Extreme networks

Data Sheet

ExtremeAnalytics™ for ExtremeCloud™ IQ Site Engine

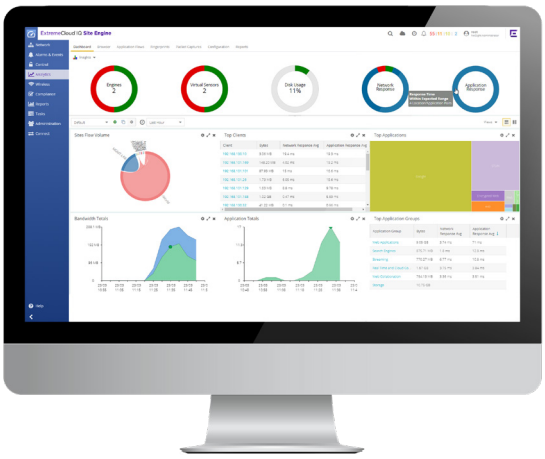
Highlights

Increase operational efficiency

- Centralized views of application traffic across different sites and multiple layers facilitate real-time analysis.
- Proactive alerting when application performance changes beyond standard deviation ensures the end-user experience.
- Real-time views into application usage, users, locations, and devices facilitate root cause analysis.
- Privacy settings can be adjusted to protect the end user's identifying information.

Enhance Network security and control

- Security forensics analyze and record suspicious traffic to helps identify suspect or unapproved applications and shadow IT.
- Integration with ExtremeControl and similar third-party products enable advanced network access control (NAC).



Application and security insights from the edge to the data center.

Consistently delivering business services requires understanding user behavior on the network, identifying the level of user engagement, and ensuring the delivery of applications for optimized quality of experience (QoE). ExtremeAnalytics™ is a component of ExtremeCloud IQ™ Site Engine and provides administrators with an easy-to-understand dashboard inventory and network topology with the ability to drill-down to a granular view of users, devices, and applications. When Site Engine is used with ExtremeAnalytics, it speeds up troubleshooting by separating network performance and application performance, so administrators can quickly identify root causes. IT operations can use ExtremeAnalytics to quickly pinpoint and address performance issues before they become apparent to end-users.

ExtremeAnalytics correlates all data collected from users, devices, and applications in a single data store. It uses deep packet inspection (DPI) to monitor application telemetry on Extreme Networks switches and ExtremeCloud IQ Controller. Administrators can analyze application flows from every part of the network without requiring dedicated probes. With accelerated troubleshooting and automatic performance alerting, staff spend less time on monitoring application performance and resolving issues. Application fingerprint techniques facilitate security forensics allowing administrators to analyze and record suspicious traffic.

The optional deployment of the Virtual Sensor allows real-time analysis in third-party environments. Integrations with Google Cloud Platform (GCP), Amazon Web Services (AWS), and Microsoft Azure allow users to obtain workload and application flow visibility into their cloud environment.

Increase Operational Efficiency

The ExtremeAnalytics component of Site Engine aggregates application telemetry across a wide variety of Extreme devices and delivers insights without the need for standalone sensors or collectors. The Analytics Engine within ExtremeAnalytics extends application visibility from edge devices through the campus, branch, and data center. Integrations into Extreme Networks' Universal Switch Platform Series, VSP series, Summit Series, ERS series, and ExtremeCloud IQ Controller provide application layer visibility and latency calculations for traffic flows. Additionally, the integration of private cloud solutions based on VMware ESXi and Microsoft Hyper-V provides a unique capability of a single analytics toolset that covers campus and data center. The optional deployment of the Virtual Sensor allows real-time analysis in third-party environments.

The Analytics Engine monitors and classifies layer 7 application information based on data from switches and reports that information to ExtremeCloud IQ Site Engine, where it is managed and displayed. Site Engine displays reports based on K-mirror technology combined with NetFlow or IPFIX that combination provides application-level traffic flows. (NetFlow or application telemetry can be enabled on the switch to allow flow collection for the device interfaces.) ExtremeAnalytics can import stream flow data from ExtremeControl and ExtremeCloud IQ Controller or export flows to third-party applications via integrations.

A real-time dashboard provides views of all applications in wired and wireless networks across locations. It correlates the performance of applications to core network services such as domain name system (DNS), Radius, and active directory (AD), so users can quickly understand whether the application or the network is at the root of the performance issue. There is also a custom dashboard that administrators can create using a drop-down list.

Network administrators can view traffic across different sites and multiple layers for real-time analysis to optimize network performance and resolve issues quickly. The Tracked Applications dashboard contains two graphs for each application, one displays the average response time over a selected time and the other displays the individual response times over that period for each site.

ExtremeAnalytics includes dynamic threshold functionality for the Network Service and Tracked Applications dashboards. It automatically measures and provides an alert when the QoE of a designated application changes beyond a standard deviation, so administrators are proactively alerted before end-users complain. IT operations teams can also track application usage to determine the return on investment (ROI) associated with application deployments. Three collection privacy level settings allow for the restriction of identifying information collected by the ExtremeAnalytics engine. Increasing the privacy level protects the end user's identifying information from being viewed by IT staff.

