

Highlights

Keep Your Network Secure

- Improve network security through deep visibility into unapproved applications, unusual traffic, and shadow IT
- Know who, where and what is using your network with actionable insights to keep your network secure
- Easy to use, always-on security forensics through centralized packet capture at any point of the network

Business Insights from the Edge to the Data Center

- Get actionable business insights into your application usage, users, locations, and devices across campus, DC, and cloud environments
- Monitor and optimize application performance for an exceptional end-user experience
- Gain insights from analytics that don't slow down your network with highly scalable transport layer independent application detection and decoding
- Real-time view into application flows across all types of users, IoT devices, and virtual machines.

Increase Operational Efficiency

- Avoid business disruptions through proactive monitoring of application performance
- Simple tool for level 1 and level 2 IT staff to quickly diagnose network or application issues
- Single pane of glass for management, policies, access control, and analytics that reduces the need for staff specialization



ExtremeAnalytics™

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

Keep your network secure through granular visibility and analytics into your applications and network from the edge to the data center. With integration into our VSP and SLX platforms you get application layer visibility and latency calculations for traffic flows all the way into the data center.

For context-based visibility into everything that's going on with your network we correlate all data collected from users, devices, and applications in a single data store. Application telemetry on ExtremeSwitching, and our wireless access points (APs) allows you to analyze application flows from every part of the network without requiring dedicated probes.

Our Virtual Sensor offers you real-time analytics across your VMWare based virtual environments. Our integrations with Google Cloud Platform (GCP), Amazon Web Services (AWS) and Microsoft Azure allow you to obtain workload and application flow visibility into your cloud environment.

With ExtremeAnalytics, you can better understand user behavior on the network, identify the level of user engagement, and assure business application delivery for optimized quality of experience. Track application usage to determine the return on investment associated with application deployments. When performance issues come up, you can pinpoint them quickly, and fix them before they become apparent to end-users. With accelerated troubleshooting and automatic performance alerting you can spend less time on monitoring application performance and focus IT time and resources on strategic business initiatives.

Eliminate Virtualization Blindspots and Monitor Application Flows to the Multicloud

Get visibility and analytics extended to virtual environments with our Virtual Sensor that can be easily deployed as a virtual appliance with support for vSphere Hypervisor. It gives you actionable business insights into your virtual applications, monitors and optimizes virtual workloads, and by revealing shadow IT and unapproved virtual applications increases your network security. In addition, this granular visibility enables you to speedily troubleshoot virtual application issues.

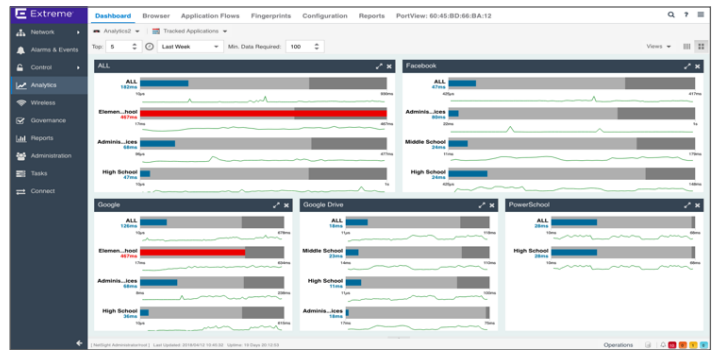


Figure 3: Actionable Application Insights

Analyze Data Traffic Across Different Sites

ExtremeAnalytics enables you to see and analyze the traffic across your entire organization with Geo Location. It provides a geo map that gives visibility into the data traffic going between different sites. It answers questions on how the network is performing across all the sites, or who are the users. It sends automatic alerts when an application slows down, helps identify root causes, and shows what users are impacted. In addition, you can see who the users of each site are and detect any anomalies that might point to a cyber attack.

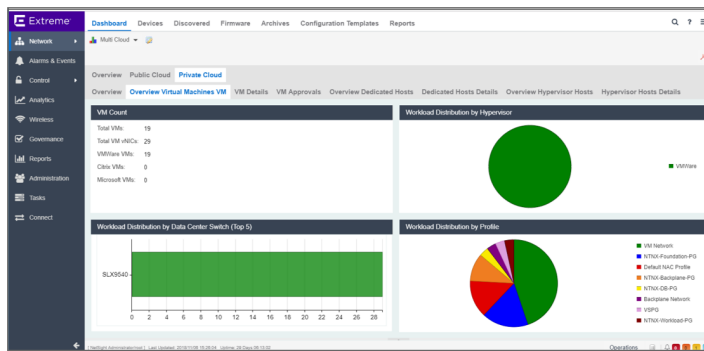


Figure 1: Visibility into VMs

Full view of application flows between VMs and to cloud instances (AWS, GCP, Microsoft Azure) helps you improve security. With integrated packet capture you can capture data packets with one mouse click from a centralized console for any site. This lets you analyze suspicious data packets for forensics.

