Security in the Digital Era – What Does That Really Mean?

Despite the various benefits and advantages that cloud networking brings to organizations, cloud security is an on-going concern. The frequency and sophistication of malicious, cybersecurity attacks only continue to increase; the best cloud companies must always be diligent to not only keep up with latest security standards but stay steps ahead of the always-changing threats.

So, what truly is needed to keep your organization's cloud secure in this digital era? It begins by looking at the security eco-system as a whole. It's about being able to simplify and scale network segmentation, and having visibility of all applications, users, and devices. At Extreme, we take threats to the availability, integrity, and confidentiality of our clients' information seriously. Whether onboarding guest or corporate-issued devices, monitoring IoT devices, or providing context-aware policy enforcement, the security and accessibility of our security solutions lie within the automatic actions that are taken predominately by the network itself. Additionally, Extreme provides the network foundation to interact with and support 3rd party security systems and components that are integrated into a holistic security ecosystem. Extreme Networks understands the value of a rich ecosystem and has an open technology partner program that allows best of breed integrations for our products. These integrations can be as simple as passing data with our APIs to being incorporated into the ExtremeCloud IQ workflows or configuration menus.

Integrations for Extreme Networks are categorized as horizontal (typically found in every network deployment) or specialized (found in specific verticals such as Healthcare, Retail, SLED, etc.).

Here are a few of the integral security elements that make our cloud solution stand out from the rest:

ISO/IEC 27001 Certification

Extreme Networks is the first and only major cloud-managed networking vendor recognized by the global standard for commitment to information security management systems best practices and controls. To ensure the highest levels of information systems and data protection, management, and compliance, Extreme Networks' ExtremeCloud IQ cloud platform is ISO/IEC 27001 certified by the International Standards Organization (ISO). Although our competitors claim SOC2 compliance from their hosting vendor, there are no vendors with SOC2 on their own cloud management platform. Extreme Networks is the only vendor who has gone beyond this basic claim riding on the back of our providers and added the additional ISO27001 end-to-end certification on top of what is already provided by AWS, GCP, and Azure.

Cloud Services

Our Cloud Services are hosted within Amazon AWS (Amazon Web Services), Microsoft Azure, and Google data centers, taking advantage of inherent AWS, Microsoft, and Google security and compliance capabilities at the data-center layer.

For added security, our cloud networking solution also encrypts the data traffic while in transit between a customer's site and the RDC (regional data center) containing the customer's ExtremeCloud IQ Public Cloud instance. The RDCs also do not collect or retain any data traffic generated on the customer networks.

Role-Based Access Control

Within ExtremeCloud IQ, role-based access control allows you to create different user policies based on individuals with different roles in the organization. With those roles comes a unique set of rules to how they are going to access technology and resources. Context-based networking gives you the power to identify users, devices, and applications, and either prioritize or restrict depending on the benefit for your network and your organization. This way you can limit the performance of a guest or BYOD device vs a corporate device, block torrents or illegal streaming media, while enhancing the service to legitimate voice or video apps.

WPA3 and Beyond

Extreme's APs can support and offer the highest level of security available on the client devices. This allows Extreme to provide the latest levels of security, yet still support legacy technologies while providing isolation between the two groups.

Context-Based Networking

Context-based networking gives you the power to identify users, devices, and applications, and either prioritize or restrict access depending on the benefit for your network and your organization. This way you can limit the performance of a guest or BYOD device vs a corporate device, block torrents or illegal streaming media, while enhancing the service to legitimate voice or video apps. This role-based access and context-based networking does not necessarily have to happen on the SSID level. User profiles are a great way to segment users under the umbrella of a single SSID. You can assign clients a list of access settings based on preset conditions.

PPSK

Private Pre-Shared Keys, what we call PPSK, truly bridge the gap between complex 802.1X and unsecure PSK. This is great for guest networks or for devices that don't support 802.1X, or even in cases where 802.1X is just too hard to deploy and monitor. Many of the new IoT devices don't support certificates but need to be segmented on the network for obvious security concerns, and PPSK is a wonderful option for this type of use case. With PPSK, each user or device gets a unique key, which enables an IT team to establish rules based on user and device.

Private Client Groups

Private Client Groups (PCG) deliver a unique, secure, and simple way to manage micro-segmentation networking capability. It is a unique capability that enables an IT administrator to setup "private groups" of wireless and/or wired client devices that can still seamlessly connect to as they roam across a common SSID/domain.

Layer 2-7 DPI

Layer 2-7 deep packet inspection gives you full visibility into what applications are running on your network, how much bandwidth they are using, what time of day they are running, and even who is using the applications.

Cloud-Managed Network Access Control

An option for additional cloud networking security is ExtremeCloud A3 – an innovative Cloud-Managed Network Access Control (NAC) solution. It secures, manages and controls all devices on your network, and provides complete functionality for device onboarding, guest management, automated device provisioning, device profiling and access control. A3 is vendor agnostic and can be deployed on all major vendors' access networks.

Some additional measures Extreme takes to secure our cloud-based applications:

- Firewalling, to control and protect inbound and outbound traffic
- Threat detection, with continuous monitoring for malicious and unauthorized behavior, including unauthorized system access and brute-force attacks
- DDoS-attack prevention and flow control with industry-leading tools
- Staging all ExtremeCloud IQ releases and patches with continuous penetration scanning for application vulnerabilities, to prevent any issues prior to actual deployment in production
- Industry-standard OS hardening processes for production server deployment
- Daily backups of production-network data, and storage of backups in an encrypted state
- Securing access to the underlying computing infrastructure with features like VPC, NAT, TLS encryption, reporting tools and automated password protection
- Strictly limiting access to the AWS cloud infrastructure to a small number of designated Extreme Networks DevOps engineers
- Monitoring and tracking DevOps-personnel activities in the AWS environment, with a server/application audit trail.

Extreme enables administrators to ensure their networks are not being abused or infiltrated, and if so, identify threats and adjust security policies accordingly.