ExtraHop

Business Value for XYZ Corp

XYZ

Real-Time Operational Intelligence Findings

Prepared by:
Joanna Smith, Director of IT, XYZ Corp
Nick Tesla, Systems Engineer, ExtraHop
Ada Lovelace, Regional Sales Manager, ExtraHop

EXECUTIVE SUMMARY: BACKGROUND AND OBJECTIVE

PROJECT BACKGROUND

A non-invasive, automated, and real-time IT operational assessment was conducted from October 2, 2015 – October 22, 2015 by XYZ Corp and ExtraHop, a next-generation IT Operation Analytics (ITOA) vendor. The following report explores the capabilities and benefits of real-time analysis of all data in motion, referred to as wire data analytics. The technology serves as the basis for a more adaptive, comprehensive, and cost-effective approach supporting XYZ Corp heterogeneous and dynamic environment.

PROJECT OBJECTIVE AND GOALS

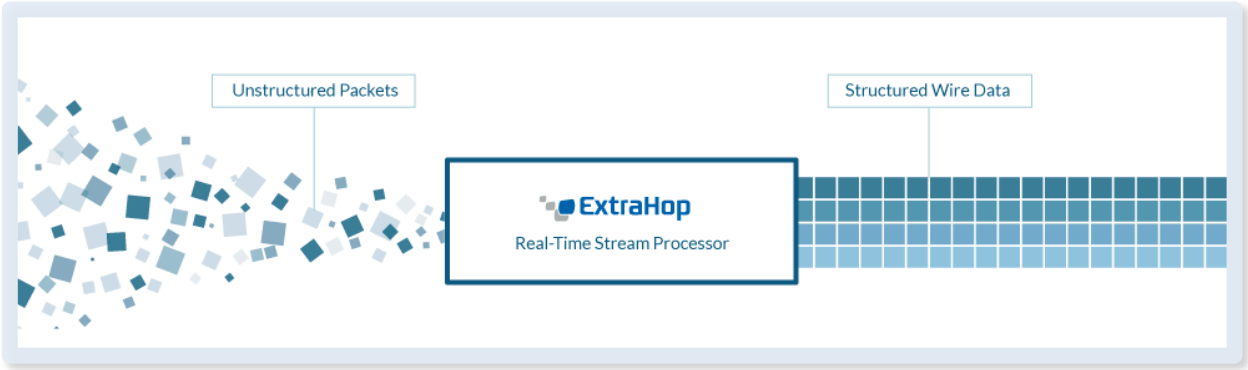
The objective of this project is to create a more efficient, integrated, and data-driven approach to how we measure, run, and improve IT Operations. The measurable goals are to drive down costs, enable Tier I staff to perform at Tier II or higher levels, provide a visibility platform for better cross-team coordination reducing MTTR, mitigate availability and security risks, and provide insights that can increase revenue while improving IT agility and end-user satisfaction.

To accomplish this objective, the project explored whether the ExtraHop wire data analytics platform could serve as the foundation for a data-driven model for more effective and efficient IT operations and security. We explored how to leverage this unique data set by identifying strategies to eliminate costs, improve performance, and mitigate common but blind attack vectors associated with security infrastructure like encryption, ciphers and certificates. We believe that if we could more easily see and correlate all client, application, network, and infrastructure activity, then we would have a more complete set of objective insights allowing us to adapt to change quickly and support new IT and business initiatives with greater predictability.

WHY WIRE DATA ANALYTICS AND AN ITOA PRACTICE

The drive toward a more data-driven IT operational model has seen the emergence of analyzing all data in motion (wire data analytics) as the foundation of a modern ITOA practice. The reason is that the one constant among all application, network, client, virtualization, infrastructure, and cloud behavior is the network. Regardless of the technology, where workloads may run, how many layers of abstraction exist, or how applications are constructed, all technology and business transacts via wire protocols over a network.

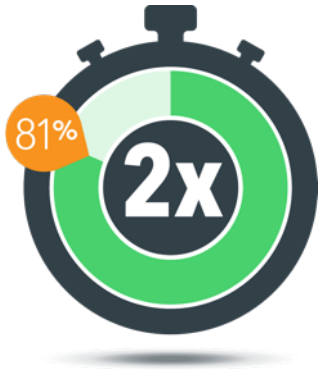
The ExtraHop platform is designed to transform unstructured packet data into structured wire data at line rate for mining real-time IT and business insight from all data in motion.



WHAT EXTRAHOP CUSTOMERS ARE SAYING

55% of surveyed IT organizations paid back their investment in ExtraHop in 6–12 months or less.

TVID: 189-0A8-F83



81%

of surveyed IT organizations improved mean-time-to-resolution by 2x or more with ExtraHop.

TechValidate

TVID: 792-E08-501

What has most surprised you about ExtraHop?

"The many, many insights you can gain from this platform. We haven't even scratched the surface."

– Brian Bohanon, IT Director, Aaron's, Inc.

http://www.techvalidate.com/tvid/A59-E9B-B75

"In the tech business, you always hear from vendors that their solution will be easy to install, will be flexible to operate, or will have an exceptional ROI. These promises are almost always too good to be true. ExtraHop has these stories as well, but they consistently exceed expectations every time."

– Todd Forgie, IT Vice President, MEDHOST

http://www.techvalidate.com/tvid/A6A-E5A-80B

EXECUTIVE SUMMARY

The following report details the prescriptive findings and quantifies the value of real-time wire data analytics for our environment. The project objective explored whether the ExtraHop platform could drive more effective and efficient IT operations and security.

ROI SUMMARY	
Cost of Investment	**$250,000**
Hard ROI	**$573,195**
Time Taken to Earn Back Investment	**<6 months**
Soft ROI (Hard ROI + Risk Mitigation)	$5.9 million
Time Taken to Earn Back Investment	< 1 month

ROI DRIVERS

Hard ROI

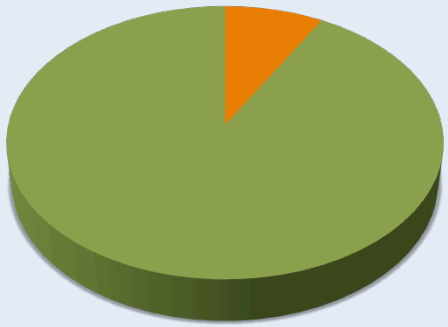
Revenue Drivers - $47,500

Cost Savings - $525,600

Soft ROI (Hard ROI + Risk Mitigation)

Lower Downtime Risk - $4,350,000

Lower Security Risk - $1,785,000



EXECUTIVE SUMMARY

KEY FINDINGS FOR OBSERVED PERIOD

Cipher Suite and Encryption 5,660 weak cipher sessions were observed over 20 hosts. This represents a security risk.	**DNS** 15% of DNS requests are failing due to IPv6 issues having a 2-4 second impact on end-user performance.	**Citrix** The longest Citrix login during the observed period was 2.46 minutes.
Database 4,100 DB errors occurred and the slowest query process time was over 10s.	**Storage** A frequent backup script slowed down storage performance and is congesting the network.	**Asset Discovery** Two FTP servers were discovered in areas of the network where this protocol is not allowed.
SMTP There were 5,000 unencrypted SMTP sessions, indicating a potential security risk.	**Web Optimization** Our website is returning 3.5K server errors each hour, wasting server resources.	**Network** 1.04 million TCP retransmission timeouts were observed, adding roughly 5 second delays for end users.
Real User Monitoring Website responses for Safari browsers are 39% slower than other browsers.	**VOIP** A high number of SIP errors represent end-users that cannot make calls.	**Security Point Solutions** 2,500 Shellshock attempts were detected in HTTP and DHCP payloads.
Cloud Applications 3 GB of data has been sent to cloud storage apps outside of corporate policy.	**FTP** There were no FTP requests originating outside of corporate headquarters, which is expected.	

CIPHER SUITE AND ENCRYPTION MONITORING – FINDINGS

KEY FINDINGS FOR CIPHER SUITE AND ENCRYPTION MONITORING

5,660 insecure sessions	• Sensitive information may be exposed to malicious actors, which can directly cause further data loss and security breaches.
64,000 sessions	• Sessions using RC4 encryption are considered insecure and expose your company to data theft.
1,900 days	• It has been 400 days since the oldest SSL certificate expired. This exposes the enterprise and customers to malicious cybercrime.
1,650 Insecure sessions	• Number of sessions observed using SSLv3, an insecure version vulnerable to man-in-the-middle attacks.

See the Appendix for Cipher Suite and Encryption dashboards

INDUSTRY FACTS

- A data breach cost U.S. companies an average of **$6.5M per incident** in 2014 – Ponemon Institute
- The average global 5,000 company spends **$15 million** to recover from a certificate outage—and faces another **$25 million** in potential penalties – Ponemon Institute
- **Only 40% of HTTP servers support TLS or SSL** and present valid certificates – Redhat (scan of Alexa top 1M sites)
- **20% of servers are using broken cipher suites** making encrypted data vulnerable – Redhat
- RC4 is still used in **>18% of HTTPS servers** – Redhat

CIPHER SUITE AND ENCRYPTION MONITORING – VALUE

Cost Savings

Time spent per month to manually locate servers with weak ciphers (hours)	6	*XYZ Corp*
Annual cost of any tools used to locate impacted servers	$25,000	*XYZ Corp*
Annual cost of any consultants used to locate impacted servers	$0	*XYZ Corp*
Average salary of Security Engineer	$95,000	*Glassdoor*
Labor savings	$30,130	

Time spent per month to manually audit certificates and encryption (hours)	6	*XYZ Corp*
Annual cost of any tools used to locate impacted servers	$0	*XYZ Corp*
Annual cost of any consultants used to locate impacted servers	$10,000	*XYZ Corp*
Average salary of Security Engineer	$95,000	*Glassdoor*
Labor savings	$15,130	

Risk Mitigation

Average # of records that are exposed in a breach (US)	28,000	*Ponemon Institute*
Average per record cost of a breach (US)	$217	*Ponemon Institute*
% risk reduction due to improved cipher and encryption visibility	5%	
Avoided costs due to breached records	$303,800	

Total Annual Savings	**$349,060**

BUSINESS VALUE

- Force multiplier for the Security team – shorten time to remediation by up to 50%
- Move to a proactive state ensuring constant compliance without additional staff
- Eliminate costs associated with manual audits
- Reduces chances of a breach that could damage company brand and reputation and result in lost business

DNS MONITORING AND ANALYSIS – FINDINGS

KEY FINDINGS FOR DNS MONITORING AND ANALYSIS

298,000 **request timeouts**	• Timeouts will have an impact on application performance and user experience. If associated with fee-based API driven services you may be overcharged.
35% **of request timeouts**	• Sauce Labs, a cloud-based automated testing service is causing 35% of timeouts. This should be investigated to ensure you're not being billed for this traffic.
1,160 **AAAA look-ups**	• Thousands of IPv6 requests have been potentially causing 2 – 4 second delays for clients and applictions. This should be fixed immediately.
15,000 **DNS response errors**	• DNS errors may be caused by misconfiguration. Fixing these may resolve application issues and slowness.

See the Appendix for DNS Monitoring dashboards

INDUSTRY FACTS

- **DNS errors and issues cause greater than 20%** of Internet and application outages – Ars Technica
- **A DNS Dashboard** for performance, availability, and risk mitigation is recommended best practice for any enterprise by DHS and the ITSRA working group along with ICANN – U.S. Department of Homeland Security

DNS MONITORING AND ANALYSIS – VALUE

Cost Savings

# of people on DNS/Network team	2	*XYZ Corp*
% of time spent per month troubleshooting DNS issues	20%	*XYZ Corp*
Average salary of DNS Admin	$75,867	*Glassdoor*
Annual labor savings	$18,208	

Risk Mitigation

Annual DNS unplanned downtime across all domains (hours)	8.75	*Verisign*
Potential reduction in downtime using ExtraHop	10%	*TechValidate Survey*
Downtime cost per hour	$100,000	*IDC*
Savings due to reduction in downtime risk	$87,500	

Total Annual Savings	**$105,708**

BUSINESS VALUE

- Force-multiplier for the Network, Application, and Security teams – Shorten time to remediation by up to 50%
- Prevent overcharges from fee-based API driven subscription services
- Performance improvement opportunity impacting revenue
- Increase cross-team knowledge and understanding of the importance of DNS
- If outsourcing DNS, ensure accountability and SLAs of managed service provider

DATABASE HEALTH AND PERFORMANCE MONITORING – FINDINGS

KEY FINDINGS FOR DATABASE HEALTH AND PERFORMANCE MONITORING

4,100
errors

- High error rates have a negative impact on the health and performance of your databases. ExtraHop shows SQL transaction details to troubleshoot errors.