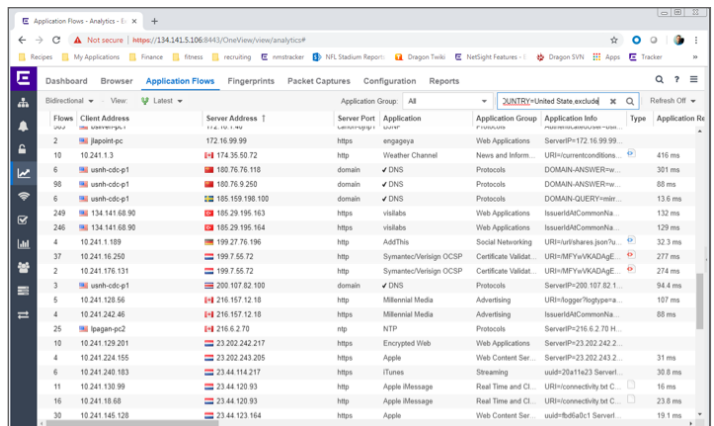


Figure 4: Granular Application Flow Visibility

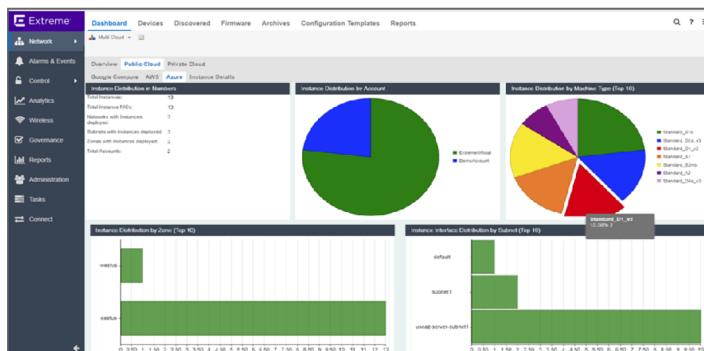
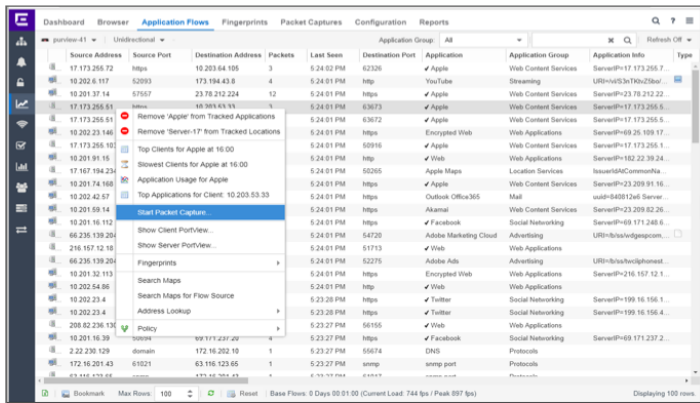


Figure 2: View of Flows to Cloud Instances

Analyze and Record Suspicious Traffic for Security Forensics

Smart Packet Capture lets you capture data packets with a click of the mouse from a centralized console for any site. You can analyze data packets that look suspicious even when they exist for only a short time to keep your network secure.



