White Paper

Table of Contents

ExtremeCloud™ IQ: Cloud Security and Architecture Overview

Product Overview

Extreme Networks ExtremeCloud IQ is a globally distributed, cloud-based, network management solution offered as Software-as-a-Service (SaaS) and sold as a subscription through Value-Added Resellers around the world. ExtremeCloud IQ provides centralized configuration orchestration and network monitoring, reporting, alarms, and statistics for all cloud-enabled Extreme Networks devices.

Architecture Overview

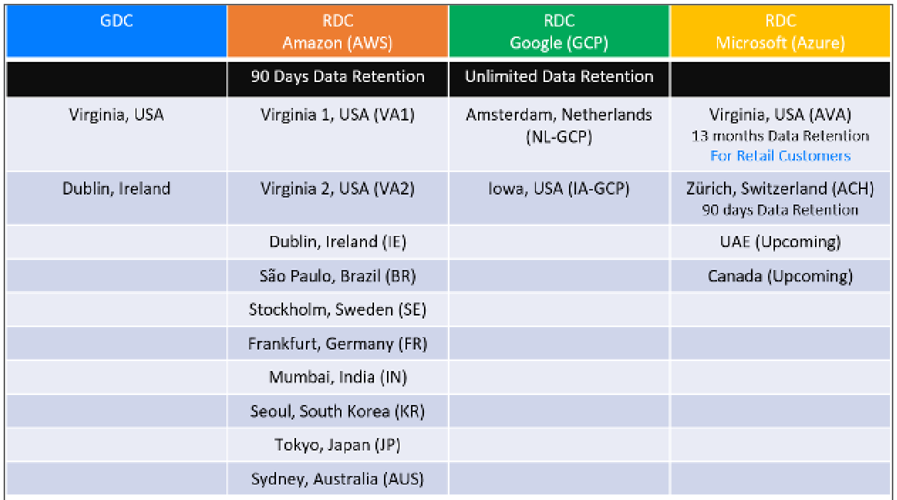
Geographically Distributed

ExtremeCloud IQ operates in 17 regional data centers (RDC) and two global data centers (GDC) as of the publication of this document. An RDC is a geographic instance of the SaaS solution where customer data is hosted. The service leverages only major commercial cloud hosting providers. Today, over 90% of the solution is hosted via Amazon AWS. Other providers used consist of Google GCP and Microsoft Azure.

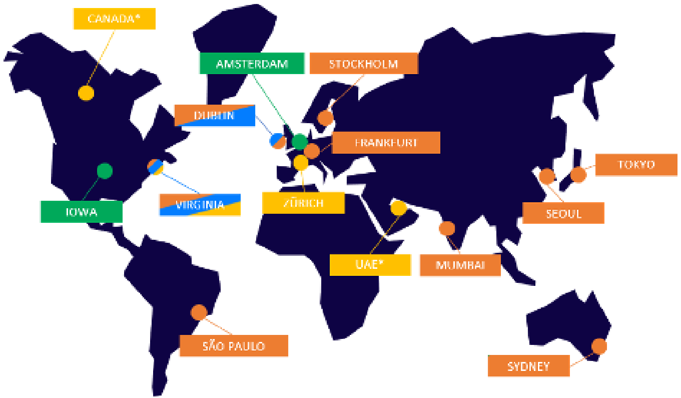
v1.0 - October 2020

Table of Contents (cont.)

GDC



GDC	RDC Amazon (AWS)	RDC Google (GCP)	RDC Microsoft (Azure)
	90 Days Data Retention	Unlimited Data Retention	
Virginia, USA	Virginia 1, USA (VA1)	Amsterdam, Netherlands (NL-GCP)	Virginia, USA (AVA) 13 months Data Retention For Retail Customers
Dublin, Ireland	Virginia 2, USA (VA2)	Iowa, USA (IA-GCP)	Zürich, Switzerland (ACH) 90 days Data Retention
	Dublin, Ireland (IE)		UAE (Upcoming)
	São Paulo, Brazil (BR)		Canada (Upcoming)
	Stockholm, Sweden (SE)		
	Frankfurt, Germany (FR)		
	Mumbai, India (IN)		
	Seoul, South Korea (KR)		
	Tokyo, Japan (JP)		
	Sydney, Australia (AUS)		



