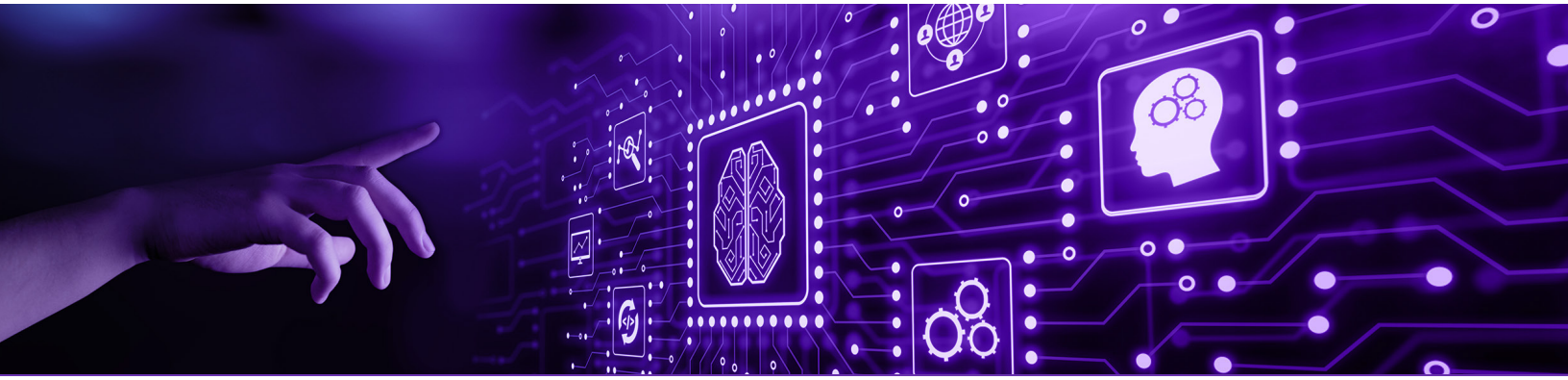

Universal ZTNA Competitive Guide

Universal ZTNA Advantages

- Modern cloud-native architecture
- Seamless integration with existing Extreme infrastructure unlike many vendor agnostic solutions
- Unified remote access and campus security in a single solution
- One solution to manage and enforce identity-level zero trust policy for all users as well as IoT devices
- Cost-effective and reliable way to adopt a Zero Trust architecture

Universal ZTNA Target Customers

- Current or new customers that have not begun or are early in their adoption or implementation of a Zero Trust framework
- IT buyers that have both network and security responsibility
- Organizations that need to implement or scale remote access for hybrid work
- Organizations that need guest access and/or IoT support
- Organizations that want to implement a cloud-based approach for NAC

Introduction

Many vendors are rushing into an already crowed and confusing market with Zero Trust solutions. These solutions are heavy in features and functionality and are also often complicated and challenging to implement and manage.

However, many customers are just beginning their transition to zero trust and are finding it difficult to navigate the numerous solutions with many different approaches and features and functionality. Extreme is bringing a simplified, but powerful approach to helping them advance in their Zero Trust journey.

Extreme is the only major vendor delivering a modern cloud-native unified NAC (Network Access Control) and ZTNA (Zero Trust Network Access) solution. Many competing vendors offer stand-alone, non-interoperable NAC and ZTNA solutions or provide zero trust access to networks or to applications, but not both.

Cisco

Identity Services Engine (ISE)

Traditional full-featured complex NAC with multi-vendor support, deployed as appliances (physical and VM) and in the cloud

DISADVANTAGES

- Expensive capex investment for appliances plus device license
- Complex and time consuming to deploy, troubleshoot, upgrade and manage
- Catalyst (DNA) Center is required for advanced visibility and setup automation
- IoT only available through specialized version
- Difficult to deploy and integrate with Extreme infrastructure
- Not integrated with Cisco ZTNA solutions
- Complex, expensive licensing structure with many features requiring advanced licenses

Cisco has confusing, overlapping solutions marketed for **ZTNA:**

- **DUO** – cloud-based MFA
- **Umbrella SIG** (Secure Internet Gateway) – Cloud-delivered managed ZTNA service
- **Secure Access** - Secure Security Edge (SSE) solution includes ZTNA and more in a comprehensive suite

DISADVANTAGES

- No solution is 'just right' – either too much or not enough
- Complex and expensive licensing structure
- High cost of Umbrella managed service
- No NAC integration – delivers application-level security

Extreme Positioning

- Unified cloud native ZTNA and NAC solution
- No additional unwanted components that add cost and complexity
- Simplified cost-effective licensing model
- Easy to deploy and manage
- Best solution for Extreme infrastructure

HPE

Aruba Clearpass

Traditional full-featured NAC with multi-vendor support

DISADVANTAGES

- Expensive capex investment for appliances
- Remote access through VPN
- Using with Extreme infrastructure is challenging
- Deployment and troubleshooting are complex
- Guest access, BYOD, and policy management require more expensive or add-on licenses

Aruba Cloud Auth

Cloud-based NAC, component of Networking Central product

DISADVANTAGES

- Requires purchase of Aruba Central cloud management
- Additional components increase cost and complexity

HPE Aruba Security Edge Platform

Complex, expensive SSE platform with ZTNA included (not yet available)

Extreme Positioning

- Unified cloud native ZTNA and NAC solution
- No additional unwanted components
- Simplified cost-effective licensing model
- Easy to deploy and manage
- Best solution for Extreme infrastructure
- Subscription includes all features and functionality

Juniper

Mist Access Assurance

Cloud-based NAC (recently launched)

