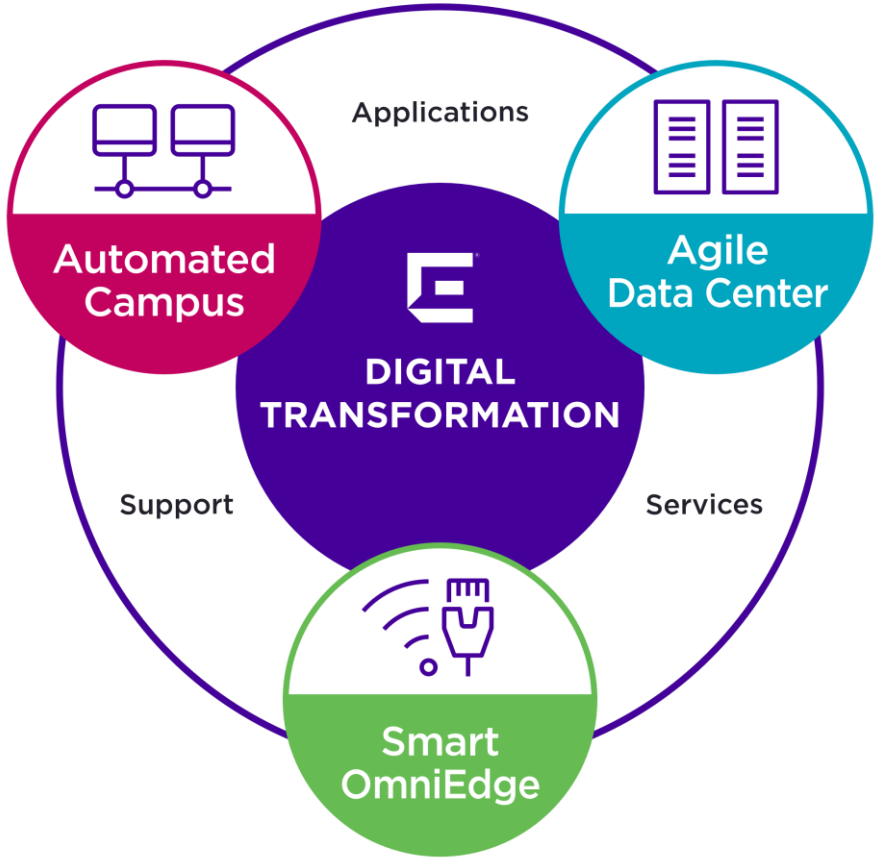
Extreme Management Center (XMC) – centrum kontroli sieci.

Piotr Kędra
pkedra@extremenetworks.com

Extreme™
Customer-Driven Networking

Extreme Networks: Enabling Digital Transformation



Cyberattacks Continue to Rise

Who's behind the breaches?

73% perpetrated by outsiders

28% **involved internal actors**

2% involved partners

2% featured multiple parties

50% of breaches were carried out by organized criminal groups

12% of breaches involved actors identified as nation-state or state-affiliated

What tactics are utilized?

48% of breaches featured hacking

30% included malware

17% of breaches had errors as casual events

17% were social attacks

12% Involved privilege misuse

11% of breaches involved physical actions

Who are the victims?

24% of breaches affected healthcare organizations

15% of breaches involved accommodation and food services

14% were breached of public sector entities

58% of victims are categorized as small businesses

What are the commonalities?

49% of non-POS malware was installed via malicious email

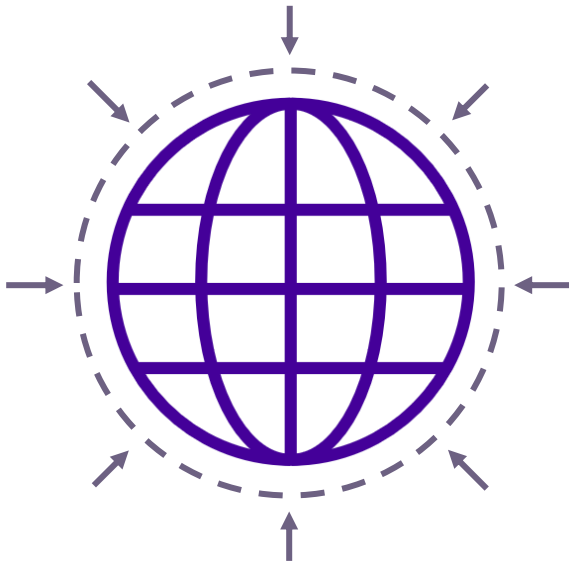
76% of breaches were financially motivated

13% of breaches were motivated by the gain of strategic advantage (espionage)

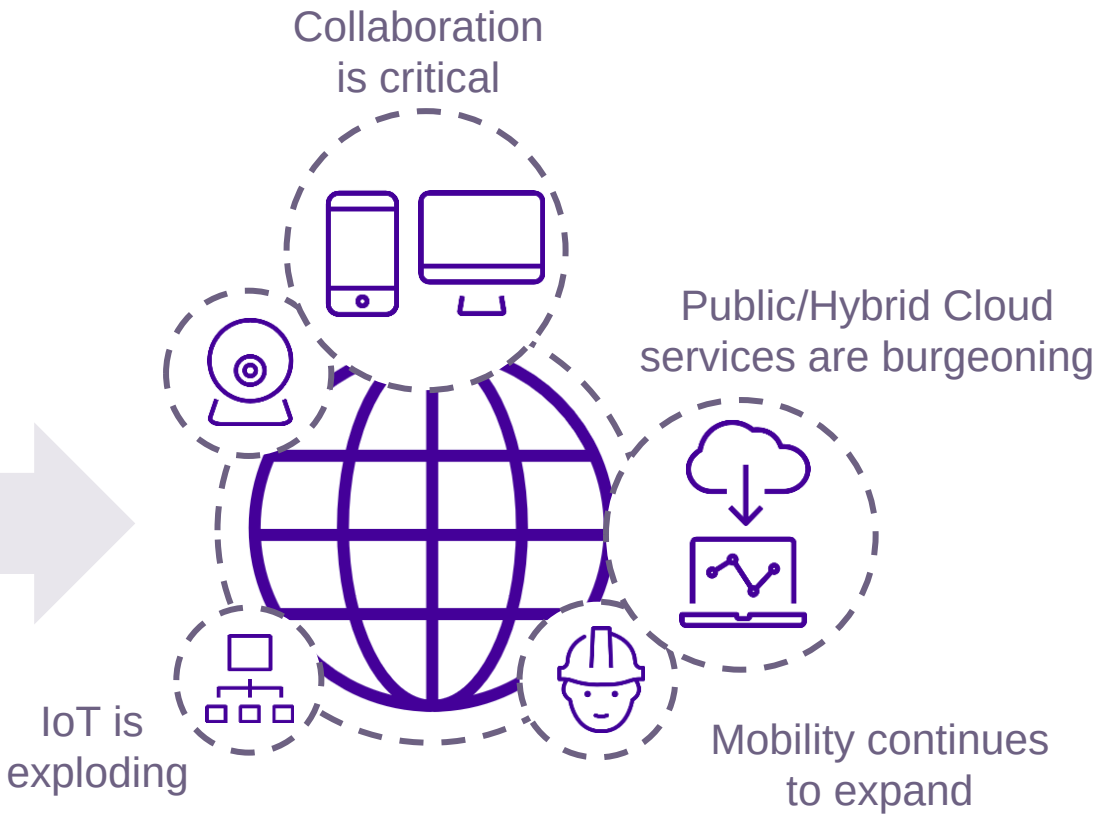
68% **of breaches took months or longer to discover**

Source: Verizon 2018 Data Breach Investigations Report, 11th edition

The Attack Surface Expands



In the past the perimeter was well defined.