Private RDCs:

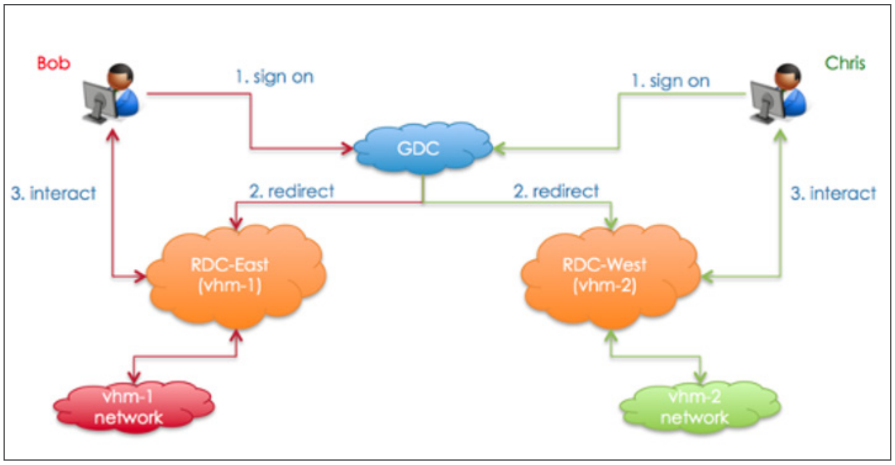
1. Ohio, USA
2. Dublin, Ireland
3. Sydney, Australia

The GDC, or Global Data Center is geographically disbursed and load-balanced between the US and Ireland. US login information exists only on the US instance of the GDC, while EU and other nations exist in the Ireland instance to maintain geographic data protection.

In addition to serving as the primary authentication mechanism to the ExtremeCloud IQ SaaS platform, the GDC also performs device redirection and other global services as required. All instances of the GDC are hosted within Amazon AWS.

RDC

The RDC, or Regional Data Center, is hosted among various cloud providers depending on data retention time and location. The RDC consists of virtual environments known as a VIQ. Each customer has their own VIQ, which is where all interaction with the product occurs and where customer-owned devices connect. The VIQ exists only on a single RDC, resulting in all customer data being stored within that particular location.



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.

Cloud Providers

ExtremeCloud IQ leverages the following cloud providers. For the purposes of GDPR compliance, these providers can be considered sub-processors.

- Amazon AWS
- Google GCP
- Microsoft Azure

For additional information on data privacy and sub-processors, see our data privacy link.

Container-Based Solution

ExtremeCloud IQ is a micro-service driven SaaS application that makes extensive use of containers hosted within our cloud provider environment. These containers are orchestrated in a 100% Kubernetes environment, and are maintained, monitored, and operated continuously by Extreme Networks Cloud Operations.

Certifications

ExtremeCloud IQ utilizes Amazon AWS, Google GCP, and Microsoft Azure 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:

- https://aws.amazon.com/compliance/programs/
- https://cloud.google.com/security/compliance/offerings/
- https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home

Extreme Networks reviews vendor capabilities, scale, and SLAs on a regular basis. ExtremeCloud IQ is ISO27001 Certified. See https://cloud.kapostcontent.net/pub/d8b0c577-e7f3-457d-9669-daa3d666df61/iso-27001-certification-1

ExtremeCloud IQ is actively pursuing Cloud Security Alliance STAR Level 1, ISO 27017, ISO 27701, to be completed by December 2020, and SOC 2 Type 2 completed in 2021.

International Compliance

ExtremeCloud IQ adheres to geographic data policies. The European-based data center performs data replication solely within the EU region and all backups are kept solely within the EU.

