



NetNordic University

Chris Carr – Principal Solutions Architect – EMEA Strategic



Who am I?



Extreme Networks
EMEA Strategic SaaS Team
Principal Solutions Architect





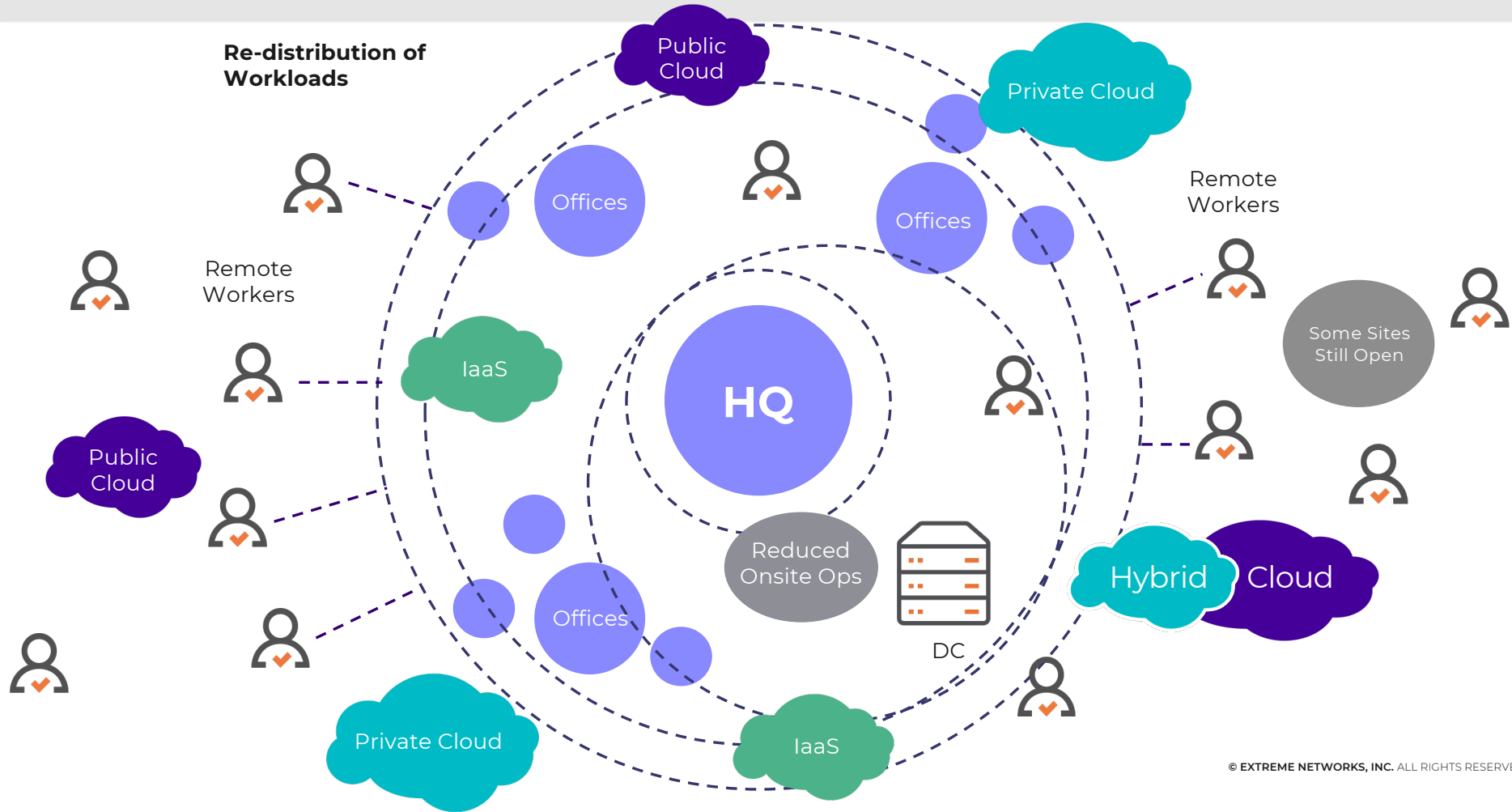
The Problem with Zero Trust Networking

Chris Carr – Principal Solutions Architect – EMEA Strategic



What is Perimeter Based Security?

Where is the perimeter?



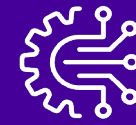
What is Zero Trust Networking?



