Table of Contents

ExtremeCloud™ IQ Cloud Services Platform

Security and Availability Controls Overview

What is ExtremeCloud IQ?

Extreme Networks ExtremeCloud IQ Cloud Services Platform is a globally distributed cloud-based infrastructure offered as Software-as-a-Service (SaaS). ExtremeCloud IQ provides access to configuration and network monitoring statistics for all managed Extreme Networks devices.

Data Centers

Geographically Distributed

ExtremeCloud IQ leverages only major commercial cloud hosting providers. Today, over 90% of the infrastructure is hosted via Amazon AWS. Other providers used consist of Google GCP and later in 2020, Microsoft Azure.

ExtremeCloud IQ utilizes geographically distributed data centers to optimize customer network connectivity. Facilities used are located in North America, South America, Europe, Asia, and Australia.

Certifications

ExtremeCloud IQ utilizes Amazon AWS, Google GCP, and Microsoft Azure (late 2020) as infrastructure providers. These providers feature public statements of SOC 1, 2, 3, PCI, ISO, and other compliance which can be reviewed at the following locations:

- AWS Compliance Programs
- Google Cloud
- Microsoft Compliance Offerings

Extreme Networks reviews vendor capabilities, scale, and SLAs on a regular basis.

ExtremeCloud IQ is ISO27001 Certified. See here.

International Compliance and Safe Harbor

ExtremeCloud IQ meets European privacy controls and Safe Harbor certification by adhering to geographic data policies. The European-based data center performs cross data replication solely within the EU region in order to meet EU privacy controls and GDPR.

Data Encryption

All data in transit to or from the platform is encrypted using DTLS, TLS, or similar protocols. All data at rest is encrypted.

Storage for certain files and backups are stored at rest using server side encryption, using AES-256 block-based encryption.

The data volumes utilized by the various database systems that support the Cloud Service are encrypted using a FIPS 140-2 compliant mechanism and key management.

Extreme Networks is solely responsible for the management and security of all encryption keys used.

Physical Access

Extreme Networks employees do not have physical access to any of the hosted data centers where ExtremeCloud IQ resides. All access to Extreme Networks corporate facilities is via secure access, and all facilities feature 24x7 security and cameras. All network access within Extreme facilities is monitored and secured.

Logical Access

Third-party cloud providers do not possess logical access to the platform. All access to the platform back end is via multi-factor authentication of vetted and authorized individuals with a need-to-know, and all access is logged and strictly controlled from authorized hosts using encrypted communications.

Cloud Operations

Cloud Operations (DevOps) teams are based in the United States, Toronto, Canada, and China. All access to the cloud infrastructure and any possible customer data created by the cloud services is accessed via VPN and multi-factor authentication. Servers in North Carolina and New Hampshire data centers are intended to be used as bastion hosts for the Cloud Operations team and QA/Engineering for access to the cloud infrastructure. These systems are logged, secured, and maintained in accordance Extreme's Business Continuity Plan and as part of the ISO 27001 ISMS.

Software Upgrades and QA

Extreme Networks performs all maintenance and updates on a regular basis to the cloud platform. All updates are tested, and QA processed prior to release, and are tested in production once released. At all times, customers control and decide when to upgrade their Extreme Networks hardware devices (access points, switches, routers) as the operating system on these devices is disparate and not dictated by the cloud platform

Change Control Policy

ExtremeCloud IQ is an ISO27001 certified platform and employs multi-stage change control process (Continuous Integration/Continuous Delivery) for all architectural changes and software releases and updates. After passing operational Quality Assurance production tests all changes are moved into a production environment during pre-scheduled, announced maintenance windows.

Data Protection

Background Checks

All Cloud Operations and other integral staff such as product management and developers all undergo background screenings prior to hire.

Privacy

No customer data traversing managed network devices (e.g., Wireless APs, switches, and routers) traverses, contacts, or is stored in the ExtremeCloud IQ SaaS Platform. Only basic monitoring statistics and configuration orchestration information is stored within the cloud platform.

Data Sensitivity

ExtremeCloud IQ provides access to device configuration, management, and network monitoring statistics. Stored data does not include items such as full name, (first and last names of registered administrative users is stored) social security, driver's license, financial account numbers, or personal medical or insurance information for connected devices and users. Only session-based usage statistics such as IP address, device type, mac address, and other information related to a connected device's experience is collected and reported against.

All customer data is private and remains the property of the customer.