…the perimeter is everywhere

70 % of successful breaches start on endpoint devices

IDC
ANALYZE THE FUTURE

No Consistent Visibility and Disparate Tools Across the Network

2018 Intel DCM Survey

Management Center Platform Components

ExtremeControl

- Role-based granular network access control and priority
- Flexible assessment
- Compliance enforcement
- Guest & remediation portals
- User & end-system tracking
- Automated incident response

ExtremeAnalytics

- Layer 7 application visibility and control
- 1,000s of fingerprints for port independent app. detection
- Dashboards, diagnostics and troubleshooting
- Status, performance and threat reporting

ExtremeManagement

- Alarm and Event management
- Configuration, inventory & change management
- Zero touch provisioning
- Capacity planning
- Discovery & topology

Information Governance Engine

- Fully automated network configuration compliance solution
- Analyzes and assesses network configurations for compliance
- Out-of-the-box audit-driven and user-defined compliance templates reports

ExtremeConnect

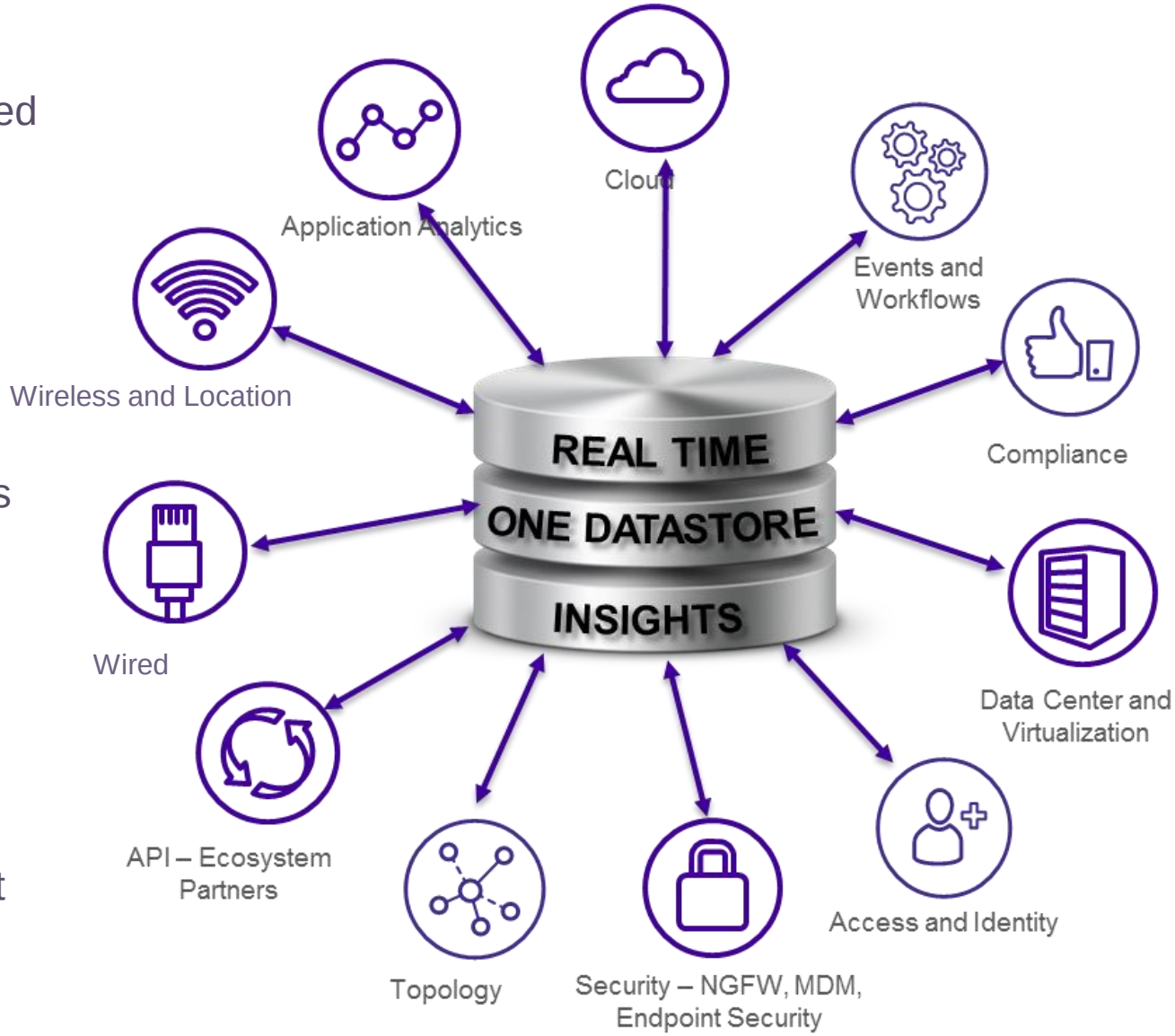
- Enables automation & integration with VMware, MS, OpenStack, BYOD, MDM, Security, NGFW, etc.
- Provides direct access to Management Center Open API – Build-Your-Own-Integration

Network Automation

- Event-driven workflow automation
- Fabric, Topology and Service provisioning (FC)
- Open to support 3rd party by using workflows and scripts
  - Service definition available through NBI and custom attributes

Tool Consolidation and Data Integration

- **Wired and Wireless**
  - It does not matter how a client/endpoint is connected to the network
- **Physical and virtual**
  - Results in “access to private cloud” approach
  - From IoT sensor to a VM in the data center, same principles
- **Single datastore**
  - Provides context
  - Delivers new insights and provides new capabilities
  - Enables to draw new conclusions
- **(Edge) automation, security and integration**
  - Control, Connect, Policy
- **Single tool for network management, access control and analytics in a heterogeneous environment**
  - Enables new capabilities through customization
  - Reduces the numbers of tools and operational cost
  - “Single Pane of Glass”



Network Access Control

IF
(user role = HR employee)

AND IF
(device = corp laptop)

AND IF
(access method = wired)