Source Address	Source Port	Destination Address	Packets	Last Seen	Application	Application Group	Application Info	Type	
17.173.255.92	https	10.202.54.106	3	5:24:02 PM	Apple	Web Content Services	Server#P17.173.255.7		
10.202.4.117	52093	173.194.43.8	4	5:24:01 PM	http	YouTube	Streaming	URL#H4S5C1K9u2Dba	
10.201.37.14	57557	23.78.212.224	12	5:24:01 PM	https	Apple	Web Content Services	Server#P23.78.212.22	
17.173.255.91		68.96.64.33		5:24:01 PM	Apple	Web Content Services	Server#P17.173.255.5		
17.173.255.91				5:24:01 PM	Apple	Web Content Services	Server#P17.173.255.5		
10.202.23.148				5:24:01 PM	https	Encrypted Web	Server#H48.26.109.17		
17.173.255.91				5:24:01 PM	Apple	Web Content Services	Server#P17.173.255.1		
10.201.91.15				5:24:01 PM	http	Web	Web Applications	Server#P182.22.39.24	
17.167.184.23				5:24:01 PM	Apple Maps	Location Services	Server#P17.167.184.23		
10.201.74.168				5:24:01 PM	https	Apple	Web Content Services	Server#P23.209.91.16	
10.202.42.87				5:24:01 PM	https	Outlook Office365	Mail	code#4001204	
10.201.63.14				5:24:01 PM	https	Akamai	Web Content Services	Server#P182.22.39.24	
10.201.16.112				5:24:01 PM	https	Facebook	Social Networking	Server#H69.171.248.6	
66.235.139.204				5:24:01 PM	Adobe Marketing Cloud	Advertising	URL#H3aVdgesoom		
246.167.12.10				5:24:01 PM	Web	Web Applications	Server#P23.209.91.16		
66.235.139.204				5:24:01 PM	https	Adobe Ads	Advertising	URL#H3aVdgesoom	
10.201.32.113				5:24:01 PM	https	Encrypted Web	Web Applications	Server#P216.157.12.1	
10.202.54.86				5:24:01 PM	http	Web	Web Applications	Server#P199.16.156.1	
10.202.23.4				5:23:28 PM	https	Twitter	Social Networking	Server#P199.16.156.4	
208.82.234.13				5:23:27 PM	https	Web	Web Applications	Server#P199.16.156.4	
10.201.16.39				5:23:27 PM	https	Facebook	Social Networking	Server#H69.171.237.2	
2.22.239.129	domain	172.16.202.10	1	5:23:27 PM	55874	DNS	Protocols		
172.16.201.43	61021	63.116.123.65	1	5:23:27 PM	smp	smp part	Protocols		

Figure 5: Smart Packet Capture

Troubleshoot and Visualize All Wireless Clients with Our Intuitive Event Analyzer

An employee walks into her office in the morning and pulls out her cell phone. She automatically connects to the nearest AP. After lunch she walks up to the second floor of the office building for a meeting, where her phone connects automatically to a different AP.

While staff moves around their offices, monitoring users' quality of experience and troubleshooting can be challenging for IT, especially given the large number of events generated by disparate systems. Extreme's Wireless Event Analyzer makes it efficient to track down issues related to wireless client roaming, AP RF load, or client stickiness with an AP.

Rich Contextual Data

ExtremeAnalytics combines flow-based technology with a rich set of application fingerprint techniques to detect and measure on-prem applications (SAP, SOA traffic, Exchange, SQL, etc.), public cloud applications (Salesforce, Google, email, YouTube, P2P, file sharing, etc.), and social media

applications (Facebook, Twitter, etc.). This set of contextual data provides a full understanding of the applications running on the network, who's using the application, the devices being used, and where they are located within the network. ExtremeAnalytics works closely with our [ExtremeControl](#) that provides visibility and control of wired and wireless devices, IoT devices and corporate/guest users. Information such as user, role, device type, and location are integrated with the application flows. ExtremeAnalytics also offers integration into select third party equipment, such as Aruba Clearpass and Wireless IPFIX. Application telemetry across a wide variety of Extreme infrastructure analytics delivers insights without the need for standalone sensors or collectors. This set of contextual data provides a full understanding of the applications.

Application Fingerprinting

ExtremeAnalytics can identify more than 2,300 applications and includes more than 10,000 behavioral detection-based fingerprints to ensure that even applications that attempt to conceal themselves, such as P2P, are detected appropriately. Through its robust fingerprinting technology, our solution is able to identify an application regardless of whether they run on well-known ports or use non-standard ports. The application fingerprints are regularly updated by us and available to you without code updates.

ExtremeAnalytics fingerprints and application groups are open and customizable allowing our customers, partners, and professional services teams to create new fingerprints and application groups to handle custom applications, specific reporting requirements and other needs. For example, many government organizations run custom applications that they do not wish to share fingerprint information for. With the customization capabilities, they are able to measure and control the quality of experience for these applications.

Manage End User Quality of Experience in One Simple View

A real-time dashboard gives you a view of all applications across locations and your wired and wireless network. We automatically measure and alert when the quality of experience of a designated application changes beyond standard deviation. We correlate the performance of applications to core network services such as DNS, Radius, and AD, so you can quickly understand whether the application or the network is at the root of the performance issue. With the application performance dashboard, you are proactively alerted about potential quality of experience issues before your end-user complain.

Appliance Options

Hardware Appliance

Our ExtremeAnalytics appliance is a rack-mountable server with all capabilities pre-installed. Purchased applications (licensed separately) are activated via license keys: The ExtremeAnalytics Appliance PV-A-305, manages up to 1.3M flows per minute (FPM)

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 appliance scalability number.