428
milliseconds

- Worst database server processing time during the observed period. More than 100ms is generally considered to have a negative impact on application performance.

99
privileged user logins

- Privileged user logins should be continuously monitored in order to identify anomalous behavior that can indicate a data breach.

See the Appendix for Database Health and Performance dashboards

INDUSTRY FACTS

- Database profilers can impact performance by **up to 20%** – Microsoft
- 25% of DBAs surveyed reported unplanned outages of up to 1 day, while **40% reported outages between 1-5 days** – Oracle

DATABASE HEALTH AND PERFORMANCE MONITORING – VALUE

Cost Savings

# of people on database team	3	*XYZ Corp*
% of time spent per month troubleshooting db issues	25%	*XYZ Corp*
Average salary of Database Admin	$67,700	*Glassdoor*
Annual labor savings	$11,424	
Performance impact of running profiler continuously	5%	*Microsoft*
Estimated annual spend on database hardware	$200,000	*XYZ Corp*
Estimated annual spend on database licenses+support	$300,000	*XYZ Corp*
Annual cost of any consultants used to help troubleshoot dbs	$5,000	*XYZ Corp*
Annual cost savings due to profiler replacement	$30,000	

Risk Mitigation

Annual database unplanned downtime for businesses (hours)	8.75	*Oracle & Unisphere Research*
Potential reduction in downtime using ExtraHop	20%	*TechValidate Survey*
Downtime cost per hour	$100,000	*IDC*
Annual savings due to reduction in downtime risk	$175,000	
Total Annual Savings	**$216,424**	

BUSINESS VALUE

- Force multiplier for the Database team
- Improved visibility into transaction performance and baselines, including cross-cluster transaction tracing
- Better-performing apps with reduced downtimes, leading to a better end-user experience and increased user productivity
- Minimize disruptions to business operations, including potential revenue loss due to downtime or databases running in degraded mode
- Understand how other resources (e.g. network) impact database performance

STORAGE MONITORING – FINDINGS

KEY FINDINGS FOR STORAGE MONITORING

38
files

- Files that should be cached based on NFS response counts. This will improve network utilization and experience for users in branch offices.

1.42K
errors

- Storage errors can be investigated to identify corrupted files, access, and performance issues.

1
scheduled backup

- A scheduled backup job is causing zero windows (extreme latency) in NAS response and causing application errors.

See the Appendix for Storage Monitoring dashboards

INDUSTRY FACTS

- **PCI, HIPAA, and Sarbanes-Oxley** all require file audit access – TechNet
- In Windows Server 2008, CHKDSK requires **6 hours to identify corrupt files** in a system with 300m files – TechNet

STORAGE MONITORING – VALUE

Cost Savings

Number of team members involved in storage troubleshooting	3	*XYZ Corp*
% of time spent per month troubleshooting storage and configuring logging	15%	*XYZ Corp*
Average salary of Storage Engineer	$99,943	*Glassdoor*
Potential reduction in MTTR using ExtraHop	25%	*TechValidate Survey*
Annual labor savings	$16,865	

Number of servers requiring file server audit software	30	*XYZ Corp*
License cost per server	$349	*Lepide*
Annual cost savings	$10,470	

Risk Mitigation

Planned downtime to correct file corruption (hours)	2	*XYZ Corp*
Unplanned downtime each year (hours)	7	*XYZ Corp*
Average cost per hour	$100,000	*VMware*
Potential reduction in MTTR using ExtraHop	25%	*TechValidate Survey*
Annual savings due to reduction in downtime risk	$225,000	

Total Annual Savings	**$252,335**

BUSINESS VALUE

- Reduce unplanned and planned downtime of critical systems
- Tune the performance of many applications dependent on storage, including database and VDI
- Improve IT productivity by immediately surfacing storage issues (such as corrupt files and operation locks) before they cause issues

SMTP MONITORING – FINDINGS

KEY FINDINGS FOR SMTP PERFORMANCE MONITORING

2,000
errors

- High SMTP error rates could indicate email delivery failures that impact employee productivity and business operations.

300
milliseconds

- Spikes in server processing time should be investigated as they could be indicators of issues like attempted overloading of mail servers, malicious spamming, or compromised clients.

5,000
unencrypted sessions

- Encrypted sessions protect sensitive information in flight. A large number of unencrypted sessions could increase potential security risks and cause non-compliance with policy.

See the Appendix for SMTP Monitoring dashboards

INDUSTRY FACTS

- In a survey of over 1,000 organizations, 72% experienced unplanned email outages in a year. Of those, 71% lasted longer than four hours – MessageOne
- ~21 billion emails appearing to come from well-know commercial senders did not actually come from their legitimate IP addresses (between October 2014 and March 2015) – Return Path
- Email was the main channel for 8.2% of all data leaks globally in 2014 – Infowatch

SMTP MONITORING – VALUE

Cost Savings		
# of people on email team	2	*XYZ Corp*
% of time spent per month troubleshooting email delivery issues	15%	*XYZ Corp*
Annual cost of any tools used to troubleshoot SMTP issues	$10,000	*XYZ Corp*
Annual cost of any consultants used to troubleshoot SMTP issues	$5,000	*XYZ Corp*
Average salary of Messaging Administrator	$68,000	*Payscale*
Annual labor savings	$30,300	
# of employees using email	1000	*XYZ Corp*
Time experiencing SMTP/delivery issues (hours each month)	0.5	*XYZ Corp*
Average salary of an employee	$51,670	*. Bureau of Labor and Statistics*
Saved employee productivity	$23,252	
Risk Mitigation		
Annual email delivery unplanned downtime for businesses (hours)	4.3	*Oracle & Unisphere Research*
Potential reduction in downtime using ExtraHop	50%	*TechValidate Survey*
Downtime cost per hour	$100,000	*IDC*
Annual savings due to reduction in downtime risk	$215,000	
Average # of records that are exposed in a breach (US)	28000	*Ponemon Institute*
Average per record cost of a breach (US)	$217	*Ponemon Institute*
% of data breaches that are due to email	8%	*Infowatch*
% risk reduction for breaches through email due to improved SMTP visibility	50%	
Avoided costs due to breached records	$249,116	
Total Annual Savings	**$517,668**	

BUSINESS VALUE

- Improved visibility into SMTP errors and performance
- Minimize disruptions to email, which can disrupt business operations, lower employee productivity, and impact customers and partners
- Better visibility into SMTP as a potential security vector, including identifying DLP incidents
- Augment messaging hygiene capabilities
- Maintain SLAs

WEB OPTIMIZATION – FINDINGS

KEY FINDINGS FOR WEB OPTIMIZATION

38
302 redirect codes

- 302 redirects indicate a temporary change in URI. Change these to 301 redirects for better SEO.

3.5k/hr
500 server errors

- 500 errors occur when a server encounters an error but can't provide more information. If this number is not zero, you have a problem.

101k/hr
404 errors

- 404 errors can indicate broken links pointing to your site, or other misplaced resources. Users seeing these may leave your site and never return.

1.6M
Requests for .gif images

- Gif files are notoriously large, and your site is seeing many requests for them. Consider a different image format to reduce bandwidth consumption on your most requested assets.

INDUSTRY FACTS

- People will visit a website less often if it is **slower than a close competitor by more than 250 milliseconds** – New York Times
- A 1-second delay in page response **decreases customer satisfaction by 16 percent**, which in turn results in a 7 percent reduction in conversions – Trac Research

See the Appendix for Web Optimization dashboards

REAL USER MONITORING – FINDINGS

KEY FINDINGS FOR REAL USER MONITORING

1 seconds	• Perceived page load time by end-users. This is good performance but should be monitored to ensure revenue, conversions, and user satisfaction.
2.4 seconds	• Server processing is the largest contributor to performance. Pages are usable sooner, but this should be watched.
330,000	• Dropped data segments forced application retransmissions impacting end-user performance and should be addressed immediately.
Microsoft Windows	• Is the most common end-user platform. Understanding platforms, browsers, and usage focuses application, network, and infrastructure tuning efforts.

See the Appendix for Real User Monitoring dashboards

INDUSTRY FACTS

- **Up to a 7% increase in conversion rate** can be achieved for every 1 second of performance improvement – KissMetrics
- **Up to 1% of incremental revenue** can be earned for every 100ms of performance improvement – Walmart Page Speed Study
- **A one second delay** can decrease customer satisfaction by 16% – Aberdeen Group

WEB OPTIMIZATION & RUM – VALUE

Cost Savings

Percent of Web Dev time spent per month on performance/availability issues	15%	*XYZ Corp*
Percent of Ops team time spent per month on performance/availability issues	15%	*XYZ Corp*
Number of people on Web Dev team	2	*XYZ Corp*
Avg. salary of a Web Dev	$95,315	*Glassdoor*
# of people on Dev Ops team	2	*XYZ Corp*
Avg. Salary of Dev Ops Engineer	$105,000	*Glassdoor*
Potential reduction in MTTR using ExtraHop	40%	*TechValidate Survey*
Personnel cost savings annually	$36,057	
Estimated hardware and infrastructure spend related to scale and performance	$250,000	*XYZ Corp*
Reduction in misallocated budget due to hardware spend	2%	*ZDNet*
Annual cost of current Real User Monitoring (RUM) solution - software, support, overhead	$75,000	*XYZ Corp*
Expected savings from reduced infrastructure spend and RUM solution costs	$80,000	

Revenue Drivers

		XYZ Corp
Unique Users per Year	1,000,000	*Google Page Speed tool*
Page load performance (seconds)	5	*Google Developer Research*
Expected improvement in page load speed (seconds)	0.025	*Aberdeen Group*
Estimated 7% increase in conversion rate for every second of improved performance	1,750	
Average revenue per user (ARPU)	$10	*XYZ Corp*
Potential revenue increase based on increased conversions	$17,500	
OR		
Annual site revenue		*XYZ Corp*
Potential revenue increase based on each 100ms performance increase	$0	

WEB OPTIMIZATION & RUM – VALUE (CONTINUED)

Risk Mitigation

Annual web unplanned downtime (hours)	8.75	*XYZ Corp*
Cost per hour of unplanned downtime	$21,000	*Trac Research*
Annual planned & unplanned degraded performance	36	*XYZ Corp*
Cost per hour for degraded performance	$4,100	*Trac Research*
Annual SLA Payouts due to Web Application Downtime or Slowtime	$5,000	*XYZ Corp*
Potential reduction in MTTR using ExtraHop	50%	*TechValidate Survey*
Potential savings due to added visibility from ExtraHop	$168,175	
Total Annual Savings	**$301,732**	

WEB OPERATIONS – BUSINESS VALUE

- Force-multiplier for the Web Development & Optimization teams – Shorten time to remediation by up to 50%
- Optimize web properties for speed and efficiency, which positively impacts conversion rates
- Reduce SLA liability from poorly performing websites or applications
- Reduce hardware and software spend related to web performance

REAL USER MONITORING – BUSINESS VALUE

- Target development and optimization priorities based on usage by mobile, desktop, platform and browser
- Support agile DevOps processes through complete cross-tier visibility
- Provide business stakeholders clear, consistent, and self-serve SLA dashboards

VOIP MONITORING – FINDINGS

KEY FINDINGS FOR VOIP MONITORING

2.88 mean opinion score (MOS)	• Minimum MOS score observed for RTP provides insight into service level violations. MOS ranks from 1 to 5 with 1 being the worst.
9 milliseconds	• RTP jitter is acceptable, with the maximum jitter reaching only 9ms. Excessive jitter makes calls unintelligible.
2,800 SIP 401 status codes	• Responses with the 401 status code indicate unauthorized activity and should be investigated.
402 SIP "bad event from client" errors	• Call initiations that failed due to "bad event from client" errors. Users could not make calls.

