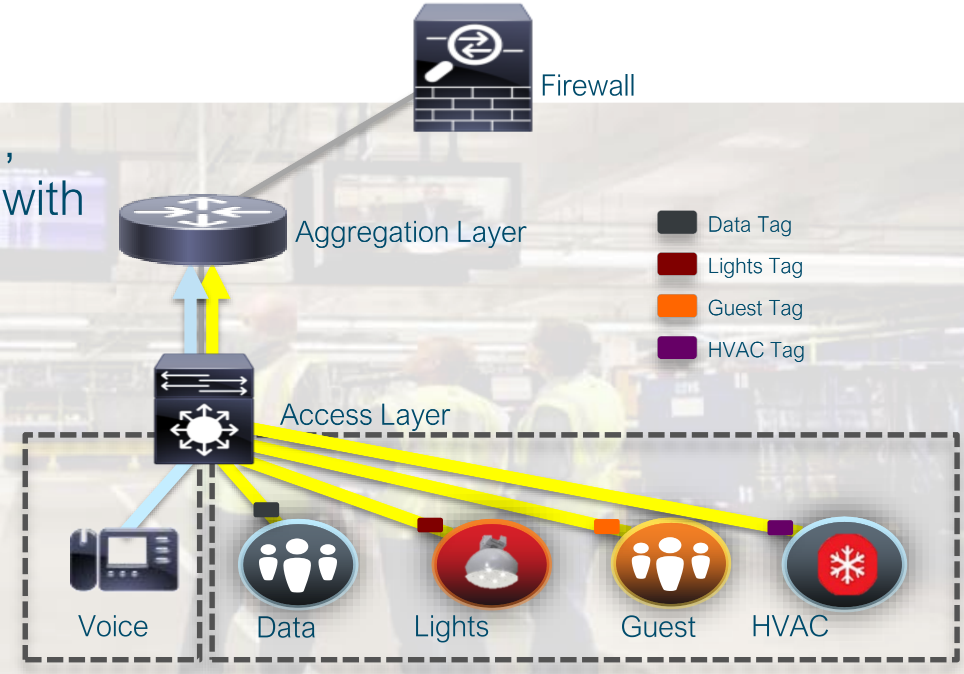
WSA NGIPS FMC NGFW

NAC Controller

Stealthwatch AMP TrustSec

Policy and Segmentation with TrustSec

Regardless of topology or location, policy (Security Group Tag) stays with users, devices, and servers



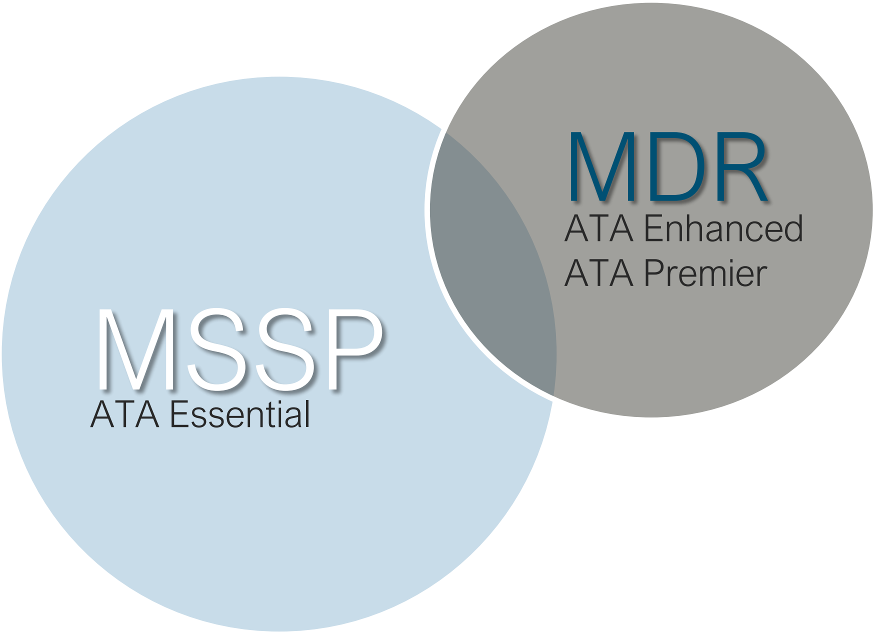
Retaining initial VLAN/Subnet Design

Big Data - Security Analytics

Big Data - Patient Diagnosis

Better Patient Outcomes

Gartner: Managed Detection and Response (MDR)



What is MDR?

It is a new category focused on improving threat detection and incident response.