THEN GRANT
CORPORATE ACCESS

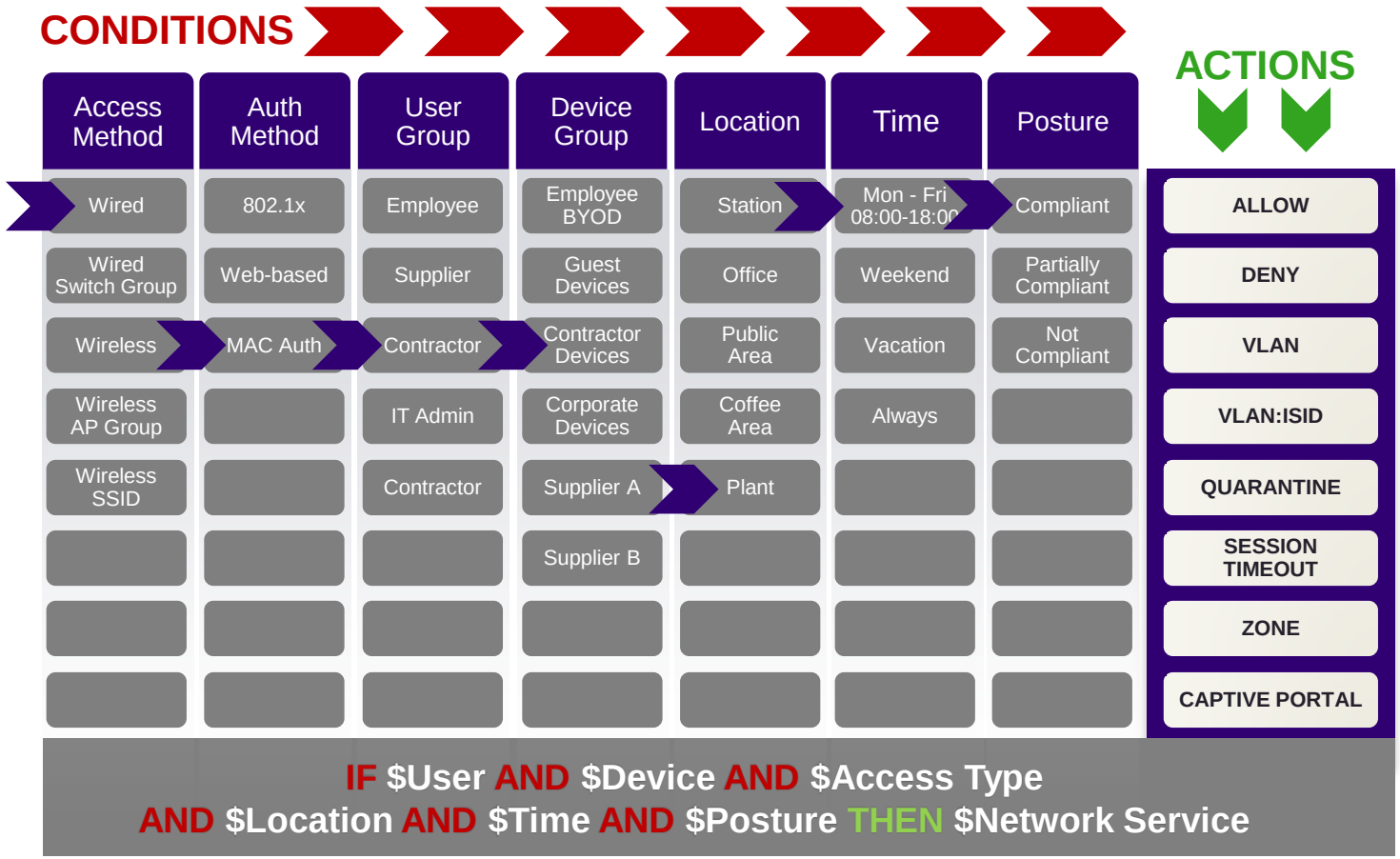
IF
(user role = HR employee)

AND IF
(device = personal iPad)

AND IF
(access method = wireless)

THEN GRANT
LIMITED ACCESS

ExtremeControl Access Policy Rules Engine



Authorization Rules may be made quite sophisticated

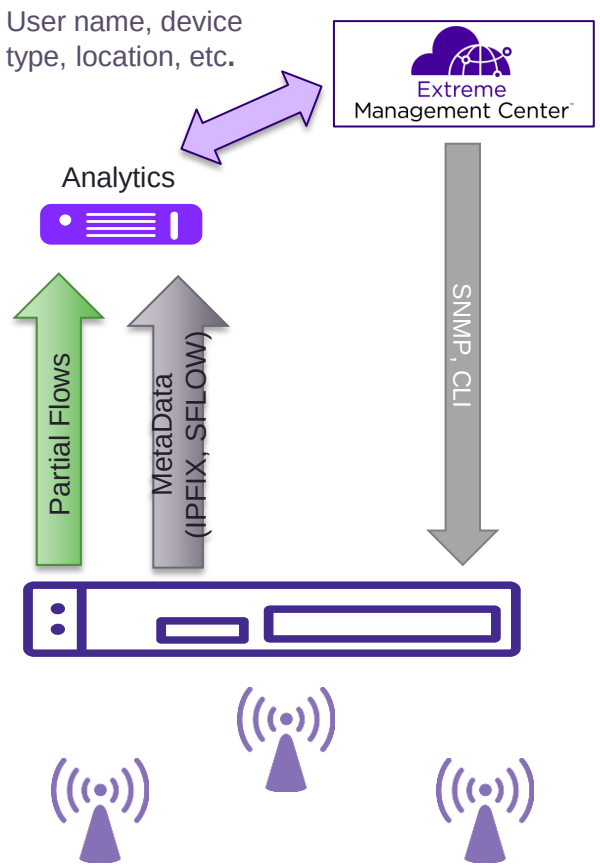
BUT

Never forget the KISS Rule

ExtremeAnalytics with Application Telemetry

- **Key Benefits:**
  - Leverage network infrastructure
  - No hardware probes
  - Application visibility at every site
  - Per flow application performance measurements

- **Application Telemetry Platform Support**
  - Edge: Summit Switches, ExtremeWireless
  - Core: VSP (Dec 2018)
  - DC: SLX, Virtual Sensor (Q1 2019)



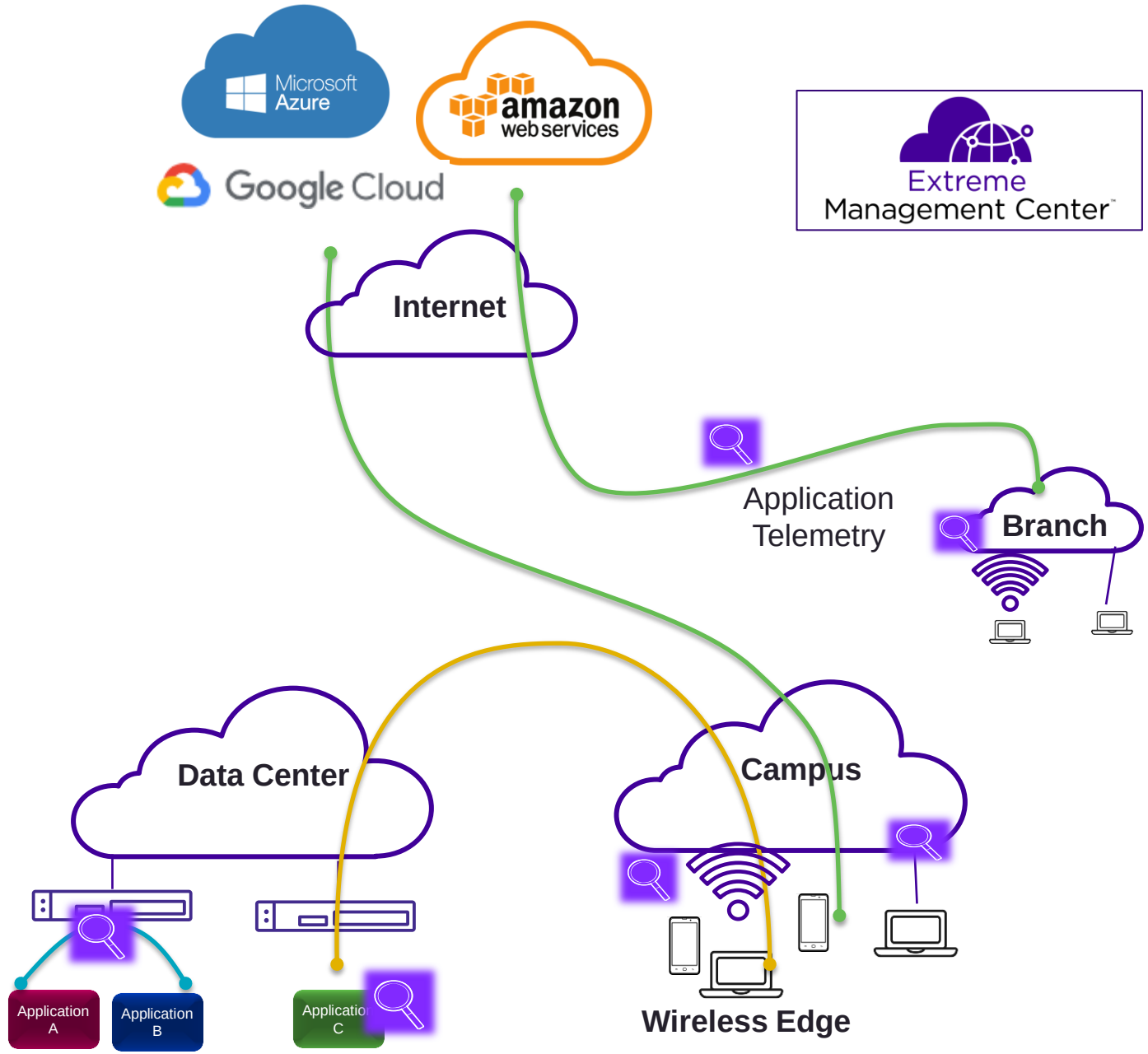
ExtremeAnalytics

Benefits:

- Strengthen security
- Deliver exceptional application experiences
- Speed up IT troubleshooting

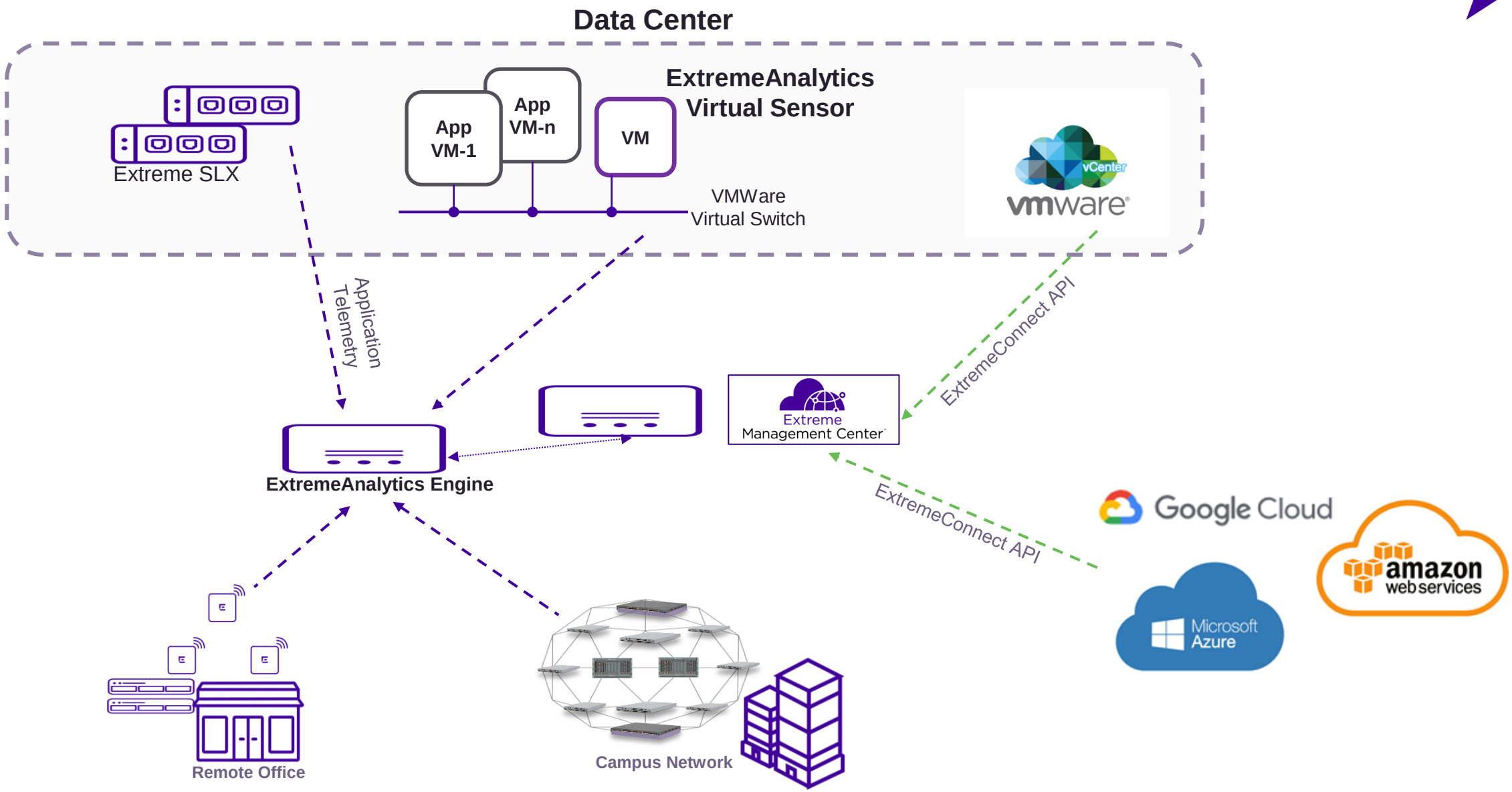
How we do it:

- Application level visibility from the edge to the DC virtual environments and multi-cloud
- Support for encrypted applications
- Over 10,000 fingerprints
- Real-time and historical reports
- Detailed application and network performance



