Intrinsieke security met SPBm LAN infrastructuur

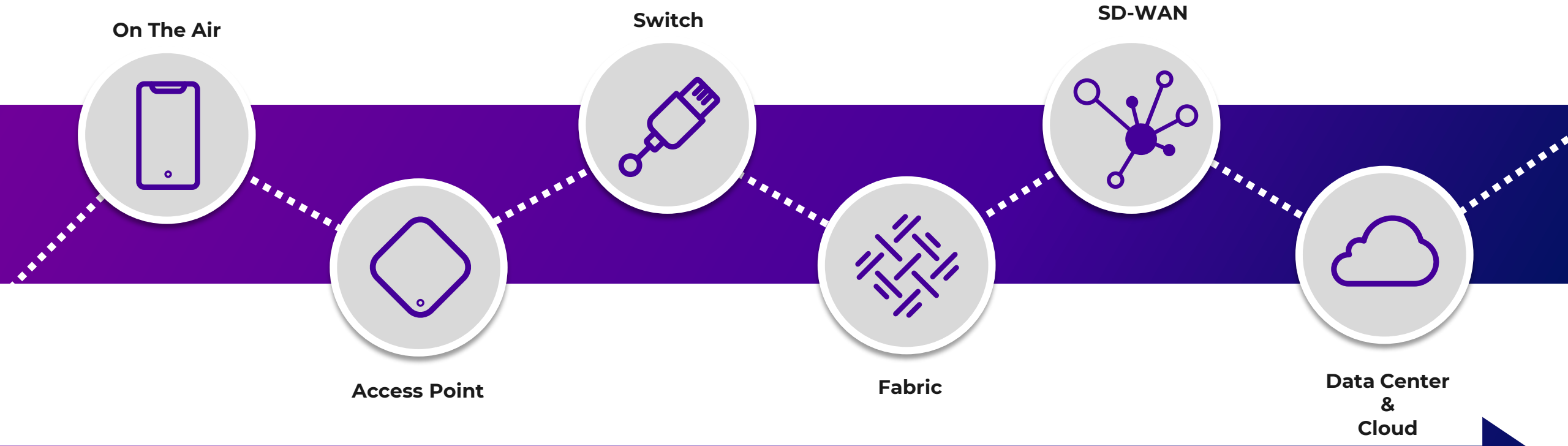
Hans Van Damme

Senior System Engineer

hvandamme@extremenetworks.com

Extreme networks

Layered Security Across Network from Edge to Data Center



Single Management GUI

AirDefense WIPS	Firewall rules DOS prevention Policy enforcement	Secure Boot Policy enforcement	Hyper Segmentation Stealth Network	IPSec tunnels Zone based firewalls	ISO certified SOC2 Certification

Extreme’s Approach to Fabric

Unified Fabric

Flexible fabric connects all places in the network and all technologies

Instant Actions

Auto provisioning streamlines deployment and operations

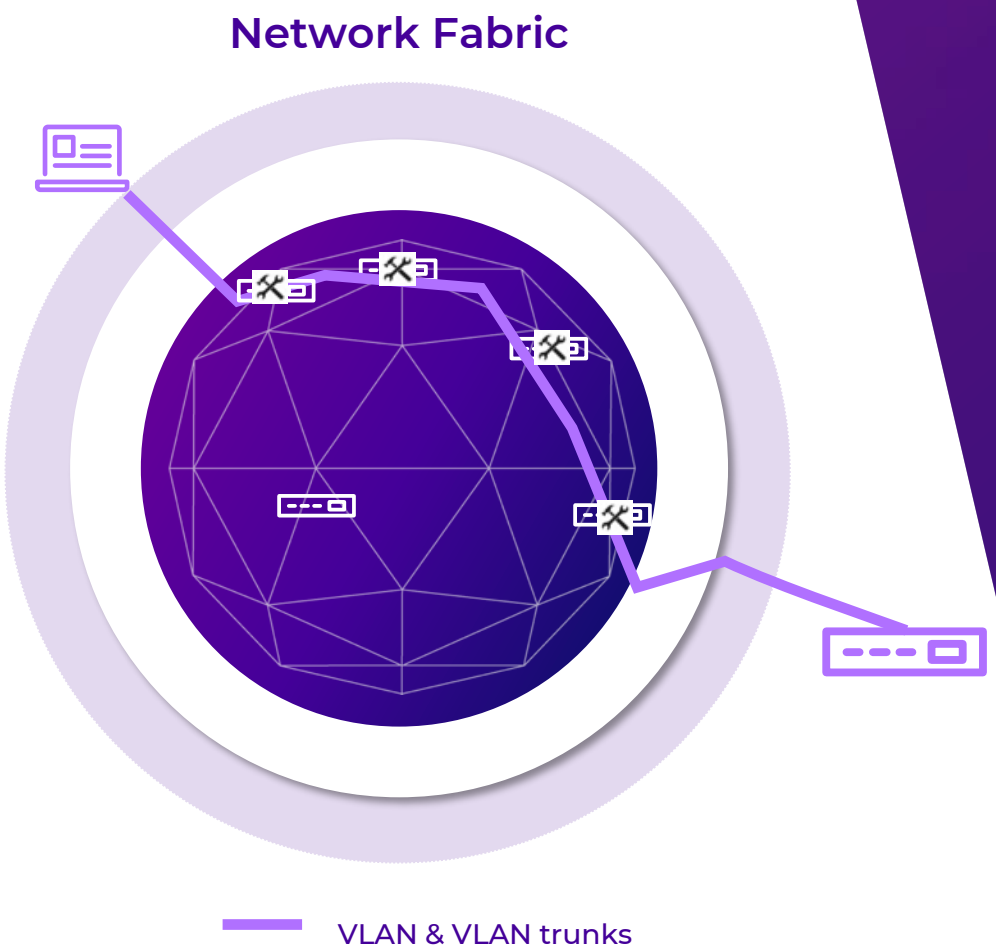
Protect the Network

Prevents lateral movement, protect against potentially unsecured devices, and minimizes points of entry

