# How to Turn Your Hospital's Network into a Strategic Business Asset with ExtremeAnalytics™

eBOOK

Extreme®
Connect Beyond the Network


## TABLE OF CONTENTS



# Chapter 1

## WHAT IS EXTREMEANALYTICS AND HOW CAN IT BE USED?

ExtremeAnalytics is a network-based business intelligence solution that captures and analyzes context-based application traffic to deliver meaningful intelligence about applications, users, locations and devices – providing hospital IT with the context to make faster and more effective decisions.

Many times, as hospital IT departments get ready to create new solutions, they need to choose between various platforms. They think they know the right answer and move ahead with a solution only to find out they made wrong assumptions. Other times, a hospital may schedule a change control outage based on feedback a specific department, such as surgery that says they don't need the systems after 8pm, then learn that the ICU uses the same systems 24/7. Only by having the right data and the ability to easily check can the hospital IT be certain to make the right decisions.

ExtremeAnalytics enables the mining of network-based clinical events and strategic information to help hospital leaders answer questions such as:

- Which apps go to which users? Are the right users taking advantage of our application investments?
- What medical devices are operating on the WLAN? Are we at risk for a compliance violation?
- What platforms are being used? Are clinicians using more workstations on wheels, tablets, or smart phones?
- Do I have a problem with Shadow IT on my network? Are employees using their own devices to access EPR data and potentially compromising security?
- Do you struggle with Information Governance? Do you have a real-time way to map applications to locations to end user?

With the right answers to these questions, hospital IT is empowered to turn the network into a strategic business asset that can now provide information insight to other lines of the hospital.

In this eBook, we will demonstrate specific use cases for how ExtremeAnalytics can be used by hospital departments to:

- Right size your wired and wireless network each and every application and the end-users they support
- Enhance security for based on roles, device, location and application
- Aggregate data for audit and business analytics across your enterprise.

ExtremeAnalytics can be used to help staff and executives to solve the information issues they face on a daily basis. In this eBook, you will find practical examples of how ExtremeAnalytics can be used to solve these real healthcare issues:

- **Perform Data Center Application Analysis –** decide if it makes sense to move an application to another location or to the cloud
- **See What Applications Are Slow –** In two mouse clicks see what applications for a particular user, group, location or device type aren't performing well
- **Troubleshoot Network Issues –** determine where the problem is, and whether it is a network problem, client, server or storage problem
- **Detect Malicious Applications –** see what applications people are using on your network and find applications running that you don't support
- **Find Shadow It or Unapproved Devices on the Network –** discover what applications might have been ordered from other "Rogue IT" departments
- **Support Medical Device Compliance** - Ensure network policies for medical devices are enforced
- **Ensure The Adoption of Applications –** determine how effective you are when it comes to deploying new applications
- **Help With License Visibility and Compliance Auditing –** ensure adoption of licensed software and that you aren't running software without licenses

**LET EXTREMEANALYTICS MAKE THE UNKNOWN BECOME KNOWN TO YOU.**

# Chapter 2

## USING EXTREMEANALYTICS FOR BUSINESS ANALYTICS

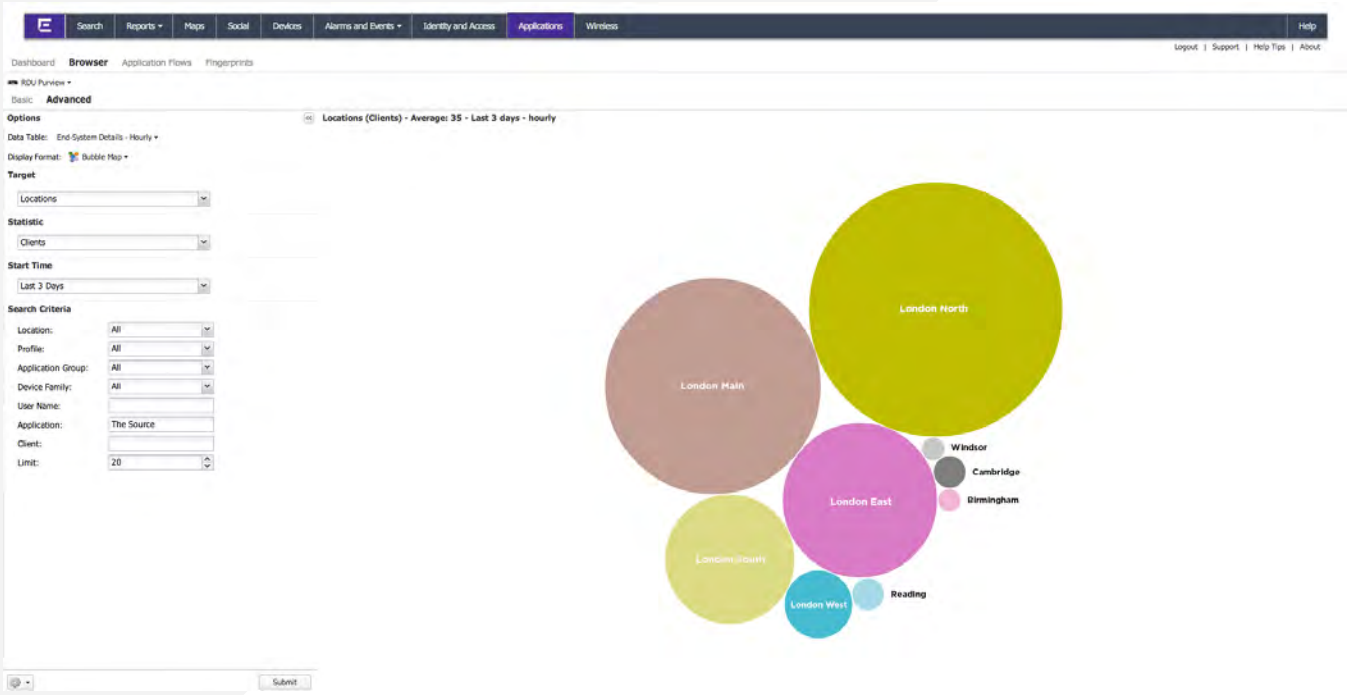
ExtremeAnalytics' capabilities make the unknown – known by being able to measure what you need to manage and transforming seemingly unrelated and detailed information into meaningful, business-focused intelligence. This enables hospitals to apply analytics to understand clinician's interactions with IT services, have visibility into reality vs perceptions, and make evidence based IT service decisions to improve patient outcomes and experiences.

With ExtremeAnalytics, a hospital is able to understand the adoption and usage of applications to ensure that investments are being maximized. What if you could have access to information about application usage by device type and the workflow of users – where they go first, what devices are connected, what applications they use, what websites they visit and at what times of the day.... Would this help you make better informed decisions? ExtremeAnalytics can even come to the rescue of hospitals faced with a software or medical device audit, by helping them to ensure that they aren't running software they aren't licensed for.

## USE CASE #1 — USING EXTREMEANALYTICS TO ENSURE THE ADOPTION OF APPLICATIONS

**What if you could** determine your ROI post implementation? ExtremeAnalytics is a great tool to help determine how effective you are when it comes to deploying new applications. Many times a hospital's IT departments assume that since they have announced that the application is available, or have installed the software on every machine, that they are done and the project is closed. This is hardly ever the case. It takes a lot of work to ensure that new applications get adopted and fully-leveraged by the hospital staff.

In this example, a hospital recently deployed a new Intranet application called “The Source”, and they are trying to get all the clinicans to use it. Using ExtremeAnalytics, it is easy to view all locations by clients to see how many people are using it. This can be viewed as a bubble map:

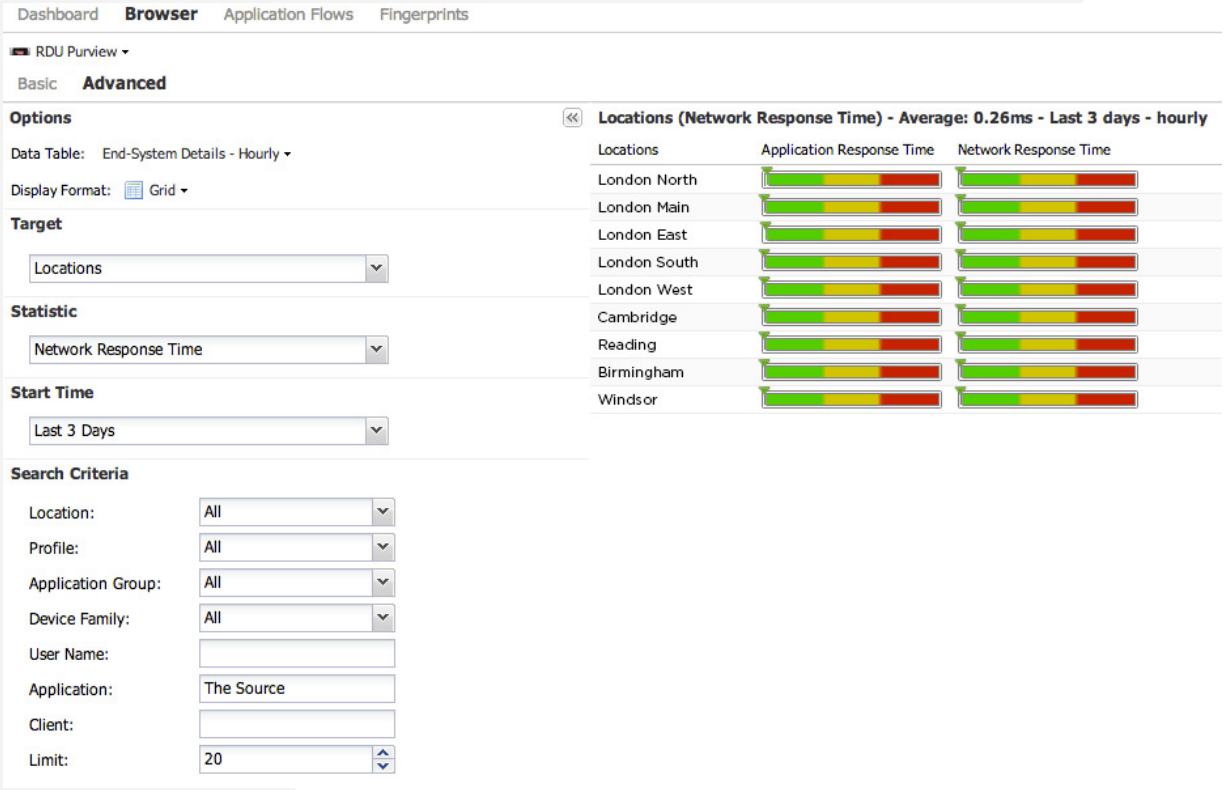



It can also be viewed as a grid with the actual numbers:

| LOCATIONS (CLIENTS) AVERAGE: 35 — LAST 3 DAYS — HOURLY | |
|---|---|
| **LOCATIONS** | **CLIENTS** |
| **London North** | 127 |
| **London Main** | 92 |
| **London East** | 47 |
| **London South** | 33 |
| **London West** | 9 |
| **Cambridge** | 2 |
| **Reading** | 2 |
| **Birmingham** | 1 |
| **Windsor** | 1 |

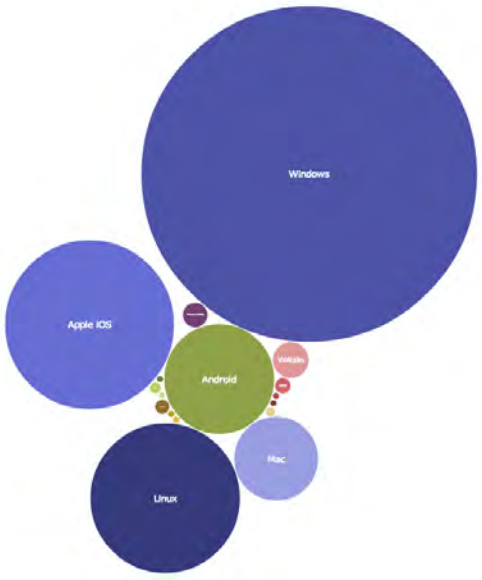
It is clear to see that the application is pretty well used in Hospital A and Clinic B, but in order to increase application adoption at some of the other sites; they may need to receive either a reminder or customized training.

By easily changing the statistic from clients to “network response time,” you can check to make sure performance is good from these other sites. In this case, you see that everyone is having good network performance.




If this graph indicated poor performance, you could look at ways to optimize the traffic to make it perform better, replicate to a local copy or upgrade the links.

If you were dealing with a mobile application, it might make sense to get the same sort of view, except broken out by device type. This can help to ensure that you are building tools for the right device for your organization. The last thing you want to do is spend a lot of time building and optimizing an app for Android, only to find out that the majority of clinicians are using iOS.

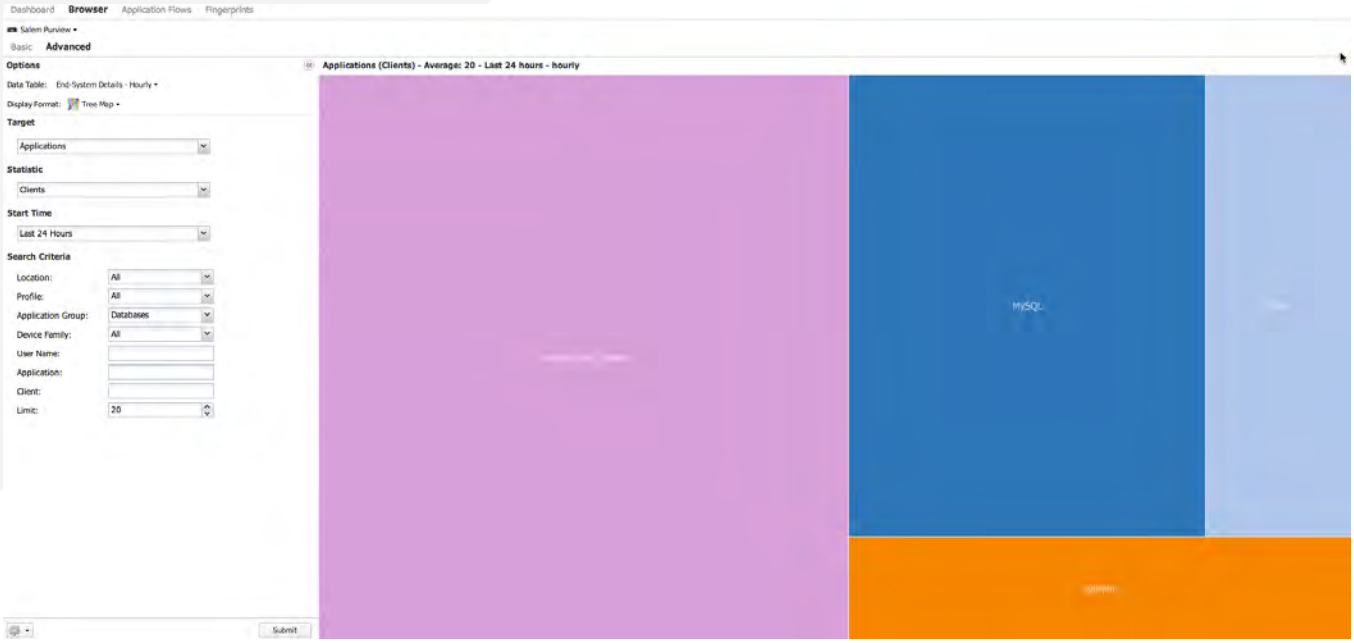



As you can see, it's easy to research how well your new solutions are being adopted when you have access to the right, accurate data.

## USE CASE #2 — USING EXTREMEANALYTICS TO HELP WITH LICENSE AWARENESS

At some point, your hospital could be subject to a software licensing audit. These audits could be driven by internal entities such as the CFO, or by external entities such as the software vendors. An internal audit might be driven based on budgeting and procurement of new software. Your CFO might ask a simple question: "Before I buy more licenses, I want context of who's using currently licensed software, from what locations and on what devices?" This type of internal audit is one realm of consideration where ExtremeAnalytics illuminates insight to help guide your business direction. An external audit, on the other hand, can cost thousands or even millions of dollars if you are using illegal software – even if you don't know you are. ExtremeAnalytics provides the context and awareness of who's using licensed software and help you ensure that licensed software is being used in your business.

For example, you may notice in the tree map view below that somewhere there are users connecting to various databases, including TNS (which is an Oracle® database service).




If you run Oracle ERP, or other Database applications that license Oracle, then it's probably no cause for concern. If you aren't aware of any Oracle purchases, you might want to investigate. This can be done by simply right-clicking on the TNS link and saying, "All Application flows for TNS". This will open up the image on the next page.

Dashboard | Browser | Application Flows | Fingerprints | **Application Flows: TNS**

| Flows | Client Address | Server Address | Server Port | Application | Application Group | Application Info |
|---|---|---|---|---|---|---|
| 2 | | | epmap | TNS | Databases | ServerOS=Windows 7 Serve... |
| 2 | | | microsoft-ds | TNS | Databases | ServerOS=Windows 7 Serve... |
| 2 | | | epmap | TNS | Databases | ServerOS=Linux 2.2.x-3.x (n... |
| 2 | | | microsoft-ds | TNS | Databases | ServerOS=Linux 2.2.x-3.x (n... |
| 2 | | 134.141.69.178 | netbios-ssn | TNS | Databases | ServerOS=Windows 7 Serve... |
| 2 | | 134.141.69.178 | microsoft-ds | TNS | Databases | ServerOS=Windows 7 Serve... |
| 2 | | | epmap | TNS | Databases | ServerOS=Linux 2.2.x-3.x (n... |
| 2 | | | microsoft-ds | TNS | Databases | ServerOS=Linux 2.2.x-3.x (n... |
| 2 | | | epmap | TNS | Databases | ServerOS=Windows 8 Serve... |
| 2 | | 10.6.83.159 | epmap | TNS | Databases | ServerOS=Windows 7 Serve... |
| 2 | | 10.6.83.159 | microsoft-ds | TNS | Databases | ServerOS=Windows 7 Serve... |
| 2 | | | microsoft-ds | TNS | Databases | ServerOS=Windows 8 Serve... |
| 70 | | 10.6.24.45 | cichild-lm | TNS | Databases | ServerIP=10.6.24.45 FlowR... |
| 288 | | 10.6.25.35 | 1753 | TNS | Databases | uuid-One_Direction=63742... |
| 2 | | | epmap | TNS | Databases | ServerOS=Windows 8 Serve... |
| 2 | | | microsoft-ds | TNS | Databases | ServerOS=Windows 8 Serve... |
| 2 | | | epmap | TNS | Databases | ServerOS=Linux 2.2.x-3.x (n... |
| 2 | | | microsoft-ds | TNS | Databases | ServerOS=Linux 2.2.x-3.x (n... |
| 2 | | | epmap | TNS | Databases | ServerOS=Linux 2.2.x-3.x (n... |
| 2 | | | microsoft-ds | TNS | Databases | ServerOS=Linux 2.2.x-3.x (n... |
| 83 | | 10.6.24.37 | ms-streaming | TNS | Databases | ServerIP=10.6.24.37 FlowR... |
| 2 | | | epmap | TNS | Databases | ServerOS=Linux 2.2.x-3.x (n... |
| 2 | | | microsoft-ds | TNS | Databases | ServerOS=Linux 2.2.x-3.x (n... |
| 2 | | | epmap | TNS | Databases | ServerOS=Windows 8 Serve... |
| 2 | | | microsoft-ds | TNS | Databases | ServerOS=Windows 8 Serve... |
| 2 | | | epmap | TNS | Databases | ServerOS=Linux 2.2.x-3.x (n... |
| 2 | | | microsoft-ds | TNS | Databases | ServerOS=Linux 2.2.x-3.x (n... |
| 2 | | 10.6.83.156 | epmap | TNS | Databases | ServerOS=Windows 7 Serve... |
| 2 | | 10.6.83.156 | microsoft-ds | TNS | Databases | ServerOS=Windows 7 Serve... |
| 2 | | | epmap | TNS | Databases | ServerOS=Windows 8 Serve... |
| 2 | | | microsoft-ds | TNS | Databases | ServerOS=Windows 8 Serve... |
| 2 | | | epmap | TNS | Databases | ServerOS=Windows 7 Serve... |
| 2 | | | microsoft-ds | TNS | Databases | ServerOS=Windows 7 Serve... |
| 2 | | 134.141.97.151 | epmap | TNS | Databases | ServerOS=Windows 8 Serve... |
| 2 | | 134.141.97.151 | microsoft-ds | TNS | Databases | ServerOS=Windows 8 Serve... |
| 2 | | | epmap | TNS | Databases | ServerOS=Linux 2.2.x-3.x (n... |
| 2 | | | microsoft-ds | TNS | Databases | ServerOS=Linux 2.2.x-3.x (n... |
| 2 | | | epmap | TNS | Databases | ServerOS=Linux 2.2.x-3.x (n... |
| 2 | | | microsoft-ds | TNS | Databases | ServerOS=Linux 2.2.x-3.x (n... |

