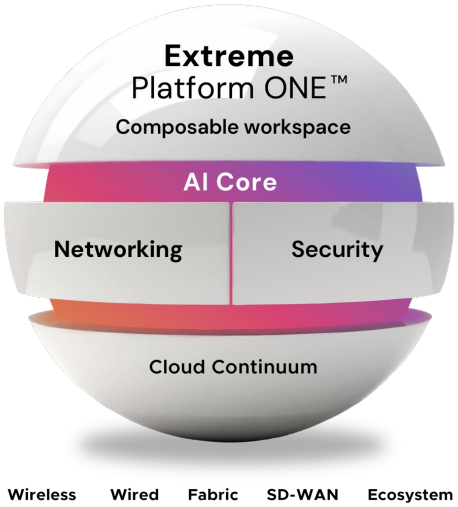
Extreme Platform ONE™ Cloud Architecture & Security

This document is a general reference guide to Extreme Networks' cloud architecture, AI architecture, and security for AI and data. All statements made are current as of the date of publication.

Table of Contents



Platform Overview

Extreme Platform ONE™ is the enterprise connectivity platform that integrates networking and security with AI into one powerful and radically simplified experience and licensing model. It supports NetOps, SecOps, and business teams with built-in AI automation and enables organizations to regain control, unlock innovation, and boost productivity.

- Get it done in ONE: one intuitive experience with cross-functional workflows saves everybody time.
- Go way, way, faster with AI: boost productivity with deep automation powered by built-in AI.
- Keep security simple: AI-assisted zero-trust security reduces time spent on policy, conflicts, and errors.
- Control costs: built-in procurement tools and inclusive licensing reduce the financial cost and complexity.

Extreme Platform ONE is a globally distributed software-as-a-service (SaaS) solution sold as a subscription through a direct sales force, value-added resellers (VARS), and managed service providers (MSPs) worldwide. The platform delivers robust capabilities and operates on Extreme's cloud architecture.

The platform was built with security in mind, with infrastructure-as-a-service (IaaS) vendor-agnostic security and privacy certifications. The software-centric architecture is cloud-hosting agnostic. It is available at points of presence (PoPs) worldwide, with a choice of providers, including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

With AI at its core, Extreme Platform ONE can support millions of infrastructure devices and hundreds of millions of client devices. It facilitates centralized configuration, orchestration, monitoring, reporting, and alerts for all cloud-enabled Extreme Networks devices.

Extreme Platform ONE Data Protection & Security

Extreme Platform ONE Cloud Infrastructure

Data Centers

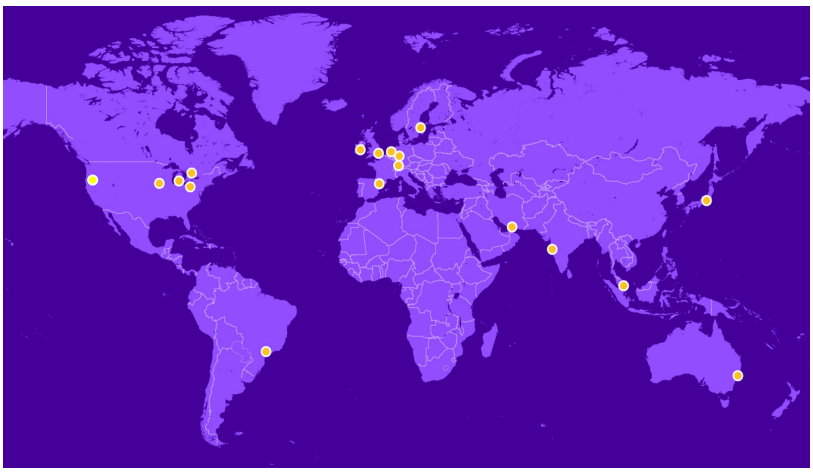
Extreme Platform ONE operates in multiple global data centers (GDCs) and regional data centers (RDCs). An RDC is a geographic instance of the SaaS solution, hosted among three cloud providers (AWS, Azure, GCP), which offer different options for data retention time and location. This is where an organization's data is hosted.

The RDC consists of virtual environments known as virtual interface queues (VIQs). Each organization has its own VIQ, where all interactions with the product occur, and business-owned devices connect.

The global data center (GDC) is geographically disbursed to maintain geographic data protection. Login information, data replication, and all backups are stored in the appropriate region.