**Never Trust,
Always Verify**

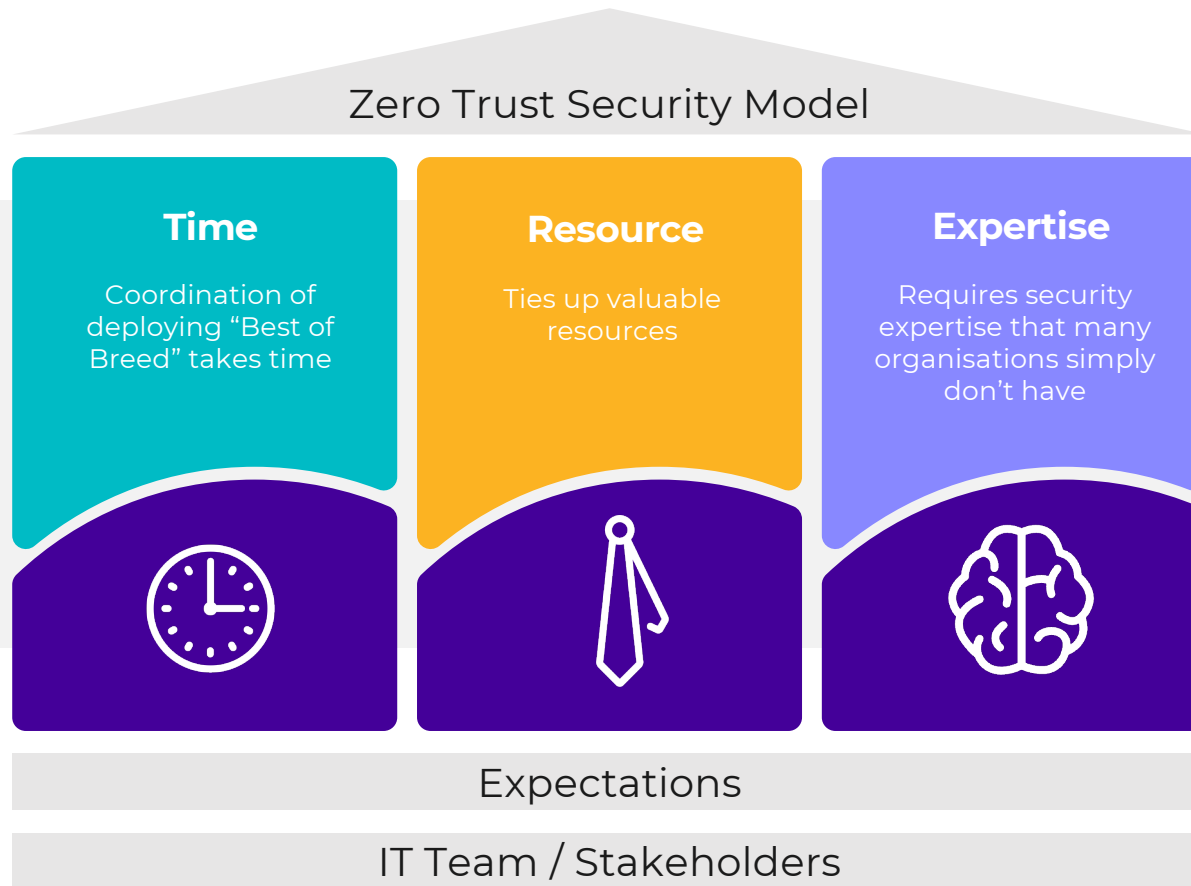


**Least Privilege
Access**



**Assume
Breach**

Implementing Zero Trust Networking – The 3 Pillars



The Problem – Organizations Left Behind



Why?

- Network managers often have security responsibilities
- Cost
- Difficult to deploy
- Difficult to manage
- Do not have the resource

Who?

- Public Sector
- SME
- Enterprise
- Retail
- Transport and Logistics



Two Approaches to Move Forward



Invest



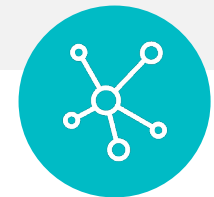
Resource



Time



Expertise



Simplify

What is Universal ZTNA?



Universal Zero Trust Network Access

is a consistent application of zero trust principles to users and devices regardless of location, remote or on-premises

Gartner[®]

“Traditional network access control offerings no longer cover emerging enterprise needs”

The Easiest Zero Trust Network Access Solution For Users Everywhere



**Frictionless user experience and consistent security policy
for applications and devices**

One solution

- Combined NAC & ZTNA for hybrid work, guest and IoT access
- Unified visualisation and reporting for enhanced insight and simplified management
- Automated enforcement through Extreme Networks Cloud Devices





Access Security for Campus and Edge Must Evolve

- Hybrid work amplifying the need for consistent security policy
- A layer of security at the identity level is a must.¹
- Zero trust must extend beyond application access into the network

