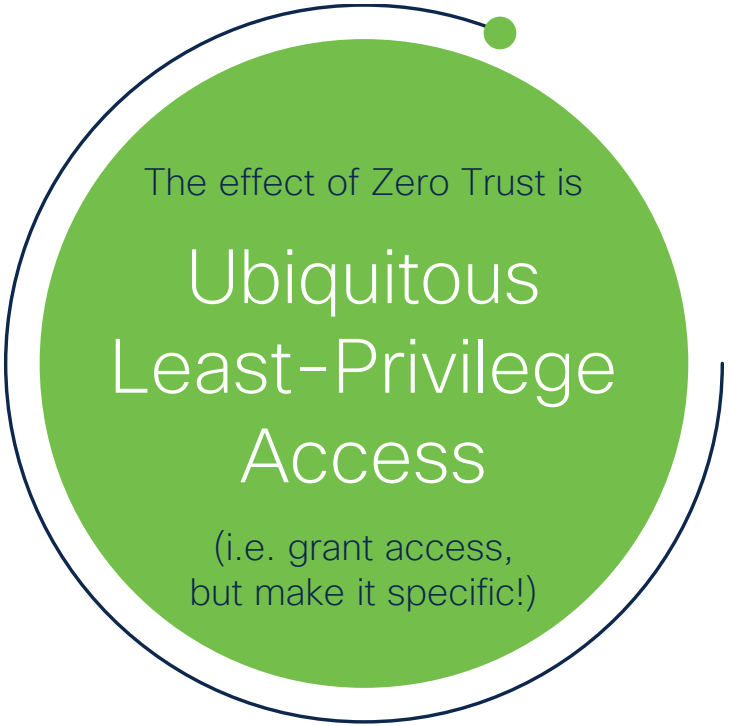
Reimagine The Firewall

Threat – Detection and Response

Timothy Snow
Architect. CyberSecurity. APJC
@TimSnowIT

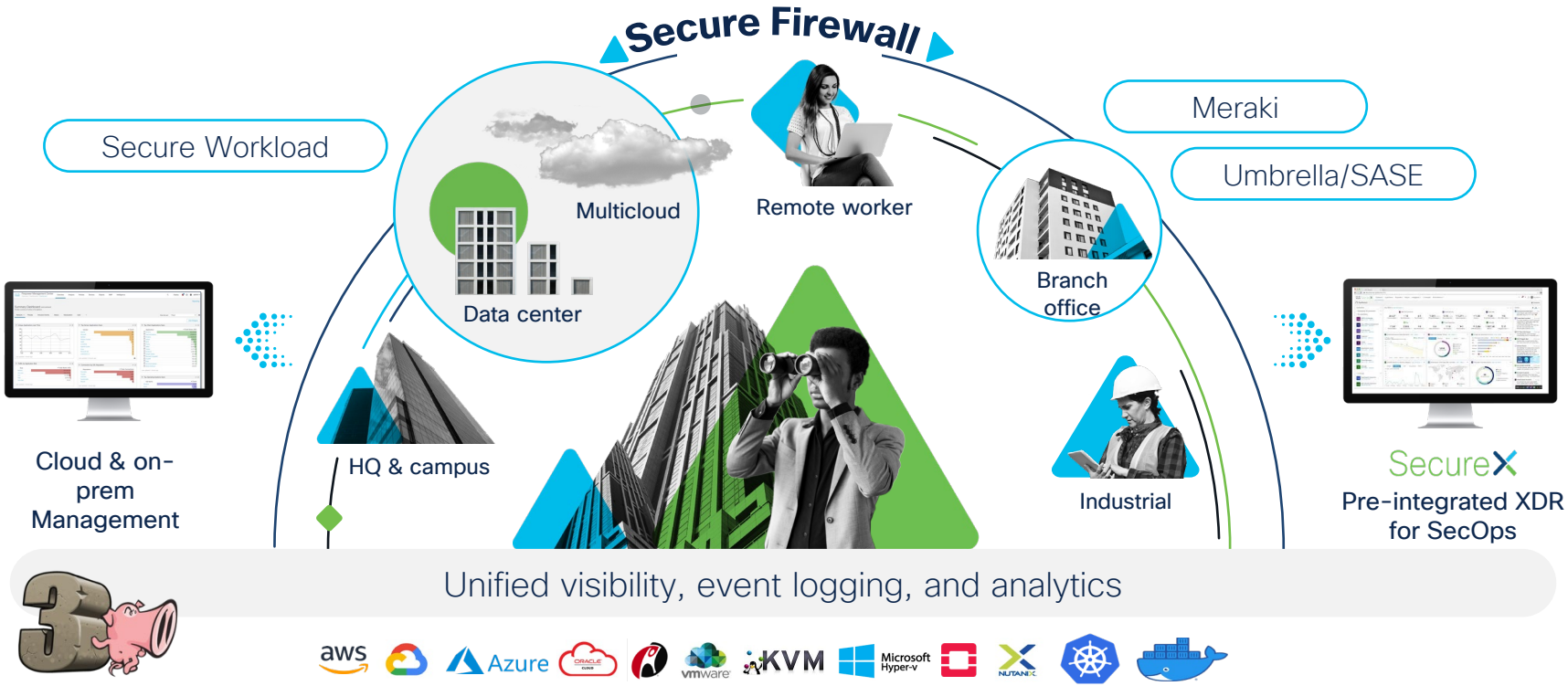
Five Fundamental Assertions of Zero Trust