Data Available in Cloud Services Platform

For a detailed list of data collected, see the attached data privacy matrix.

Monitoring and Incident Response

Extreme Networks has technical support personnel available 24x7, with additional staff on call for incident escalation responses. If Extreme were to detect any breach or other major security incident, Extreme's staff would immediately escalate, investigate, and remediate as necessary.

Breach Notifications

In the event of breach and upon determination that customer-specific data has been compromised, Extreme shall notify affected customers per the CloudIQ Privacy Policy.

Availability

Uptime

The SLA for ExtremeCloud IQ is provided in the Extreme CloudIQ Service Agreement available at: [URL]

Disaster Recovery (DR)

ExtremeCloud IQ's Disaster Recovery Plan includes daily backups for all data within a Regional Data Center and the replication of those backups between geographic regions. Backups are held for 90 days. All replicated backup data is kept within the United States for all US-based data centers, and within Europe for all other data centers to protect data sovereignty concerns.

Availability and System Monitoring

Extreme employs a distributed availability and performance monitoring system on our cloud infrastructure that operates continuously. Anomalies in the behavior and function of the application are monitored and alerts are sent to ExtremeCloud IQ Cloud Operations for immediate action as required.

It is important to note that ExtremeCloud IQ is a network management and configuration orchestration platform and is not in the data path of customer data, nor does its operation impact the ability of end users or devices to access the network.

Backup and Storage Strategy

- Cross backups are performed utilizing storage in opposing data centers.
- In order to maintain privacy and European Safe Harbor compliance, data centers in different locations within the EU region perform cross backups.
- Backups are stored on both local and remote servers (at different data centers) in a compressed and encrypted format and inaccessible to users.
- An authenticated administrative-level user is required to restore data for an entire Regional Data Center (RDC) and this access is limited to Cloud Operations personnel.
- Customer data cannot be individually restored. Customers are responsible for performing regular backups of their VIQ (Virtual Instance) of the cloud service if they anticipate needing to recover a lost object caused by administrative error, accident, or malicious employee actions. Backup of customer VIQ can be performed from the ExtremeCloud IQ GUI easily by any authorized administrator.

Cloud Scaling

ExtremeCloud IQ scales by taking advantage of the inherent elasticity of the cloud and containerized microservices. New servers and back-end infrastructure can be instantiated as needed based on load, customer, and partner growth and as a consequence of monitoring operations for learned patterns of system performance.

Traffic Encrypted and Restricted

All network traffic is encrypted. ExtremeCloud IQ uses CAPWAP and HTTPS for uploading and downloading relevant traffic such as device software image files, full configurations, captive web portal pages, and certificates. Network statistics and monitoring data are also sent via CAPWAP and HTTPS protocol.

Extreme Cloud Operations can perform traffic restriction by IP address at any time, if determined desirable. No unauthenticated users have administrative or monitoring access to the cloud platform.

Logging

All logs from connected devices can be redirected to a central syslog server. In addition, the Cloud Services Platform permits collecting all relevant Events/Alarms/Logs in a centralized manner.

Logical and Physical Security

ExtremeCloud IQ Cloud Operations proactively manages firewall and networking security policies for the services hosted. Extreme utilizes current industry best practices regarding security and access procedures to limit logical and physical access and permissions to these systems.

All access to physical data centers the ExtremeCloud IQ is hosted in are not accessible by Extreme employees for any reason. All access to Extreme Networks' facilities and properties is via continuously monitored and locked access, including security cameras. All use of Extreme Networks' network services is monitored.

Antivirus

Antivirus software is used on all Extreme Networks employee laptops and PC's.

Malicious and Vulnerable Code

All code written for the cloud platform undergoes daily malicious code and code vulnerability scanning using automated test systems. All existing code and newly developed patches and features are all subject to this analysis. The results of those tests are acted on by development and CloudOps and are not publicly disclosed, nor do we disclose any test results to external or internal customers.

System Hardening

All systems used in the cloud infrastructure are hardened according to CIS benchmarks and leverage a modified, tuned, and specifically secured operating system environment developed by Extreme Cloud Operations.

Segmented Environments

Separate environments are maintained for Development, User-Acceptance, and Production.

Third Party Software Patches

Third-party patches are applied into Extreme's systems following the same Change Control Policy as production cloud releases. Major version upgrades of third-party software are planned as part of main development cycles, implying a longer duration testing cycle and gained stability for intermediate software releases.

