At-a-Glance

ExtremeCloud™ Universal ZTNA

The Easiest, Most Complete Network Access Solution for Users Everywhere

Networks are transforming as organizations strive to create a more flexible workforce by embracing hybrid work, continuing to hire fully remote workers, and using third-party resources to fill skills gaps. Networking solutions also need to address the increased adoption of IoT devices that are enabling business transformation. Extreme Networks calls this way of working in increasingly distributed environments the Infinite Enterprise.

As networks expand to meet the needs of the Infinite Enterprise securing application and network access for both people and devices will be of paramount importance. For example, 84% of organizations claimed an identity-related breach in the last year, with 78% citing a direct business impact as a result. **The need for consistent security policy for both campus and remote access is greater than ever.**

To achieve a more secure and flexible workforce, organizations have to re-think traditional network security measures that are inherently "allow all", and instead **extend zero trust beyond applications and into the network.**

Traditional security measures enabled by CLI-based switch configuration, network access control (NAC), and VPN for remote access cannot provide a consistent level of security and frictionless end user experience. While zero trust network access (ZTNA) tools provide quick and secure remote access to applications, attempting to extend them to campus environments does not address the threats associated with network access, such as those linked to IoT and guest devices.

Unifying Cloud Managed ZTNA, NAC, AP and Switch Security

Universal ZTNA simplifies network security management with one solution that brings zero trust device and application access together.

Frictionless user experience and consistent security policy for applications and devices, including IoT

Benefits of ExtremeCloud Universal ZTNA

Universal ZTNA is the one solution that combines and enhances the best of campus and remote access security for today's work models.

Fill IT security gaps

Consistent security policy for users, devices and applications with one solution: ZTNA, NAC, with switch and AP enforcement points. Designed to manage and enforce identity-level zero trust policy for employees, guests, contractors, and IoT devices.

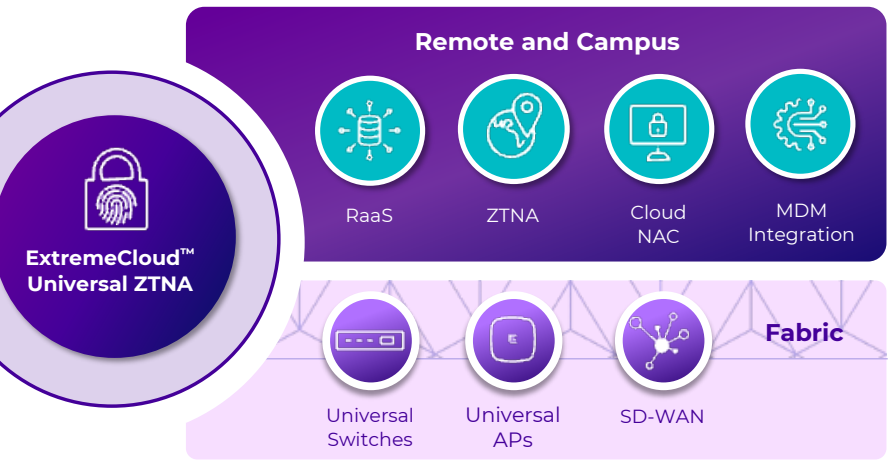
UZTNA integration with MDM solutions such as MS Intune enables augmented access decisions linked to granular device health and authentication capabilities.

Quick time to value

Deploy and scale quickly through a SaaS deployment integrated with identity providers such as Google Workspace and Azure AD to accelerate user onboarding.

Operational and cost efficiency

Reduce complexity with simplified security management delivered through a single subscription. Eliminate the need for additional platforms with inclusion of radius as a service.



ExtremeCloud manages:

- One solution that combines the best of campus and remote access security for today's work models
- Single identity-based zero trust policy engine for both networks and applications
- Unified observability, visualization and reporting for enhanced insight and simplified management
- Automated onboarding and provisioning of IoT and end user devices
- Automated configuration of NAC, SSIDs, ports and VLANs on Universal APs and switches

Summary

- ✓ **Consistent security and user experience** - Zero Trust for all devices everywhere
- ✓ **Increased performance** - Cloud proxy allows remote traffic to travel securely to the cloud
- ✓ **Designed with IoT in mind** - Secure trusted IoT devices and traffic
- ✓ **Supports multiple guest cohorts** - Comprehensive guest access segmentation
- ✓ **Enhanced posture checking** - Device access can leverage real-time health check
- ✓ **Simple to consume** - SaaS deployment
- ✓ **Simple to operate** - Automated device configuration and single reporting interface

Extreme networks