- The network is always assumed to be hostile
- External and internal threats always exist on the network
- Network locality is not sufficient for deciding trust in a network
- Every device, user, and network flow is authenticated and authorized
- Policies must be dynamic and calculated from as many sources of data as possible



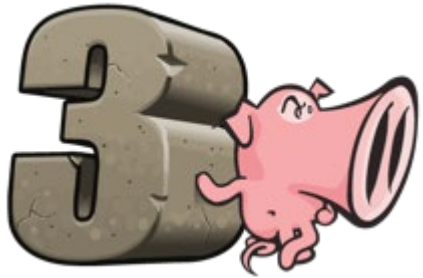
Cisco Secure Firewall – Version 7.0!

The future of firewalling, today



Superior Threat Visibility with Snort 3

Next generation of the de facto standard deep packet inspection engine, now leveraged across Cisco Security



More Powerful Rule Creation

New human-readable natural signature language

Greater Visibility

Modular Updates, Expanded inbound/outbound web application security with HTTP/2 processing

Higher Efficacy

New parallel architecture allows more rules with less resource consumption and faster/deeper pattern lookups

Now available in:

- Secure Firewall
- Meraki MX
- Umbrella SIG / SASE

Snort 2 vs. Snort 3

	Snort 2	Snort 3
Multi-Threaded Architecture		✓
Capable of running multiple Snort Processes	✓	✓
Port Independent Protocol Inspection		✓
IPS Accelerators / Hyperscan Support		✓
Modularity – for upgrading component capabilities		✓
Scalable Memory Allocation		✓
Next Gen Rules – e.g., Regex/Rule Options/Sticky Buffers		✓
New and Improved HTTP Inspector with HTTP/2 support		✓
Lightweight content updates from TALOS (LSP)		✓

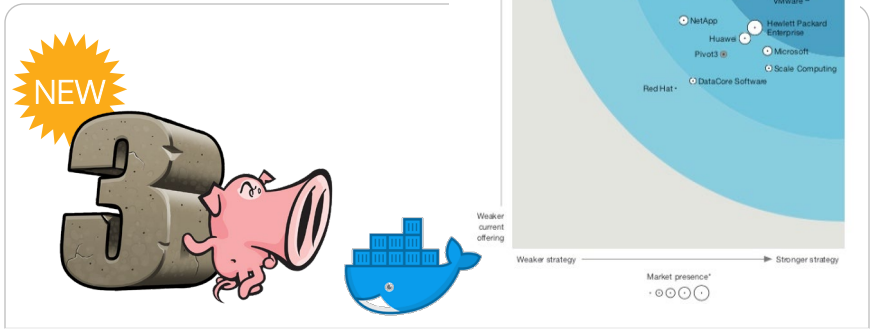
Performance Increases!

Firepower Threat Defense 7.0 Performance Improvements with Snort3		
Model	**NGFW Throughput**	**VPN Throughput**
Firepower 1000 Series	Up to 40%	Up to 80%
Firepower 2000 Series	Up to 20%	Up to 25%
Firepower 4000 Series	Up to 30%	Up to 50%
Firepower 9000 Series	Up to 60%	Up to 40%
Firepower Virtual	Up to 10% for VMW/KVM & up to 100% for Azure	Up to 40%

Note: % varies across individual appliances - Please refer to data sheets

Cisco Secure Firewall Virtual (FTDv)