See the Appendix for VOIP Monitoring dashboards

INDUSTRY FACTS

- **Packet capture** is the most relied upon troubleshooting method for VoIP issues – Cisco support forum, 2014
- Voice was ranked as the **second-most used communication method** (86%, behind email at 93%) for employees – InformationWeek Reports
- **68% of consumers would hang up** as a result of poor call quality and call a competitor instead – Customer Experience Foundation

VOIP MONITORING – VALUE

Cost Savings

Number of team members involved in VOIP troubleshooting	1	*XYZ Corp*
% of time spent per month troubleshooting VOIP issues	5%	*XYZ Corp*
Average salary of Network Engineer	$68,000	*Payscale*
Potential reduction in MTTR using ExtraHop	50%	*TechValidate Survey*
Labor savings	$2,550	
# of employees using VOIP	1,000	*XYZ Corp*
Time experiencing VOIP issues (hours each month)	0.25	*XYZ Corp*
Average salary of an employee	$51,670	*U.S. Bureau of Labor and Statistics*
Potential reduction in VOIP issues using ExtraHop	25%	*TechValidate Survey*
Saved productivity	$29,064	

Revenue Drivers

Sales calls affected by VOIP issues (includes downtime and calls with poor quality) each month	200	*XYZ Corp*
Average revenue per sales call	$25	*XYZ Corp*
Potential reduction in VOIP issues using ExtraHop	50%	*TechValidate Survey*
Recaptured revenue	$30,000	

Risk Mitigation

Customer support calls affected by VOIP issues (includes downtime and poor call quality) each month	200	*XYZ Corp*
Average cost assigned to poor customer support experience	$10	*XYZ Corp*
Brand damage/negative business impact	$24,000	

Total Annual Savings	**$85,614**	

BUSINESS VALUE

- Protect brand and revenue (preventing customer dissatisfaction)
- Ensure employee productivity
- Reduce the number of help desk tickets
- Provide SLAs to business for call quality

CLOUD APP MONITORING – FINDINGS

KEY FINDINGS FOR CLOUD APPLICATIONS

1 MB/S **bandwidth consumed by cloud apps**	• Cloud application bandwidth consumption shows the max load that is being used. High cloud app bandwidth could impact data center traffic.
6.8 GB/3 GB **compliant/non-compliant cloud storage**	• Shows the amount of data being stored in the cloud, including storage destinations that don't match your policies.
367 MB **total Facebook traffic**	• High bandwidth consumption on Facebook can indicate lost employee productivity.
9.2 GB **data used by top Spotify user**	• Large multimedia usage can impact network performance. This can be an easy area to recapture bandwidth.

See the Appendix for Cloud App Monitoring dashboards

INDUSTRY FACTS

- **Browser-based/cloud apps** were the largest source of data leakage in 2014 at 35.1% – InfoWatch 2014 Report
- Nearly 80% of employees surveyed cited non-work related Internet use or social media as a **top productivity killer** – CareerBuilder
- Estimated growth in datacenter traffic by 23% and cloud traffic 33% year over year through 2018 is driving need to **increase bandwidth** – Cisco Global Cloud Index

CLOUD APP MONITORING – FINDINGS

Cost Savings

# of people on Network team	1	*XYZ Corp*
Time spent per month troubleshooting bandwidth/cloud apps issues	25%	*XYZ Corp*
Average salary of Network Admin	$63,520	*Glassdoor*
Annual labor savings assuming reduction in MTTR by 50%	$11,910	
Average enterprise expenditure on networking equipment annually	$1,100,000	*Infonetics*
Reduced networking expenditures from traffic reduction of 1%	$11,000	
# of employees	1,000	*XYZ Corp*
Time spent per week on social media or web browsing not related to job	2	*XYZ Corp*
Average salary of an employee	$51,670	*S. Bureau of Labor and Statistics*
Estimated reduction in employee utilization of consumer/social apps by 1%	$40,303	
Replacement/elimination of current monitoring software costs	$10,000	
Total savings from using ExtraHop as an employee monitoring solution	$50,303	

Risk Mitigation

Average # of records that are exposed in a breach (US)	$28,000	*Ponemon Institute*
Average per record cost of a breach (US)	$217	*Ponemon Institute*
% of breaches that are the result of cloud or web browsing activities	35%	*Infowatch*
Estimated avoided costs of breached records based on 5% risk reduction	$106,634	
Total Annual Savings	**$179,846**	

BUSINESS VALUE

- Improved network performance and uptime
- Increased worker productivity
- Eliminate costs of manual audits
- Reduces chances of a breach that could damage company brand, reputation, and result in lost business

FTP MONITORING – FINDINGS

KEY FINDINGS FOR FTP MONITORING

242K
FTP errors

- During the observed period, there were 242,000 FTP errors (550 – Failed to open file) attributed to whoami.akamai.net.

0
FTP requests originating outside of headquarters

- There were no FTP requests originating outside of corporate headquarters. This is expected; FTP requests originating elsewhere can indicate malicious behavior.

4
files transferred

- Only four files were transferred during the observed period. ExtraHop analysis includes file names and sizes.

See the Appendix for FTP Monitoring dashboards

INDUSTRY FACTS

- **68% of organizations use FTP** as a mainstay file transfer method – Osterman Research
- **PCI Data Security Standard 2.0** requires monitoring data access and capturing audit data – PCI Standards Security Council
- FTP should be monitored for both **data breaches** and **data stashing**
- The hackers who stole millions of credit card details from **Target in 2013** used FTP to exfiltrate the data – Krebs on Security

FTP MONITORING – VALUE

Cost Savings

Number of team members involved in FTP troubleshooting	1	*XYZ Corp*
% of time spent per month investigating and troubleshooting FTP	5%	*XYZ Corp*
Average salary of System Administrator	$72,258	*Glassdoor*
Potential reduction in MTTR using ExtraHop	50%	*TechValidate Survey*
Annual cost of any managed file transfer (MFT) software license	$5,000	*XYZ Corp*
Annual cost savings	$7,710	

Risk Mitigation

Average # of records that are exposed in a breach (US)	28000	*Ponemon Institute*
Average per record cost of a breach (US)	217	*Ponemon Institute*
% risk reduction due to improved FTP visibility	1%	*XYZ Corp*
Avoided costs due to breached records	$60,760	

Risk Mitigation

Unplanned FTP downtime each year (hours)	8.75	*XYZ Corp*
Downtime cost per hour	$100,000	*IDC*
Potential reduction in downtime using ExtraHop	10%	*TechValidate Survey*
Annual savings due to reduction in downtime risk	$87,500	

Total Annual Savings	**$155,970**	

BUSINESS VALUE

- Reduce unplanned and planned downtime of critical systems
- Tune the performance of many applications dependent on storage, including database and VDI
- Improve IT productivity by immediately surfacing storage issues (such as corrupt files and operation locks) before they cause issues

SECURITY VULNERABILITY MONITORING – FINDINGS

KEY FINDINGS FOR SMTP PERFORMANCE MONITORING

2,500
Shellshock attempts

- Number of Shellshock attempts detected in HTTP and DHCP payloads.

0
HTTP.sys attempts

- Number of exploit attempts of the HTTP.sys Range Sec vulnerability in the payload of HTTP requests. This vulnerability impacts Microsoft Windows and Windows Server.

500
Heartbleed attempts

- Number of SSL heartbeats, which can be exploited by the Heartbleed bug. Validate that the correct version of OpenSSL is in use.

See the Appendix for Security Vulnerability Monitoring dashboards

INDUSTRY FACTS

- Within days of the discovery of the **Shellshock vulnerability**, CloudFlare reported blocking more than 1.1M attacks – CloudFlare
- At the time of Heartbleed's disclosure, **more than 500,00 (17%) of the internet's secure web servers** were believed to be vulnerable to attack. The Community Health Systems breach compromised 4.5M patient records – Wikipedia
- Researchers at the University of Michigan estimated that **36.7% of browser-trusted sites** were vulnerable to the FREAK attack – Threatpost

SECURITY VULNERABILITY MONITORING – VALUE

Cost Savings

# of people on Security team	3	*XYZ Corp*
% of time spent per month on vulnerability detection/incident response	5%	*XYZ Corp*
Annual cost of any forensic analysis tools	$10,000	*XYZ Corp*
Annual cost of any external incident response consultants for forensic analysis	$5,000	*XYZ Corp*
Average salary of Security Engineer	$95,000	*Glassdoor*
Labor savings	$18,206	

Risk Mitigation

Average # of records that are exposed in a breach (US)	28,000	*Ponemon Institute*
Average per record cost of a breach (US)	$217	*Ponemon Institute*
% risk reduction due to improved security vulnerability monitoring	2%	
Avoided costs due to breached records	$121,520	

Total Annual Savings	**$139,726**	

BUSINESS VALUE

- Force multiplier for the Security team
- Continuously monitor your environment to detect attempted exploits of known vulnerabilities like Shellshock as well as new exploits
- Make security reporting and proving compliance with policy easier
- Eliminate costs associated with manual audits or consultants
- Reduce chances of a breach that could damage company brand and reputation and result in lost business

CITRIX MONITORING - FINDINGS

KEY FINDINGS FOR CITRIX XENAPP AND XENDESKTOP PERFORMANCE MONITORING

20 seconds per Citrix login (95th percentile)	• Average time to logon to mission critical applications delivered by Citrix.
166 hours per month	• Lost hours of productivity due to slow Citrix login (enterprise-wide).
5% CIFS traffic resulting in errors	• A high number of CIFS errors correlated to one device indicates a likely corrupted Citrix profile. Troubleshoot immediately.
2.46 minute load times	• High maximum load times indicate that some of your Citrix users are having a bad user experience. Remediate quickly.

See the Appendix for Citrix Monitoring dashboards

INDUSTRY FACTS

- Citrix admins spend over **30% of their time troubleshooting performance issues.** (DABCC)
- Over **50% of performance issues** Citrix admins encounter are **not caused by Citrix**. (DABCC)
- **~50% logon time improvement can be achieved** with profile size reduction, growth mitigation, and appropriate profile management tactics. (Citrix)
- ExtraHop is **verified as Citrix Ready** for Citrix XenApp, XenDesktop and NetScaler.

CITRIX MONITORING - VALUE

Cost Savings - Citrix Admin & Consultant Labor

# of Citrix Admin FTEs	1	*XYZ Corp*
% of Citrix Admin FTE time spent troubleshooting/fighting fires in Citrix	25%	*DABCC*
% of Citrix Admin FTE time spent diagnosing/troubleshooting non-Citrix issues	20%	*XYZ Corp*
Citrix Admin FTE Salary	$100,515	*Payscale*
Amount spent on outside Citrix consulting in the past year	$0	*XYZ Corp*
Potential reduction in MTTR by using ExtraHop	50%	*TechValidate Survey*
Annual labor savings for Citrix Admins	$33,924	

Cost Savings - Employee Productivity

# of employees using Citrix	500	*XYZ Corp*
Hours lost due to slow Citrix login issues per employee per month	0.2	*ExtraHop Data*
Average salary of employee that uses Citrix delivered apps in your organization	$51,670	*U.S. Bureau of Labor Statistics*
Potential improvement in Citrix login times and unavailability	50%	
Productivity savings from using ExtraHop	$22,282	

Cost Savings - Replacement of Current Citrix Monitoring Tools

Annual spend on other monitoring tools for Citrix (e.g. Lakeside)	$10,000	*XYZ Corp*
Annual savings by using ExtraHop	$10,000	

Total Annual Savings	**$66,206**	

BUSINESS VALUE

- Enable Tier 1 support to be able to investigate and resolve issues that would otherwise escalate
- Reduce time loss and improve employee productivity by cutting wait times for Citrix logins, launch, and latency by 50% or more
- Improve end-user experience and restore faith in Citrix delivered applications
- Pinpoint root cause of latency outside Citrix that affects application delivery

ASSET CLASSIFICATION – FINDINGS

KEY FINDINGS FOR ASSET CLASSIFICATION

300
new active devices communicating w/TCP

- This number shows a large growth in devices communicating using TCP devices and can be a leading indicator that more capacity is needed.

2
FTP servers in use

- Could indicate a system using a protocol that shouldn't be in use has been detected.

53
DNS servers in use

- This is a sizable deployment of DNS servers and could indicate an opportunity to consolidate and save money.

See the Appendix for Asset Classification dashboards

INDUSTRY FACTS

- 45% of surveyed IT pros said they manage multiple pieces of software providing **duplicative functionality**
  – Information Week
- **20% of all racked IT equipment** isn't being used and organizations could benefit from decommissioning them
  – Uptime Institute
- It takes **205 days on average** to discover for companies to detect their environment has been compromised
  – FireEye

ASSET CLASSIFICATION – VALUE

LOCKHEED MARTIN

A leading Government and Defense Contractor discovers unexpected DNS servers post migration.

Impact
With ExtraHop they were able to see that instead of the 12 expected DNS servers post consolidation of their DNS infrastructure they had several hundred machines acting as DNS servers.

They were able to eliminate these machines:
- Improving operational efficiency
- Strengthening the security of their environment
- Free up resources for other projects

McKESSON

A leading Services Provider supporting healthcare organizations was experiencing sprawl.

Why?
- Not decommissioning testing and QA servers properly upon completion
- Source systems not decommissioned post migration
- Fear of taking down critical systems by mistake

Impact
With ExtraHop, McKesson was able to monitor all activity identify critical systems and retire nonessential equipment saving $200k annually in licensing, lower power consumption, and improve manageability.