ExtremeCloud IQ Security

Data State Protection

Data In-Transit

All network traffic to or from the solution is encrypted. ExtremeCloud IQ uses CAPWAP and HTTPS protocols which utilize DTLS and TLS respectively for uploading and downloading relevant traffic such as device software image files, full configurations, captive web portal pages, and certificates. TLS 1.2 and optionally TLS 1.3 are used, with encryption ciphers supported including AES.

Network statistics and monitoring data are also sent via CAPWAP using DTLS and/or HTTPS protocol.

Data at Rest

All data at rest within ExtremeCloud IQ stored as files or in databases are housed on encrypted storage volumes. AES-256 is used with keys managed via the cloud provider. By default, keys are rotated automatically by the providers every 3 years, or as configured by the cloud provider managed services. Customers cannot manage encryption keys.

Logging

All logs from connected devices can be redirected to a central syslog server on the customer premises. In addition, ExtremeCloud IQ 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 in which ExtremeCloud IQ is hosted are not accessible by Extreme Networks employees for any reason. All access to Extreme Networks' owned 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 and Policies

ExtremeCloud IQ provides administrative options to manage user roles and levels of permissions for end-users. A customer will have a single "super user" account with ability to create additional administrators and users with granular permissions to various application functions.

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 a customer registers at https://extremecloudiq.com The account 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)

No passwords are stored in clear text. Users can utilize the "Forgot Password" option in the login page available at https://extremecloudiq.com 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 by default and are configurable by the administrator, and all administrative access is logged to an audit log within the cloud platform

Logical Access

Third-party cloud providers, sub-processors, and contractors do not possess logical access to the platform. All access to the platform by cloud operations staff 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 bastion hosts using encrypted communications.

Cloud Operations

Cloud Operations (DevOps) teams are based in the United States, Canada, India, and China. All access to the cloud infrastructure and any 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 development, all updates are moved to a staging environment for Quality Assurance production testing, prior to being scheduled for production deployment during pre-scheduled, announced maintenance windows.

Data Protection and Privacy

Data Sensitivity

ExtremeCloud IQ provides access to device configuration, management, and network monitoring statistics. Stored data **does not** include PII (personally identifiable information) such as social security, driver's license, financial account numbers, or personal medical or insurance information for connected devices and users. Only session-based usage statistics and PII such as IP address, device type, mac address, and other information related to a connected device's experience is collected and reported against. All PII is treated to the same transmission and storage security as all data and is always encrypted.

No raw TCP/IP session (packet capture) or other data traversing managed network devices (e.g. User A logging into Server B to check banking info via managed wireless APs, switches, and routers) traverses, contacts, or is stored in the ExtremeCloud IQ SaaS Platform.

All customer data is private and remains the property of the customer and can be deleted at any time.

Data available and PII in Cloud Services Platform

For a detailed list of data collected, see the attached data privacy matrix at the end of this document.

Background Checks

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

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 ExtremeCloud IQ Service Agreement.

Disaster Recovery (DR)

Extreme Cloud 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 30 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

Backups are performed daily by Extreme Networks for the ExtremeCloud IQ environment.

Backups are retained for thirty (30) days and are duplicated. One master copy of the backup is stored within the cloud region for the RDC, and the secondary copy is stored within an alternate region. ExtremeCloud IQ adheres to geographic data policies, and all backups are replicated only within their geographic region of origin. (i.e. US backups are only replicated to US regions, and European backups are only replicated to European regions).

Backups are stored on both local and remote servers in a compressed and encrypted format and inaccessible to users. Only an authenticated administrative-level user can access any backup. Individual case-by-case customer data restoration is not possible, as backups can only be used to restore an entire Regional Data Center (RDC).

Backups are tested at least annually in accordance with documented Extreme Networks disaster recovery testing requirements.

Within the application, an individual backup of customer configuration is permitted. Customers are responsible for performing regular backups of their environment 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 and information on this can be found in the application help documentation or by contacting Extreme Networks technical support (GTAC).