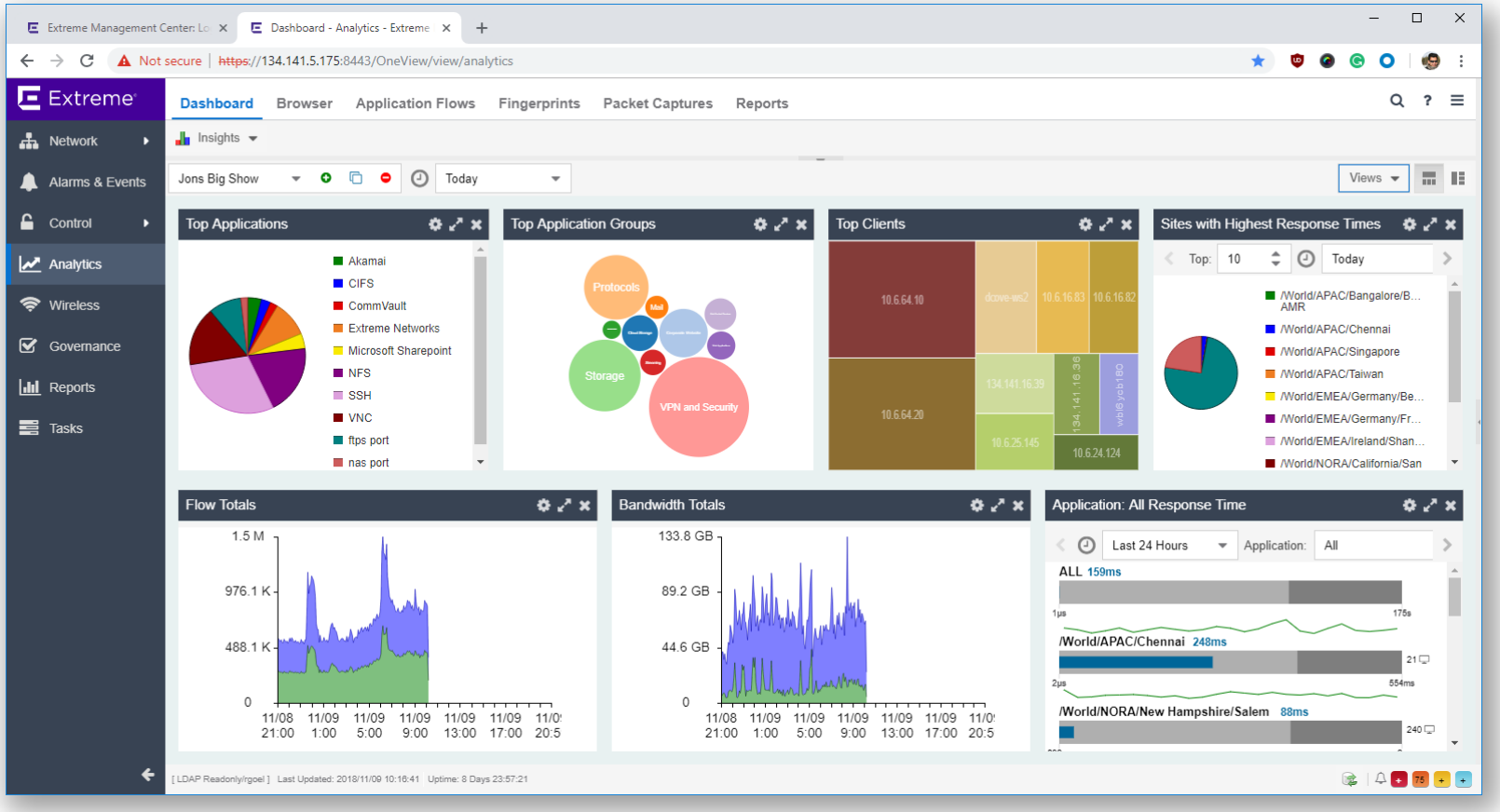
Virtual Sensor for VMWare Deployments

Q1 CY19

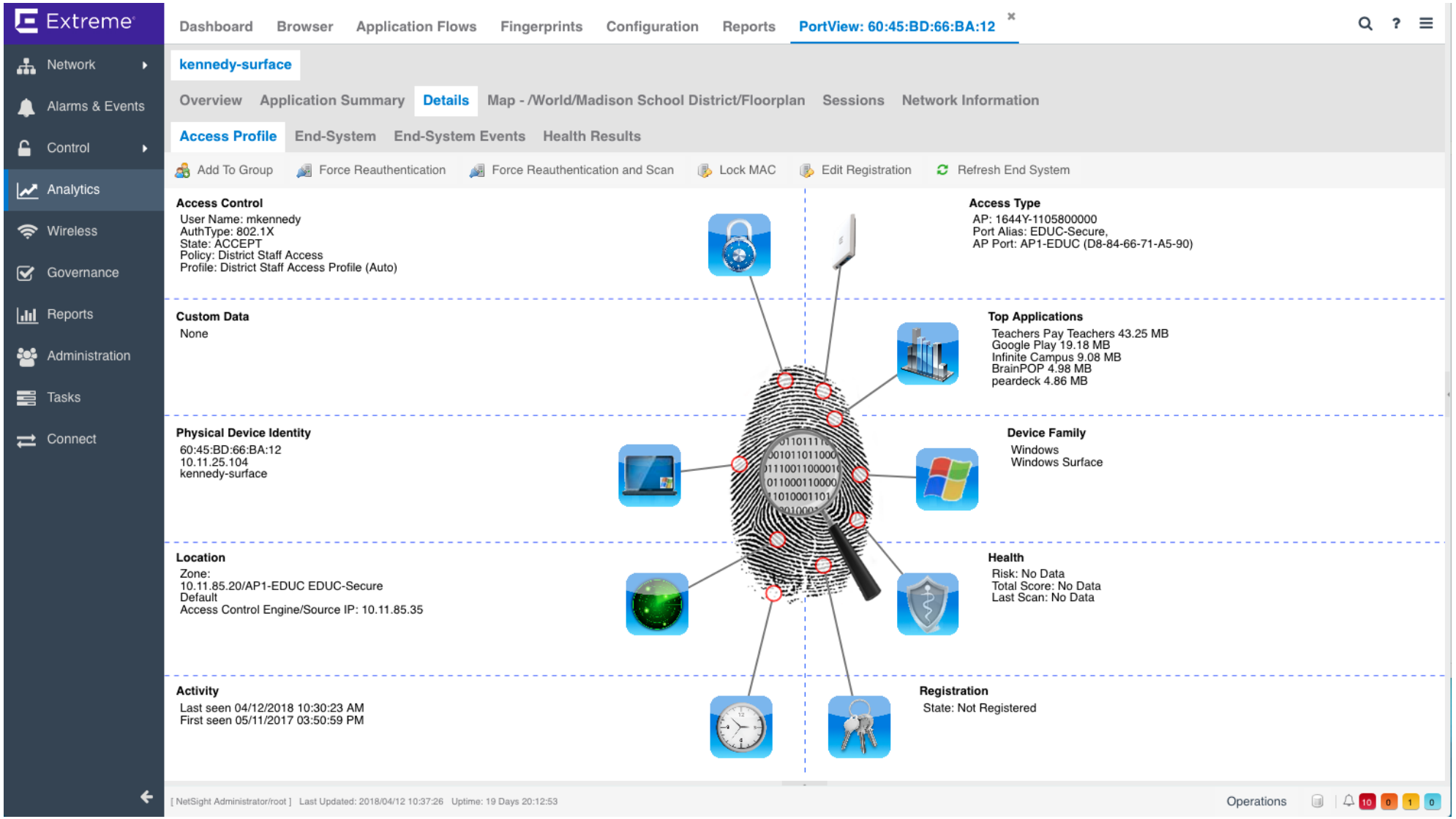


Deep insights across the entire network

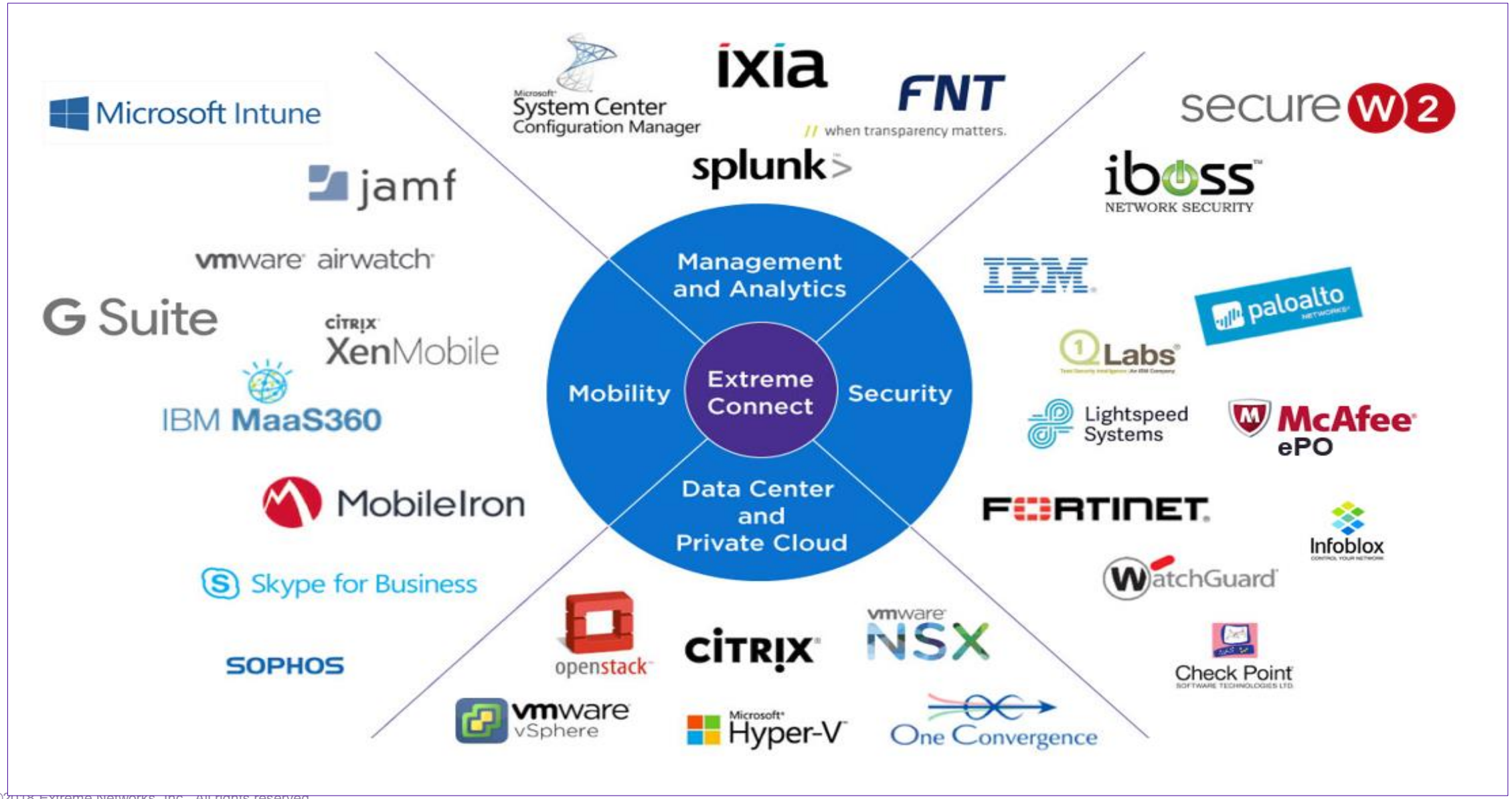
- **Customizable dashboard**
- **Real-time statistics**
- **IT Role-specific dashboards**