- Optimized for cloud and data center environments
- VMware, KVM, OpenStack, Nutanix AHV , Cisco HyperFlex, containers such as Docker
- AWS, Azure, Azure government cloud, GCP and OCI
- **15 Gbps** throughput firewall + **AVC, AVC + IPS**
- Stateful firewall, Application Visibility and Control, NGIPS, Advanced Malware Protection, URL filtering, VPN



Features & benefits

Automated risk rankings and impact flags

Threat detection time of less than a day

Unified management and automated threat correlation

Protecting Users & Applications at Hyper Scale

Capabilities

Agile → Scalable → DevOps → CI/CD → PAYG/Tiered → Multicloud

Portfolio

Secure Firewall Virtual

ASA

Threat Defense (IPS, AMP, URL)

Secure Firewall Cloud Native (Containers)

Secure Workload

aws, Azure, vmware, Microsoft Hyper-v, KVM, OPENSHIFT, openstack

Use Cases

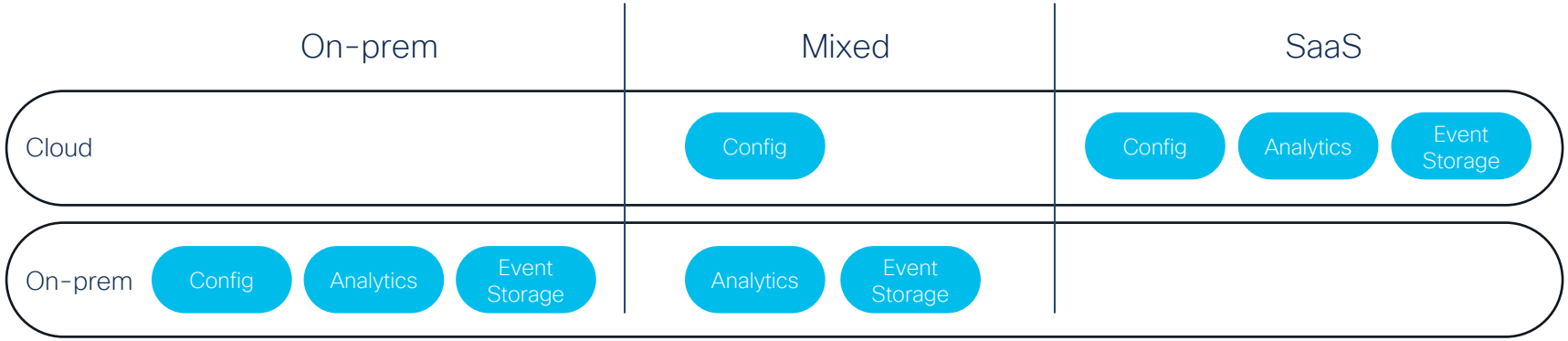
User

- Remote access VPN
- Internet/data center edge
- North-South inspection

Application

- Policy Discovery
- Micro-segmentation
- Inter VPC
- East-West Inspection
- CI/CD integrated security
- Insertion in app-cluster

What We're Delivering:
Flexibility of Management Consumption



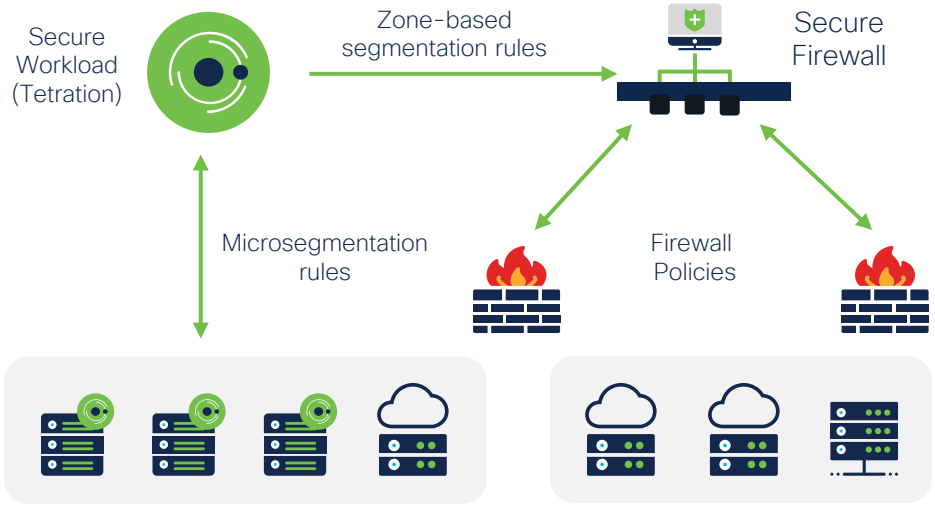
- Driven by security concerns or regulatory compliance
- Government, financials