You can go into the flow view and see all the servers and clients using the software and begin to determine if a particular group is using this software. It's possible that they have purchased a legal copy without IT's knowledge.

Even if you did knowingly buy Oracle, or other software, you need to make sure that it hasn't been installed multiple times, which could violate the terms of your software license agreement. Since some software is licensed by number of users, and others are licensed by number of servers, ExtremeAnalytics allows you to see the number of clients. In the flow data tab, you can see the number of servers as well. You can sort the list of flows by "Server Address," which will allow you to see how many servers are actually in use. You will also need to verify the number of processors on the individual servers once you identify them.

Dashboard | Browser | Application Flows | Fingerprints | **Application Flows: TNS**

| Flows | Client Address | Server Address ▲ | Server Port | Application |
|---|---|---|---|---|
| 2 | [redacted] | 10.254.82.29 | netbios-ssn | TNS |
| 2 | [redacted] | 10.254.82.29 | microsoft-ds | TNS |
| 2 | [redacted] | 10.254.82.29 | epmap | TNS |
| 2 | [redacted] | 10.254.82.30 | epmap | TNS |
| 2 | [redacted] | 10.254.82.30 | microsoft-ds | TNS |
| 2 | [redacted] | 10.254.82.31 | epmap | TNS |
| 2 | [redacted] | 10.254.82.31 | netbios-ssn | TNS |
| 2 | [redacted] | 10.254.82.31 | microsoft-ds | TNS |
| 2 | [redacted] | 10.254.82.32 | epmap | TNS |
| 2 | [redacted] | 10.254.82.32 | microsoft-ds | TNS |
| 2 | [redacted] | 10.254.82.33 | epmap | TNS |
| 2 | [redacted] | 10.254.82.33 | netbios-ssn | TNS |
| 2 | [redacted] | 10.254.82.33 | microsoft-ds | TNS |
| 2 | [redacted] | 10.254.82.34 | epmap | TNS |
| 2 | [redacted] | 10.254.82.34 | microsoft-ds | TNS |
| 2 | [redacted] | 10.254.82.35 | epmap | TNS |
| 2 | [redacted] | 10.254.82.35 | microsoft-ds | TNS |
| 2 | [redacted] | 10.254.82.36 | microsoft-ds | TNS |
| 2 | [redacted] | 10.254.82.36 | netbios-ssn | TNS |
| 2 | [redacted] | 10.254.82.36 | epmap | TNS |
| 2 | [redacted] | 10.254.82.37 | microsoft-ds | TNS |
| 2 | [redacted] | 10.254.82.37 | epmap | TNS |
| 83 | [redacted] | 10.6.24.37 | ms-streaming | TNS |
| 70 | [redacted] | 10.6.24.45 | cichild-lm | TNS |
| 48 | [redacted] | 10.6.24.45 | cichild-lm | TNS |
| 288 | [redacted] | 10.6.25.35 | 1753 | TNS |

Additionally, ExtremeAnalytics, when carefully and accurately deployed, can check all the machines running on your network for software usage, including lab machines, rogue servers and clients. Remember that even though the machine may not be managed by the hospital, the hospital can still be liable for illegal software running on it.

# Chapter 3

## USING EXTREMEANALYTICS TO OPTIMIZE NETWORK MANAGEMENT… DON'T THROW MORE GOOD BANDWIDTH AFTER BAD APPLICATION PERFORMANCE

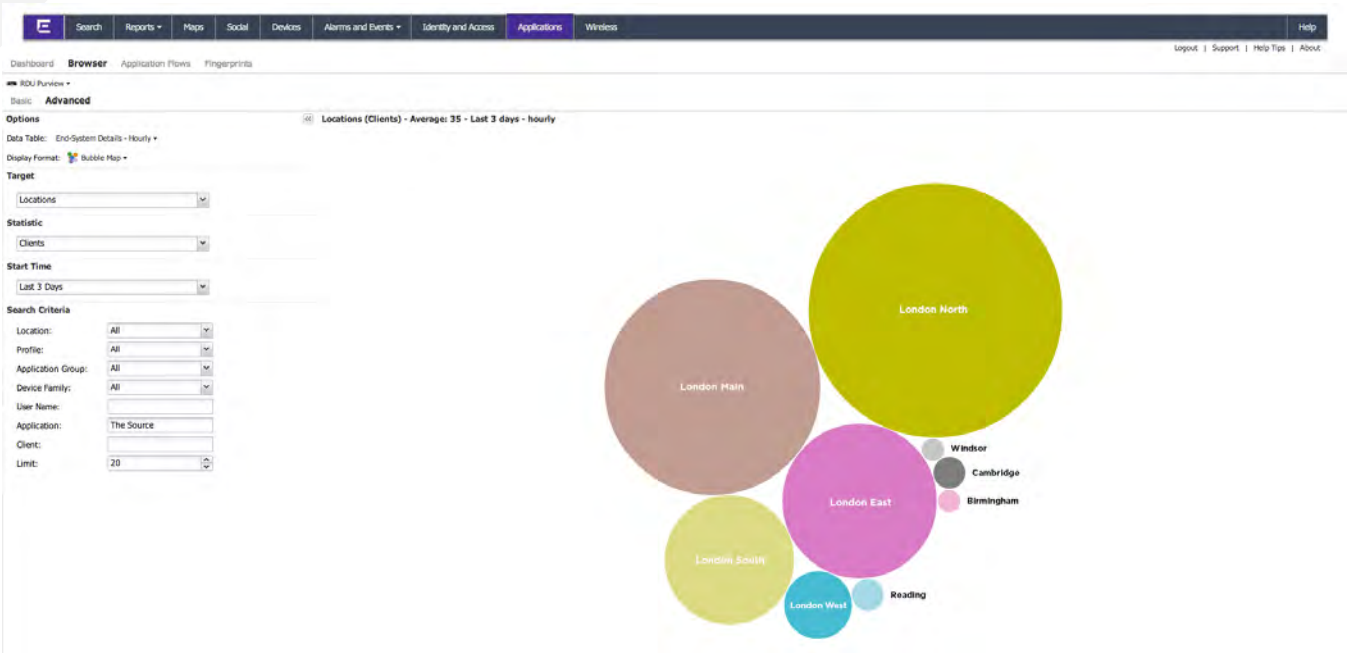
ExtremeAnalytics can be used to optimize the network and server architecture to best support bandwidth intensive applications, enhance user productivity and streamline troubleshooting. ExtremeAnalytics provides visibility into application usage and from where the application is being used.  By locating servers closest to the largest user populations for those applications, network bandwidth is freed up for other applications. ExtremeAnalytics can also be used to help to determine how to optimize performance, thereby leading to quicker application response times for users, reduced service operations and higher user productivity.

When performance or other issues are reported to the helpdesk, it is often hard to tell if the issue is the network, application, client or server. ExtremeAnalytics separates application and network response times and reports them on a per-application basis, and also a per-user basis for each application. This allows IT to focus on the true problem, eliminate finger pointing and quickly resolve the issue.