360˚ View of a user

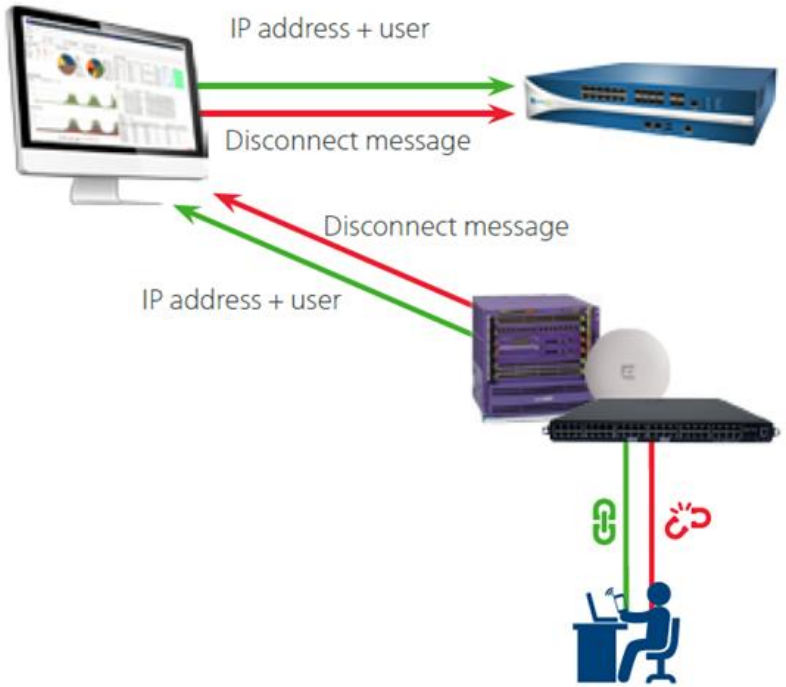


Ecosystem



Firewall Integration

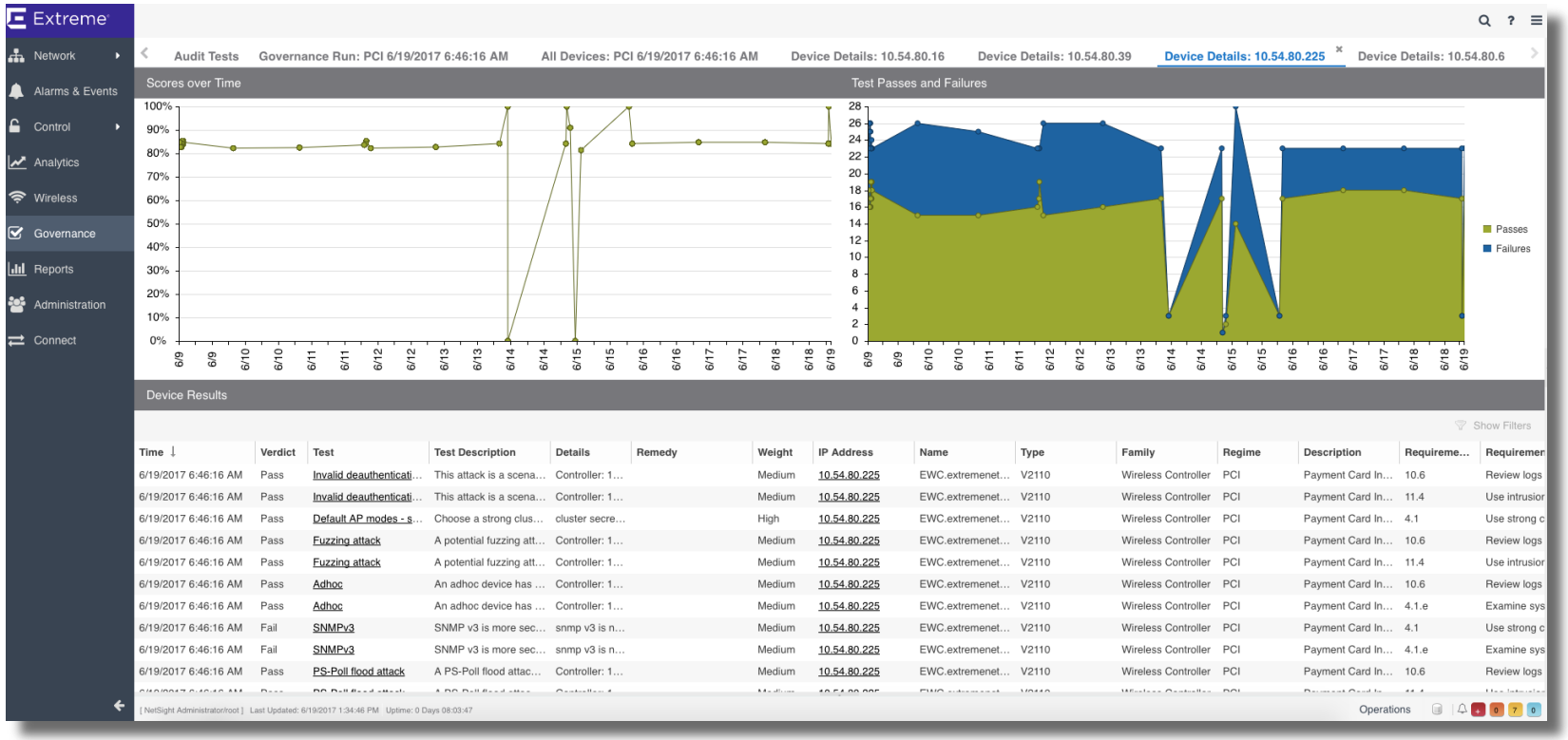
- **User ID information to firewalls**
  - Exchanges UserID & IP mapping to firewalls.
- **Distributed IPS**
  - Quarantines EndSystem upon notification fror
- **No session hijacking**
  - Delete all open sessions at Firewall if the end



Network Device Configurations Compliance

HIPAA, PCI and GDPR

- Analyzes and assesses network configurations for compliance
- Provides out-of-the-box audit-driven and user-defined compliance templates reports
- Outputs a detailed set of remediation next-steps



The Information Governance Engine is NOT:

- A replacement for a network scanner (Qualys, Nessus, etc.)
- A replacement for a SIEM.
- A compliance management solution for applications, servers, storage, operating systems, or end-systems.