Understanding the problem and security issue

Classical Networking

- Hop-by-hop provisioning
- Changes – any moves, adds, changes – a require Core configuration
- Needs Change Window & prone to human error
- When end system is removed service is open for hacking



"Before Fabric Connect, we had to configure 36 uplinks on 17 devices to extend a VLAN between two data centers… Now we don't have to configure any uplinks: we just set up the VLAN on two devices"

– City University in London

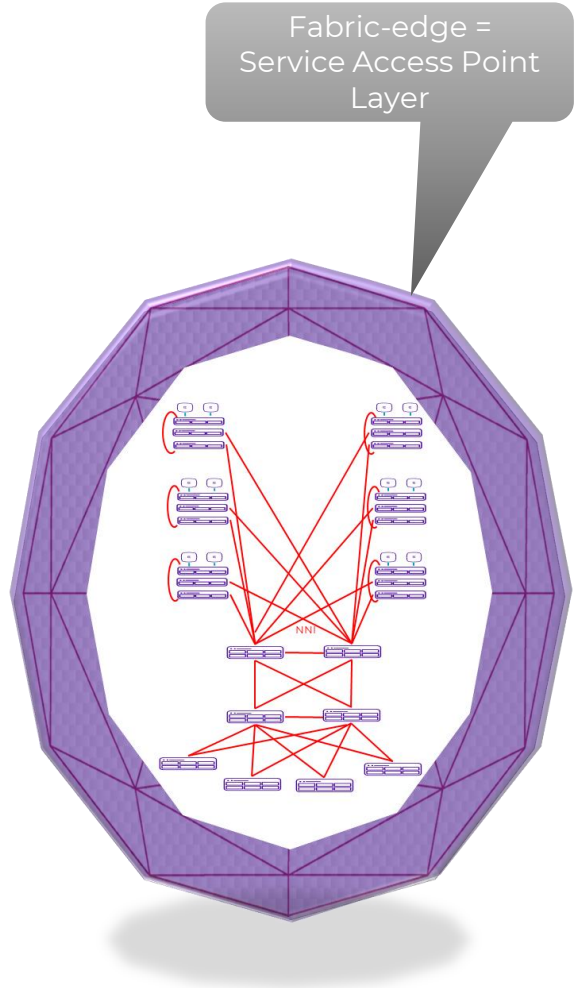
Architectural Goals of Fabric to the Edge

- Reduce the config effort on the edge switches to a minimum
- Automate network device interconnects
- Automate client attachments
- Support plug-and-play deployments
- Focus on central management (on-prem and off-prem)

What are the benefits of an end-to-end fabric?