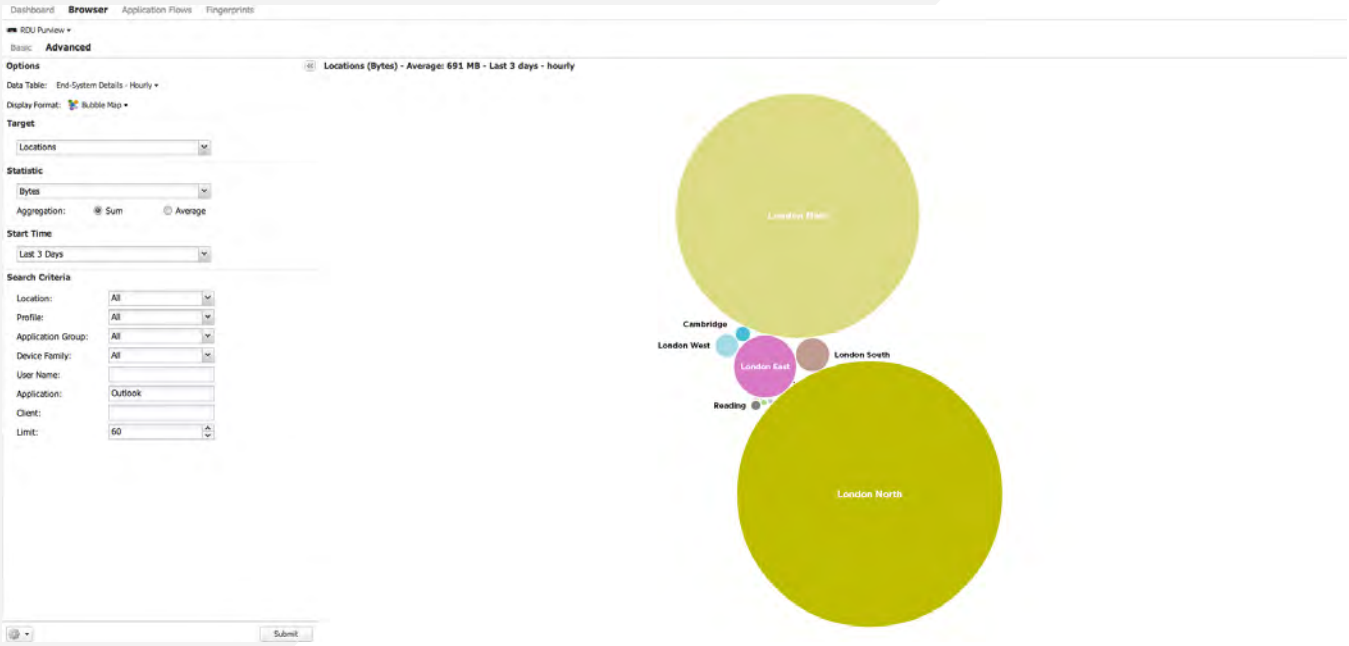
## USE CASE #1 — USING EXTREMEANALYTICS FOR DATA CENTER ANALYSIS

When you are thinking about moving an application from one location to another, you must first investigate how the application is being used and determine what other dependencies on other systems exist to decide if you can break up servers. For example, if there is a web application and a database, but that database also serves up other applications, it might not make sense to move one without the other.

Imagine that you have two main data centers, one in London North and one in London Main. Your main on-premise email server is in London North and you are wondering if it makes sense to move it to London Main. There are more total users in London Main, so at first glance; it appears to be a good idea.



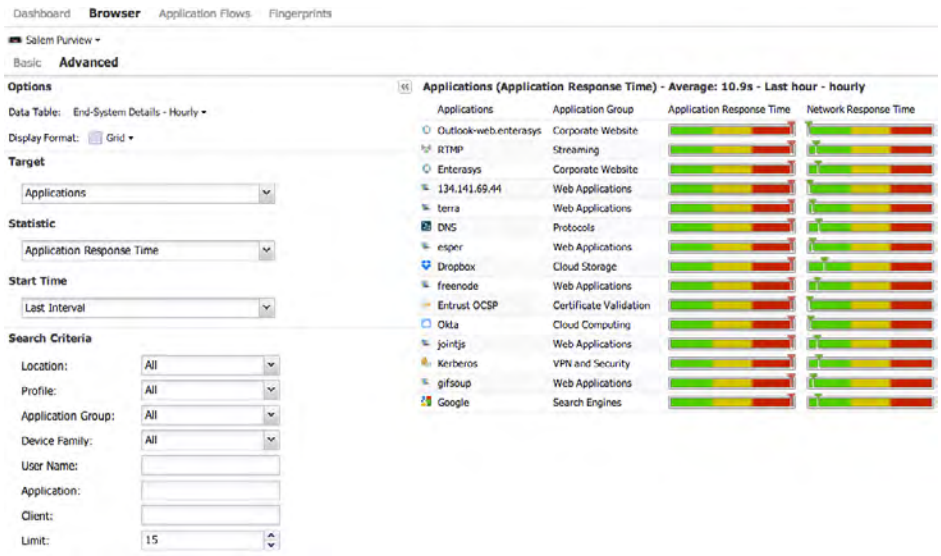
However, if we look closer and see how much traffic is actually used, the London North location suddenly makes a lot more sense. Although there are more users in London Main, they don't appear to be using the application as much as the users in London North.

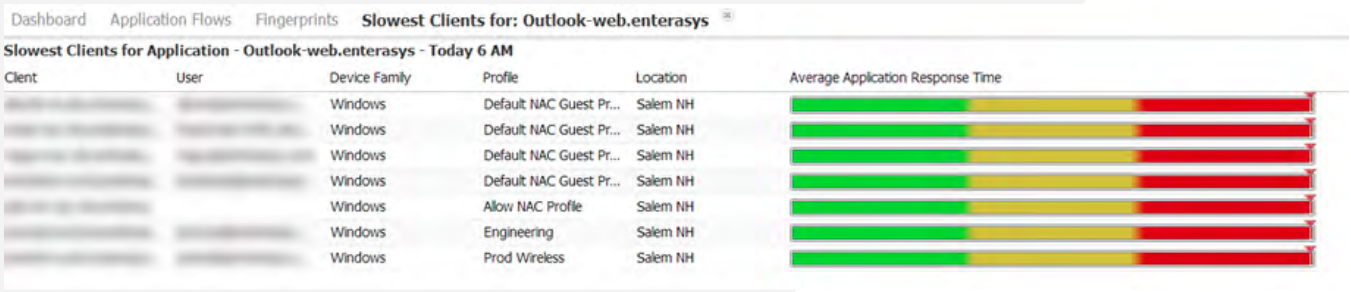



## USE CASE #2 — PROACTIVE TROUBLESHOOTING… USING EXTREMEANALYTICS TO SEE WHAT APPLICATIONS ARE SLOW

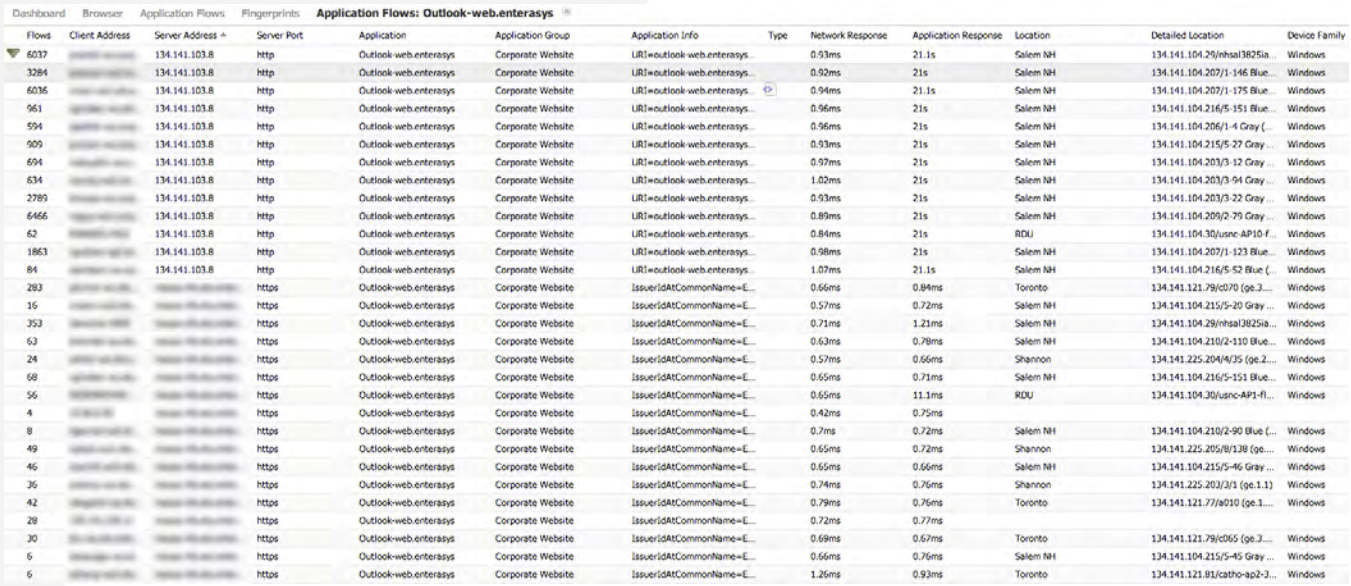
In seconds, ExtremeAnalytics allows you to easily see what applications for a particular user, group, location or device type aren't performing as well as desired. By regularly taking a look at what applications are struggling or under-performing, a service desk can proactively fix issues and/or alert users to known problems and avoid needless calls to the help desk.

In this example, imagine that you were looking at slow performing applications and noticed that one application was always listed – e.g., Cerner Millennium.






However, when the server was looked at, no performance issues were found. By looking at the particular flows, it can be determined that the client was actually pointing to the wrong server.




Once the client was configured to point to the correct server, the application performance improved drastically for these users.

It's interesting to note that although there were several users having this issue, none of them actually reported the problem to the helpdesk. Apparently, although it was annoying, it wasn't annoying enough to open a ticket.

If the service desk is using ExtremeAnalytics, the technicians can see what is really going on and can proactively fix these issues without the users ever having to call-in and complain (or submit a service ticket).

With a simple click, you can change the query to discover the network and application response times for applications in use. In this screenshot, we can easily see that all network and application response times are good for this user.

Since all of these application performance scores are green, there doesn't appear to be a network issue.

## USE CASE #3 — HELP DESK SUPPORT USING EXTREMEANALYTICS AND ONEVIEW TO TROUBLESHOOT NETWORK ISSUES

Imagine that you received this email:

Hey, The network is slow again, can you look at it?