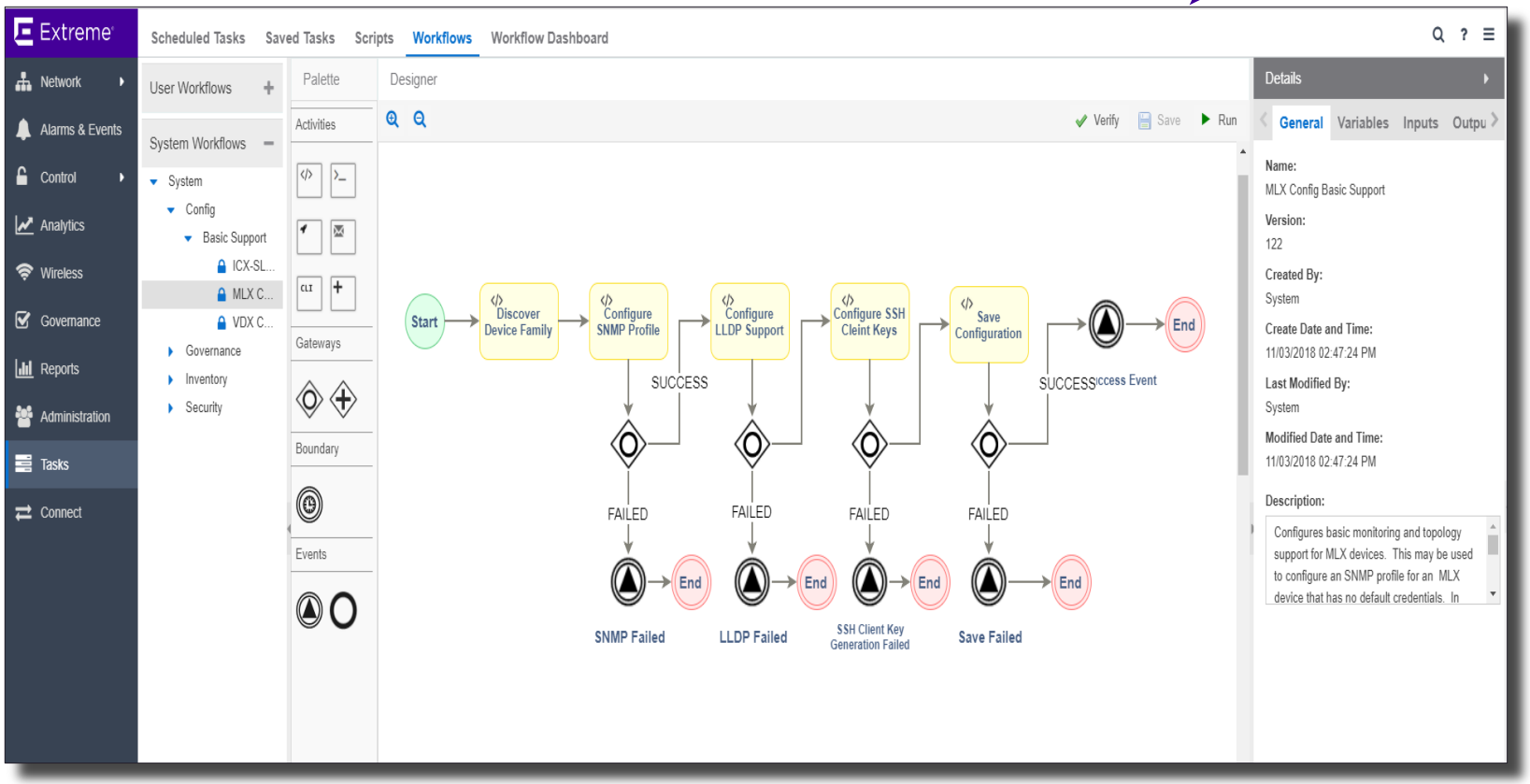
Note: IGE can “assist” organizations in assessing their HIPAA, PCI and GDPR compliance readiness; we cannot claim 100% GDPR support / readiness

Orchestration & Automation – XMC Network Workflow Automation

Supported with XMC 8.2 or later

Automate routine task:

- Automatically provision your entire network with secure zero touch (including SLX platform)
- Save operations time
- Eliminate human error and adjust to changes automatically



Extreme Management Center – Addressing Key Challenges

Policy-Based Infrastructure from edge to campus/DC to multicloud

- Automated device and fabric deployments based on site policies
- Finger printing and access policy control for users, devices, and application
- Virtual machine visibility and policy control for VMWare and multi-cloud environments

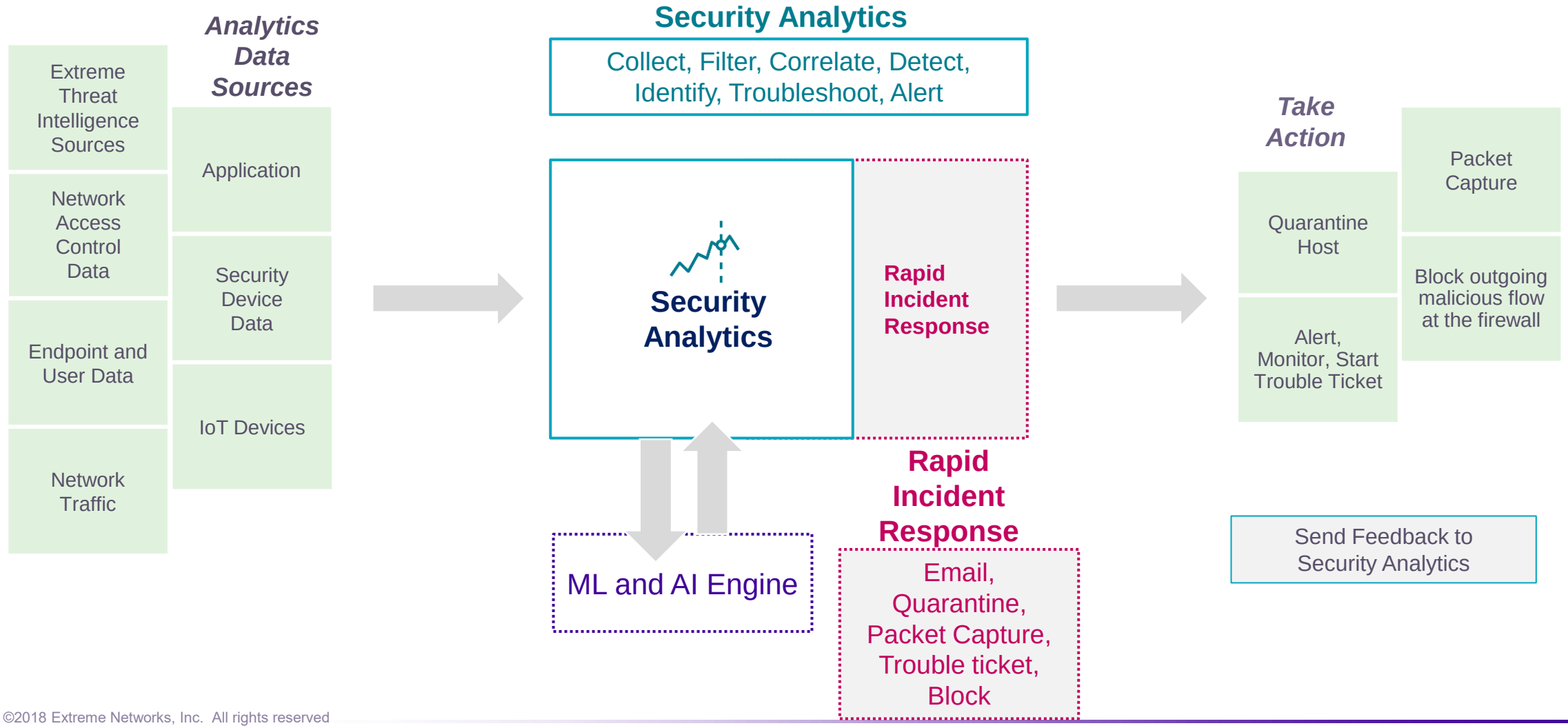
Network Assurance

- Quick resolution of service tickets through deep visibility into network and applications
- Fast troubleshooting with alerts for application performance degradations to prevent service Interruptions
- Machine assisted tuning of network and application performance threshholds
- Visibility of data breaches inside the network and smart packet capture for forensics
- Device configuration checks for compliancy with GDPR, PCI, HIPAA