77%

Of surveyed companies adopting a hybrid work model²

74%

Of all breaches include the human element through error, privilege misuse, stolen credentials or social engineering³

84%

Claim an identity-related breach in the last year with 78% citing a direct business impact as a result¹

73%

Number of organizations that lack visibility and control of every user and device's activity⁴

¹ [2022 Trends in Security Digital Identities, Dimensional Research, June 2022](#)

² [Envoy Workplace Trends Report 2022](#)

³ [2023 Verizon DBIR Report](#)

⁴ [Campus Network Security and NAC are Ripe for Market Disruption](#)

Traditional Network Security Approaches Cannot Support Hybrid Work



Legacy solutions are inherently 'allow all'

Remote

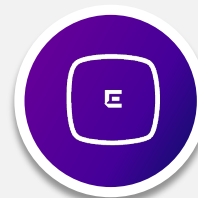


VPN

Legacy solution not designed to scale

- One persistent tunnel for all traffic
- Basic authentication
- Not designed for cloud apps
- Inconsistent user experience

On-prem



AP Config



Switch Config



NAC Config

Trade-off between security and provisioning skills / resource

- Manual config cumbersome
- Rework needed when new device onboarded
- Policy consistency issues
- NAC dependent on switch config



Strengths:

- Strict authentication and access control based on identity and context
- Each application session handled separately
- Access limited to specific resources
- Fast, direct access to applications

ZTNA

Gaps:

- No network access security
- Cannot secure IoT devices
- Cannot provide or secure guest access

Multi-Product Approach Increases Cost and Complexity

- Multiple Complex Licenses
- On-Prem Appliances & HW
- Multiple Dashboards
- Disparate Device & User Management
- Complex Deployment



NAC




ZTNA




Universal
ZTNA

Foundations of Access Control




 ExtremeCloud™
Universal ZTNA

RADIUS as a Service



Security Policy Engine





Video Ports
Only (DVR)