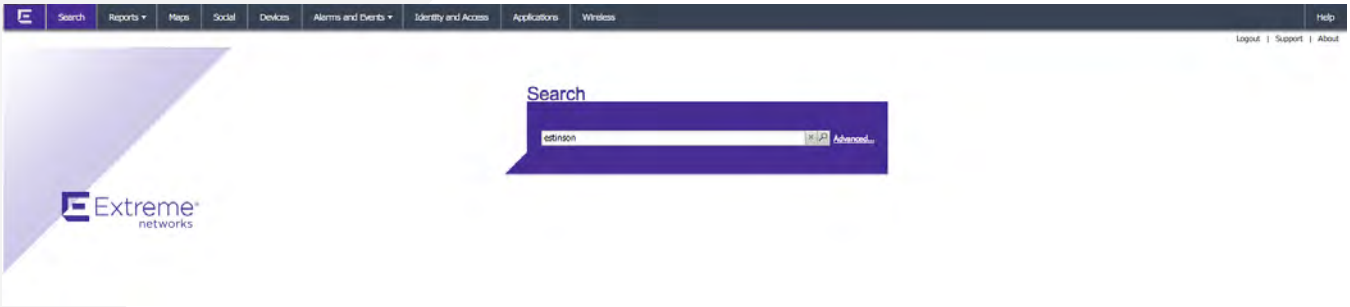
— Dr. Schmidt

The email above generates many questions:

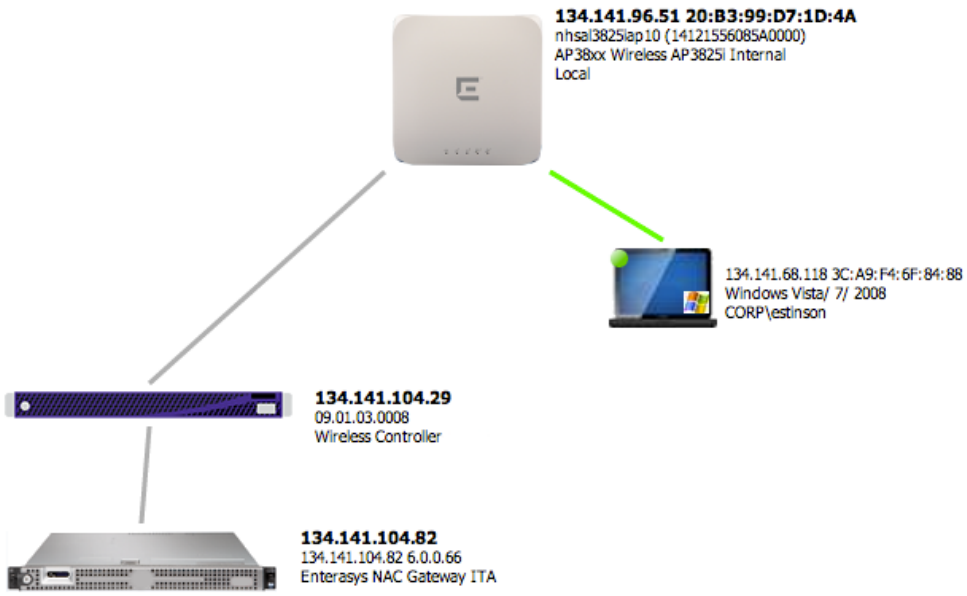
- Where is the user located (i.e., the hospital, remote clinic, etc.)?
- What device are they on (e.g., iPad®, Android phone, corporate laptop, etc.)?
- How are they connected (wireless or wired)?

While the user indicates that he is experiencing a network problem, it could in fact be that a particular application is having an issue. If it's an application, then is just this user affected or is the entire company unable to work because of it?

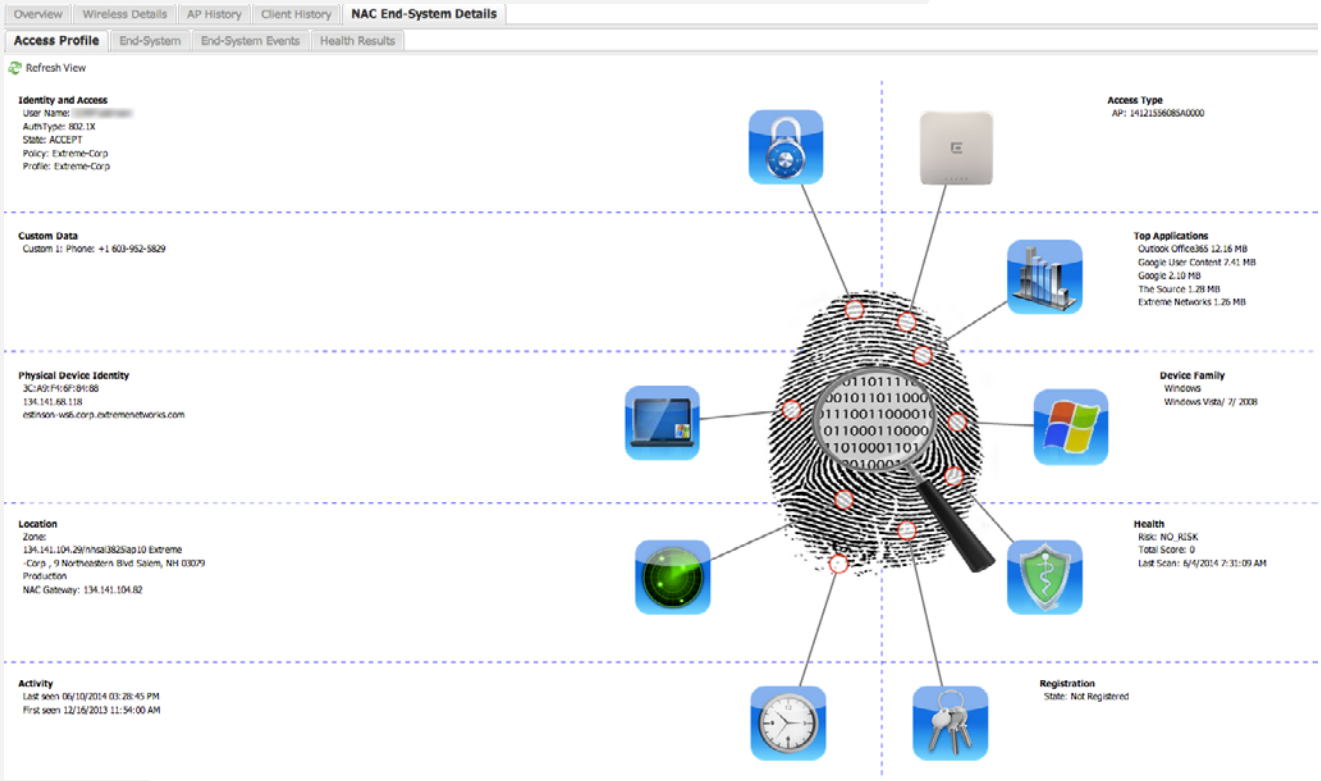
You can troubleshoot this issue easily when using ExtremeAnalytics with an Extreme network. The first step is to figure out where the user is located. When using OneView, click on search and simply enter their username.




In a few seconds, you can easily see that there is only one device this person is using – a laptop, in London Central, on wireless.

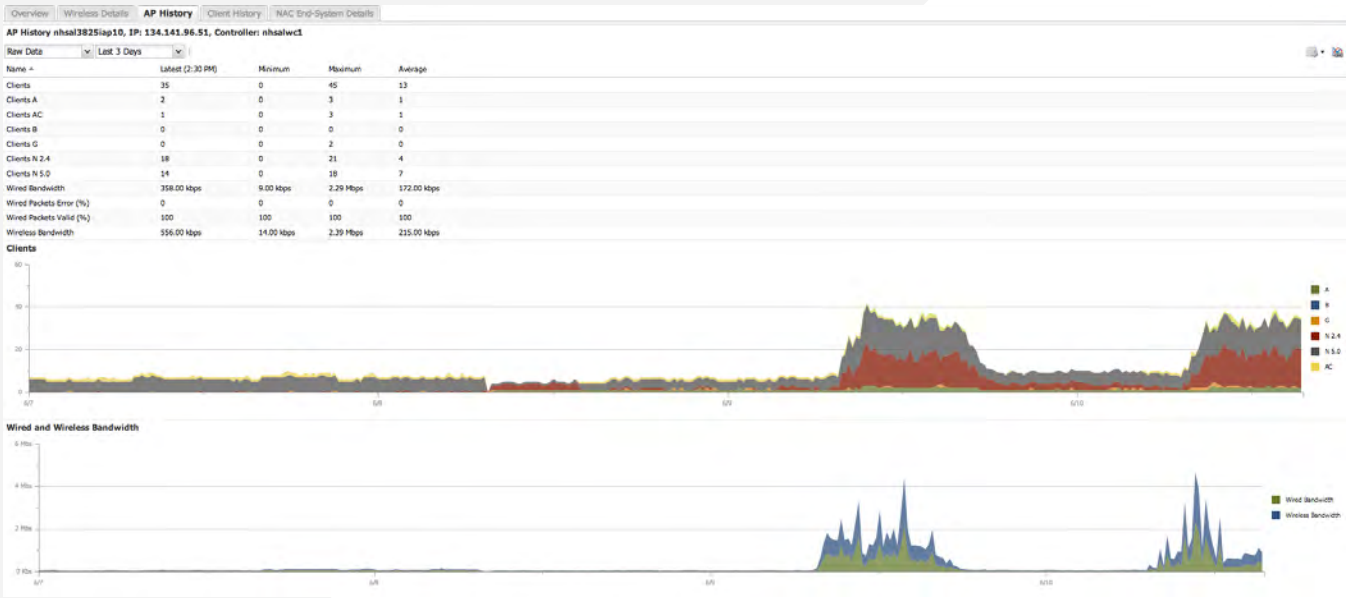


With the problem narrowed down, you can now easily click and get detailed statistics on the user's wireless connection, details on the AP that he is connected to and the wireless appliance that the AP is connected to. At first glance, everything looks good.