BUSINESS VALUE

- Being able to isolate rogue and non-compliant infrastructure quickly
- Identify consolidation candidates
- Improve predictability in budgeting and buying
- Validate migrations and consolidation efforts have been completed correctly

NETWORK HEALTH AND UTILIZATION – FINDINGS

KEY FINDINGS FOR NETWORK HEALTH AND UTILIZATION

3.2m
IPv6 frames

- A number of servers and clients are using IPv6 even though this is not our internal policy. This can cause delays as these lookups resolve.

4.9TB
bytes sent over TCP

- Over the observed period, there was 4.9TB sent over TCP compared with 475GB sent over UDP. This baseline should be monitored to track growth of custom protocols based on UDP.

1.04m
retransmission timeouts

- TCP retransmission timeouts represent roughly 5 second delays for the user as the client and server attempt to complete a transaction. Servers with high RTOs may be overloaded.

See the Appendix for Network Health and Utilization dashboards

INDUSTRY FACTS

- Average orgs spend 11% of their IT budget on network and telecommunications.
  – ESG Research
- **39% of organizations** have turned off firewall functions to improve network performance
  – Intel
- Datacenter traffic will grow 23% CAGR between 2013 and 2018
  – Cisco Global Cloud Index Survey

NETWORK HEALTH AND UTILIZATION – VALUE

Cost Savings

# of people responsible for network monitoring	1	*XYZ Corp*
% of time spent per month troubleshooting network issues	25%	*XYZ Corp*
Average salary of Network Admin	$63,520	*Glassdoor*
Potential reduction in MTTR using ExtraHop	50%	*TechValidate Survey*
Annual labor savings	$11,910	

Average enterprise expenditure on networking equipment annually	$500,000	*Infonetics*
Increased efficiency due to tuning and optimization	3%	*XYZ Corp*
Defrayed networking expenditures from traffic reduction	$15,000	

Total Annual Savings	**$26,910**	

BUSINESS VALUE

- Continuous network utilization baseline for capacity planning, anomaly detection, and troubleshooting
- Assess impact of equipment upgrades, application changes, policy changes, etc.
- Tune the performance of application delivery controllers (ADC)

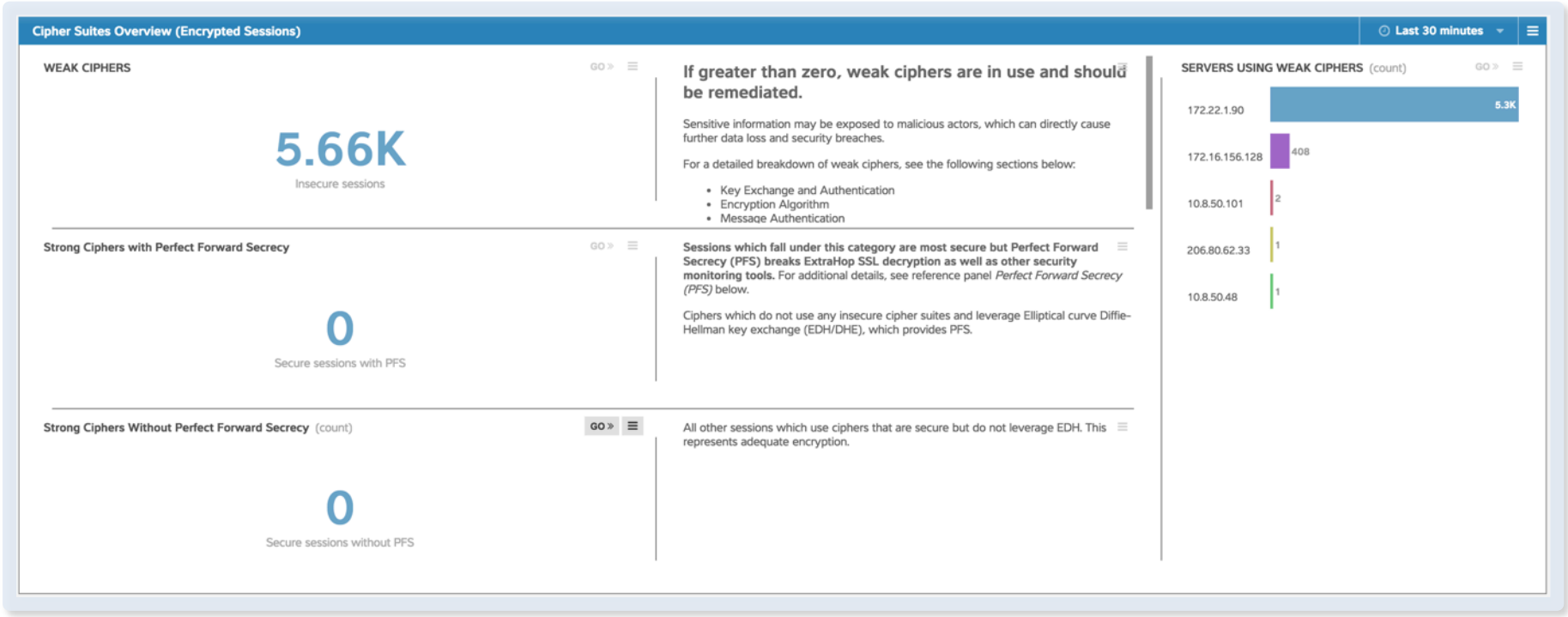
APPENDIX

ExtraHop Dashboards

CIPHER SUITE AND ENCRYPTION MONITORING DASHBOARDS

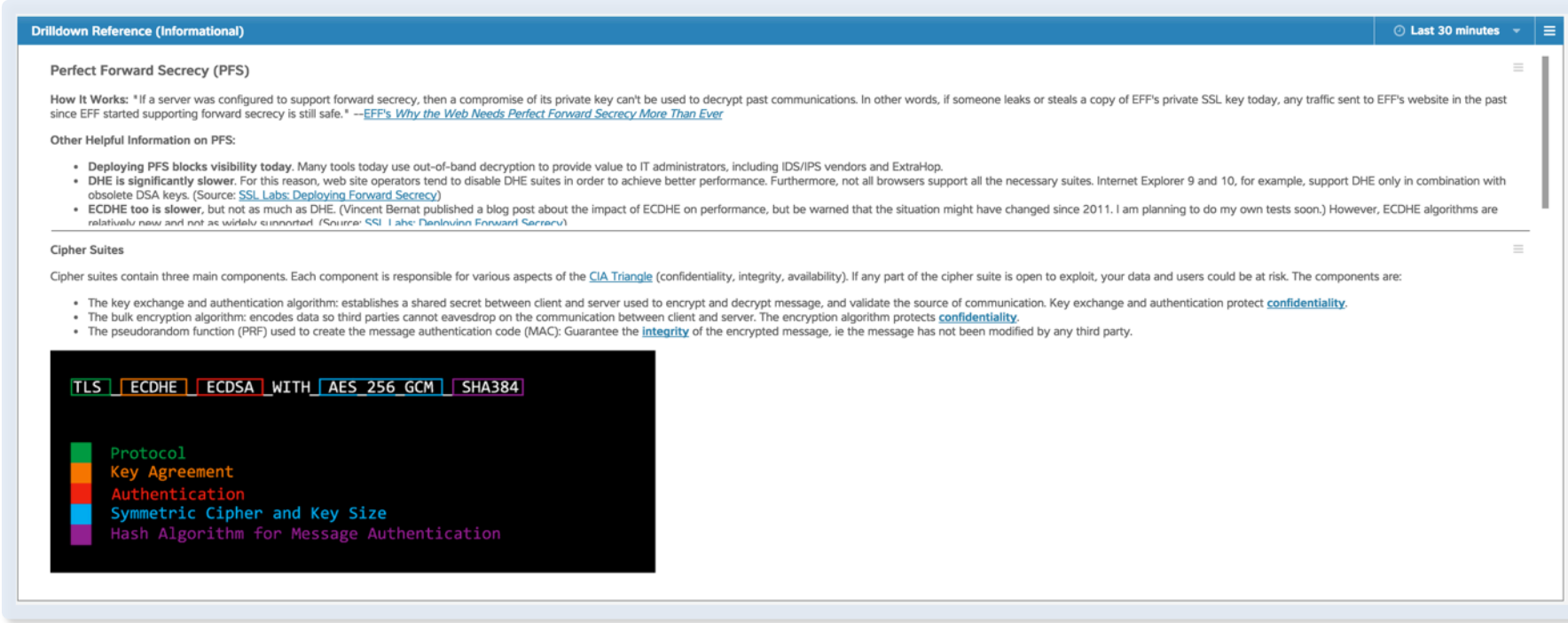
The ExtraHop platform performs continuous SSL envelope analysis to determine the ciphers used, the expiration dates of keys, and other critical metrics that must be monitored to ensure proper application functionality and security. The the Cipher Suite and Encryption dashboard shows observed behavior and activity during the project period and should be referenced by the InfoSec team.

The section of the the Cipher Suite and Encryption dashboard below provides a complete picture of the strength or weakness of ciphers on your network, and your weakest points that require immediate remediation.

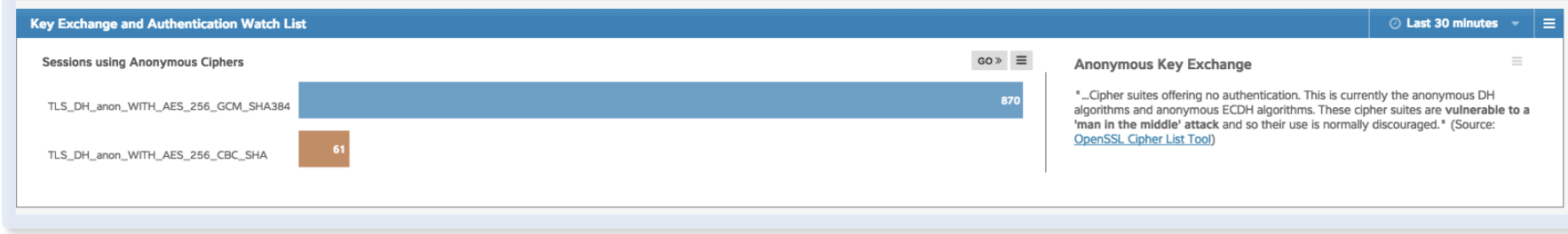


CIPHER SUITE AND ENCRYPTION MONITORING DASHBOARD

This dashboard section describes the latest issues in modern encryption, so you can be as secure as possible without hampering visibility.

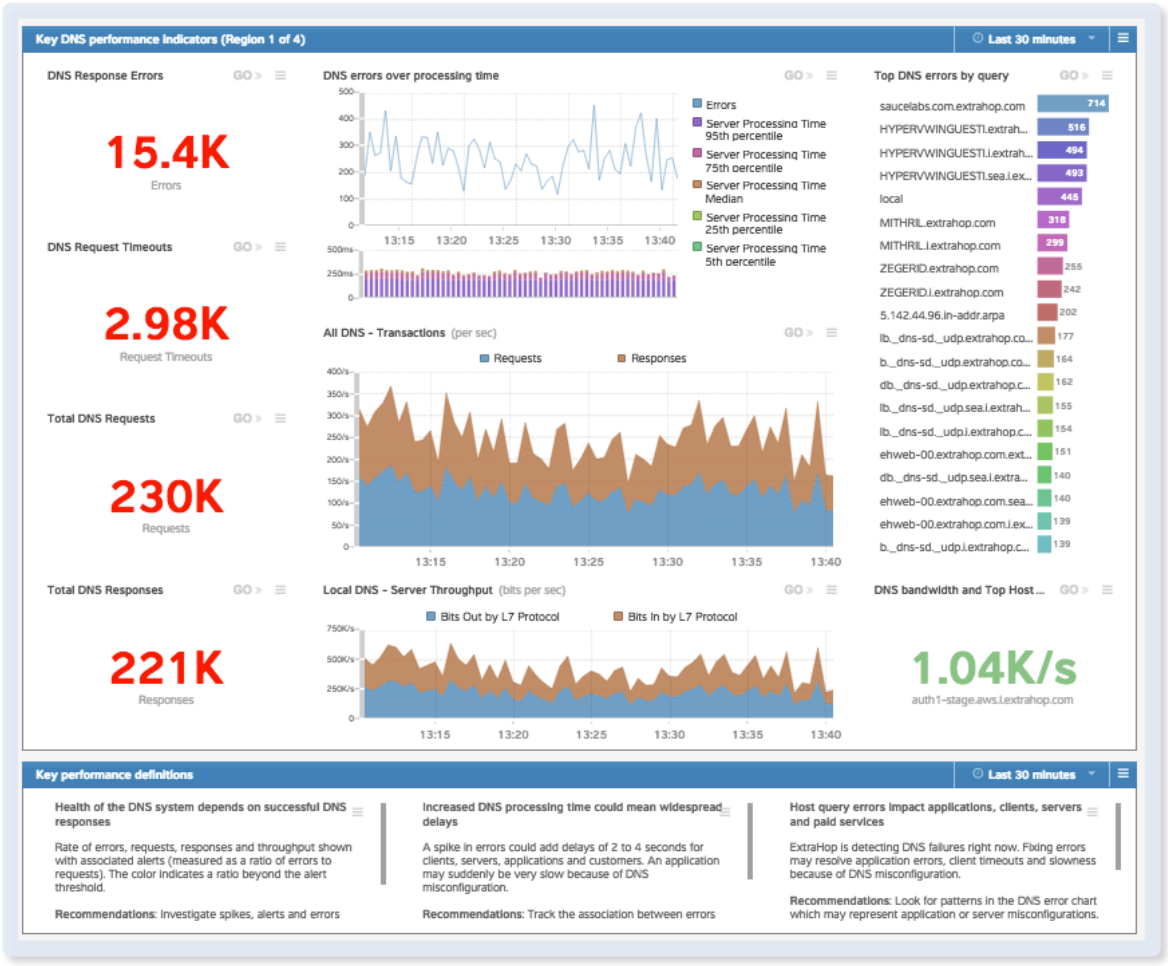


This section shows the number of anonymous ciphers in your system, which are vulnerable to hacking through man-in-the-middle attacks.