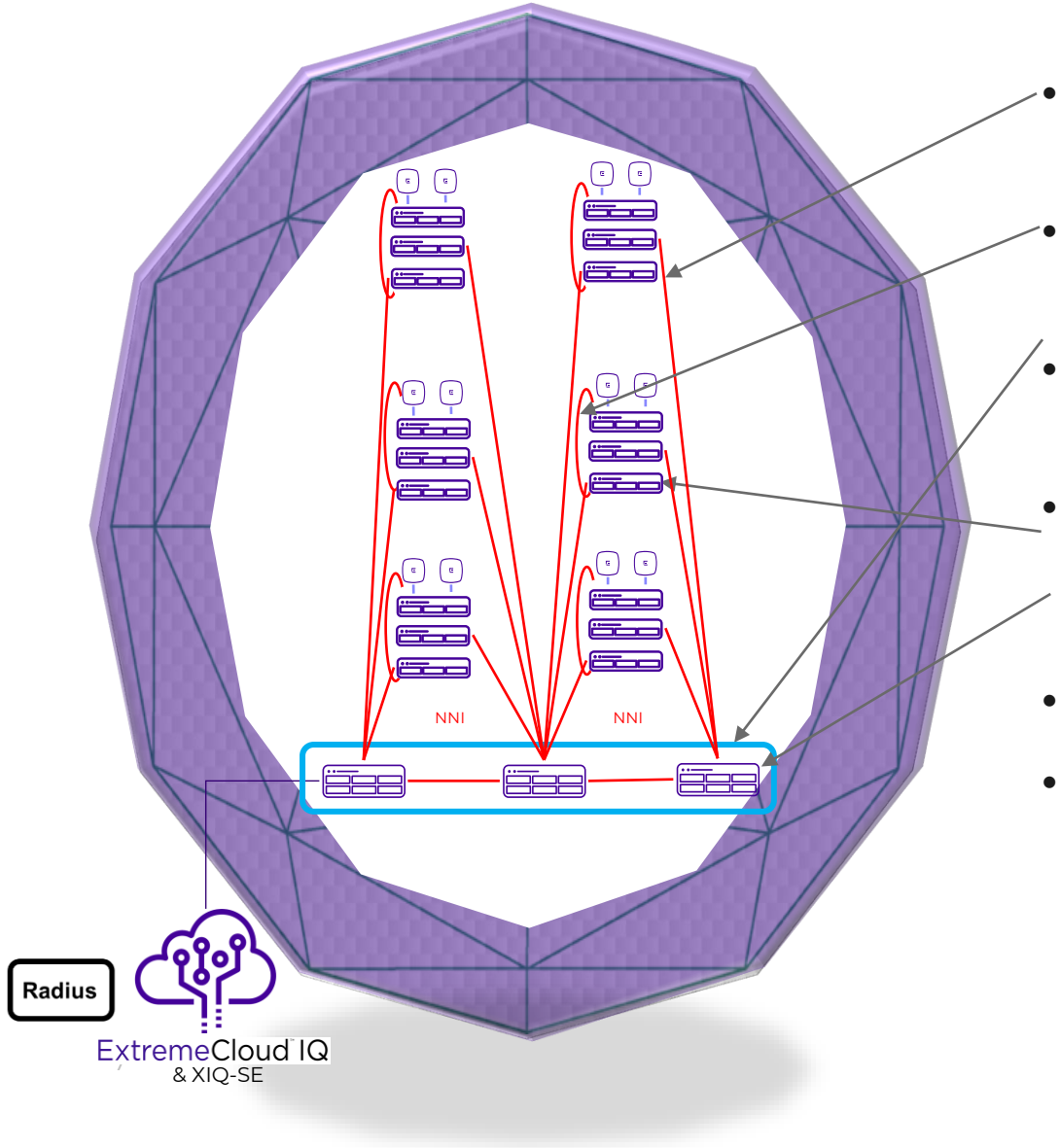
Effortless networking

- Zero Touch Network Deployment
  - Automated Fabric Network Deployment with automated onboarding to Network Management Infrastructure
- Consistent Network Access Experience with
  - Service provisioning at the network edge only
  - Rapid Time to Service - New Services deployed in minutes
  - Full service-deployment automation capabilities
- Simplified operations
  - Single network protocol for all networking needs
  - Always clean config, no “lingering” config fragments
  - Implicit end-to-end automation removes human error element
  - Reduced network maintenance required
- Flexible topology
  - Any network topology supported - use your infrastructure investments as is.
  - Suitable for Campus Core-Edge, Data Center, MAN and WAN
  - Shortest Path Bridging and Routing
- Fast failure recovery
  - Rapid failure recovery for any network connectivity service



Architecture Elements of a Fabric to the Edge Network

Architectural Goal: Access devices w/ as little config as possible

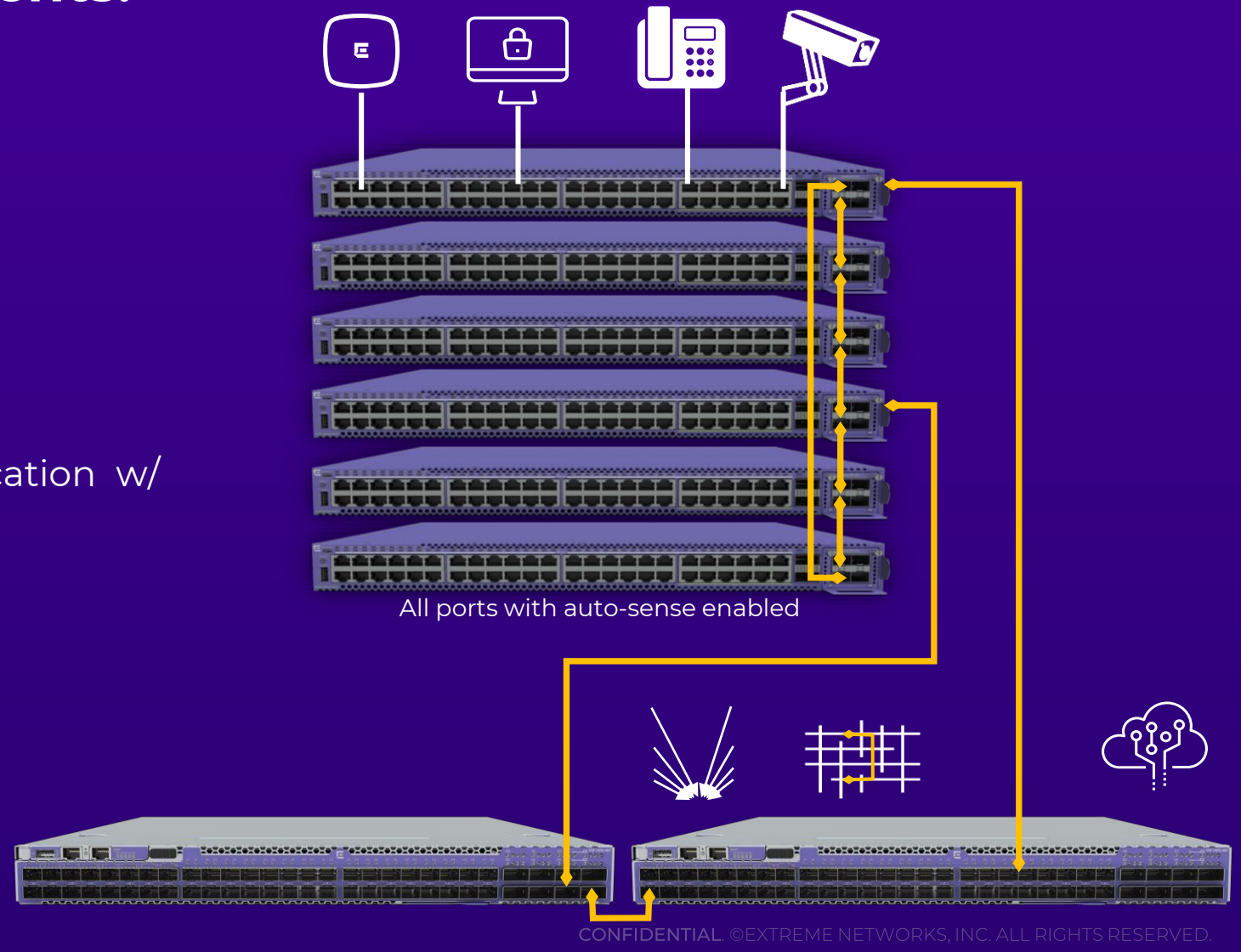


- All Inter-Switch Links are Network-to-Network (NNI) Interconnection.
- Edge switches are “stacked” with Ethernet based NNI connections
- Campus Access provisioned as Layer 2 or Layer 3 VSN’s
- For dynamic service assignments access ports remain in **auto-sense** port mode with EAP/NEAP & RADIUS enabled
- Simple to add multicast
- For IP Voice integration auto-sense voice and data VLAN pre-provisioned.