User Roles Policies

ExtremeCloud IQ provides administrative options to manage user roles and levels of permissions for users. A customer will have a superuser account with ability to create users with granular permissions within the realm of his/her account.

Customers having accounts managed by an Extreme partner (an integrator or managed service provider) will be able to restrict/grant access to their parent partner (i.e. for preventing partner staff from monitoring or configuring their system, or alternatively granting them access for partner maintenance). Partners can disable a customer account (i.e. for non-paying or terminated customers).

Account Provisioning

New accounts are provisioned when Cloud Services Platform applications are being evaluated by or sold to a customer. The new user will be registered with Admin permissions and can create other users within the account realm. Extreme's Cloud Operations have potential logical access to the system for troubleshooting purposes.

Password Policies (Resets, Storage)

Only an administrator who has sufficient permission to administer other users within his/her account realm can perform password resets. No passwords are stored in clear text. Users can utilize the "Forgot Password" option in the login page to reset passwords.

SSO, Session Timeouts

ExtremeCloud IQ supports SSO using SAML. SAML is not available by default and must be separately requested and configured by Extreme Cloud Operations for the customer.

Sessions automatically time out after 30 minutes, and all administrative access is logged to an audit log within the cloud platform.

Data Privacy Information

Provider	End User Personal Data Visibility Details
Infrastructure Provider (AWS, Google, Azure)	Cloud Infrastructure providers are not authorized to access/view data in ExtremeCloud IQ. All access is isolated to private instances only accessable via Extreme Networks assets and by a limited set of Extreme Networks employees.
Customer Support Provider (Extreme GTAV)	NO DATA IS ACCESSIBLE TO GTAC UNLESS SHARED BY CUSTOMER o ENGINEERING.
DevOps / Development (Extreme Engineering)	Access to list of customer (MSP, Customers) who purchased ExtremeCloud
	End User Device-Specific Data
	MAC Address
	Device Manufacturer (Apple, Samsung, Intel, etc…)
	Last assigned IPv4 and IPv6 Address
	Hostname
	Radio attributes and capabilities
	Location (WiFi AP to which the device is associated)
	Location (WiFi AP to which the device is associated)
	Last time user was seen on the network
	Last AP connected
	Network VLAN assigned
	Historical roaming history (where have you been at X time)
	Last specific Network/SSID connected
	Last specific Network/SSID connected
	Geographic location where user was last seen
	Specific “Site” where user was last seen
	Specific “Site” where user was last seen
	End Device Network Usage Data
	wireless statistics and summary events over time
	Error rates over time
	Last radio channel, band and RSS reported for user’s device
	Applications used by the device/user
	Applications used by the device/user
	If using 802.1x, logged in user name
	If using PPSK, PPSK user name or email address
	Email address
	User Specific Data (Guest Captive Portal/Social Login)
	Telephone numnber (if submitted and required, for PPSK authentication)
	Telephone numnber (if submitted and required, for PPSK authentication)
	Administrator Data (Used to create cloud administrators)
	Administrator Data (Used to create cloud administrators)
	Admin Email Address
	Admin City, State, Country
	Company Name
	Company Business Vertical (Retail, education, etc)
	Admin Phone Number
Vendors	Vendors have no access to data

About Extreme Networks

Extreme Networks, Inc. (EXTR) is the industry's first cloud-driven, end-to-end enterprise networking company. Our best-of-breed technology solutions, from the wireless and IoT edge to the data center, are flexible, agile, and secure to accelerate the digital transformation of our customers and provide them with the fastest path to the autonomous enterprise. Our 100% in-sourced services and support are number one in the industry. Even with 50,000 customers globally, including half of the Fortune 50 and some of the world's leading names in business, hospitality, retail, transportation and logistics, education, government, healthcare, and manufacturing, we remain nimble and responsive to ensure customer and partner success. We call this Customer-Driven Networking™. Founded in 1996, Extreme is headquartered in San Jose, California. For more information, visit Extreme's website or call 1-888-257-3000

Global Headquarters
6480 Via Del Oro
San Jose, CA 95119
+1 408-579-2800
Toll-free: +1 888-257-3000
Fax: +1 408-904-7002
http://www.extremenetworks.com

Extreme networks

http://www.extremenetworks.com/contact

©2020 Extreme Networks, Inc. All rights reserved. Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. For additional information on Extreme Networks Trademarks please see http://www.extremenetworks.com/company/legal/trademarks. Specifications and product availability are subject to change without notice. 32369-0720-10