Data Sheet

ExtremeCloud Universal ZTNA

Highlights

Complete Access Security

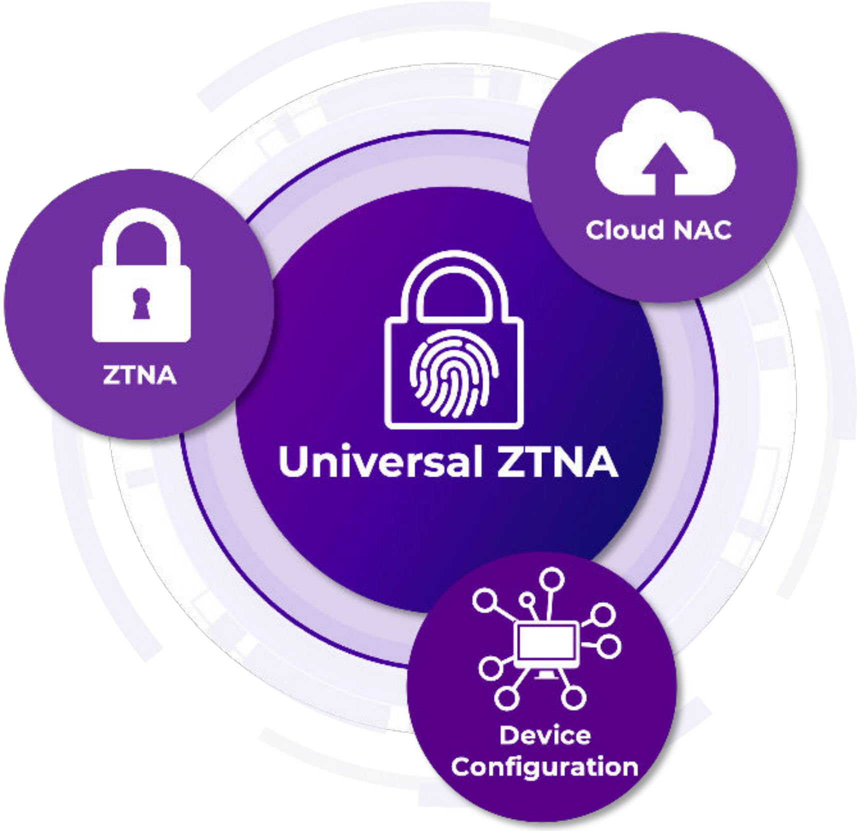
- Cloud NAC and ZTNA in a single, easy-to-use SaaS offering
- One zero-trust policy engine orchestrates access policy end-to-end
- Unified management of network infrastructure and security from ExtremeCloud

Frictionless Experience

- Consistent user experience from anywhere
- Secure access to applications in the cloud and data center
- Easy to adopt and manage for administrators
- Agent-based and agentless deployment options enable multiple use cases

Automation via Universal Platforms

- Universal ZTNA-driven automated security configuration and enforcement
- Designed to work with the industry's most robust Universal Platforms
- Integrated with Extreme Fabric, Universal ZTNA becomes part of the fabric services that allow the network to flex effeiciently while keeping security policy consistent end-to-end



ExtremeCloud™ Universal ZTNA simplifies network security management by unifying Cloud NAC and ZTNA in a single, easy-to-use SaaS offering, with a single zero trust policy engine and automated configuration and enforcement, ensuring consistency and unified observability.

The solution covers various scenarios for organizations aiming to enhance access security for remote, on-site, and hybrid employees. This includes those interested in implementing a cloud-based NAC, those seeking an alternative to VPN for remote access, and those looking to bolster security measures and transition their organization to a more comprehensive Zero Trust network approach.

Complete Access Security

Unlike many network security solutions that are fragmented and complex, Universal ZTNA is one solution that combines the best of on-site and remote access security by unifying Cloud NAC and ZTNA. One zero-trust policy engine manages secure access to networks and applications when on-site, and secures remote access to applications when off-site. Cloud NAC includes RADIUS as a service reducing the number of extra services to buy and manage. No on-site NAC appliances are required simplifying deployment, and a single licensing construct makes buying easier.