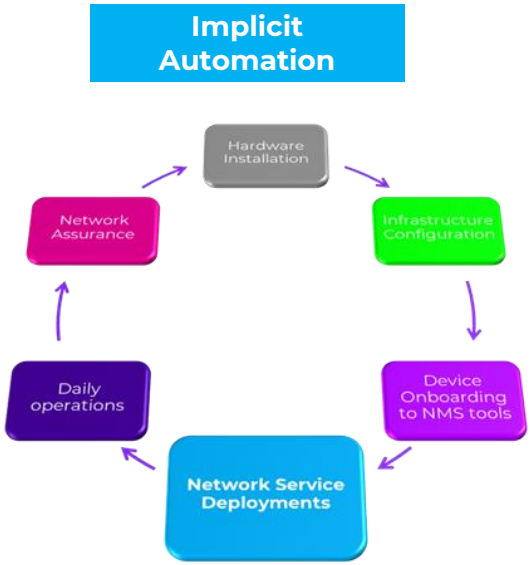
Fabric Edge – Overview

Automation / Security Elements:

- Zero-Touch-Fabric
- Auto-Onboarding Segment
- Auto-Onboarding to XIQ-SE/XIQ
- EAPoL/NEAP based User authentication w/ VLAN/I-SID and Policy assignment
- Auto Fabric Attach
- Auto IP Phone Integration
- FA Zero-Touch-Client