The next screenshot shows that there is traffic going to the wireless laptop and it doesn't seem to be enough traffic to be causing performance issues. It also shows a good signal based on the RSS we see from the client. Lastly, this screen shows that there are not a lot of dropped packets going to this laptop.

On the following screenshot, we can see the performance of the access point that the user is connected to. Again, everything looks good. There is traffic, but not enough to cause problems. There are other clients, but not enough to cause bottlenecks or bandwidth constraint issues.




Overview | **Wireless Details** | AP History | Client History | NAC End-System Details

**Client - 134.141.68.118 3C:A9:F4:6F:84:88**

| | | | | | |
|---|---|---|---|---|---|
| SSID: | Extreme-Corp | Bandwidth (in/out): | 8.0 Kbps/1.0 Kbps | WLAN Name: | Extreme-Corp |
| Authenticated: | True | Packets (in/out): | 89 pps/29 pps | WLAN Clients: | 263 |
| Auth/Priv: | Dot1x/WPA | Errors (in/out): | 0 pps/0 pps | WLAN Failed RADIUS (All Clients): | 29 |
| Policy Name: | Extreme-Corp | Duration: | 0 Days 00:17:32 | | |
| Topology Name: | Extreme-Corp | Protocol: | b/g/n 2.4 GHz | | |
| Connection Capability: | Unknown | RSS: | -60 dBm | | |

**Controller - nhsalwc1 134.141.104.29**

| | | | | | |
|---|---|---|---|---|---|
| Availability Status: | Paired | Pair IP: | 134.141.104.30 | VNS Count: | 4 |
| Physical Ports: | 7 | Total APs: | 78 | VN Local Clients: | 544 |
| Clients: | 544 | Active APs: | 31 | VN Foreign Clients: | 0 |
| Tunnels: | 0 | AP Registration Requests: | 1 | VN Total Clients: | 544 |
| Tunnels TX/RX Bandwidth: | 0 bps | Uptime: | 3 Days 05:57:15 | | |

**AP - nhsal3825iap12 Role: Access Point Location: /World/NORA/Salem/Salem building**

| | | | | | |
|---|---|---|---|---|---|
| IP Address: | 134.141.96.54 | Status: | Approved | State: | Active |
| MAC Address: | 20:B3:99:D7:1D:EA | Clients: | 71 | Uptime: | 3 Days 05:47:53 |
| Serial Number: | 14121636085A0000 | | | Protocols in Use: | a (2), g (2), n2.4 (31), n5.0 (30), ac (6) |
| Home: | Local | | | | |

**Radio 1 5.0 GHz Protocol: a/n/c**

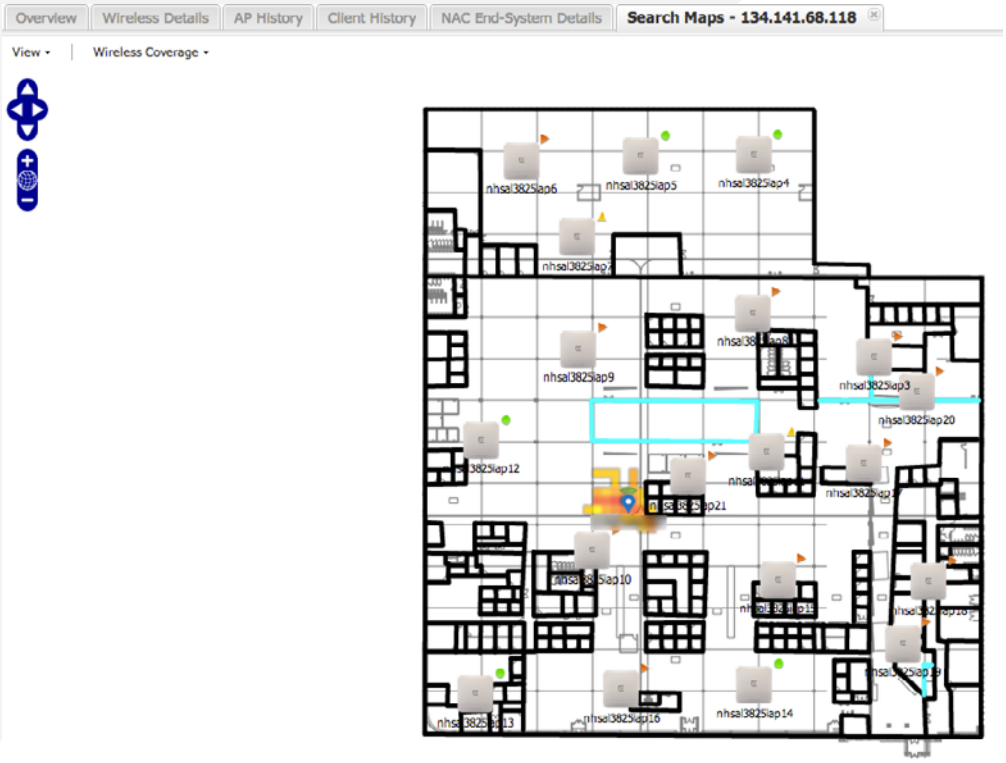
| | | | | | |
|---|---|---|---|---|---|
| Channel: | 48: (5180,5200,5220,[5240]) | Discards (in/out): | 0 pps/0 pps | Current Power Level: | 14 dBm |
| BSSID/SSID | 20:B3:99:D8:27:F1 Prod Guest | Errors (in/out): | 0 pps/6 pps | Minimum Basic Rate: | 6 |
| | 20:B3:99:D8:27:F2 Prod Wireless | Bandwidth (in/out): | 2.0 Mbps/1.0 Mbps | Average Busy Channel %: | 1 |
| | 20:B3:99:D8:27:F0 Extreme-Corp | Unicasts (in/out): | 3.0 Kpps/3.0 Kpps | Maximum Busy Channel %: | 2 |
| | | Multicasts (in/out): | 170 pps/1.0 Kpps | Average RX Channel Utilization: | 5 |
| | | Broadcasts (in/out): | 127 pps/5.0 Kpps | Maximum RX Channel Utilization: | 5 |

**Radio 2 2.4 GHz Protocol: b/g/n**

| | | | | | |
|---|---|---|---|---|---|
| Channel: | 1: (2412) | Discards (in/out): | 0 pps/269 pps | Current Power Level: | 13 dBm |
| BSSID/SSID | 20:B3:99:D8:27:F9 Prod Guest | Errors (in/out): | 0 pps/486 pps | Minimum Basic Rate: | 1 |
| | 20:B3:99:D8:27:FA Prod Wireless | Bandwidth (in/out): | 1.0 Mbps/8.0 Mbps | Average Busy Channel %: | 80 |
| | 20:B3:99:D8:27:F8 Extreme-Corp | Unicasts (in/out): | 7.0 Kpps/7.0 Kpps | Maximum Busy Channel %: | 83 |
| | | Multicasts (in/out): | 0 pps/1.0 Kpps | Average RX Channel Utilization: | 33 |
| | | Broadcasts (in/out): | 0 pps/5.0 Kpps | Maximum RX Channel Utilization: | 34 |

If the laptop had been connected to a wired port, you could quickly discover detailed information about the physical port it is connected to. You would be able to just as easily detect errors on the physical port which could indicate a bad cable, port or NIC.

If it did look like a wireless infrastructure problem, you could easily locate the device on a map so you know exactly where that user and device is located.




Since everything looks good on the wireless network, you need to dig a bit more. From here, it's easy to click over to ExtremeAnalytics under applications and see all the applications that this user is running.

Dashboard **Browser** Application Flows Fingerprints

Salem Purview

**Basic** Advanced

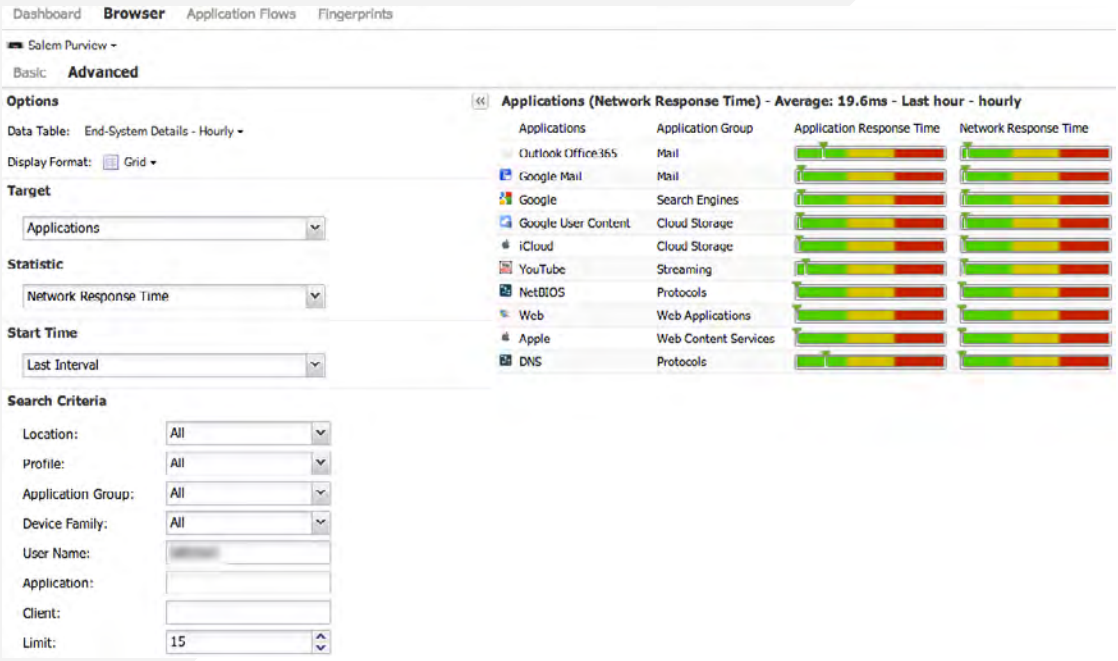
Show: Most popular applications for client Submit