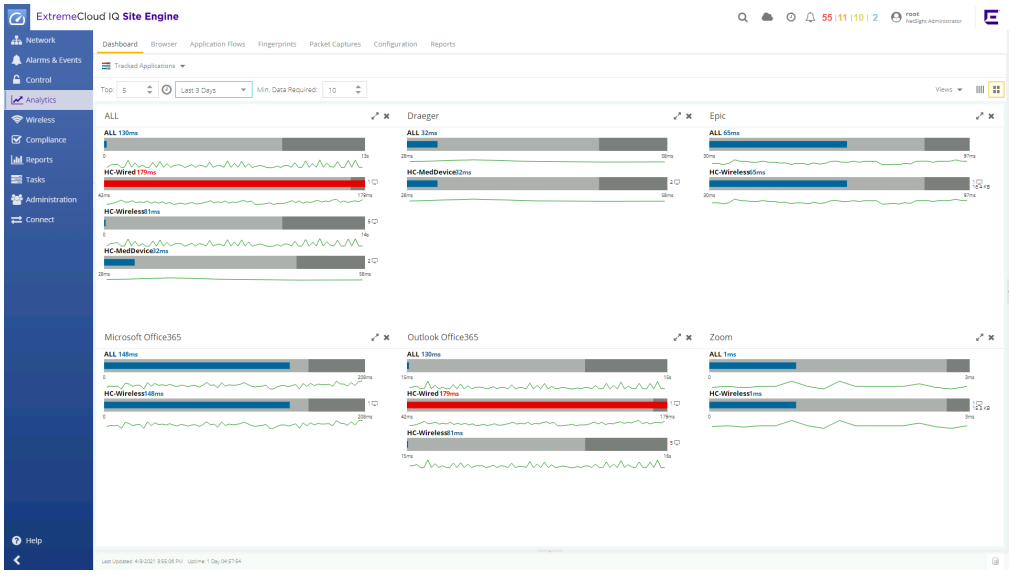


Figure 1: Tracked Applications Dashboard

Network Security and Control

This capability combines flow-based technology with a rich set of application fingerprint techniques. A fingerprint is a description of a pattern of network traffic which can be used to identify an application. ExtremeAnalytics can identify over 8,000 applications and includes more than 10,000 behavioral detection-based fingerprints. It can detect and measure on-premises apps (such as SAP, SOA traffic, SQL), software as-a-services (SaaS) and cloud apps (such as Salesforce, Office360, file sharing), and social media apps (such as Facebook, LinkedIn, X) to optimize the QoE. New and updated fingerprints are provided via a fingerprint update website.

The Fingerprints feature provides detailed information about the patterns used by ExtremeAnalytics to identify application flows. Administrators can choose to view in-use and customized fingerprint data. ExtremeAnalytics provides security forensics by allowing administrators to analyze and record suspicious traffic. It monitors unusual traffic, so it can identify shadow IT, report malicious or unwanted applications, and helps with security compliance.

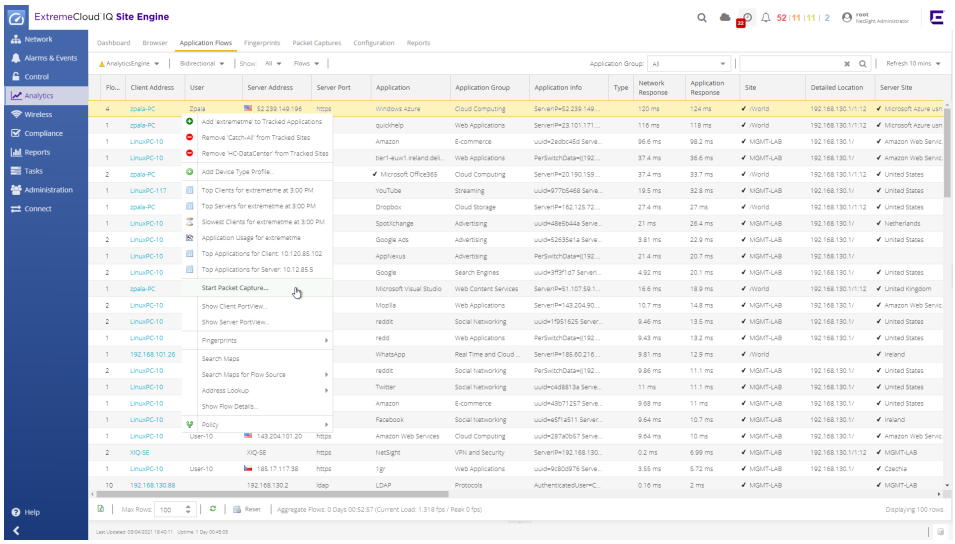


Figure 2: Application Flow Details

ExtremeAnalytics is a component of ExtremeCloud IQ Site Engine, and both applications are included in the ExtremeCloud IQ Pilot license. It works closely with ExtremeControl for Site Engine, an application of the ExtremeCloud IQ suite that is licensed separately, to provide network access control. ExtremeControl data can be integrated with flow data to provide additional insights on end user devices and systems. ExtremeAnalytics is integrated with ExtremeCloud IQ controller, Extreme's on-site wireless controller to manage wireless APs. It also offers integration into select third-party NAC tools, such as Aruba ClearPass and Wireless IPFIX.

Product Specifications

Virtual Appliances

The ExtremeAnalytics virtual engines must be deployed on a VMWare or Hyper-V server with a disk format of VHDX. The VMWare Management Center virtual engines are packaged in the .OVA file format (defined by VMware). The Hyper-V Management Center virtual engines are packaged in the .ZIP file format.

Refer to the Release Notes for information on Virtual Appliance scalability.

Services and Support

Extreme Networks provides comprehensive service offerings that range from Professional Services to design, deploy, and optimize customer networks, to customized technical training, to service and support tailored to individual customer needs. Please contact your Extreme account executive for more information about Extreme Service and Support.

Ordering Information

ModelNumber	Model Description
XIQ-PIL-S-C-EW	ExtremeCloud IQ Pilot SaaS Subscription and ExtremeWorks SaaS Support for one (1) device (one year)
XIQ-PIL-S-C-PWP	ExtremeCloud IQ Pilot SaaS Subscription and PartnerWorks Plus SaaS Support for one (1) device (one year)

Extreme networks

http://www.extremenetworks.com/contact