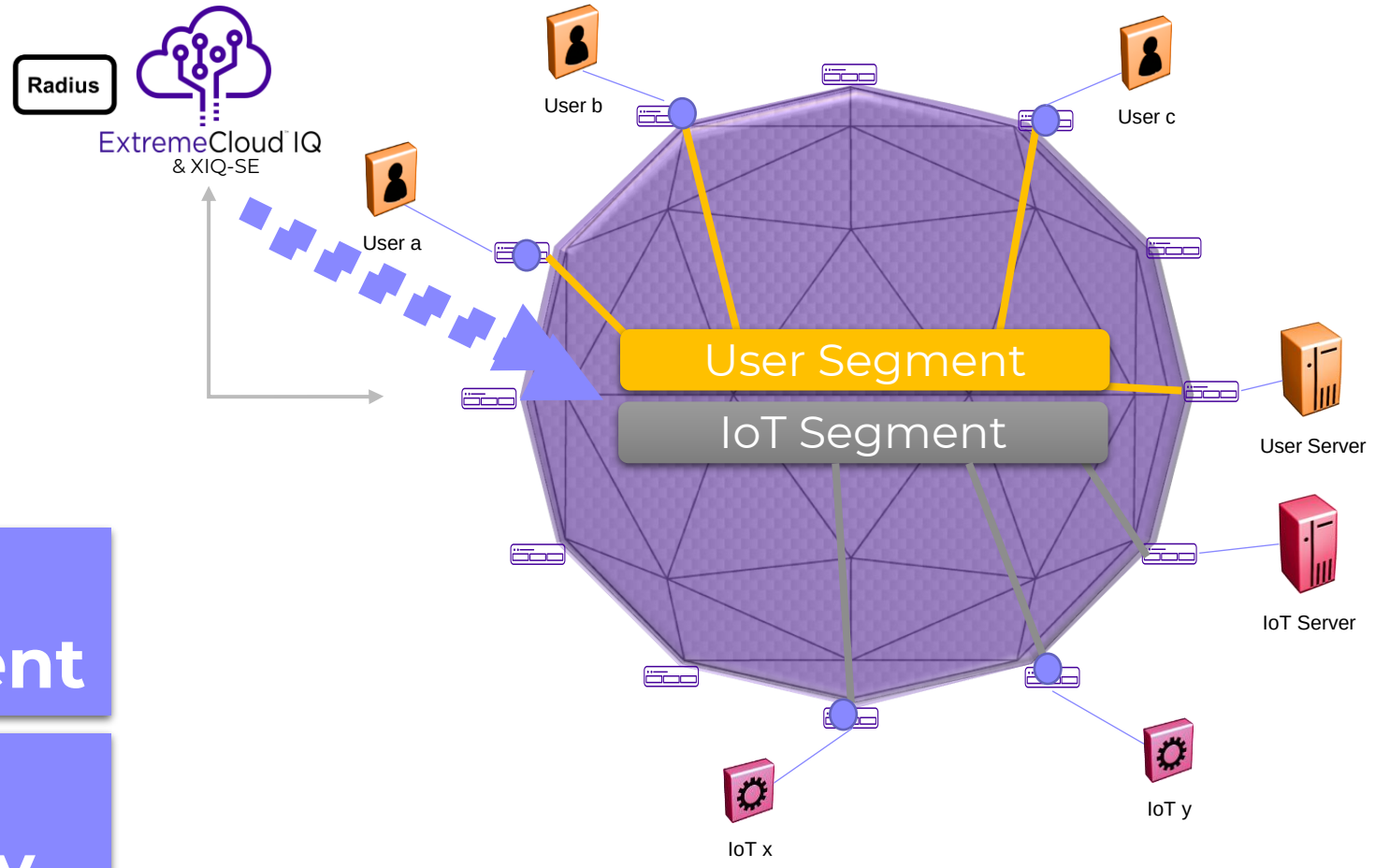
Automated Network Service Deployments



Segments deployed based on Operator Intent

Clients/hosts join segments dynamically

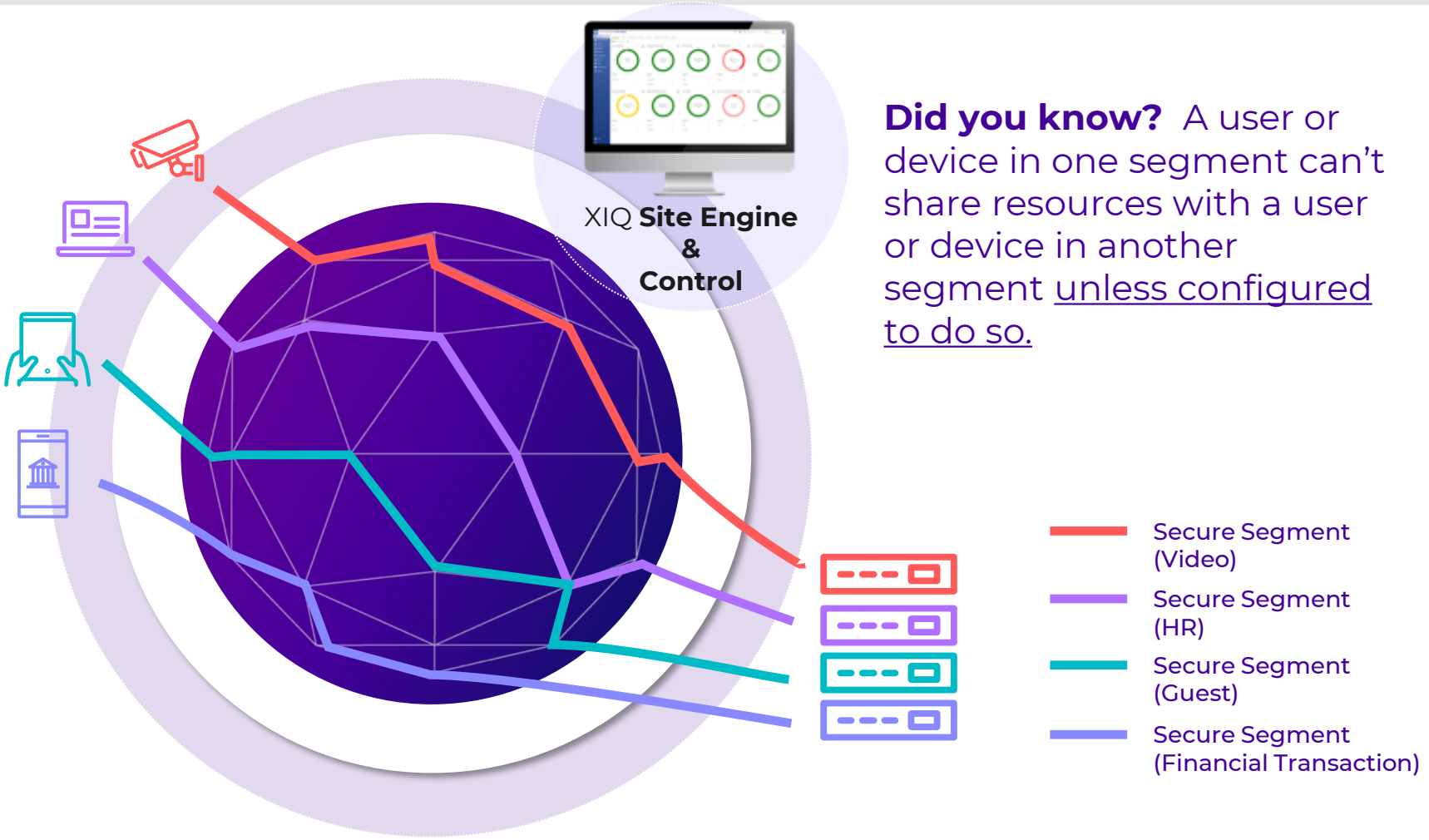
Unified end to end Fabric



SECURE: Hyper-segmentation locks down network traffic, services

Key Values:

- **Isolated by design:** Segments are separate and secure
- **Provisioned at the edges:** Users and devices are hidden from the core
- **Massive scaling:** Assignments follow the user or device
- **Segments extend network-wide**
- **Control** secure segment access through policy/NAC