Check Printing
VLAN

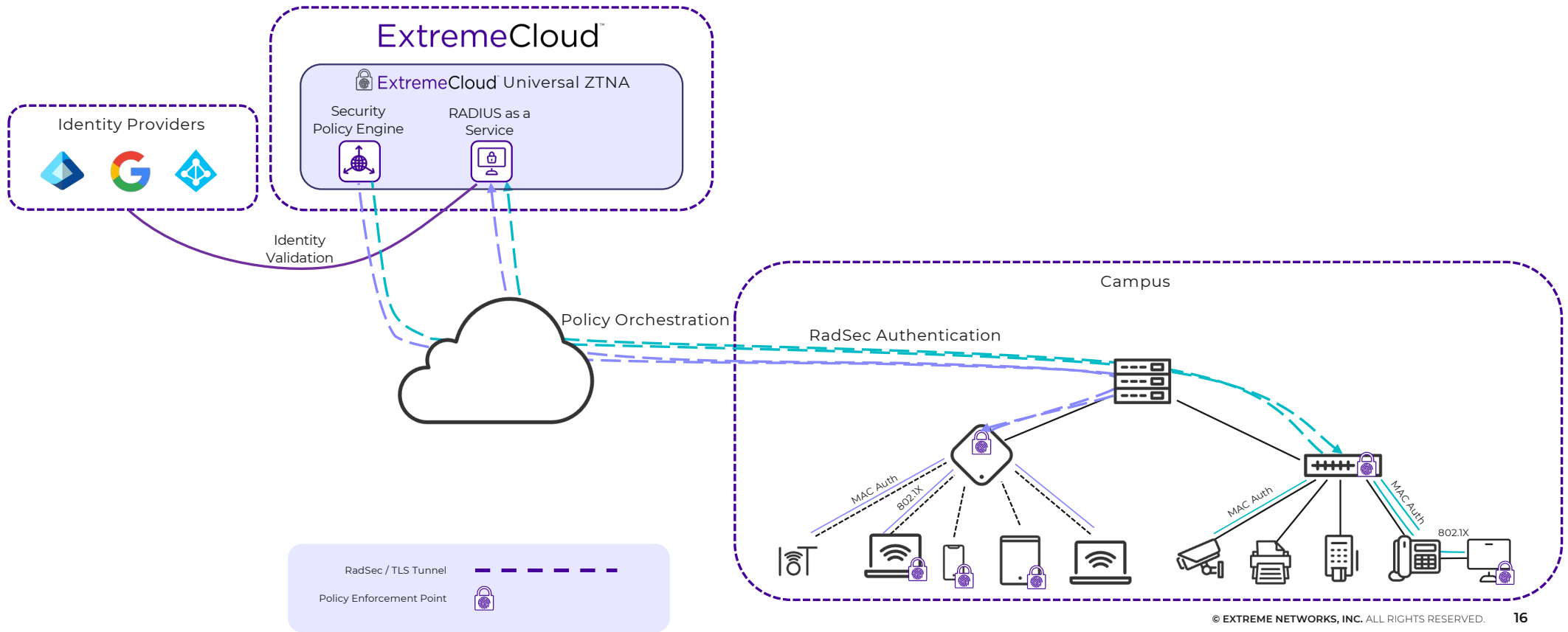


Internet
Only

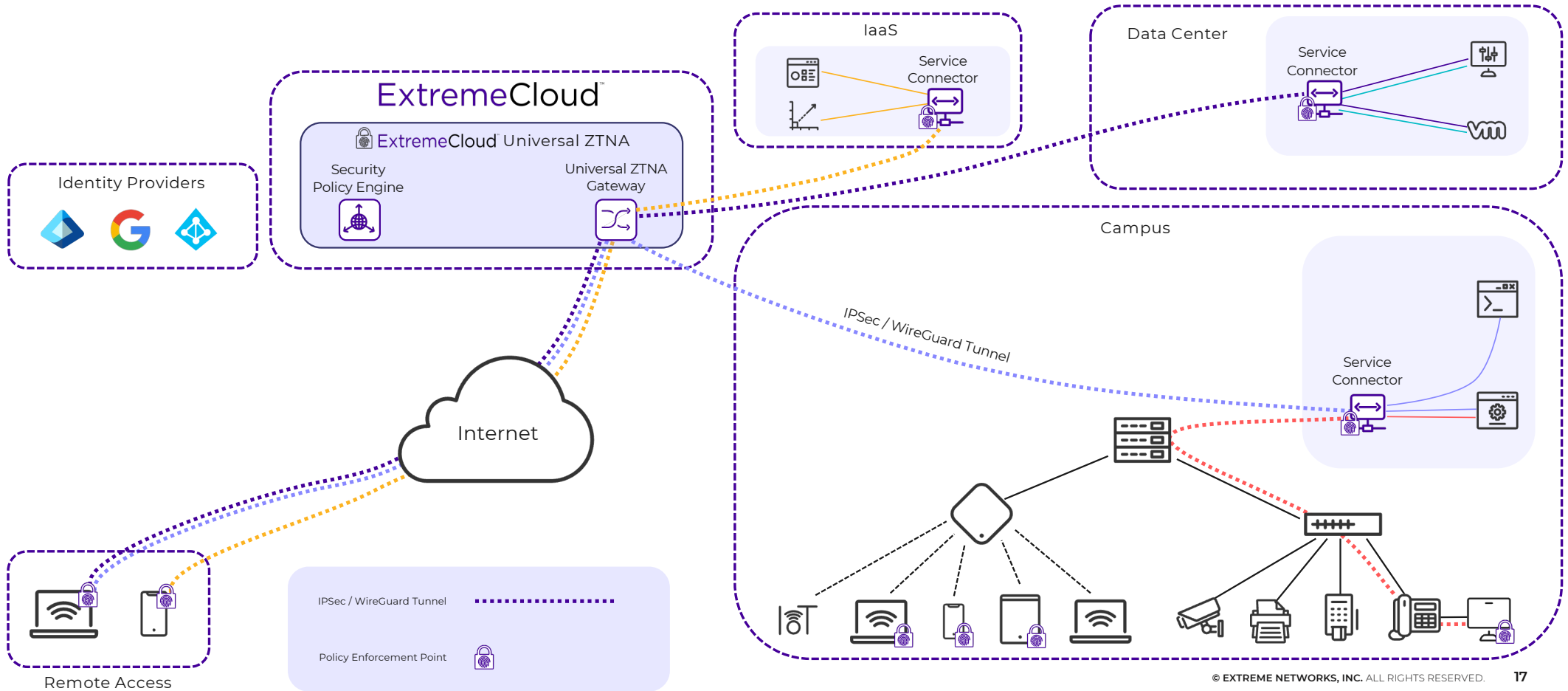


Quarantine

Network Access Architecture



Application Access Architecture



Universal ZTNA: Unified Cloud Managed ZTNA, NAC, AP and Switch Security
Limited Availability: Now!! General Availability: October 28th!



**Consistent Security
and User
Experience**

Zero Trust for all
devices everywhere



**Designed with
IoT in Mind**

Secure trusted
IoT devices and
traffic



**Simple to
Consume**

Cloud-managed
SaaS deployment



Simple to Operate

Automated device
configuration and single
reporting interface



ADVANCE
WITH US™