- Sensitivities around customer data
- Retail, financials

- Cloud-first approach
- Technology, startups

Increasing customer cloud acceptance

Dynamic Policy Across Multicloud Environments



Seamless Integration

Unified segmentation policy across Secure Firewall & Secure Workload

Dynamic Policies

Policy updated dynamically based on application communications information

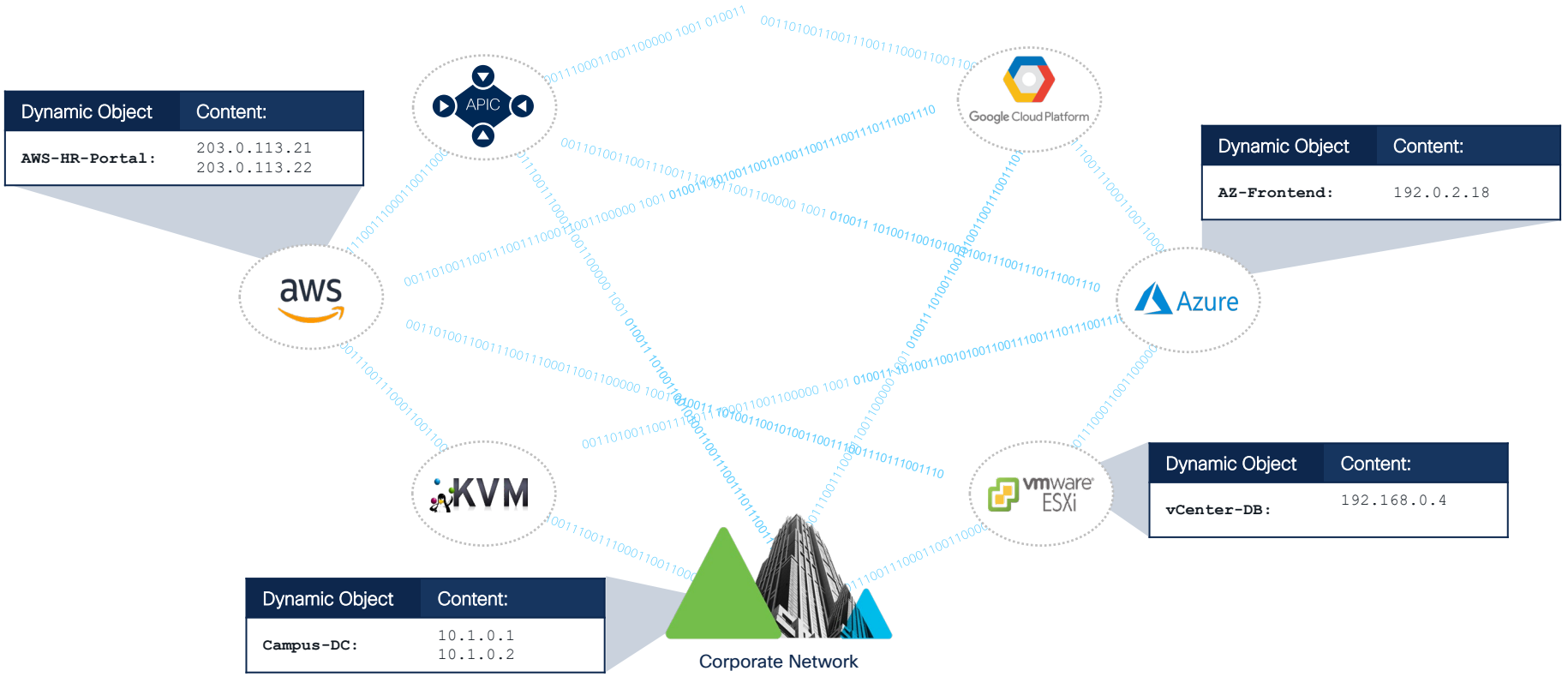
Expanding to Cloud Providers

This fall, extending recommendation functionality to AWS and Azure security groups