It generally relies on threat intelligence and advanced analytics, with several offerings leveraging big data platforms for advanced detection.

It is an emerging market:

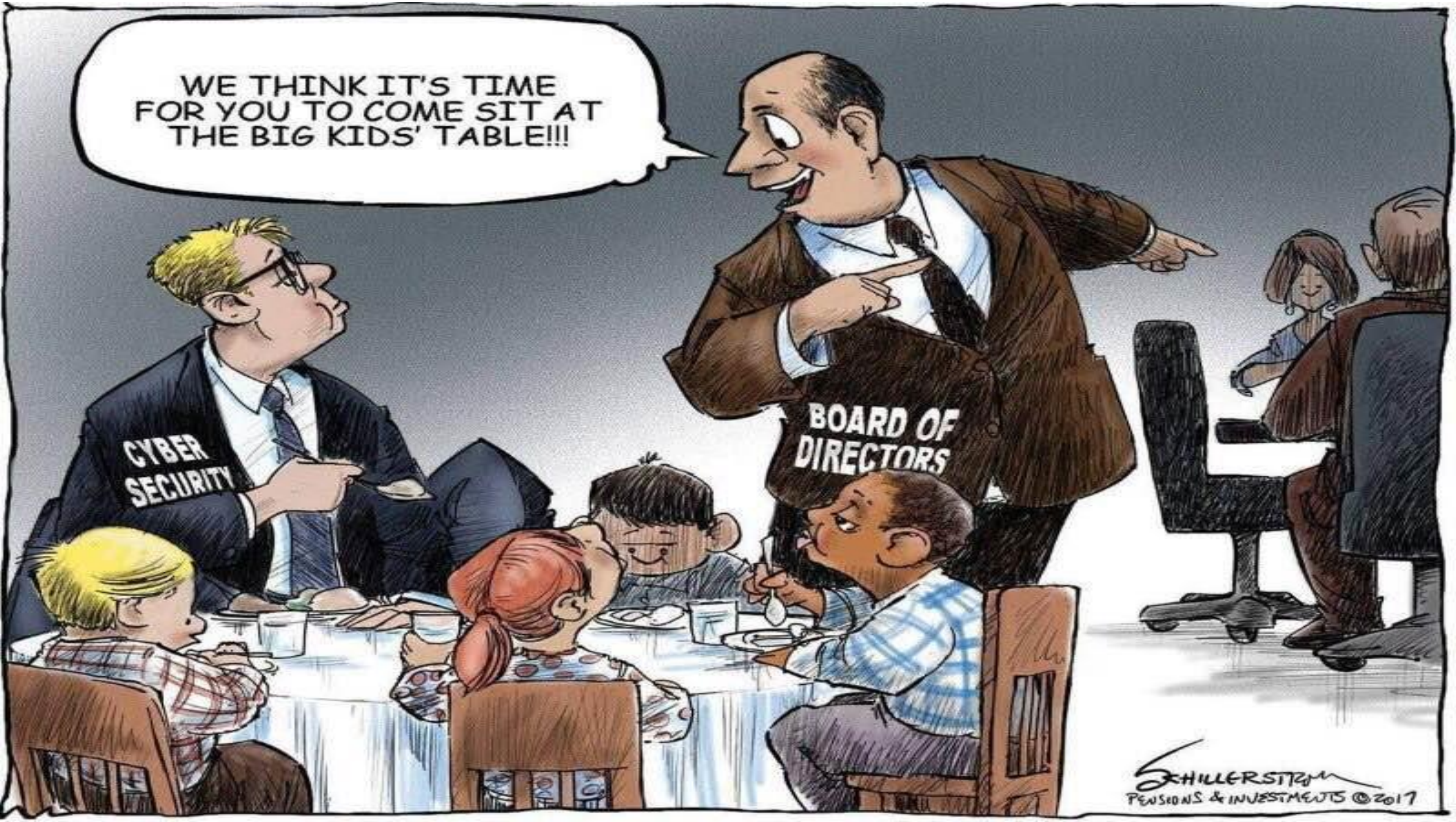
- By 2020, Gartner expects 15% of organizations will be using MDR and 50% of MSSP’s will offer MDR services