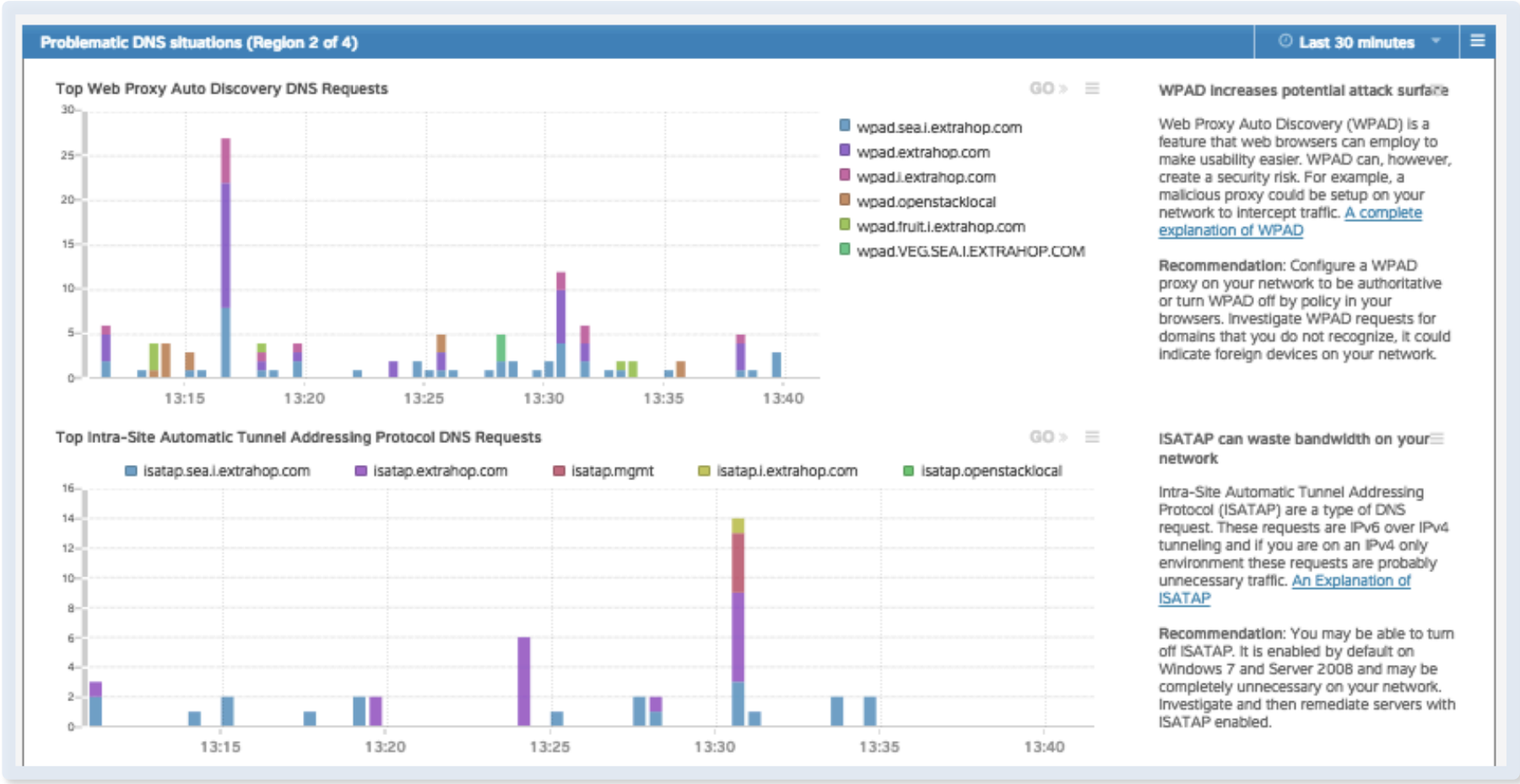
DNS MONITORING AND ANALYSIS DASHBOARD

DNS errors and issues cause greater than 20% of Internet and application outages. DNS response errors and request timeouts can cause performance issues for application users. Furthermore, DNS is a common and vulnerable attack vector for botnets running distributed denial of service (DDOS) attacks. This dashboard surfaces DNS metrics that can warn you of potential performance issues or security vulnerabilities in your environment.



DNS MONITORING AND ANALYSIS

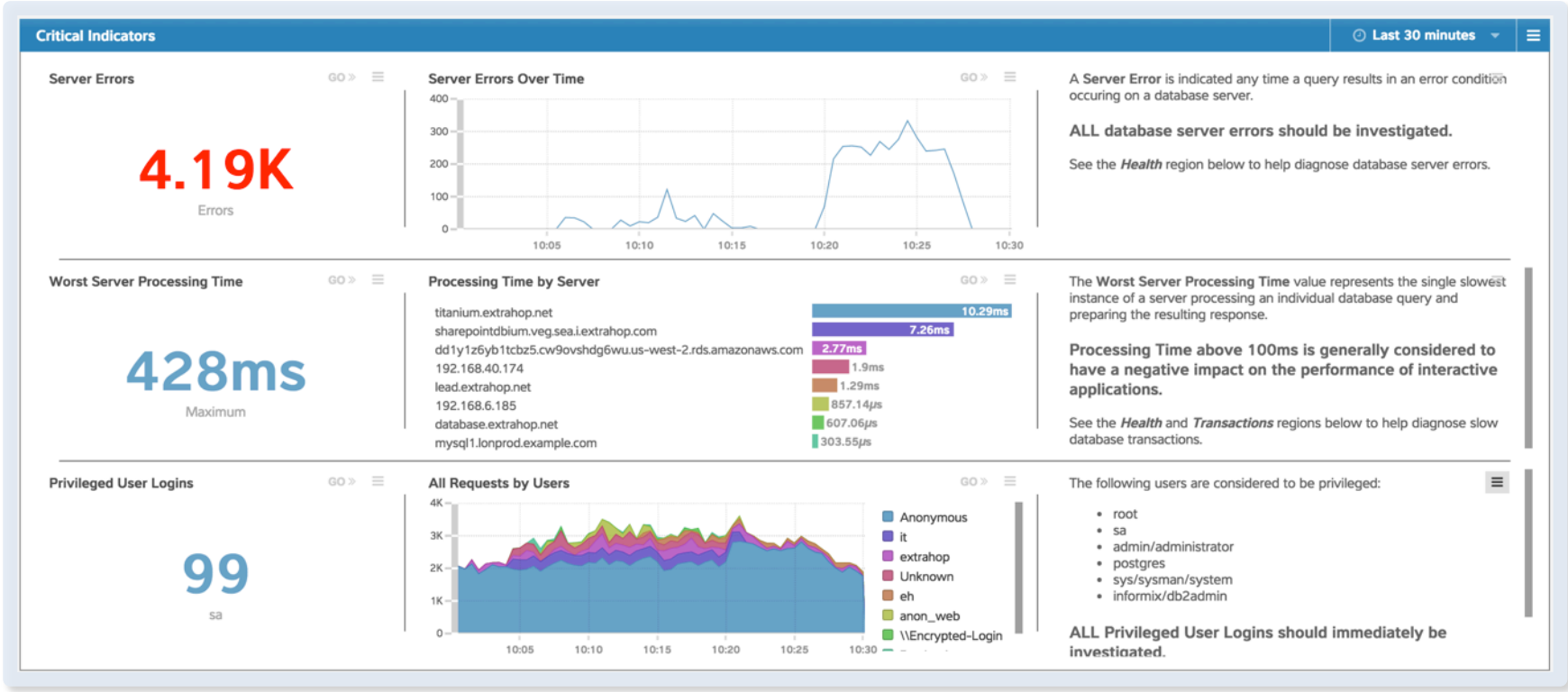
This dashboard displays instances of two types of DNS requests that can affect the performance and security of your network. The first is WPAD, which can provide an attack vector into your network, and the second is ISATAP, which wastes bandwidth if enabled unnecessarily.



DATABASE HEALTH AND PERFORMANCE MONITORING DASHBOARD

The Database Monitoring dashboard provides visibility into the health, performance, and transactions of the databases in your environment. Get real-time insight into a wide range of metrics, from the number of database server errors to total requests and responses over time. The time comparison feature also lets you compare current performance to historical trends, enabling easy baselining and ensuring that your have the visibility you need to proactively monitor the heath of your databases.

Database server errors and high processing times should be investigated since they impact application performance.



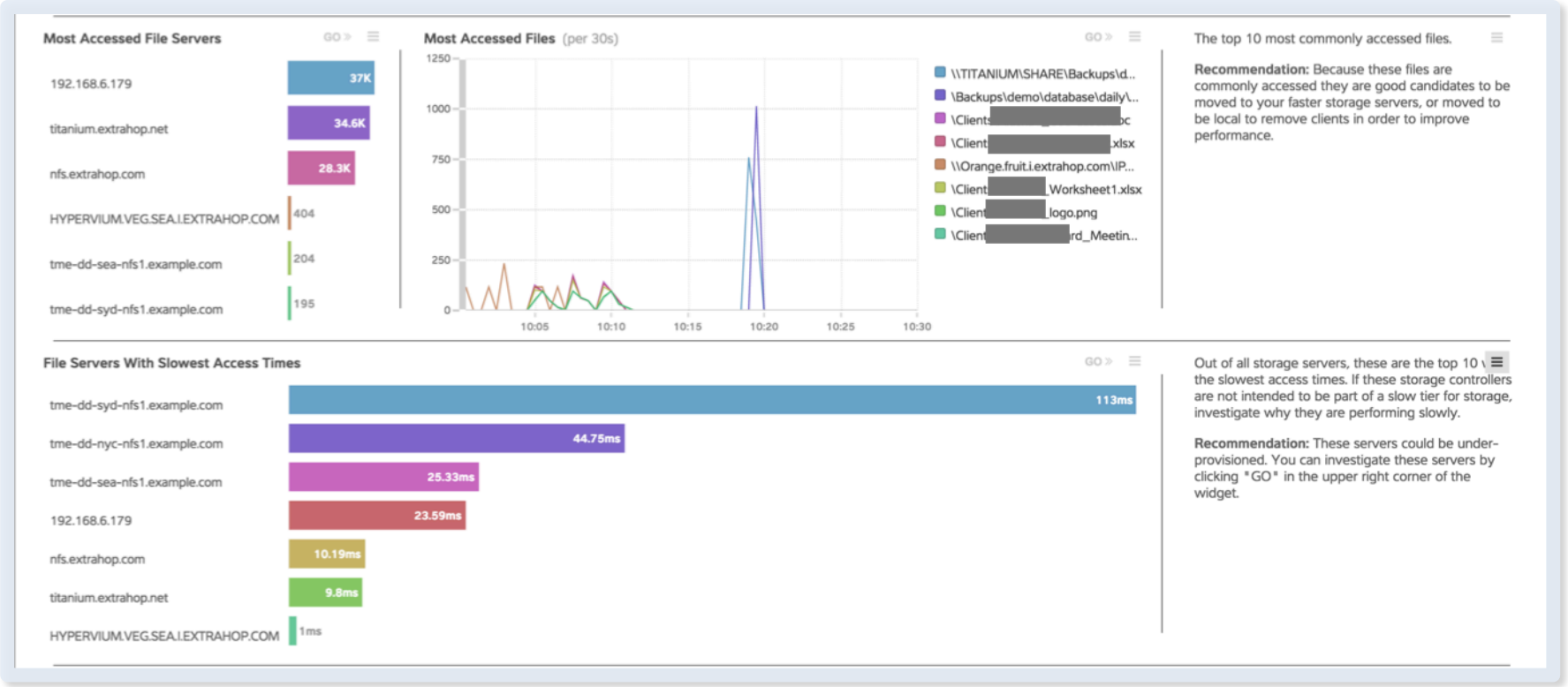
STORAGE MONITORING DASHBOARD

The Storage Monitoring dashboard surfaces storage metrics for CIFS, iSCSI, and NFS transactions. Storage performance is a crucial element for many applications, including database, virtualization, and VDI. The storage dashboards included in the project provide both the high-level overview and transaction-level details that storage teams need to rapidly identify, proactively fix, and avoid waste or unnecessary upgrades. Correlating storage activity the network and application level analysis. storage problems.