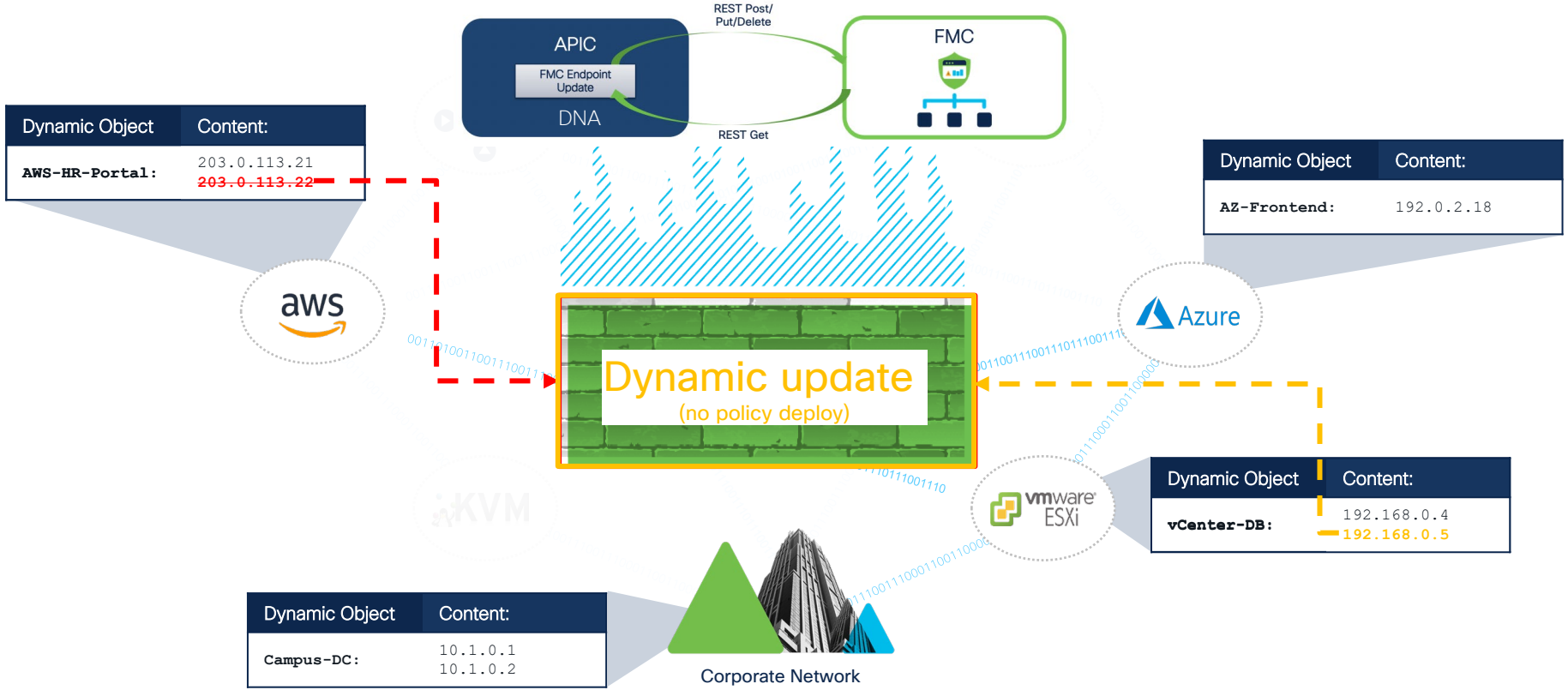
“ Eagerly awaiting this! Integration across our multicloud controls will help drive better security in our distributed environment. ”