Frictionless User Experience

Balancing security and user experience for employees and administrators is difficult when managing multiple systems and asking users to change how they access resources depending on where they work that day. Universal ZTNA solves that problem by providing a consistent user experience for employees and admins. Admins can apply agent-based and agentless deployment options that address multiple use cases. The management interface is easy to adopt and manage for administrators and provides alerts and enhanced insight with unified observability, visualization, and reporting.

Automation via Universal Platforms

Universal ZTNA works in concert with Extreme's robust Universal Platforms to automatically configure devices to enforce security policy. When used in concert with Extreme Fabric, Universal ZTNA becomes part of the fabric services that allow the network to flex for efficiency and resiliency while keeping security policy consistent end-to-end.

Key Capabilities and Components

Capabilities	Description
One Zero Trust Security Policy Engine	Creates consistent security across the network with identity-based policies that grant limited access for users and managed BYOD or IoT devices based on multiple factors, with context, like device health, location, time of day, and granular authentication of users and devices.
Cloud-managed NAC with RADIUS as a Service	Defines and enforces unique access control policies based on roles, locations, and device types. Across network access layers, risk assessment policy configuration capabilities monitor the risk posture of connected devices continually.
Zero Trust Application Access	Provides agent-based and agentless secure remote and on-site access to enterprise apps via encrypted IPsec or Wireguard tunnels and cloud-managed security policies to create a secure segment between an authorized user and a specific named application.
Automated Configuration with Universal platforms	Enforces policies with tight integration to Extreme Universal switches and APs (cloud-managed and non-cloud-managed). Extreme Instant Secure Port can be leveraged to simplify security configuration in switches where it is enabled.
Enhanced Insight, Simplified Management	Unified observability, visualization, and reporting based on identity speeds time to troubleshoot incidents. Device discover and fingerprinting automates secure onboarding and provisioning of IoT and end-user devices.

Product Specifications

Specifications	Description
Dashboard	**Health Status:** Service Connector, Availability Trends, Application status (Web, Secure Shell, Remote Desktop, Network Resources), RadSec Proxy Status **Usage Metrics:** Authentication Status, Top 5 End Systems, Policy Status, Application Usage **Trends:** Top 5 apps, Users and End Systems, Service Connector and RadSec Proxy Availability, Number of Policy Conditions, Top 5 Usage
Compliance Check	Enforces the appropriate compliance policies for endpoints through a persistent client-based agent or a query to external MDM Microsoft Intune. Enables the device posture check at a global level, checks for the minimum OS version, browser version, latest antivirus, and mobile PIN-lock.
Universal ZTNA Agent/ Agentless	Universal ZTNA provides both agent-based and agentless options for application access. The Universal ZTNA Agent supports Microsoft Windows, Apple Mac OS and iOS, Linux, Chrome OS (Chromebook), and Android. For BYOD use cases, an agentless option is supported where browser-based access is used for the authorized applications.