Here you can see the most accessed files. By optimizing the way these are delivered, you can improve user experience and reduce network resource expenditure.

STORAGE MONITORING DASHBOARD

Here you can see the most accessed files. By optimizing the way these are delivered, you can improve user experience and reduce network resource expenditure.



SMTP MONITORING DASHBOARDS

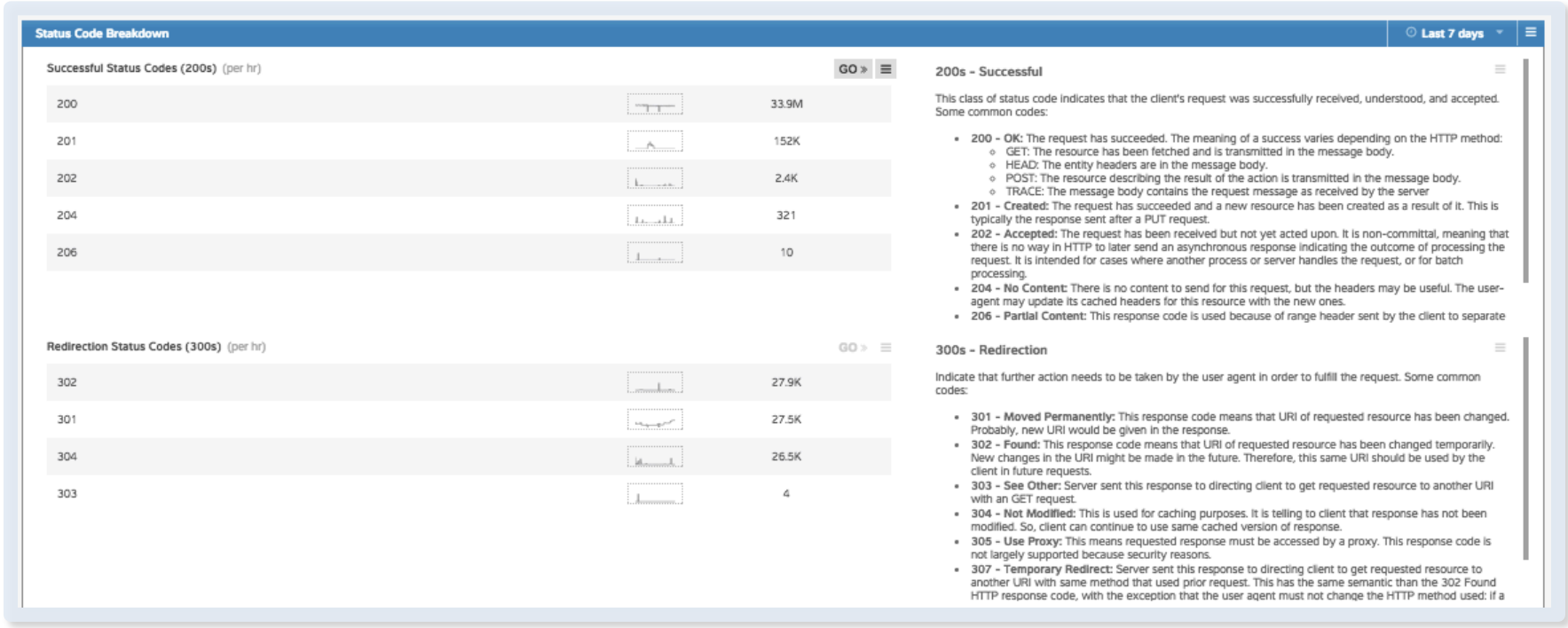
The SMTP Monitoring dashboard provides visibility into all SMTP traffic in your environment, helping you monitor SMTP performance that impacts email delivery. Track key metrics like request/response activity, errors, server processing time, and the number of unencrypted sessions in real time to quickly locate email issues that could disrupt business operations.

WEB OPTIMIZATION AND INSIGHTS DASHBOARDS

The Web Optimization Dashboard shows errors, frequently requested resources, responses and response-types, and round-trip-time measurements for requests on your website and web applications. For businesses that earn business, generate leads, or make sales through their websites, improving performance and reducing errors leads to significant improvement in conversion rates and revenue.

WEB OPTIMIZATION AND INSIGHTS DASHBOARDS

This dashboard region shows occurrences of successful status codes and redirects, which are indicators of how frequently your users are getting what they expect or being redirected to another asset. If you're seeing too many of any of these codes except for 200s, there may be a problem or an opportunity for optimization in your website.



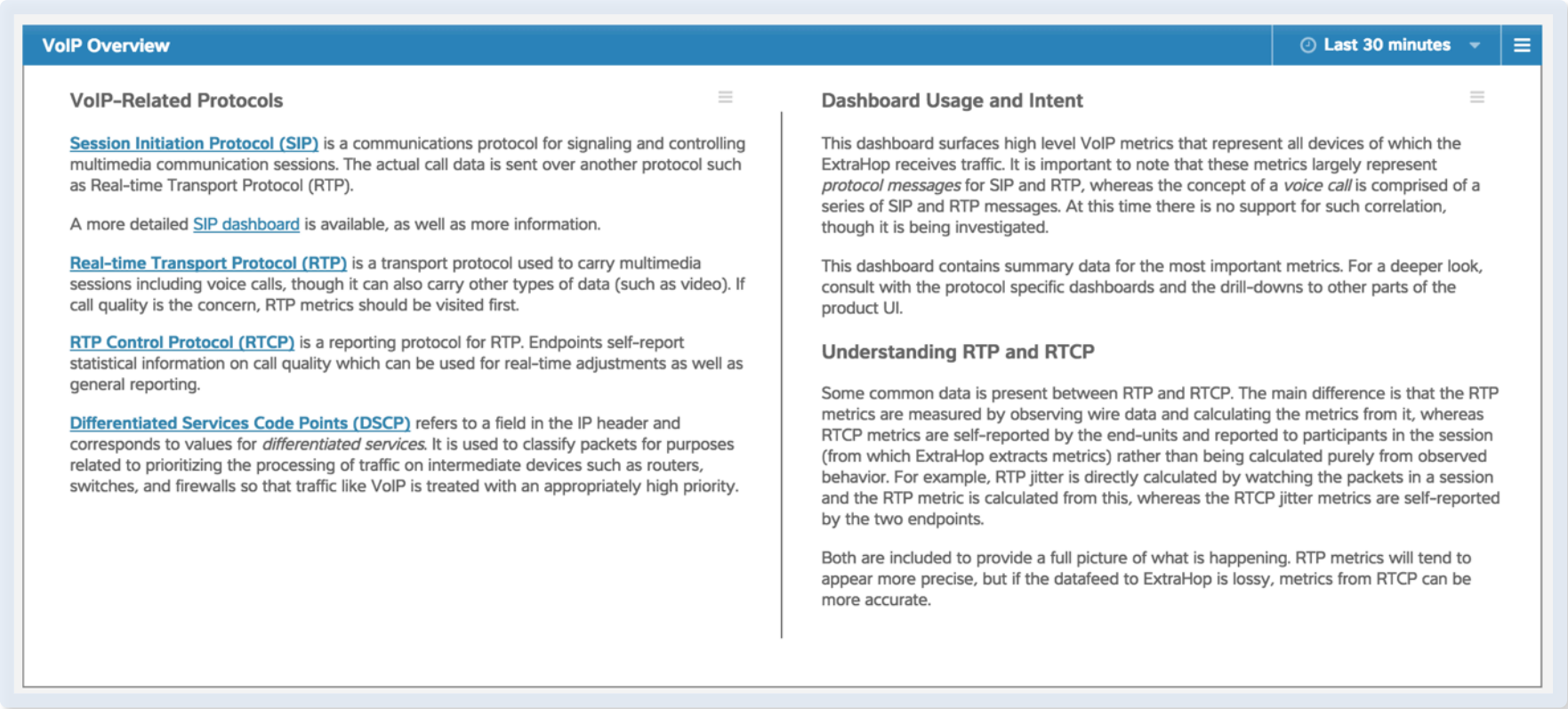
VOIP MONITORING DASHBOARD

The VoIP Monitoring dashboard surfaces high level VoIP metrics that represent all devices for which the ExtraHop receives traffic. The ExtraHop platform performs real-time analysis for call setup and control, and call quantity and quality for all VOIP sessions. In addition to an overview dashboard for all VoIP protocols, the project also includes a dashboard for observed detailed metrics for the Session Initiation Protocol (SIP) as well as for combined detailed metrics for Real-time Transport Protocol (RTP), RTP Control Protocol (RTCP), and Differentiated Services Code Points (DSCP).

Here you see the worst MOS scores and jitter from the observed period. MOS and jitter are the metrics used to determine call quality, so you should use this view to track VoIP service levels.

VOIP MONITORING DASHBOARD

The VoIP Monitoring overview dashboard also includes explanatory text concerning the purpose of the dashboard and the protocols that it displays metrics for. This section also contains explanations for and links to four sub-dashboards that drill down into each protocol activity.



CLOUD APP MONITORING DASHBOARDS

The Cloud application dashboard shows what activities are driving the most Network Traffic and how that corresponds to total network traffic. This gives the organization visibility into the types of cloud applications and web services that are being consumed by its users and systems creating a holistic view of network performance, cloud investments, employee productivity, and activities that fall out of compliance.

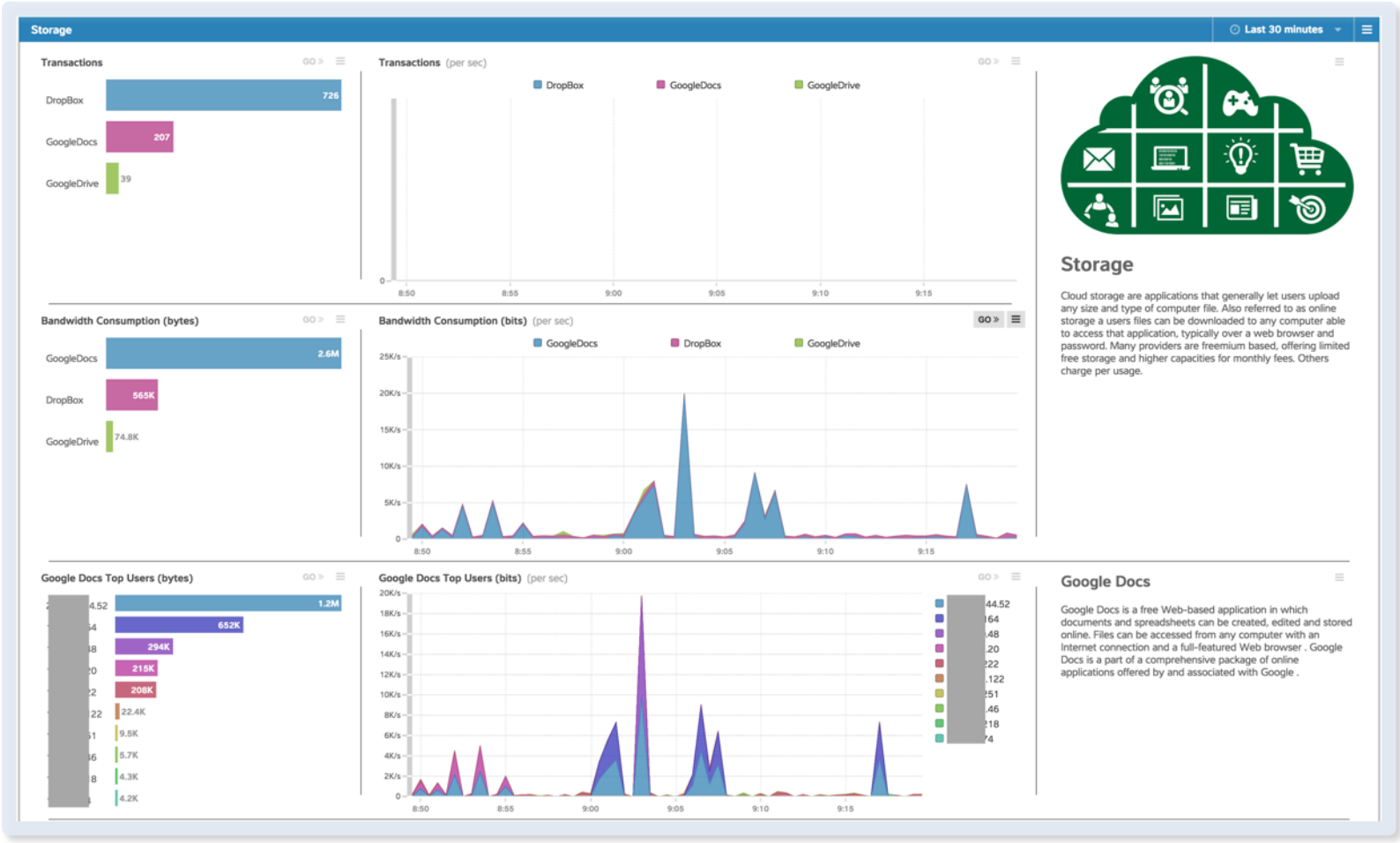
*The **Cloud Application overview** section of the dashboard shows bandwidth being consumed by internet usage and cloud applications. There are several views varying from total amount of bytes consumed, to utilization over time, as well as a breakdown of total network bandwidth vs. cloud application bandwidth consumed. This information can be critical when the network is reaching max load, or is experiencing a slowdown in isolating the root cause or finding low value workloads to reduce bandwidth consumption on.*