Why Cisco - Analytics Methods

Service Differentiator

	Deterministic Rules-Based Analytics (DRB)	Statistical Rules-Based Analytics (SRB)	Data Science-Centric Analytics (DSC)
Examples	• Signature based detection • Alerting when predefined thresholds are exceeded • Identification of outbound communication to known C&C domains or IPs	• Unusual system changes such as from non-standard administrator accounts or bulk changes at unexpected times • Highlight abnormal levels of data export from critical systems	• Automated categorization of data, such identifying classified documents • Alert on activity gathering around a high value asset. Ex) a classified asset is port scanned, then logged into from a foreign IP, then injected with malware
Characteristics	• Mature method of analysis • Covers a majority of known threats • Fast to detection	• Anomaly detection based on historical context (i.e. highlighting atypical behavior) • Dynamic outlier detection independent of predefined thresholds	• Adaptive learning to automatically tune system for useful alerts • Clustering information around specific attributes to identify behavioral anomalies • Extrapolation of future threat behavior to reduce time to detect
Effort Required	• Creation of rules library based on current known threats • Ongoing maintenance and tuning of rules library	• Accurate tuning of false positives to be fed back into the system • Intimate knowledge of use cases and environment to train models	• Accurate tuning of false positives to be fed back into the system • Intimate knowledge of use cases and environment to train models

As always, for security, it starts with designing the right policies & processes


WE THINK IT'S TIME FOR YOU TO COME SIT AT THE BIG KIDS' TABLE!!!
CYBER SECURITY
BOARD OF DIRECTORS
SCHILLERSTROM
PENSIONS & INVESTMENTS © 2017

Questions to Ask Yourself

1. What business benefits it will provide to the organization?
2. How will it impact Patient Care and Patient Safety?
3. How will it improve a Physician Workflow?
4. What business risk gaps will each tool address? (Business Justification)
5. What legacy tools it will retire? (You don’t want more to manage)
6. How easily can each tool be integrated into the existing infrastructure?
7. How long will it take to implement?
8. What are the Integration costs?
9. What is the TCO including staff training?

To Summarize:

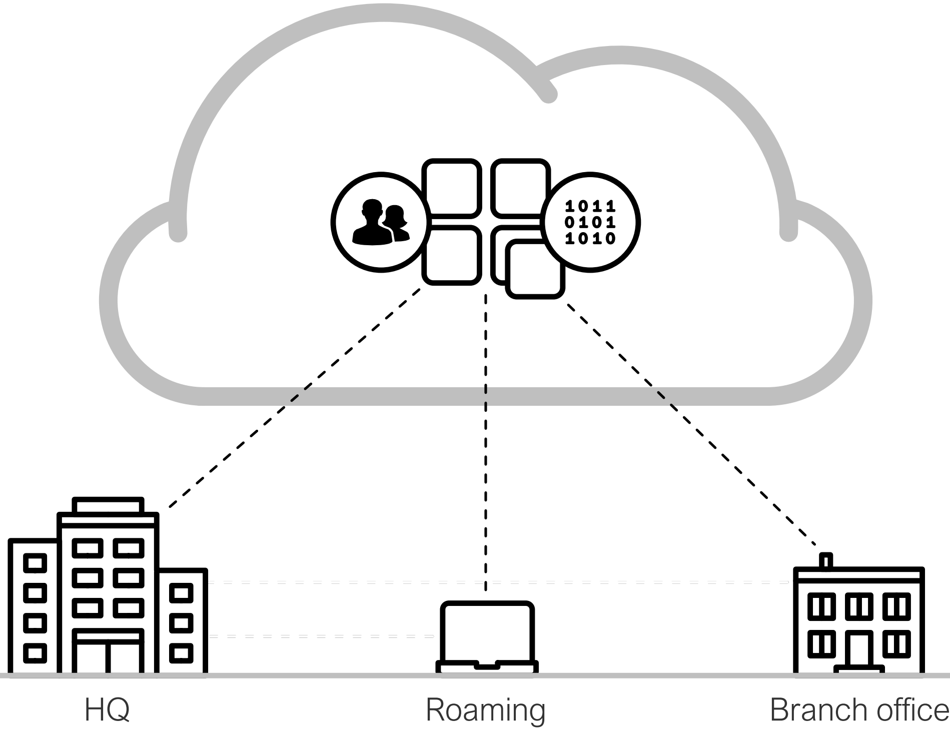
Use Secure Internet Gateways and CASB solutions for users who are no longer protected by corporate network controls

Inspect all traffic for malicious behavior including encrypted and unencrypted data

Ensure that Internet of Everything devices are secure and segmented

Employ Managed Detection and Response solutions – Full Packet Capture, Big Data combined with Behavioral and Statistical Analytics for an East West as well as North South view of threats to detect what you don't know

Establish good governance practices to align the needs of the business with IT and Security


1011
0101
1010
HQ
Roaming
Branch office