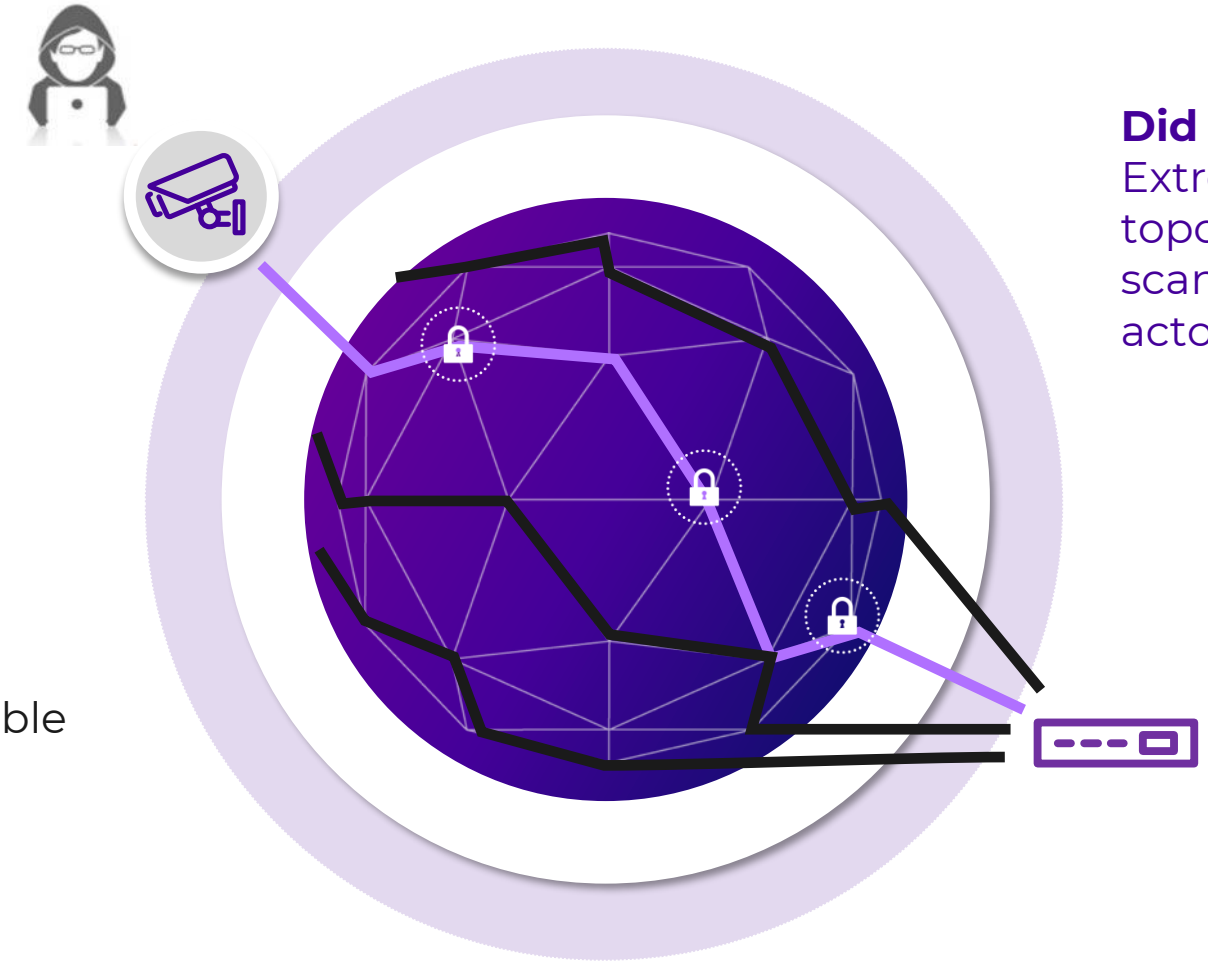
Did you know? A user or device in one segment can't share resources with a user or device in another segment unless configured to do so.

SECURE: Stealth networking prevents lateral movement

Key Values:

- Core network topology concealed.
- With no IP in the core, common scanning techniques used by hackers won't work.
- Ethernet Switch Paths keep IP addresses invisible in the core

Breaches contained; damage minimized

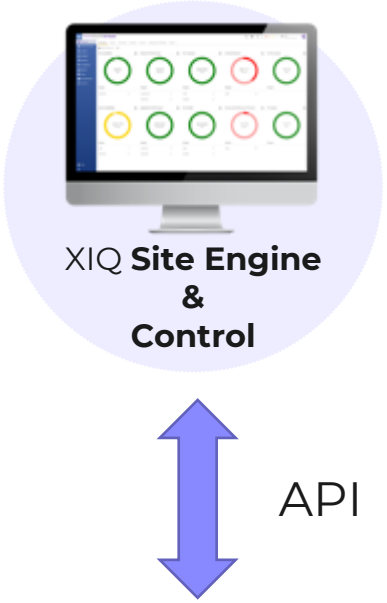


Did you know? An Extreme Fabric network topology is **dark** when scanned by a malicious actor.

Automated Security: Policy-based Access

Key Values:

- Individual end-to-end segments deliver secure traffic separation: **Hyper-Segmentation**
- **Isolate** critical applications, information or users
- **Denies Hackers** the borderless environment that they use to hop from one compromised system to the next
- Leverage Extreme policy and/or control to secure auto-attachment of Users/Devices to **hyper-segment**
- Enables granular control over **who and what has access to a segment**
- **Both hyper-segmentation and policy enforcement for auto-attach are dynamic**



MAC Security support on all universal switches

- Media Access Control Security (MACsec) is based on the IEEE 802.1AE standard that allows authorized systems in a network to transmit data confidentially and to take measures against data transmitted or modified by unauthorized devices.
- MACsec provides
  - data confidentiality (encryption)
  - data integrity (Integrity Check Value added to original frame)
  - data authenticity (peer node has to use same key)
- Every frame exchanged between MACsec enabled hosts is encrypted and decrypted using a MACsec Key.
- Data frames are encrypted at the originating MACsec host and then decrypted at the destination MACsec host thereby ensuring delivery of the frame in its original condition to the recipient host. This ensures secure data communication.
- MACSec configuration is done at port level.