CLOUD APP MONITORING DASHBOARDS

*The **Marketing Cloud Applications** dashboard provides usage statistics on all cloud marketing applications. This can provide IT with an understanding of the behavior and performance of the applications critical to driving revenue in the business. In addition this dashboard provides a count of active users which can assist in Cloud License Management to keep costs down. Visualizations of transactions by cloud app., bandwidth consumed, user count, and top users are all surfaced.*

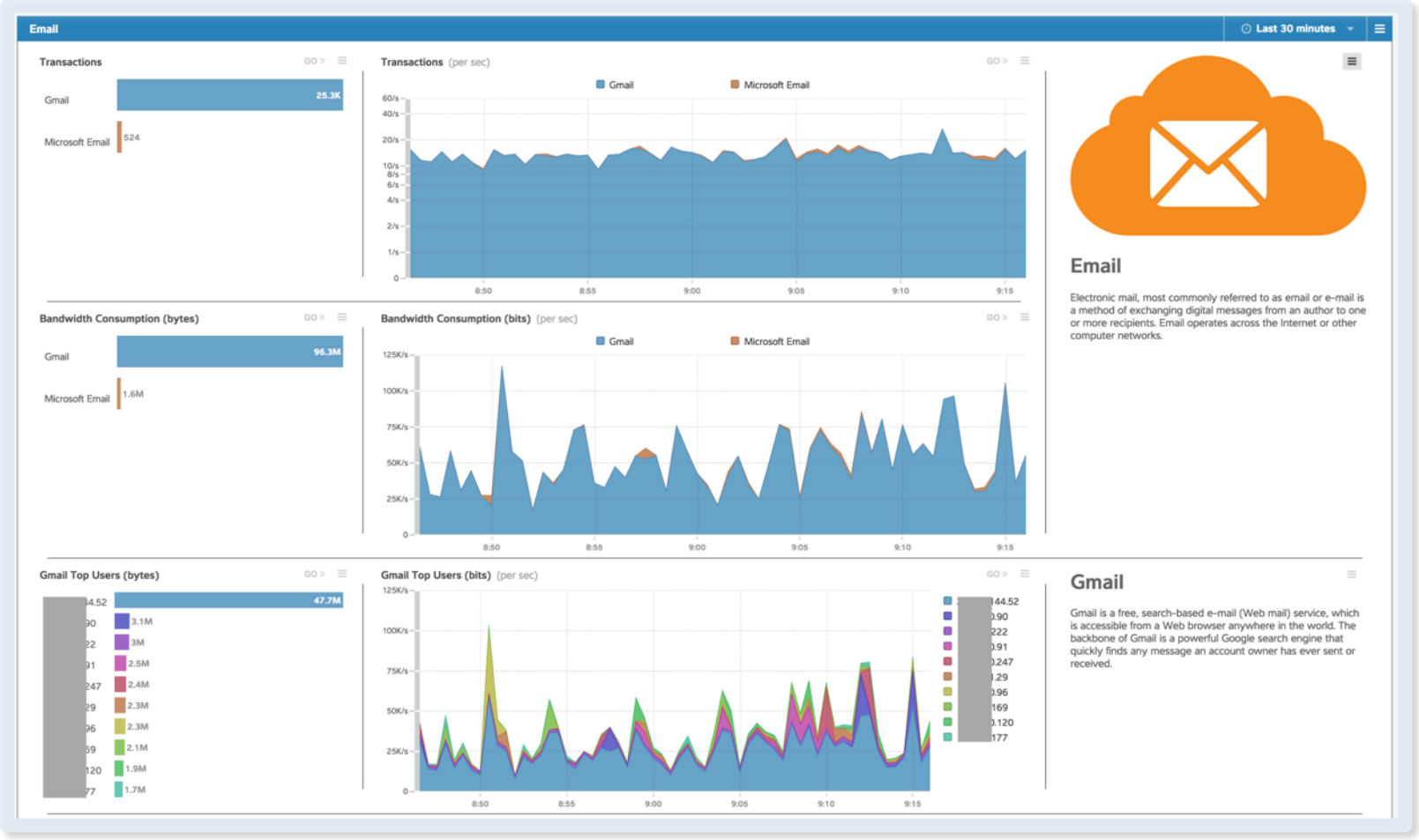
CLOUD APP MONITORING DASHBOARDS

*This section of **Cloud Storage Applications** dashboard focuses on cloud storage traffic. Depending on your internal security and compliance objectives this could be useful in uncovering areas where there may be failures to adhere to policy, and can also identify data exfiltration as it is occurring. Visualizations of this data include the amount of data stored, top users, as well as geo-location.*



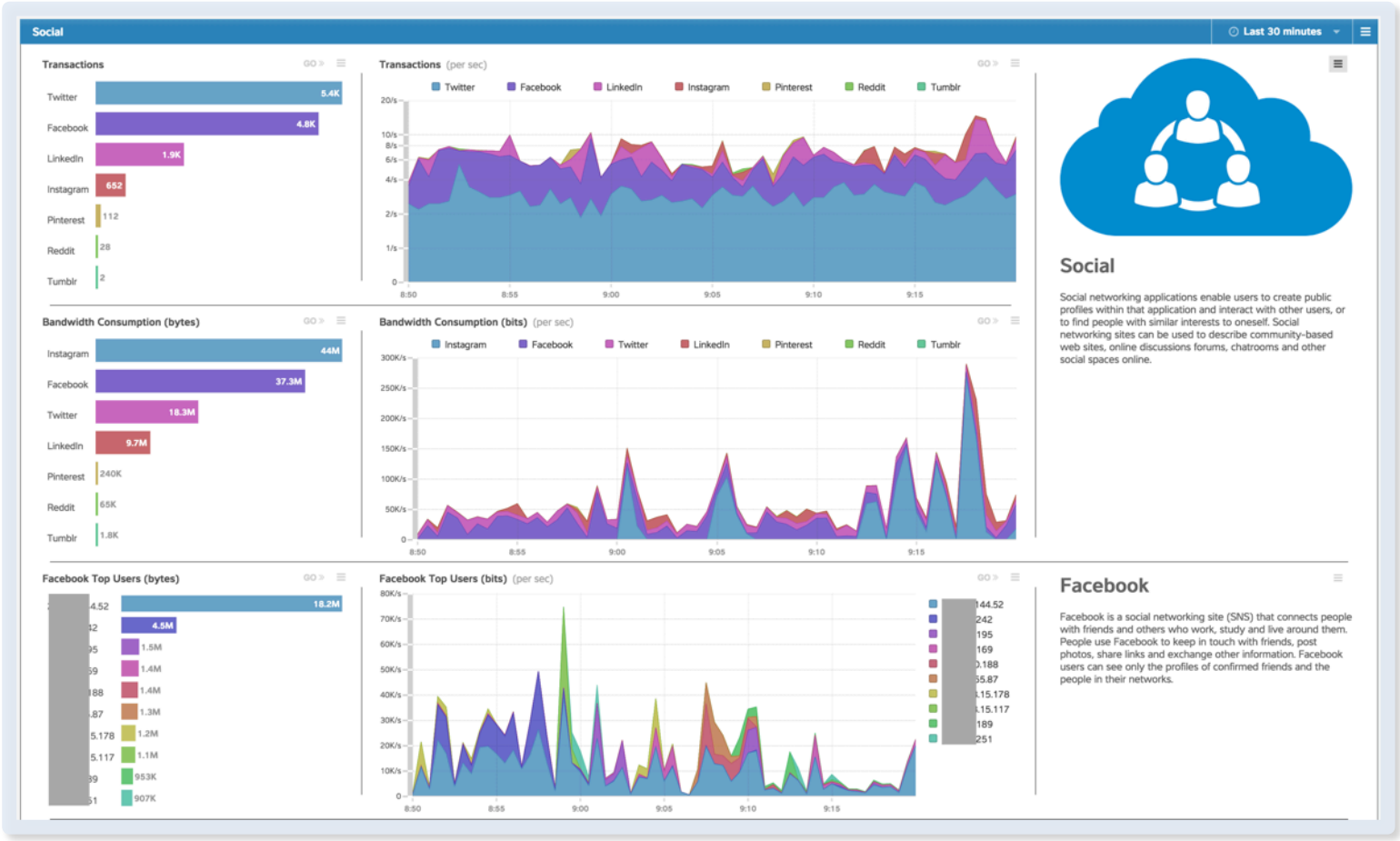
CLOUD APP MONITORING DASHBOARDS

*The **Cloud Email Applications** dashboard provides usage for cloud based email services. This can be used either to manage a company's own email systems or to monitor for security & violations using consumer based emails to transfer data. Visualizations of transactions by cloud app., bandwidth consumed, user count, and top users are all surfaced.*

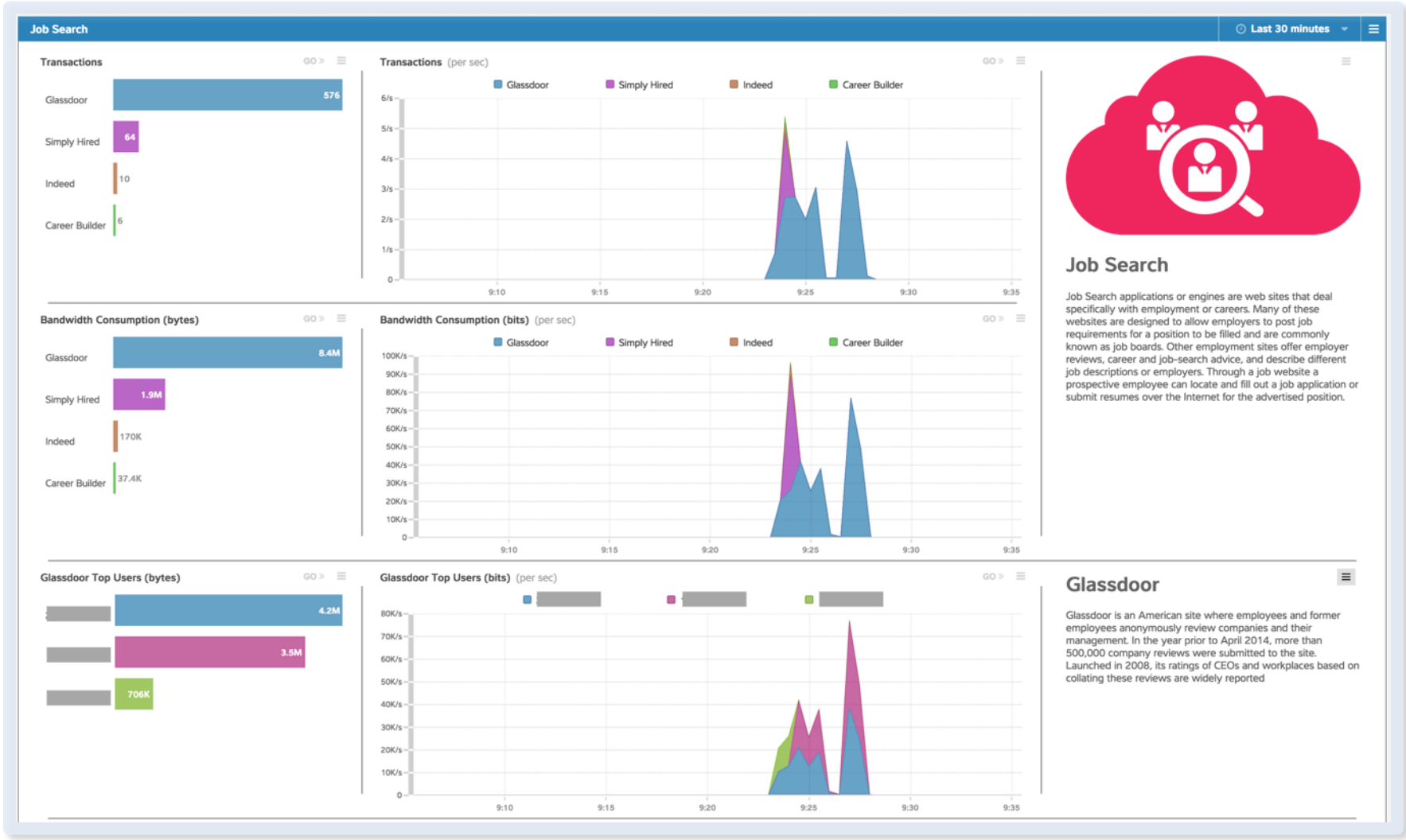


CLOUD APP MONITORING DASHBOARDS

*The **Social Cloud Applications** dashboard monitors social media traffic which can be an indicator of employee productivity losses, and in some cases can have a detrimental effect on your network. Dashboards include transactions by site, bandwidth consumed, and top users all across major social media networks.*