DISADVANTAGES

- Not a true enterprise NAC policy platform
- Add-on subscription to Mist AI
- Requires the purchase of Mist AI
- No application-level security

Secure Edge

DISADVANTAGES

- Complex, expensive SSE platform
- Need to purchase a lot of additional components to get ZTNA
- Campus and Branch support requires SD-WAN
- Security Director Cloud required for management

Extreme Positioning

- Unified cloud native ZTNA and NAC solution
- Simple licensing model
- No additional solutions are required
- Campus and Branch support is included with integrated NAC
- Management abilities included – no separate product or license
- Centralized policy engine with distributed enforcement for higher performance

Fortinet

FortiNAC

Traditional full-featured NAC with multi-vendor support

DISADVANTAGES

- Expensive capex investment for appliances
- Virtual appliances are not cloud native
- Unintuitive and outdated user interface with high learning curve
- Integration with Extreme infrastructure is difficult. Limited documentation available
- Complex NAC endpoint licensing also required
- Advanced licensing tiers for additional functionality like BYOD and Guest Management
- Doesn't include ZTNA functionality.
- Requires manual updates

ZTNA

Included in FortiGate firewalls as embedded in FortiOS operating system. Also included in FortiSASE.

DISADVANTAGES

- Expensive capex investment for appliances
- Virtual appliances are not cloud native
- Requires Enterprise Management Server (EMS) license
- FortiClient ZTNA purchase and installation on every end-user device
- Additional software adds complexity and cost
- Multiple licenses with multiple tiers of functionality
- BYOD requires a higher license tier

Extreme Positioning

- No client or server software purchase
- Cloud native - No physical client to purchase, deploy, maintain
- Unified NAC and ZTNA in a single solution
- Simple licensing model, no upfront expensive capex investment
- Scalable – appliances are only scalable by purchasing new ones
- All features and functionality are included
- Intuitive user interface

Zscaler

Zscaler Private Access (ZPA)

A comprehensive cloud-based zero trust application access solution that is vendor-agnostic.

DISADVANTAGES

- Complex to configure, troubleshoot, and manage
- No network traffic visibility
- Complex and difficult user interface
- Relies on public internet instead of a private backbone which exposes WAN traffic
- Performance issues from centralized policy enforcement
- Only for private applications. Additional costly solution required for SaaS applications
- No pricing transparency - Custom, expensive quote is provided after engagement

Extreme Positioning

- Includes NAC to secure the network
- Easy and seamless integration and interoperability for Extreme environments
- Centralized policy control and distributed enforcement
- One solution for both private and SaaS application access
- Higher performance and better security from private DC backbone and distributed policy enforcement
- Simplified, transparent licensing strategy

Objection Handling

Q. How is this different from other solutions?

A . Many vendors are rushing into an already crowded and confusing market with Zero Trust solutions. These solutions are heavy in features and functionality and are also often complicated and challenging to implement and manage.

However, many customers are just beginning their transition to zero trust and need something far simpler - a Zero Trust LAN security solution with remote application access. Extreme gives them a simplified, but powerful approach to help them advance their zero trust journey.

Q. Juniper, Cisco, and HPE recently announced new SASE and SSE solutions. Why wouldn't I go with that approach?

A. Security Service Edge or SSE is a framework introduced by Gartner as the security component of SASE. As it is a framework, vendor approaches and solutions differ in terms of components, capabilities, complexity and more.

Transitioning to SSE is a big, complex project. Extreme's approach to Zero Trust enables customers to adopt it at their own pace instead of all at once. Universal ZTNA is significantly less expensive and complex than SSE.

Q. Why shouldn't I go with a ZTNA solution like Zscaler?

A. Most ZTNA solutions only provide application-level security. Universal ZTNA goes beyond this approach by integrating ZTNA with NAC or Network Access Control to secure LANs as well.

Q. How is Universal ZTNA a better option than NACs like HPE Clearpass and FortiNAC?

A. Universal ZTNA is a modern cloud-native solution for easy deployment and management as well as scalability as security needs change. Traditional NACs scale by replacing obsolete appliances with new, expensive investments.

Q. I already have a single vendor security strategy.

A. A single vendor can't provide all the security needed – there is always some inherent risk or area of vulnerability. Adding additional layers of security is often needed. Universal ZTNA is an easy, cost-effective approach to providing additional security between applications and devices and networking infrastructure.

Q. I can get ZTNA for free with Fortinet's firewalls.

A. While ZTNA is a capability included in FortiGate firewalls that have FortiOS version 7.x installed, there is significant additional cost required to make it operational including the licensing and deployment of the FortiClient servers and client software which adds significantly to the cost. Additionally, many find FortiOS 6.x to be more stable.

While Universal ZTNA currently requires a client-side agent, there is no additional cost. Agentless is on the roadmap for CY2024.

Q. What unique benefits does Universal ZTNA offer?

A. Extreme is the only major networking vendor delivering a modern cloud-native unified NAC and ZTNA solution. Many competing vendors offer stand-alone, non-interoperable NAC and ZTNA solutions or provide zero trust access to networks or applications, but not both.

Universal ZTNA works seamlessly with Extreme's cloud managed devices enabling customers to quickly strengthen their network security. While other solutions are vendor agnostic, they will not integrate as quickly and easily with Extreme infrastructure.

Additional benefits include Universal ZTNA's simplified licensing model. A Universal ZTNA license for a single user identity covers secure access to applications and networks for the user regardless of location - campus, remote, anywhere; the same license covers all use-cases for a better ROI.

Please note that this information is subject to change.

Extreme networks | TD SYNNEX Public Sector | DLT

http://www.extremenetworks.com/contact