Client: 134.141.68.118

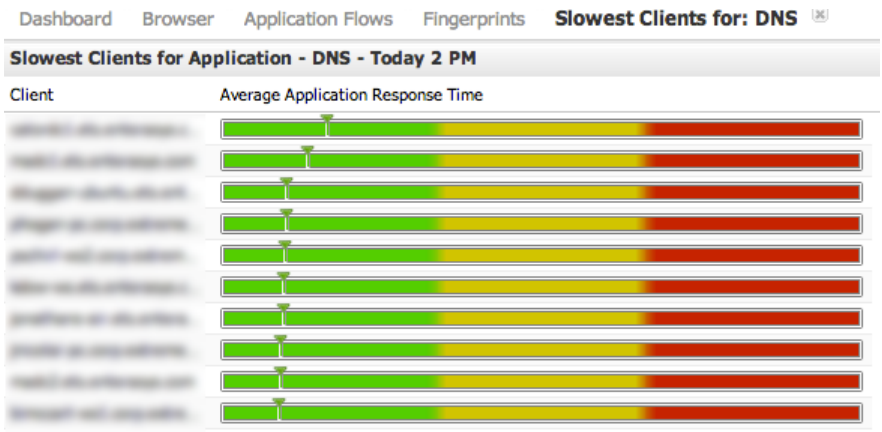
**Applications (Bytes) - Average: 2.71 MB - Today - hourly**

| Applications | Application Group | Bytes | Sent Bytes | Received Bytes |
|---|---|---|---|---|
| Outlook Office365 | Mail | 12.16 MB | 3.89 MB | 8.27 MB |
| Google User Content | Cloud Storage | 7.41 MB | 204.92 kB | 7.20 MB |
| Google Mail | Mail | 2.24 MB | 1.05 MB | 1.18 MB |
| Google | Search Engines | 2.10 MB | 633.95 kB | 1.46 MB |
| Extreme Networks | Corporate Website | 1.26 MB | 425.57 kB | 835.14 kB |
| Windows Live | Web Content Services | 916.32 kB | 459.29 kB | 457.03 kB |
| Salesforce | Business Applications | 362.91 kB | 271.22 kB | 91.69 kB |
| DCERPC | Protocols | 313.31 kB | 172.77 kB | 140.54 kB |
| DNS | Protocols | 294.62 kB | 102.02 kB | 192.60 kB |
| Dropbox | Cloud Storage | 82.36 kB | 44.84 kB | 37.52 kB |

With a simple click, you can change the query to discover the network and application response times for applications in use. In this screenshot, we can easily see that all network and application response times are good for this user.




Since all of these application performance scores are green, there doesn't appear to be a network issue – yet DNS is showing poor application response time. From here you can get a list of slowest clients using DNS that may be impacted as well.




In the screenshot above, everyone else looks good, but if it was just this laptop, then it would indicate a client problem for only a single user. If, however, there are many users having issues with the DNS server, then it's likely a problem with the server. You can even look at the server and see if it's having any issues, e.g., such as poor performance to an iSCSI drive it is using.

Within minutes you can determine where the problem is, and whether it is a network, client, server or storage problem. Using the capability of ExtremeAnalytics it's quick and easy to diagnose even the most complex issues accurately.

# Chapter 4

## USING EXTREMEANALYTICS TO ENHANCE YOUR SECURITY

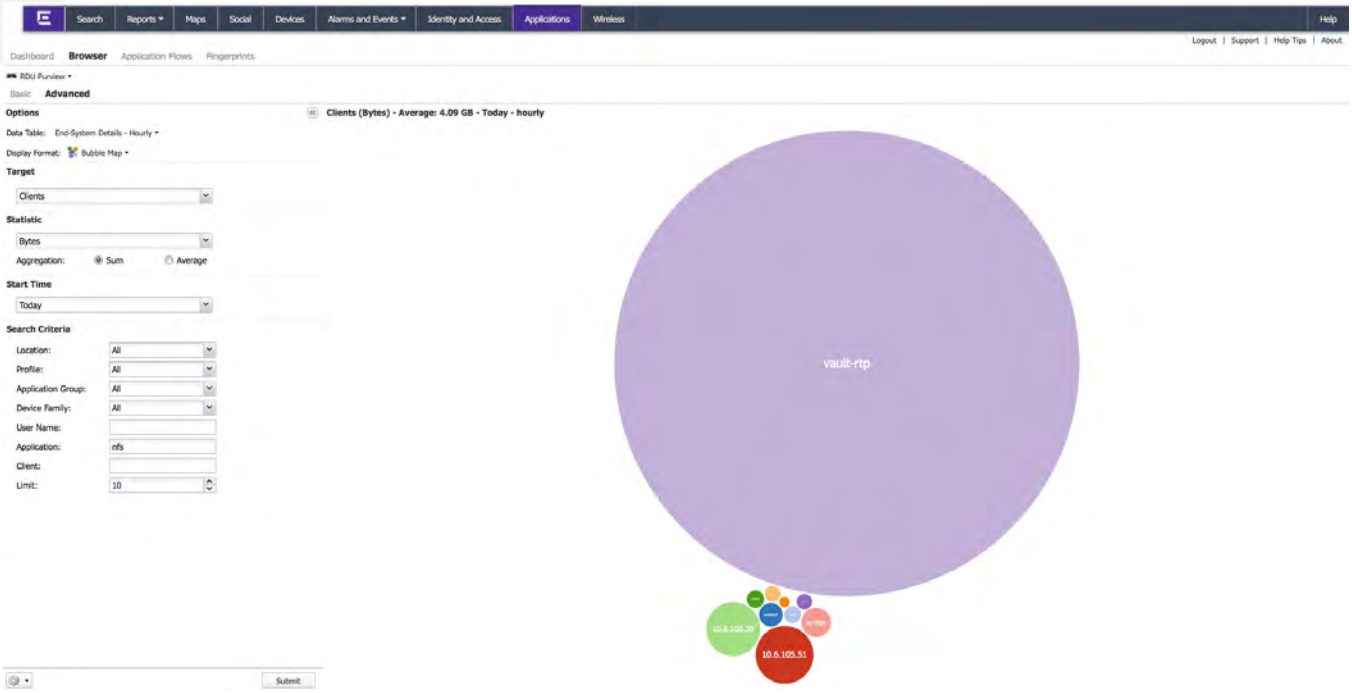
ExtremeAnalytics can be used to help detect malicious applications and find Shadow IT or unapproved applications on the network. With users' easy access to so many applications and websites, including those not provided by the hospital, there is a need to understand whether or not the applications in use on your network meet security requirements. ExtremeAnalytics allows you to understand what applications are in use and how they are being used to understand if the right products are being supported.

While not all unapproved applications are a security or compliance risk, they can still impact IT. ExtremeAnalytics allows applications to be monitored to understand which applications are in use that are not on the approved list. By understanding the type of users who are using these applications and which applications they are, IT can then start to understand why they are being used. This allows IT to not only proactively identify potential security risks, but to also help analyze whether the approved applications are meeting the needs of the business, as compared to unapproved ones. This allows IT to collaborate with lines of business to ensure organization success.

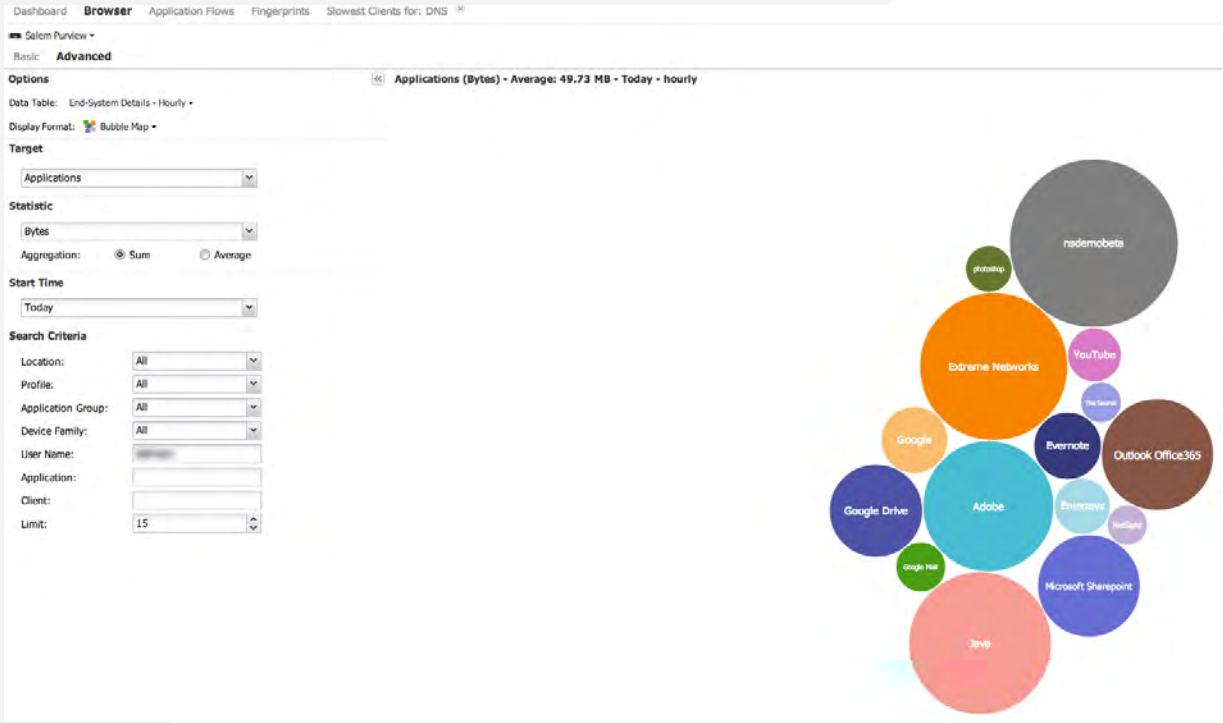
## USE CASE #1 — USING EXTREMEANALYTICS TO HELP DETECT MALICIOUS ACTIVITY

The application tree map view in ExtremeAnalytics allows you to see what applications people are using on your network and find applications running that you don't support. Many ExtremeAnalytics customers were surprised to find out how many cloud applications were running on their "on-premise only" hospital network. The following two scenarios demonstrate how security issues can easily be found using ExtremeAnalytics.