-- Global payments and fleet management enterprise

Dynamic Objects

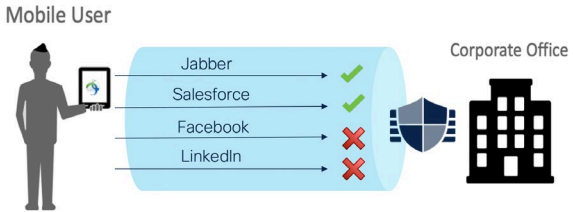


Dynamic Objects

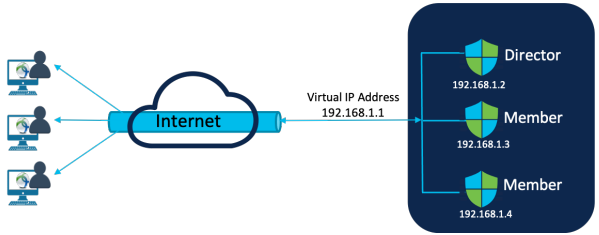


Remote Worker Enhancements

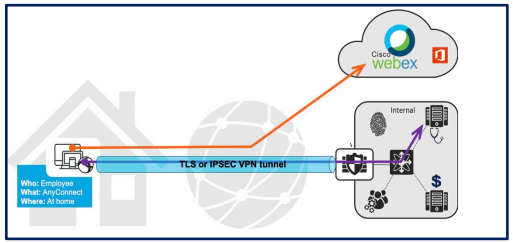
Delivering rapid, secure remote access



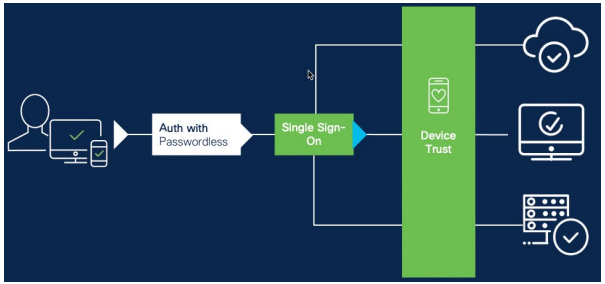
Per App VPN Tunneling



VPN Session Load Balancing



Dynamic Split Tunneling
(Exclude/Include)