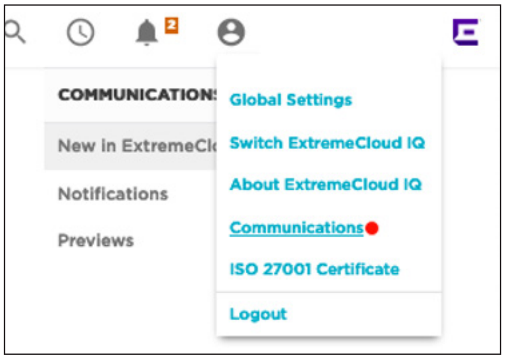
Notification and Support

Technical Support

Support for ExtremeCloud IQ is available 24x7x365 via the support portal. Tickets with GTAC (Global Technical Assistance Center) can be opened here, as well as access to a full knowledgebase and documentation.

Customer Notifications

Notification to customers for upcoming releases, standard maintenance, and other bulletins is provided via the Notification Tab within Extreme Cloud IQ. To access this, click on the upper-right corner of the screen when logged in, and visit the “Communication” link as shown below.



On rare occasion, ExtremeCloud IQ Cloud Operations may notify you by email for urgent or otherwise important maintenance announcements that may require action on behalf of the customer, in addition to the notification page.

We highly recommend that you permit all emails from "communication@extremecloudiq.com" within your SPAM solution and email client to avoid missing important notifications.

For email notifications as indicated above, notification will be sent thirty (30) days in advanced of any maintenance or update that will require customer action. A final notice will be sent seven (7) days prior to the commencement of activity.

Shared Responsibility Model

As with any SaaS solution, security of your data is a shared responsibility. Extreme Networks will work hand-in-hand with you, as only together can we provide a secure environment.

Extreme Networks Responsibility

Extreme Networks is responsible for

- Maintaining operational posture of the ExtremeCloud IQ platform, including
  - Networking and Connectivity
  - Operating systems, containers, and container management solutions (Kubernetes)
  - Storage and data retention
  - Disaster recovery planning, testing, and backups of the solution.
- Maintaining the SLA of ExtremeCloud IQ at or above the published SLA requirements
- Ensuring timely security patches and maintenance for all services and systems that make up ExtremeCloud IQ
- Securing all data at rest and data in transit using industry standard encryption protocols and methods and managing all cryptographic controls within the solution
- Protecting data with architecture and processes to maintain data durability

Customer Responsibility

The subscriber (customer) using ExtremeCloud IQ is responsible for

- Creating and implementing all managed device configurations and individual device security standards used in the customer environment
- Ensuring that configuration and security practices used to configure and secure devices on the customer network meet industry best practices
- Maintaining internet connectivity through proper firewall rules and appropriate bandwidth and latency to guarantee managed device connectivity to ExtremeCloud IQ
- Securing usernames and passwords and other credentials used to access ExtremeCloud IQ to prevent their disclosure to unauthorized persons

- Updating attached network device firmware and applying issued patches for security concerns as recommended by Extreme Networks
- Performing backups of their VIQ environment using tools within the application to assist the customer in recovering from customer administrative error, accident, or malicious employee actions
- Use the solution in a manner consistent with the ExtremeCloud IQ Cloud Terms of Service
- Timely addressing GDPR or other data privacy requests that you receive and addressing any requests that you have with Extreme in an expedient manner

Data and PII Available in ExtremeCloud IQ

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 GTAC)	**No data is accessible to GTAC unless shared by customer 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...)
	Las assigned IPv4 and IPv6 address
	Hostname
	Radio attribures and capabilities
	Location (Wi-Fi Ap to which the device is associated)
	End user "Where in the network" data
	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
	End user "which network location" data
	Geographic location 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
	User specific data (non captive portal)
	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 number (if submitted and required, for PPSK authentication)
	Email address (if submitted and required, for PPSK authentication)
	Administrator date (used to create cloud administrators)
	Admin first and last name
	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**

Extreme networks

http://www.extremenetworks.com/contact