Multi-Vendor Capable Tools

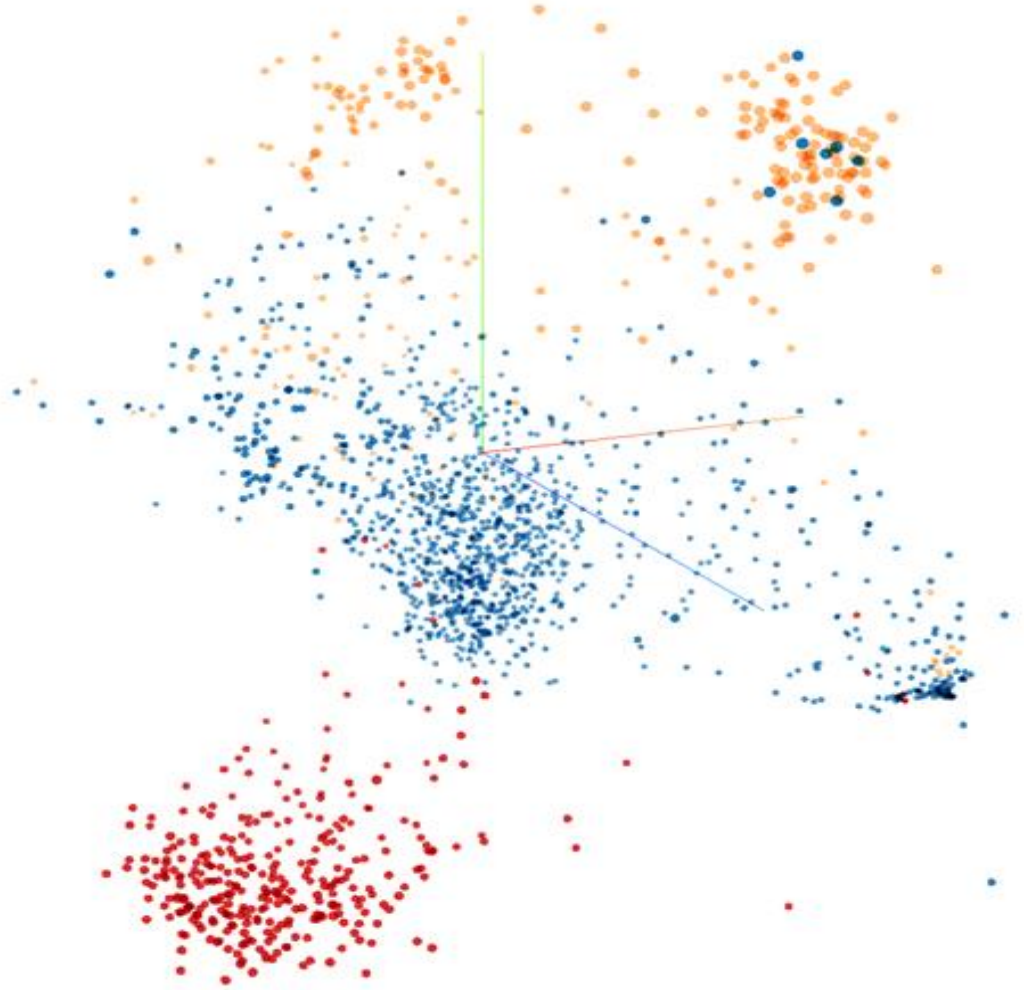
- Management visibility and control for multi-vendor devices
- Open API based connectors with key security infrastructure vendors and industry-leading applications

Security Analytics - The Decloaking Tool



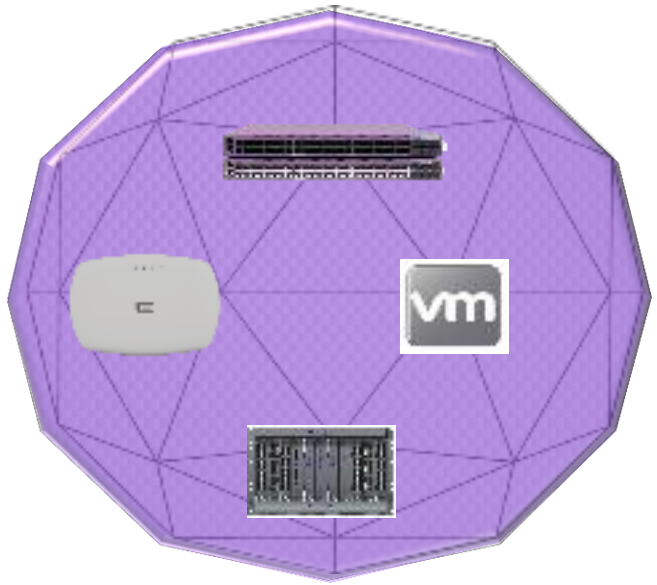
Example Use case - Behaviour-based Anomaly Detection

- Detect anomalies based on abnormal behaviors
- Millions of end-points or servers can be modelled
- Near real-time analysis
- Does not require user-sensitive data
- Can be deployed using on-prem appliances or Cloud based service
- Patent-pending



Extreme IT – NOC data on tensorflow projector

Security Assisted Networking



Secure Insights-Enabled Network Infrastructure

Comprehensive Security Analytics

Best of Breed Partner Solutions & Intelligence

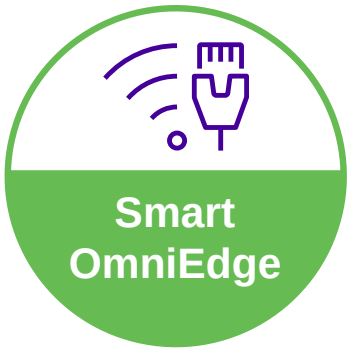
Network Enhanced Security: Multi-level, Partner Augmented

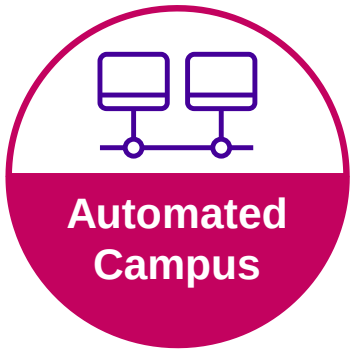
"Security Assisted Networking delivers a Secure Network Solution with integrated and automated Threat Detection, Intelligence, and Mitigation capabilities"

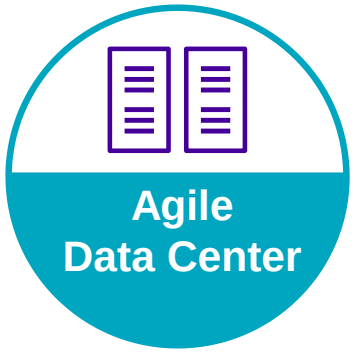
End-to-End Visibility and Control

Extreme Management Center

Network Asset Management, Inventory, Monitoring, Fault Management
Network Automation, Workflow Automation, Configuration Management,
Access Control and Policy, Analytics (Network, Device, Application,
Security), Compliance and Auditing, Ecosystem Integration







WWW.EXTREMENETWORKS.COM