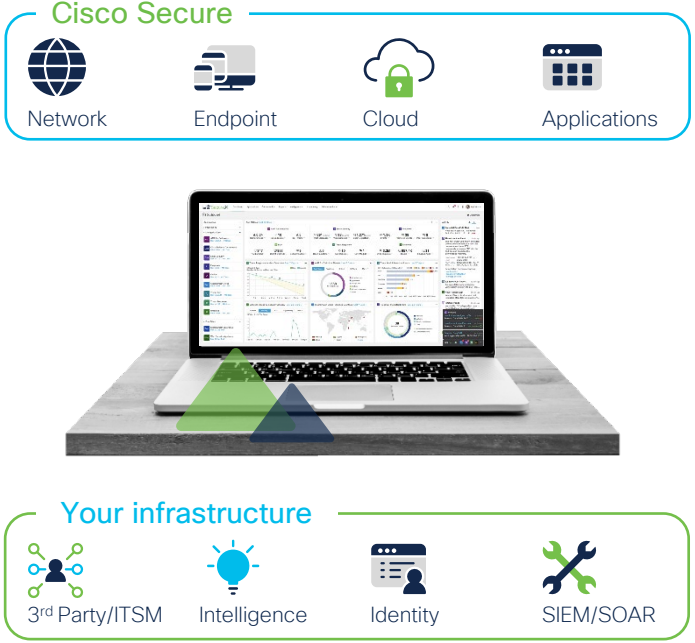


The move to passwordless with MFA

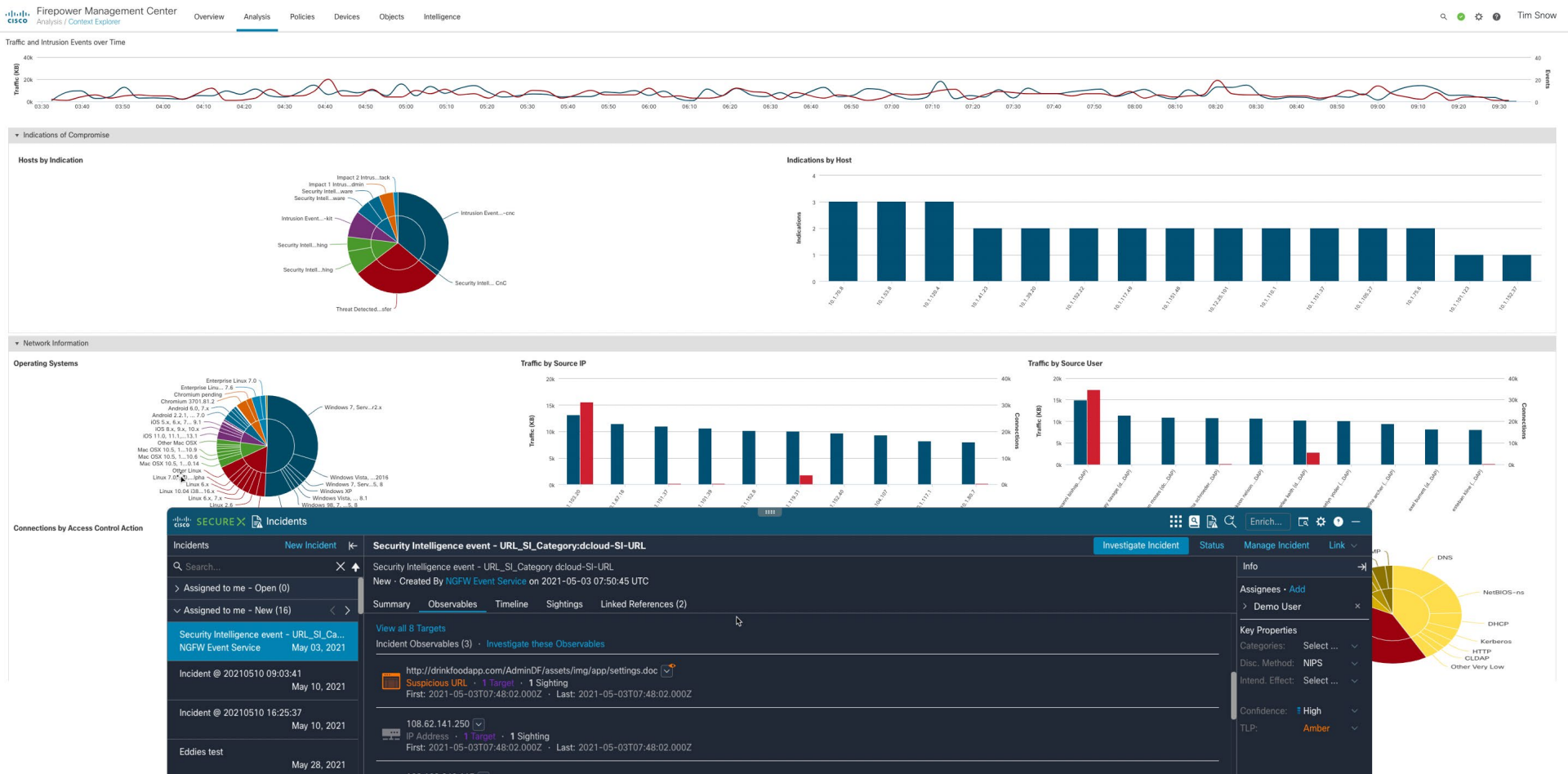
Cisco SecureX is a force-multiplier for your firewalls

Connect Cisco's integrated security portfolio to your existing infrastructure for a consistent experience that can:

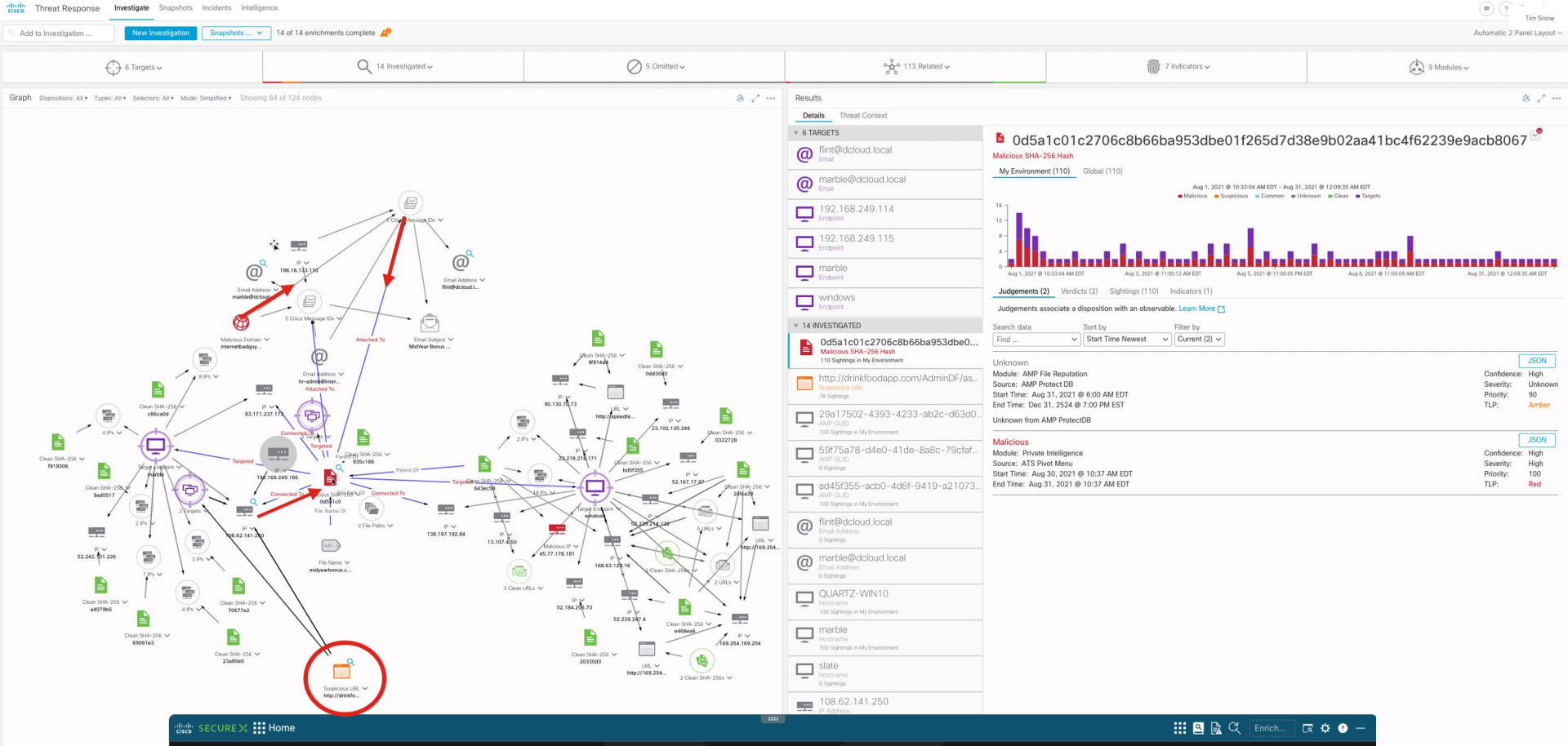
- **Orchestrate pre-built playbooks;** simplifying incident response
- **Enhance collaboration** between NetOps, ITOps and SecOps
- **Strengthen breach defense** unifying visibility with alerts correlated and prioritized from other integrated Cisco Secure and third-party solutions
- **Optimize network performance,** automating VPN capacity management to facilitate continued remote worker productivity