Third Party Firewall INTEGRATION

User ID information to third party firewalls

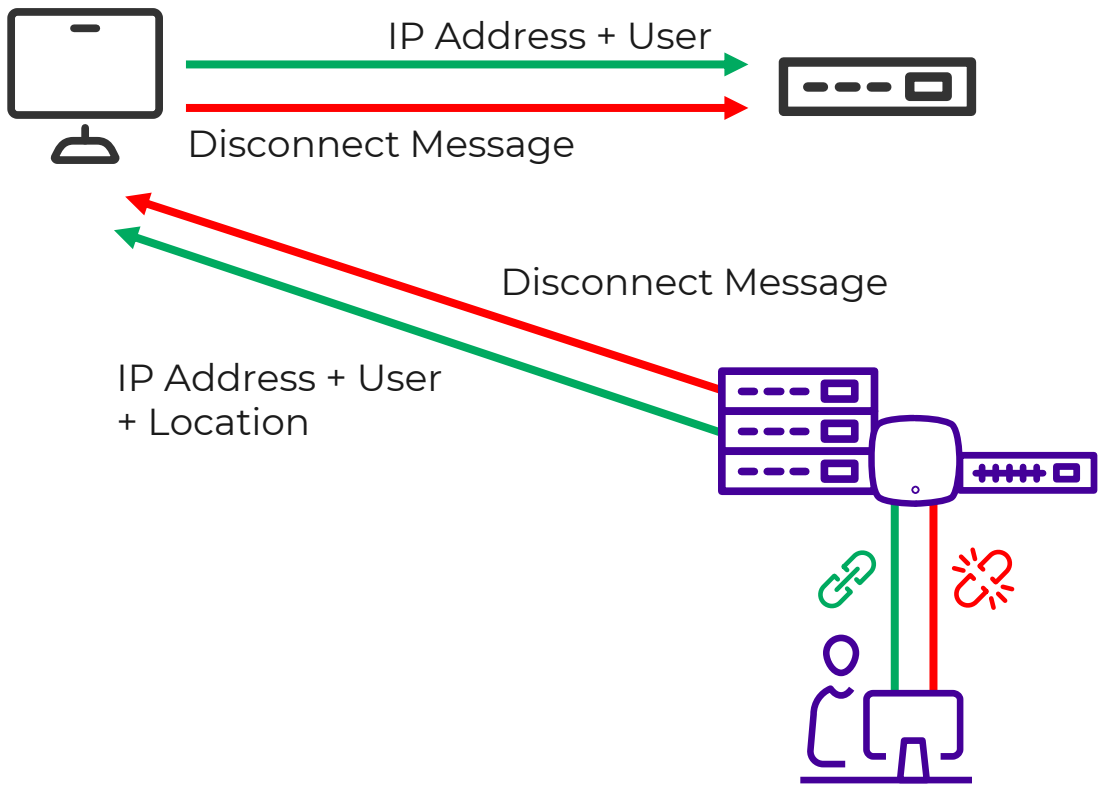
Exchanges User ID & IP mapping to third party firewalls.

Distributed IPS

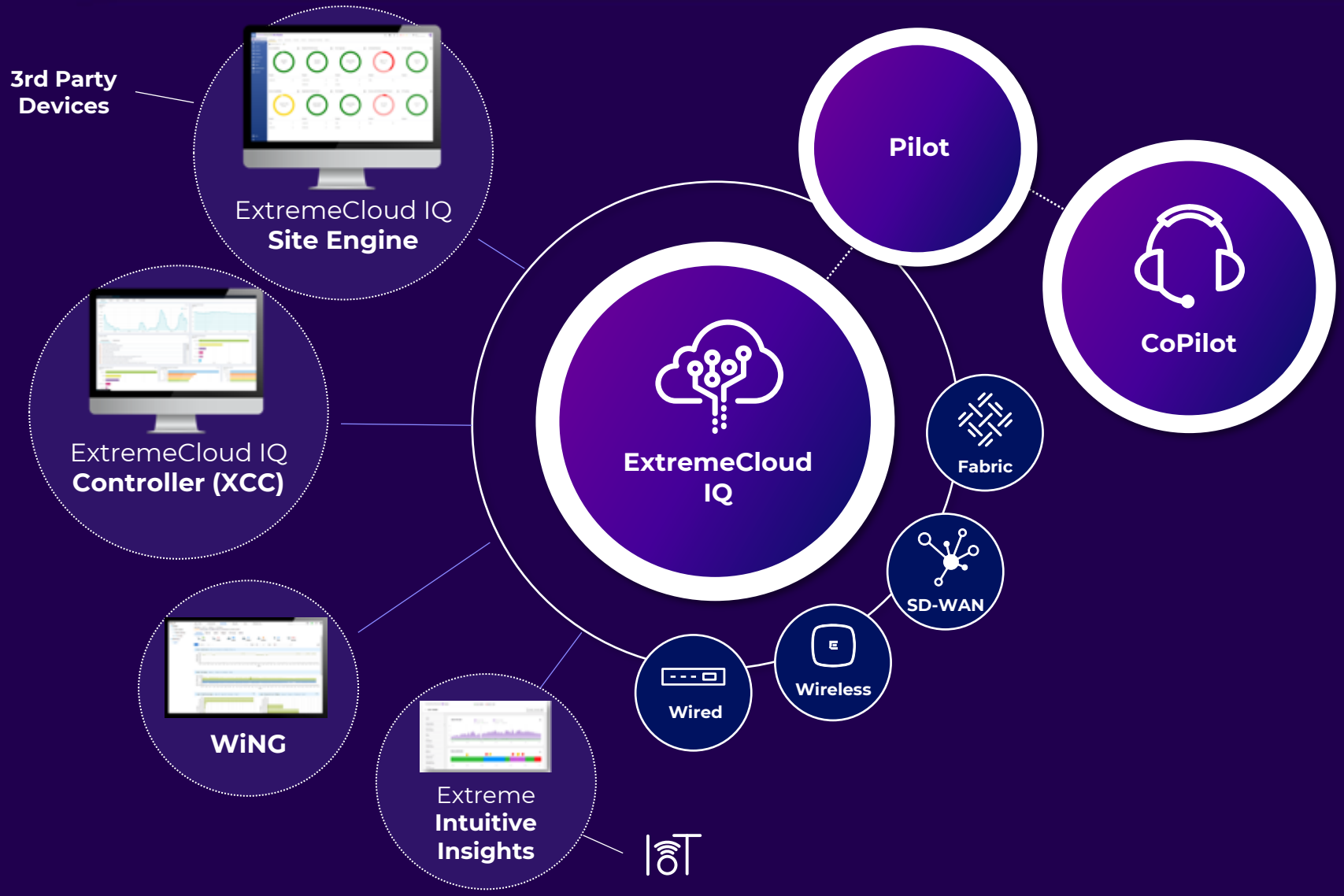
Quarantines End System upon notification from third party Firewall

No session hijacking

Delete all open sessions at Firewall if the end system is disconnected.