Hardware Appliance Specifications

Product Name	PV-A-305 (88100)
Appliance Specifications	
Storage	960GB Enterprise SSd
RAID Configuration	N/A
Networking	2 x 1GbE
Graphic Ports	Front VGA, Rear VGA
Serial	RJ45
USB	2 x Front, 3 x Rear
TPM Version 2.0	Yes
Appliance Scale Number	Up to 1.3M Flow per minute
Power Specifications	
Power	750W 80+ Platinum Hot Pluggable
Power Supply Type	AC Redundant
AC Input Voltage	90Hz to 132V and 180V to 264V
AC Input Frequency	47Hz to 63Hz
Physical	
Rackmount	1U Rack
Dimensions (WxDxH)	16.93" x 27.95" x 1.72"
Weight	29 lb. (13.15 kg) Max
Environmental	
Operating	ASHRAE Class A2 - Continuous Operation. 10° C to 35° C (50° F to 95° F) with the maximum rate of change not to exceed 10°C per hour
	ASHRAE Class A3 - Includes operation up to 40C for up to 900 hrs per year.
	ASHRAE Class A4 - Includes operation up to 45C for up to 90 hrs per year.
Shipping	-40° C to 70° C (-40° F to 158° F)
Humidity (Shipping)	50% to 90%, non-condensing with a maximum wet bulb of 28° C (at temperatures from 25° C to 35° C)
Vibration (Unpackaged)	5 Hz to 500 Hz 2.20 g RMS random
Warranty	
Hardware	1 year parts and Labor

Ordering Information

Part Number	Description
ExtremeAnalytics Client Count Licenses**	
88201	ExtremeAnalytics 1K Client License
88202	ExtremeAnalytics 3K Client License
88203	ExtremeAnalytics 12K Client License
ExtremeAnalytics* Flow Licenses	
PV-FPM-100K	Purview License - Visibility for 100K Flows/Minute
PV-FPM-500K	Purview License - Visibility for 500K Flows/Minute
PV-FPM-1M	Purview License - Visibility for 1M Flows/Minute
PV-FPM-3M	Purview License - Visibility for 3M Flows/Minute
ExtremeAnalytics Application Sensor	
PV-FC-180	Purview Application Sensor - 4 ports 10GBASE-X via SFP+, front to back cooling (Power Supplies not Included - please order separately)
PV-FC-180-G	TAA Purview Application Sensor - 4 ports 10GBASE-X via SFP+, front to back cooling (includes 2 SSA-FB-AC-PS-B)
SSA-FB-AC-PS-B	AC power supply, 15A, 100-240VAC input, I/O
ExtremeAnalytics Virtual Sensor	
88211	EA Virtual Sensor VS100, 10 Instance Licenses
88212	EA Virtual Sensor VS250, 10 Instance Lic
ExtremeAnalytics Appliance	
88100	ExtremeAnalytics PV-A-305 Appliance - up to 1.3M Flows per minute (FPM)
ExtremeAnalytics Systems	
PV-V-50K-SYS-2	Purview 50K flow system with virtual engine includes: NMS-ADV-5, 50K FPM flow license, PV-FC-180, (3) MGBIC-02, (2) SSA-FB-AC-PS-B
PV-50K-SYS-2	Purview 50K flow system with hardware engine includes: NMS-ADV-5, 50K FPM flow license, PV-A-305, PV-FC-180, (3) MGBIC-02, (2) SSA-FB-AC-PS-B
ExtremeAnalytics Per-User Subscription Pricing	
97208-27001	ExtremeControl + ExtremeAnalytics subscription per-user subscription pricing. Includes unlimited number of end-system licenses, priced per user per year.

***Note:** ExtremeAnalytics was formerly known as Purview.

****Note:** Client = Laptops, mobile devices, IoT devices, etc.

Warranty

As a customer-centric company, Extreme is committed to providing quality products and solutions. In the event that one of our products fails due to a defect, we have developed a comprehensive warranty that protects you and provides a simple way to get your product repaired or media replaced as soon as possible.

The ExtremeAnalytics appliance comes with a one year warranty against manufacturing defects. Software warranties are ninety (90) days and cover defects in media only. For full warranty terms and conditions please go to:

[Extreme Networks Product Warranty.](#)

Service and Support

Extreme Networks provides comprehensive service offerings that range from Professional Services to design, deploy and optimize customer networks, 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.



<http://www.extremenetworks.com/contact>

©2019 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. 6553-0719-23