ExtremeControl for ExtremeCloud IQ - Site Engine

Highlights

Access Security

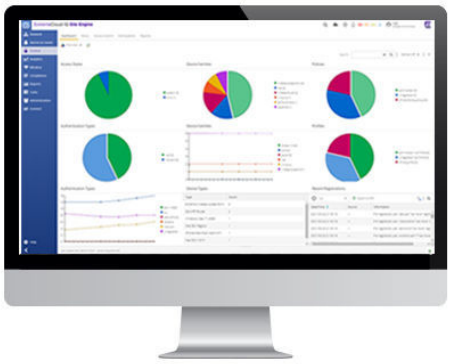
- Role-based network access control for all devices including third party networking devices
- Secure guest access and BYOD onboarding
- Integration with third party solutions such as NGFW, SIEM, CMDB, internet security and EMM/MDM
- Secure IoT network access

Operational Efficiency

- Automatic performance alerting
- Single screen for management, policies, access control, and application analytics
- Accelerated troubleshooting via separation of network from application issues

Business Aligned

- Context driven, consistent policies from edge to data center
- Network access prevention for unauthorized users and compromised endpoints
- Critical initiatives like BYOD and IoT securelyenabled



aws qualified device internet of things

Keep the network edge secure with end-point security.

With most data breaches starting at endpoints, granular control is needed over users and IoT devices and consistent policies across the entire network into multicloud. With ExtremeControl™, an application available as part of ExtremeCloud™ IQ – Site Engine1,users have centralized in-depth visibility and control over all endpoints across their network through one simple, flexible, and easy to consume dashboard.

ExtremeControl securely enables BYOD and IoT to protect the network against external threats. It provides central management and the ability to define granular policies to meet compliance obligations, locate, authenticate, and apply targeted policies to users and devices.

ExtremeControl is integrated with major enterprise platforms including solutions for network security, enterprise mobility management, analytics, cloud, and data center. In addition, it offers an open northbound API for customized integrations to key enterprise platforms.

Granular Policy Control

ExtremeControl enables the application of granular controls over users and endpoints allowed on the network. Users can enable secure BYOD, guest access and IoT by rolling out real-time policies based on the security posture of devices. ExtremeControl matches endpoints with attributes, such as user, time, location, vulnerability, or access type, to create an all-encompassing contextual identity. Role-based identities follow a user, regardless from where or how they connect to the network. They can be used to enforce highly secure access policies to prevent unauthorized users and compromised endpoints from accessing the network.

Advanced Reporting

ExtremeControl makes it easy to monitor issues on the network — all on one simple-to-read dashboard. It sends advanced, customizable reports and alerts about the authentication, guest access, onboarding, device profiles and authentication, as well as end- system health. When rolling out large projects, reduce risk by testing new policies and using passive policies for what-if-scenarios prior to enforcement. ExtremeControl identifies threats by profiling and tracking users and devices, as well as monitoring the health and compliance of devices before and after access. ExtremeControl can also accommodate policy audits provided by third party integrated MDM/EMM solutions to either ensure defined policies are working or to enforce those policies. It can also provide hit reports and the status regarding the number of non-compliant and/or decommissioned devices that have restricted network access with additional context regarding where, when, and how. ExtremeControl enables compliance auditors and security teams with the relevant data they need to make informed decisions regarding their network access policies.

Ecosystem Integration

ExtremeControl is integrated with Extreme Networks' ecosystem of partners to expand network security and threat response. For example, ExtremeControl is integrated with next-generation firewall solutions and can orchestrate endpoint isolation and remediation based on the alerts received. It shares contextual information such as users, IP address, and location for powerful policy enforcement at perimeter firewalls. Policies based on ID-IP mapping follow users. ExtremeControl also offers third-party policy support, via user-based ACLs, ensuring granular control of the entire network. To prevent the accessing of a client's network from non-compliant and un-enrolled devices the integration with existing EMM/MDM partners, such as VMware Workspace ONE UEM (Airwatch), Citrix, and MobileIron is simplified.