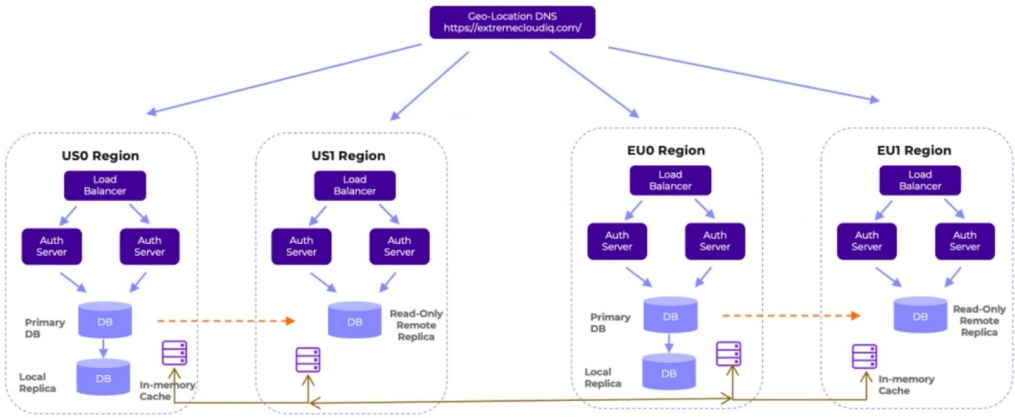
In addition to serving as the primary authentication mechanism for Extreme Platform ONE, the GDC also performs device redirection and other global services as required. All instances of the GDC are hosted within AWS.

Image 1 below provides an overview of the Extreme GDC and RDC locations as of the publication date.



Cloud Usage

The Extreme cloud infrastructure scales by leveraging the cloud's inherent elasticity and containerized microservices. New servers and back-end infrastructure can be instantiated as needed based on load, organization, and partner growth. This process is supported by monitoring operations that identify learned patterns of system performance.



Extreme Platform ONE is a microservice-driven SaaS application that extensively uses container-based solutions hosted within the Extreme cloud provider environment. These containers are orchestrated in a cloud-native environment and are maintained, monitored, and operated continuously by the cloud operations team at Extreme Networks.

Extreme Platform ONE leverages the following cloud providers. For privacy compliance, these providers can be considered sub-processors:

- Amazon AWS
- Google GCP
- Microsoft Azure

API Policy

Extreme Networks extensively uses an API-driven architecture to provide robust, consistent data directly to its applications and end users. We endeavor to support each API in its native form as long as possible; however, to improve the capability and performance of the API, some may be deprecated. Where an API is to be deprecated, advance notice will be given before the deprecation date. Post-deprecation, the backward compatibility will be maintained to provide a sufficient time window for partners and end users to migrate their API-dependent applications. Notifications will be sent out as part of the regular feature updates.

Cloud Operations Security

Logical and Physical Security

The cloud operations team for Extreme Platform ONE proactively manages firewall and networking security policies for the services hosted. Extreme Networks uses best practices for security and access procedures to limit logical and physical access and permissions to these systems. All access to physical data centers in which Extreme Platform ONE is hosted is not accessible by Extreme Networks employees for any reason. All access to Extreme Networks owned facilities and properties is secured through locked access and continuous monitoring with devices including security cameras. All use of Extreme Networks' network services is monitored.

Logical Access

Third-party cloud providers, sub-processors, and contractors do not possess logical access to the platform. Cloud operations staff have full access to the platform via multi-factor authentication of vetted and authorized individuals granted need-to-know access. Access is logged and strictly controlled by authorized bastion hosts using encrypted communications.

Extreme's cloud development teams are geographically located worldwide using a follow-the-sun support method.

All cloud infrastructure and customer data created by the cloud services are accessed via VPN and multi-factor authentication. Servers in data centers located in the northeast 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 following Extreme's Business Continuity Plan and as part of the ISO 27001 ISMS.

Software Upgrades and QA

Extreme Networks performs all maintenance and updates to the cloud platform regularly. All updates are tested, and QA processed before release and are tested in production once released. The organizations always have 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.

Malicious and Vulnerable Code

All code written for the cloud platform undergoes daily scanning for malicious code and code vulnerabilities using automated test systems. All existing code and newly developed patches and features are all subject to this analysis. Our internal development team acts on the results of the tests, which 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 the Center of Internet Security (CIS) benchmarks and leverage a modified, tuned, and specific secured operating system environment developed by ExtremeCloud Operations. Separate environments are maintained for development, user acceptance, and production.

Third-Party Software Patches

Third-party patches are applied to Extreme 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

Extreme Platform ONE provides administrative options to manage user roles and levels of permissions for end users. An organization will have a single "super user" account with the ability to create additional administrators and users with granular permissions to various application functions.