New UI and SecureX Integration



New UI and SecureX Integration



BBVA

"We wanted to standardize on a single networking architecture globally. We chose Cisco networking with Cisco DNA Center, Secure Firewall, and SD-Access because of the complete zero trust security it offers with continuous monitoring and verification of trust in our connected endpoints."

~ Carlos de Liniers, Senior Manager, Network Architecture & Global Deployment, BBVA

Industry: Financial
Region: Americas - Colombia
Use Cases: Network Device Onboarding, Campus Network Segmentation, Zero trust security, trust analytics

Challenges

- IT in BBVA sites across the world are maintained by local teams – sometimes leading to inconsistencies
- IT infra to adapt to agile digital transformation requirements securely.
- Malware in connected endpoints could compromise personal and financial data

Products/Capabilities

- Cisco Networking
- Cisco DNA Center
- Cisco Identity Services Engine (ISE)
- Cisco Catalyst 9000 series of switches
- Cisco Meraki Wi-Fi access points
- Cisco Secure Firewall 9300, FPR4K (NGIPS, ASA, FTD) and Cisco ISE software licenses

Results

- A standard secure access architecture removed inconsistencies and led to more predictable outcomes
- No manual effort required for employee movement as access policies handle configuration changes automatically
- Posture monitoring of all endpoints detects and isolate /flag any anomalous behavior

https://blogs.cisco.com/networking/bbva-uses-cisco-dna-center-and-sd-access-to-verify-trust-and-prevent-financial-fraud?oid=pstswt026154

Cisco is a Leader
2020 Forrester Wave for Enterprise Firewalls

Cisco firewalls recognized as a leader!

- #1 in Current Offering with top marks for
  - Zero Trust, workload protection, Threat Intelligence, cloud-delivered components, micro-segmentation, firewall-as-a-service, and usability
- #1 in Market Presence
- A leader in Platform Strategy
- Earned a perfect 5/5 for Product Vision!

Source: The Forrester Wave™: Enterprise Firewalls, Q3 2020, by David Holmes, August 10, 2020

Fit-for-purpose firewalls

From the Industrial Firewall to the high end multi-terabit Data Centers and Service Providers

Increase uptime & performance w/ clustering, integrated Radware DDoS protection

ISA 3000

1000 Series

2100 Series

4100 Series

9300 Series

industrial | branch | enterprise | campus | data center | service provider

Snort 3 increases efficacy, enables feature velocity and huge performance benefits

Azure

aws

Google Cloud

ORACLE Cloud Infrastructure

Our virtual firewalls support public, private, & hybrid cloud

Eliminate gaps! Integrates with Cisco SecureX, Secure Endpoint, Duo, & Umbrella.

Thank you