**Scenario 1:** In the screenshot below, you can see that NFS is used a lot. It's mostly used for PACS imaging file storage, although it has some other data on it as well. From here, you can right click and see which clients are using NFS.

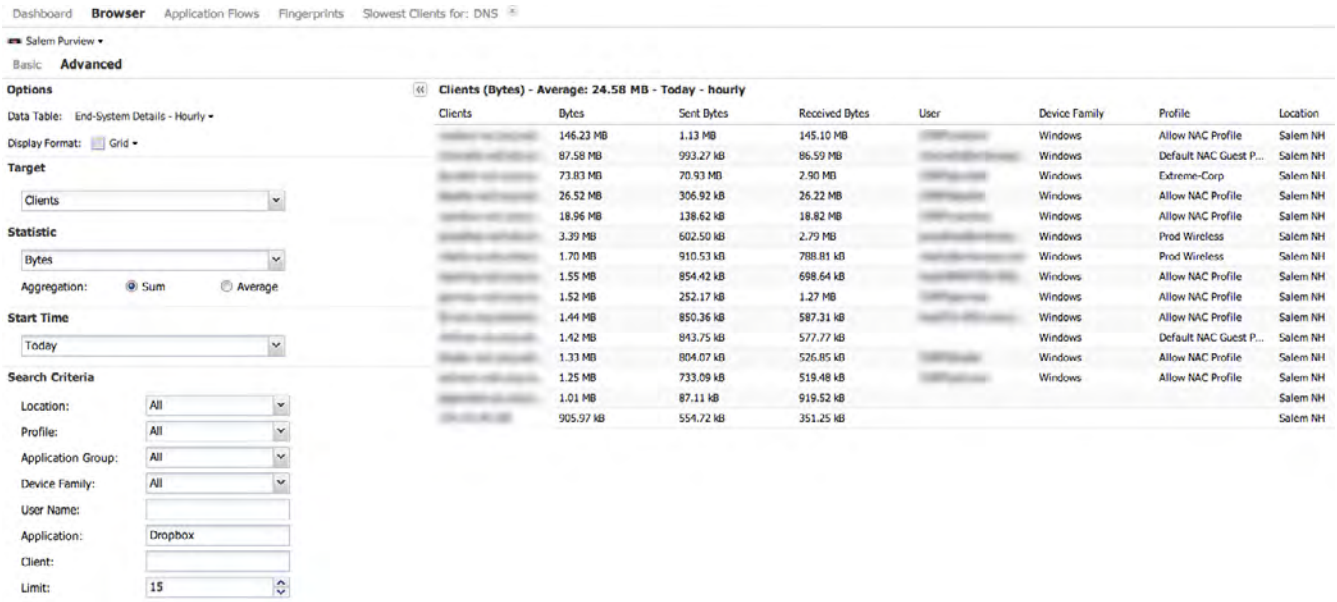


Imagine that you notice that one of the user names is the new intern in Finance. Since Finance data isn't actually stored on NFS, this seems odd. You can dig deeper and see what other applications this intern is using. If Dropbox is also heavily used, a red flag might go up.




If you go back and look at all the applications used over the last three days, and see PayPal®, Bitcoin or some other payment site, it might be time for a full investigation. While there might be a valid reason, it could also be a case where this intern is misusing or sharing your private healthcare data with entities external to your organization.

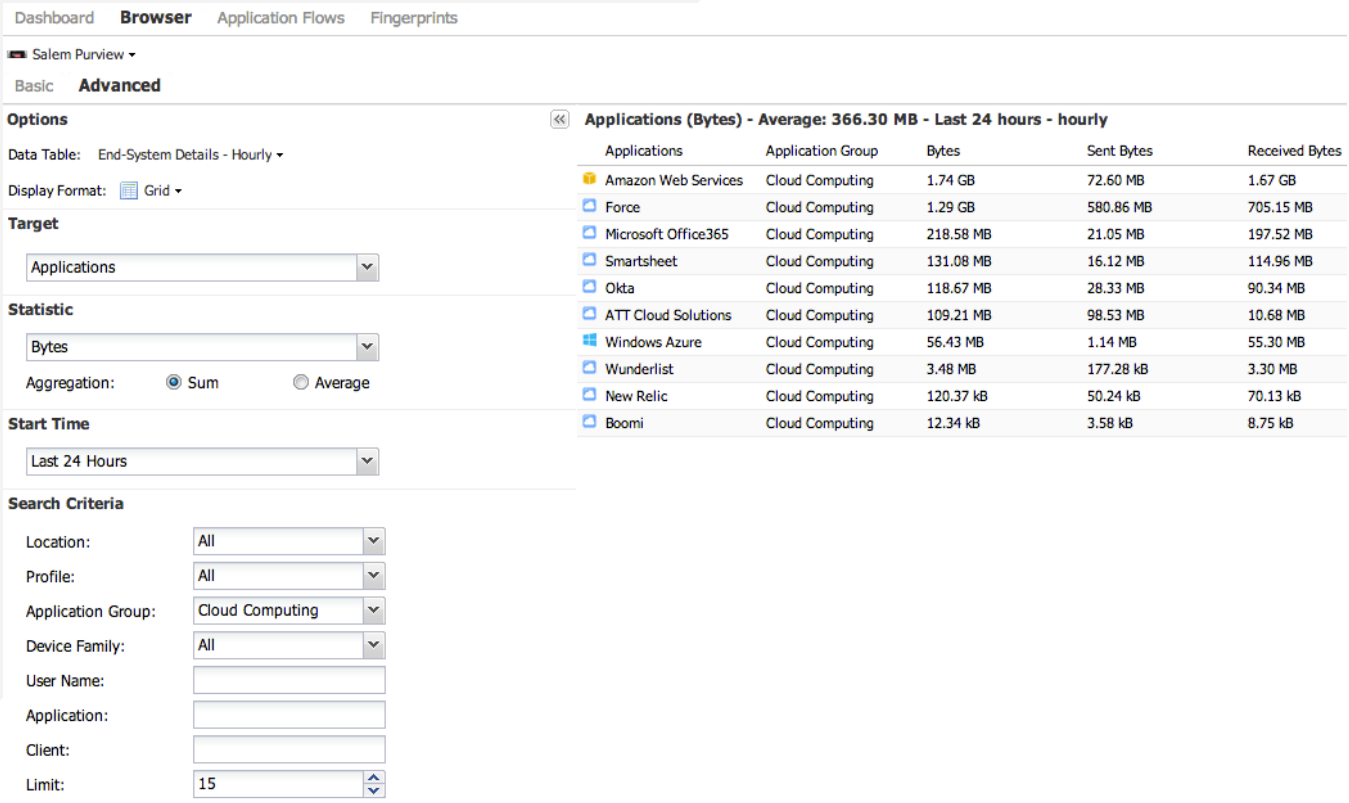
**Scenario 2:** Another example would be seeing that someone is using a lot of cloud storage, such as Dropbox. If you don't use Dropbox for corporate sanctioned storage, that might raise a red flag as well.



While there isn't any drastic Dropbox usage, if one user had several GB of data transferred, you could right click on their name and see what other applications they were running. If there was a large amount of corresponding data being used with NFS or CIFS (both file sharing protocols) then it might warrant a further investigation.

## USE CASE #2 — USING EXTREMEANALYTICS TO FIND SHADOW IT OR UNAPPROVED APPLICATIONS ON THE NETWORK

ExtremeAnalytics is also a great tool to discover what applications might have been ordered from other departments – the so called "Rogue IT" departments. For example, it's really easy to look at the tree map view and see what else is running, or to run a special query to look for "Cloud Computing".




The above screenshot shows 1.74GB of Amazon Web Service (AWS) traffic. You can easily drill down into the top users of these applications to determine if another department is deploying services on a cloud service without the knowledge of IT. While this could be perfectly reasonable, it could also point to a larger security issue if compliance isn't followed.

# Chapter 5

## CONCLUSION

The use cases in this eBook demonstrate just a few examples of how ExtremeAnalytics can be used to gain more insight into your business and add value to your organization. There are many other countless ways to use ExtremeAnalytics to provide business value through:

- Optimized resource utilization and capacity management for business-critical applications
- Troubleshooting and managed application services
- Application traffic management
- Network and application response time management
- Providing application usage data for compliance reporting
- Analyzing customers' application usage profile to better understand your customers

No matter what type of business you serve – education, healthcare, hospitality, government or manufacturing – ExtremeAnalytics can provide more context and insight into who is using what, when, where and how to ensure the deployment of new applications that enable more efficient business processes and pave the way for you to make better business decisions using network-powered insights.