Specifications	Description
Resources	Universal ZTNA Cloud Gateway Universal ZTNA Cloud Gateway is deployed across multiple Regional Data Centers (RDC) and routes traffic to a Service Connector deployed on-premises and/or IaaS. The role of the Cloud Gateway is to route traffic based on where the applications are deployed. The data traffic is not decrypted in the gateway. Service Connector Service Connector is a resource that needs to be deployed closer to where the applications are in Data Center, Campus, and/or IaaS providers like AWS (Amazon Web Services), GCP (Google Cloud Platform), and Microsoft Azure. The service connector initiates an outbound connection to the Cloud Gateway. A secure tunnel (IPsec or Wireguard) is established from the agent to the Service Connector through the Universal ZTNA Cloud Gateway. The tunnel is end-to-end encrypted. Only private application traffic will go through the tunnel. RadSec Proxy Extreme Universal Switches and Access Points natively support RadSec. Deployment of an on-prem RadSec proxy is supported (optional). A RadSec tunnel will be established between the RadSec proxy and RADIUS server in the cloud. Deployment Options for Service Connector and RadSec Proxy Containerized (docker container), Packaged, OVA (VMware environment)
Policy Engine	Three policy types are supported: Secure Application Access Secure Application Access Policy offers precise control over secure access to designated applications within a network. This policy empowers administrators to specify which users or user groups possess access rights to applications or groups of applications, fostering granular access management. Additionally, Secure Application Policies offer optional conditions, including user location and time-based restrictions, enabling administrators to enforce access permissions based on geographical boundaries or time intervals. By leveraging this comprehensive set of controls, organizations can enforce tailored access management strategies, ensuring both system integrity and mitigating potential risks in application usage. Secure Network Access Secure Network Access Policy establishes a robust framework for ensuring secure network access within an organization. This policy empowers administrators to precisely define which devices or device groups can access specific VLANs along with specifying permitted IPs, ports, and protocols for authenticated devices. Authentication methods, including 802.1x and Mac authentication, offer flexibility in verifying device identity. Additionally, administrators have the option to incorporate conditional access controls based on the geographic location of the device and time-based restrictions to govern access during designated intervals. By implementing this comprehensive set of controls, organizations can effectively manage network security while facilitating authorized connectivity tailored to their specific requirements. Secure Hybrid Access Secure Hybrid Access Policy represents a comprehensive approach to access management, seamlessly integrating both network and application access to ensure a consistent user experience across office and remote environments. On the network side, this policy establishes secure network access by enabling administrators to specify which devices or device groups can access designated VLANs along with defining permitted IPs, ports, and protocols for authenticated devices. Authentication methods such as 802.1x and Mac authentication offer versatile device verification options. Simultaneously, on the application policy side, administrators can define secure access to one or more applications by delineating user or user group permissions for application access. Optional conditions based on user location and time-based restrictions further enhance control over access parameters. By harmonizing network and application access controls, organizations can uphold stringent security standards while ensuring a seamless and equitable user experience irrespective of their location or mode of access.
Supported Infrastructure	Extreme Universal Switches and Access Points • Switches: 4120, 4220, 5420, 5520, 5720, x435 • Access Points: AP5020, AP5010, AP5050U/D, AP4000, AP3000/X, AP410C, AP305C/CX

Specifications	Description
Integrations	User identification and authorization via Microsoft Entra ID, Google Workspace, On-premises AD Device identification and authentication via Microsoft Intune SIEM via Splunk and LogPoint
Security and Privacy	Customer data traverses ExtremeCloud network (Data goes through cloud gateway and is encrypted) SSO for ExtremeCloud IQ via SAML (using same as XIQ via common services) Option to use multi-factor authentication with Google Authenticator for administrators

Security and Operation

- Accounts are password protected and accessed via secure SSL with Single Sign-On to Universal ZTNA
- Management traffic is encrypted and restricted using HTTPS and industry proven CAPWAP protocol protected by DTLS
- Multi-Factor authentication with Google Authenticator for administrator accounts
- Multi-tenant architecture with secure account separation
- Centralized monitoring and management
- Optional value added reseller (VAR) and partner management capabilities including account provisioning and maintenance

Ordering Information

Tiers	SKU	SKU Description
ExtremeCloud Universal ZTNA Secure Tier Subscription	XC-SUI-S-C-EW	ExtremeCloud Secure Tier, includes Network Access Control and RADIUS as a Service, minimum of 50 qty required for initial order, SaaS Subscription and EW SaaS Support per user identity, per year
ExtremeCloud Universal ZTNA Secure Tier Subscription	XC-SUI-S-C-PWP	ExtremeCloud Secure Tier, includes Network Access Control and RADIUS as a Service, minimum of 50 qty required for initial order, SaaS Subscription and PWP SaaS Support per user identity, per year
ExtremeCloud Universal ZTNA Secure Plus Tier Subscription	XC-SPUI-S-C-EW	ExtremeCloud Secure Plus Tier, includes Universal ZTNA, minimum of 50 qty required for initial order, SaaS Subscription and EW SaaS Support per user identity, per year
ExtremeCloud Universal ZTNA Secure Plus Tier Subscription	XC-SPUI-S-C-PWP	ExtremeCloud Secure Plus Tier, includes Universal ZTNA, minimum of 50 qty required for initial order, SaaS Subscription and PWP SaaS Support per user identity, per year

Service and Support

Extreme Networks provides comprehensive service offerings that range from Professional Services to design, deploy, and optimize customer networks, customized technical training, to service and support tailored to individual customer needs.

For more information about Extreme Networks service and support, contact your Extreme Networks account executive or visit Extreme Networks Support.

Additional Information

For additional technical information on ExtremeCloud Universal ZTNA, visit https://www.extremenetworks.com/solutions/security/ztna.