ExtremeCloud:
Managing 1 Network from 1 Cloud Reduces Risk, Simplifies Operations



Unified

- Manage all your devices (Extreme cloud-enabled, non-cloud Extreme, 3rd party, and IoT)
- End-to-end management of wireless, switching, and SD-WAN

Automated

- Actionable, explainable AI insights and recommendations to proactively improve network & client performance
- Simplified cloud migration

Secure

- AIOps solution that is ISO 27001/27701/27017-certified, SOC2 & CSA certified, GDPR compliant

UNIFIED - Fabric Extend to the Edge

Fabric Extend

- Run transparently over the WAN or any IP network
- Support multiple environments and services
- Extend Fabric services across geographically dispersed sites
- Includes the ExtremeCloud SD-WAN solution

The Value of Extreme Fabric Connect

What You Get

Anywhere, any service connectivity – DC, campus, branch

Unified Wired/Wireless Fabric services

Plug and play deployment, faster time to service

Highly scalable segmentation with stealth

Streamlined, scalable multicast services

Benefits

Flexible, **secure** services across the enterprise

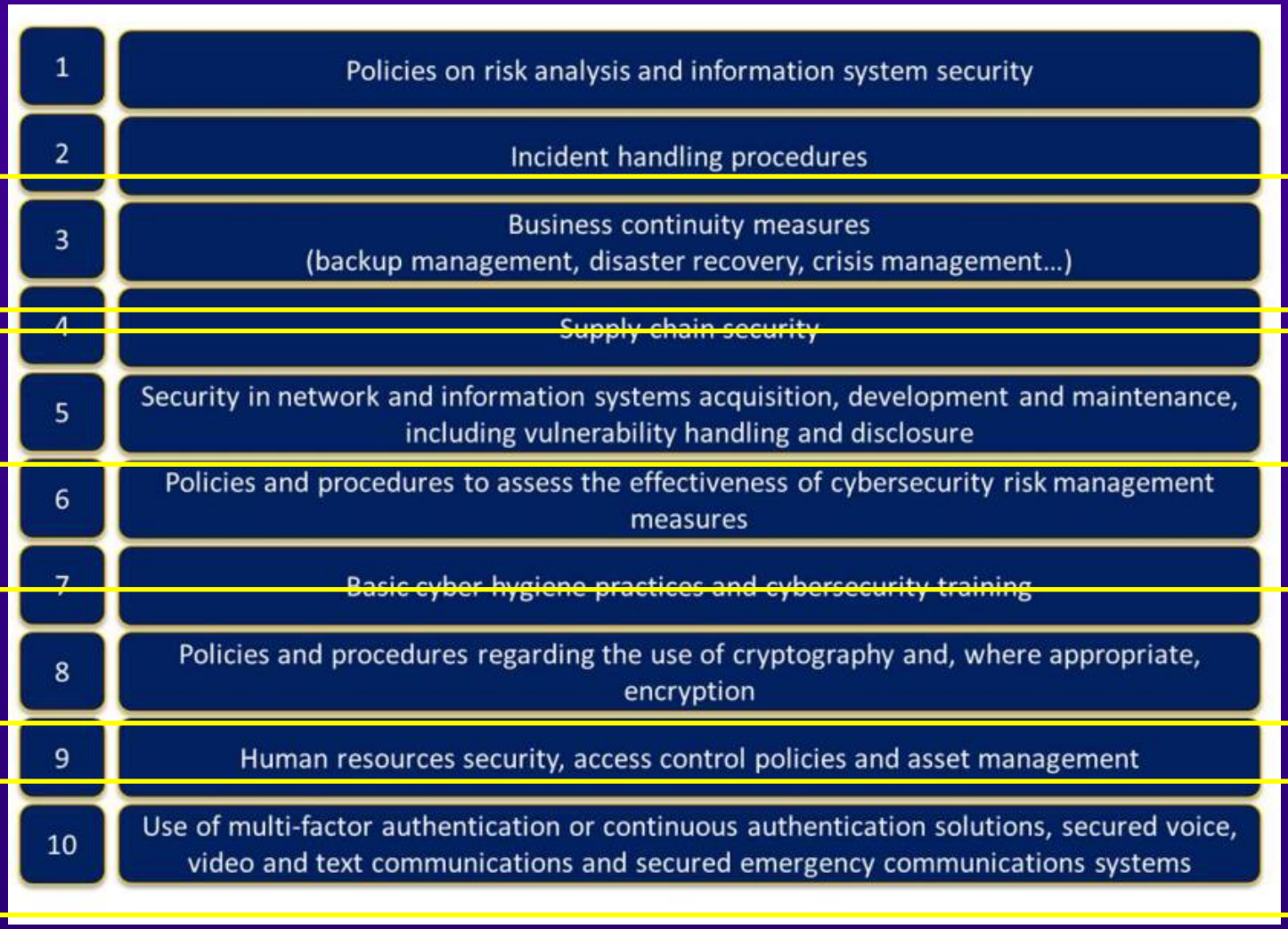
Simplified, common services

Reduced cost and IT burden

End-to-end unbreachable security

Superior user experience, more efficient management

NIS2 directive



Layered Security Across Network from Edge to Data Center