Organizations with accounts managed by an Extreme Networks partner (an integrator or managed service provider) can restrict or grant access to their parent partner (e.g., to prevent partner staff from monitoring or configuring their system or to grant them access for partner maintenance). Partners can also disable a customer account (e.g., for non-paying or terminated customers).

Account Provisioning

New accounts are provisioned when an organization registers with the Extreme cloud. The account will be registered with admin permissions and can create other users within the account realm. Extreme cloud operations has potential logical access to the system for troubleshooting.

Password Policies (Resets, Storage)

No passwords are stored in clear text. Users can reset passwords by using the "Forgot Password" option on the login page.

SSO, Session Timeouts

Extreme Platform ONE supports SSO using SAML. SAML is unavailable by default and must be separately requested and configured by Extreme cloud operations for the organization. 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.

Change Control Policy

Extreme Platform ONE employs a multi-stage change control process (continuous integration/continuous delivery) for all architectural changes, software releases, and updates. After development, all updates are moved to a staging environment for quality assurance and production testing, prior to being scheduled for production deployment during pre-scheduled, announced maintenance windows.

Technical Support

Device, firmware, and software support for Extreme Platform ONE is included with every license and delivered by Extreme's industry-recognized, 7x24x365 global tech support team. Optional premier services, professional services, and resident engineering services are available to provide expertise from planning to migration.

The Extreme Platform ONE service agreement provides the SLAs for uptime, availability, and system monitoring, the backup and storage strategy, disaster recovery, background checks for Extreme staff, security incident monitoring and response, and breach notifications.

Data Protection Overview

All network traffic to or from the solution is encrypted in transit and at rest. Extreme Platform ONE uses CAPWAP and HTTPS protocols, which utilize DTLS and TLS, respectively, for uploading and downloading relevant traffic such as device software image complete configurations, captive web portal pages, and certificates. TLS 1.2 and 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.

All data at rest within Extreme Platform ONE, stored as files or in databases, is housed on encrypted storage volumes. AES-256 is used with keys managed via the IaaS cloud provider. By default, providers regularly rotate keys automatically, or as configured by the cloud provider's managed services. Organizations cannot manage encryption keys.

Extreme Platform ONE provides access to device configuration, management, inventory, contract, security policy, and network monitoring statistics data. Stored data does not include personal data such as social security numbers, driver's licenses, financial account numbers, or personal medical or insurance information for connected devices and users.

Only session-based usage statistics are collected and reported, such as IP address, device type, MAC address, and other information related to a connected device's experience. Some of this data, such as IP and MAC addresses, may be considered personal data. All personal data is treated with 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 Extreme Platform ONE. All customer data is private and remains the organization's property; it can be deleted at any time. For a detailed list of data collected, see the PII Table at the end of this document.

For additional information on data privacy, please see the Extreme Networks Privacy Policy.

AI Architecture, Data, and AI Security

Extreme Platform ONE leverages AI in four ways:

- The AI core is the central intelligence layer that provides advanced AI services, automation, and security enforcement.
- A conversational front-end interface, enables users to interact with data and knowledge through natural language.
- An interactive canvas interface allows users to create insights and dashboards by using natural language.
- AI agents execute workflows and tasks based on their deployment and action scope. The default level of agency is set with a Human-In-The-Loop (HITL) configuration to help ensure that the user is always in control before actions are taken. In addition, any activity by AI is logged and done with the same access privileges and role-based access as the user who initiated it and is engaging with it.

AI Core Architecture

Extreme Platform ONE's AI core delivers a unified environment for the entire data and AI lifecycle, from data ingestion and preparation to model development, training, deployment, and monitoring as well as orchestration. It addresses the key challenges organizations face when implementing AI, including data silos, complex model management, and the need for robust governance and compliance.

It comprises three components: orchestration, services, and data hub.

The **orchestration layer** includes a set of mechanisms and tools to scale and organize the services layer, including AI services, AI agents, and AI safety guardrails.

- Safety and guardrails build trust and help ensure that AI operates safely, ethically, and reliably in the following ways:
    - Protect systems and users from malicious inputs and unreliable outputs.
    - Detect and block harmful content (e.g., violence, hate speech, self-harm).
    - Prevent prompt injection attacks and jailbreak attempts.
    - Identify and mitigate AI hallucinations to help ensure accurate and grounded outputs.
    - Monitor for copyrighted material and provide attribution for reused content.
    - Provide a centralized platform for cataloging and registering data and AI models, enabling effective monitoring, management, and auditing to help ensure data reliability and proper resource utilization.
    - Help ensure compliance with ethical and legal standards through transparency and user controls.

Services is a collection of intelligent, modular, cloud-scale services for AI and ML model serving, model inference, and training, as well as agent communication. These services include:

- A system for cataloging and registering AI and ML models, enabling effective monitoring, management, and auditing to help ensure data reliability and proper resource utilization
- An agentic system for complex workflows, multi-agent interaction, and proactive task management
- Agent communication infrastructure and lifecycle management, including versioning, change management, upgrades, quality assurance, and security
- Model management and hosting for various AI and ML models with the flexibility to integrate different types of models such as LLMs, SLMs, traditional ML models, and explainability tools tailored to diverse tasks and use cases
- Offer "Model as a Service" functionality for real-time and batch inference

A **data hub** consisting of management, governance, and ingestion pipelines is the central ecosystem for managing, processing, and governing data to improve AI performance and decision-making. The hub includes:

- Data Ingestion Service - Provides a robust data ingestion pipeline to efficiently capture and process both structured and unstructured data from diverse sources including databases, APIs, and file systems.
- Data Lake and Processing - Offers a scalable data lake for storing and managing large volumes of structured and unstructured data. Advanced data processing capabilities enable real-time and batch inference for AI models, driving timely insights and decision making.
- Knowledge management - Establishes and maintains complex relationships between data entities using a robust knowledge graph that leverages metadata and data catalog information from diverse sources (technical, operational, business, and content).
- Metadata Management - Offers a robust metadata management solution that tracks data lineage, ownership, purpose, usage, and classification. By centralizing metadata, Extreme Networks helps ensure adherence to data and AI governance requirements, enhances data reliability, and facilitates data discovery and utilization.
- RAG (Retrieval Augmented Generation) as a Service - Provides a platform for RAG that leverages a knowledge base to retrieve and incorporate relevant information into AI model inputs, improving the quality and accuracy of generated outputs.
- Auto Compliance - Provides automated auditing and monitoring capabilities to proactively identify and address potential compliance gaps, helping to ensure adherence to data privacy regulations.

Data Protection and Security

Extreme Networks has implemented a comprehensive governance framework based on the values stated below to enable the trusted and responsible use of AI and data. This framework encompasses all data operations, from ingestion to usage, and addresses the unique requirements of generative AI, agents, and LLMs. This will help ensure data quality, compliance, and ethical AI practices, ultimately driving business value and innovation.

Values

- Technology-driven (enforcement, monitoring, and auditing)
- Continuous oversight
- Responsible AI

To help ensure the accuracy and reliability of our AI models in everyday operations, Extreme has implemented a multi-faceted approach:

- Curated Data Sources: We use curated public and private data to ground our AI system. This helps ensure that the data is relevant, up-to-date, and comprehensive. For unstructured data, we use RAG retrieval augmented generation. For specific use cases, zero-shot and few-shot learning are used, as well as fine-tuning with domain-specific data and reflection techniques.
- Extensive Quality Assurance (QA): Each piece of data ingested into our system undergoes rigorous QA processes. These include validation against a set of ground-truth questions and answers to verify its accuracy and relevance.

- Continuous Monitoring and Updates: Our models are continuously monitored and updated to adapt to new data and changing conditions. This helps maintain their reliability over time and avoids drift issues.
- Feedback Loops: We incorporate feedback from users and stakeholders to identify and correct any inaccuracies, helping to ensure the models remain accurate and reliable.
- Robust Testing: Our models undergo extensive testing in various scenarios before deployment to help ensure they perform reliably under different conditions.

Extreme Networks is committed to safeguarding AI's privacy, security, and ethical use within our platform. Our data/AI governance platform automates audit and compliance. To achieve this, we implement the following measures:

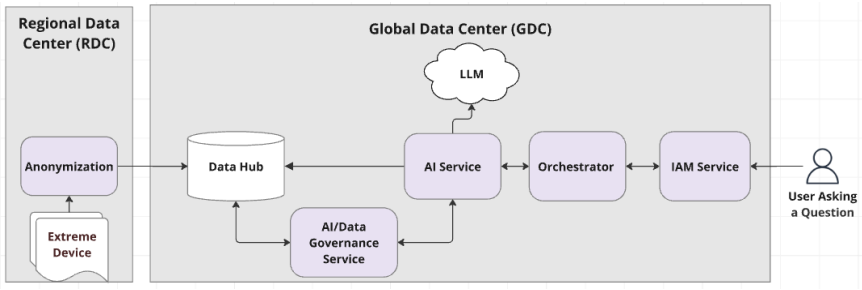
- Robust Data Encryption: We employ advanced encryption techniques to safeguard data at rest and in transit, minimizing the risk of unauthorized access.
- Secure Access Controls: We implement stringent access controls, including role-based access, policy-based access control, and multi-factor authentication, to limit access to authorized personnel.
- Regular Security Audits: We conduct regular security audits and vulnerability assessments to identify and address potential security threats.
- Compliance with Data Privacy Regulations: We adhere to relevant data privacy regulations to help ensure that data is handled responsibly and ethically. Our platform provides proactive governance and compliance capability to help ensure we protect personal data and comply with its usage.
- Data Minimization: We collect and store only the necessary data to fulfill the platform's purpose, minimizing the potential for data breaches.
- Incident Response Plan: We have a comprehensive incident response plan to address any security incidents or breaches quickly.
- Regular Security Training: We provide regular security training for our employees to raise awareness of potential threats and best practices.
- Data Retention Policies: Implement clear data retention policies to determine how long data is stored and when it should be deleted or anonymized. Queries to AI Expert and the answers delivered by AI Expert are visible only to the employee initiating the query and can only be shared explicitly by that employee.
- User Privacy Settings: Provide users with granular control over their data, allowing them to choose what data they share and how it is used. For example, queries to AI Expert and the answers delivered by AI Expert are visible only to the employee initiating the query. They can only be shared explicitly by that employee.

Our customer data is only used to train models for their solution. All personal data is anonymized for usage, and data usage meets all compliance requests, including the purpose of processing and the user privacy agreement.

Our AI models are trained on diverse and representative datasets to minimize bias and help ensure fairness. We continuously monitor and evaluate our models to identify and mitigate potential biases.

Data Flow in the AI Core

Data from all RDCs (Regional Data Center) is anonymized during the ingestion flow. Integrating an anonymization service directly within the data ingestion pipeline, before data lands in the data hub, offers significant benefits for the AI core by enhancing data privacy, regulatory compliance, and the responsible use of AI. This "shift-left" approach to anonymization streamlines data governance and empowers AI development while mitigating privacy risks. In addition, data is not moved out of the organization's region if prohibited by law.



Appendix

Data and PII Available in Extreme Platform ONE

Provider	End User Personal Data Visibility Details
Infrastructure Provider (AWS, Google, Azure)	Cloud infrastructure providers are not authorized to access/view data in Extreme Platform ONE. All access is isolated to private instances, accessible only via Extreme Networks assets and a limited set of Extreme Networks employees.
Customer Support Provider (Extreme GTAC)	No data is accessible to GTAC unless shared by the customer
DevOps/Development (Extreme Engineering)	Access to list of customer (MSP, Customers) who purchased Extreme Platform ONE
	End user device-specific data
	MAC address
	Device manufacturer (Apple, Samsung, Intel, etc...)
	Las assigned IPv4 and IPv6 address
	Hostname
	Radio attributes 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 was user 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 data (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

Availability

Uptime

The SLA for Extreme Platform ONE is provided in the Extreme Platform ONE Service Agreement:

PlatformOneTerms

Disaster Recovery (DR)

Extreme Platform ONE'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 stored within the United States for US-based data centers and within Europe for all other data centers, to address data localization 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 Extreme Platform ONE Cloud Operations for immediate action as required. It is important to note that Extreme Platform ONE 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 Extreme Platform ONE environment

Backups are retained for thirty (30) days and are duplicated. One master copy of the backup is stored within the geographic region for the RDC, and the secondary copy is stored within an alternate RDC within the same geographic region. Backups are tested at least annually in accordance with Extreme Networks' documented disaster recovery testing requirements.

Backups are stored on both local and remote servers in a compressed and encrypted format and are 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).

However, within the application, an individual backup of the customer configuration is permitted.

Customers are responsible for performing regular backups of their environment in case they need to recover a lost object due to administrative error, accident, or malicious employee actions. Backup of customer VIQ can be performed from the Extreme Platform ONE 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).

Shared Responsibility Model

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

Extreme Networks' Responsibility

Extreme Networks is responsible for:

- Maintaining operational posture of Extreme Platform ONE , 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 Extreme Platform ONE at or above the published SLA requirements
- Ensuring timely security patches and maintenance for all services and systems that make up Extreme Platform ONE
- 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's Responsibility

The subscriber (customer) using Extreme Platform ONE 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 Extreme Platform ONE
- Securing usernames and passwords and other credentials used to access Extreme Platform ONE 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 Extreme Platform ONE Cloud Terms of Service
- Timely addressing data privacy requests that you receive and addressing any requests that you have with Extreme in an expedient manner