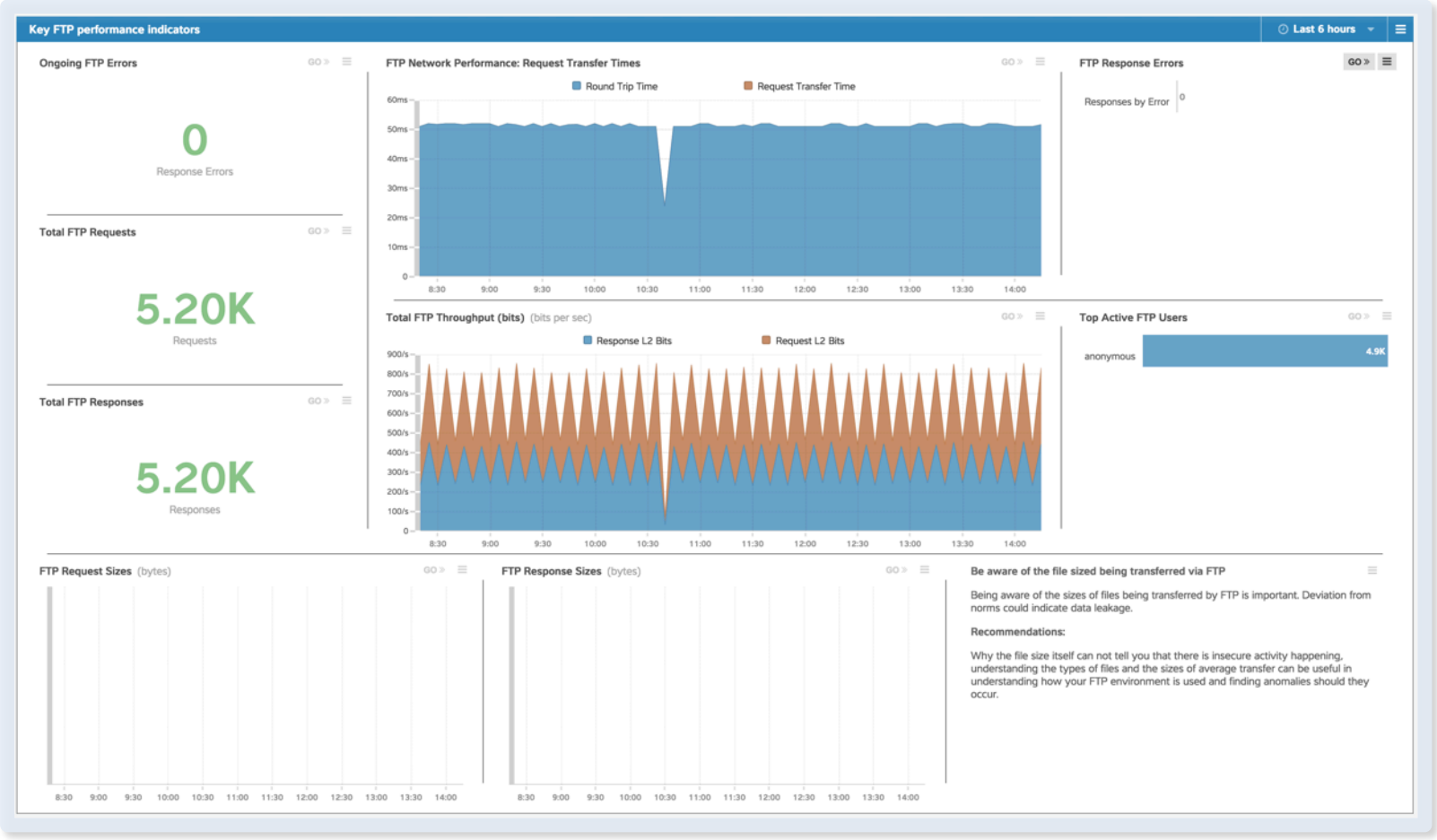
CLOUD APP MONITORING DASHBOARDS



FTP MONITORING DASHBOARDS

The FTP Monitoring dashboard provides a comprehensive view of all FTP activity in your environment. Details such as file names and the geographic origin of requests are also available. With this holistic, real-time view, IT staff can identify unauthorized or insecure FTP activity, monitor business-critical FTP services, and troubleshoot FTP issues.

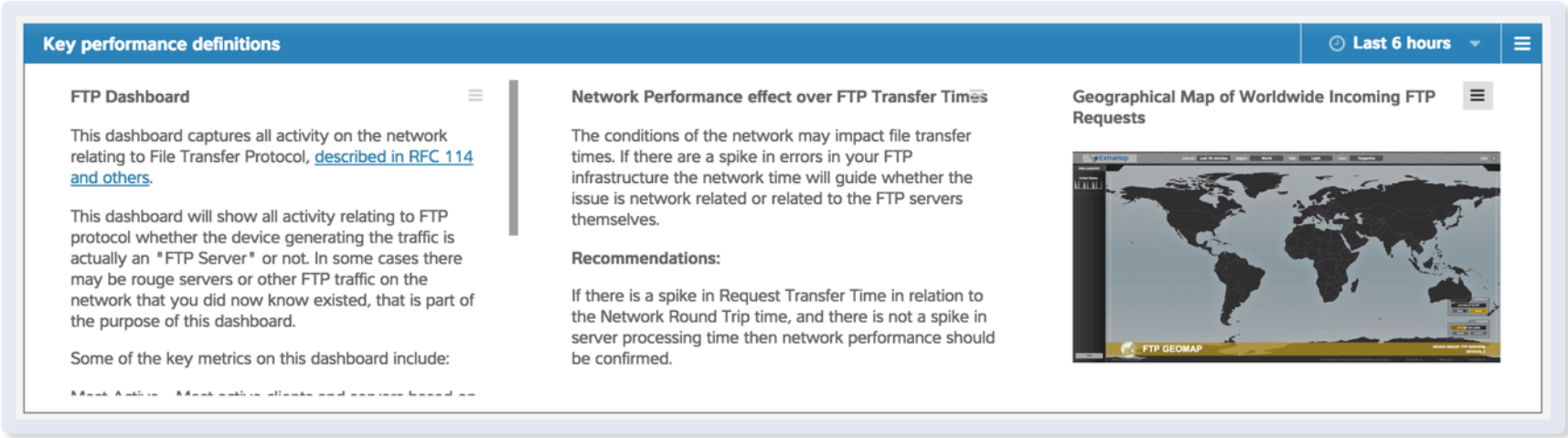
Here, at the top of the dashboard, you see errors, network impact, top users, and overall activity metrics.



FTP MONITORING DASHBOARDS

The dashboard includes explanatory information regarding key performance indicators for FTP services and how network performance can impact FTP performance.

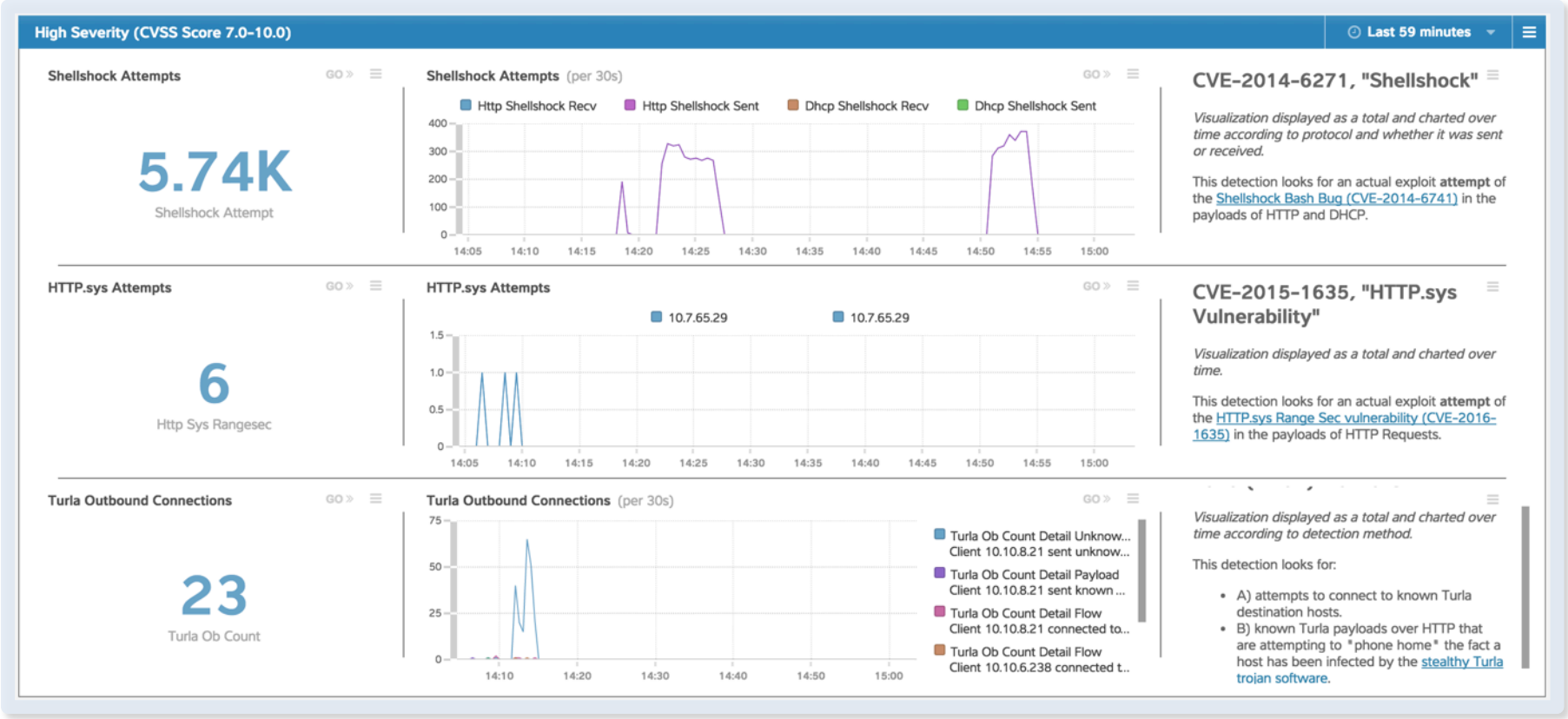
In addition, there is a link to a geomap that displays the geographic origin of FTP requests. Requests that originate outside of known business locations should be investigated as they could represent hackers attempting to exfiltrate data.



SECURITY VULNERABILITY MONITORING DASHBOARDS

The Security Vulnerability Monitoring dashboards track specific exploit attempts in your environment. It is important to note that these are attempts and not necessarily successful attacks. The ExtraHop platform detects these attempts through the analysis of communications on the wire. Exploits and malware tracked include Shellshock, HTTP.sys, Turla, Heartbleed, BIND DNS TKEY, POODLE, Logjam, and FREAK.

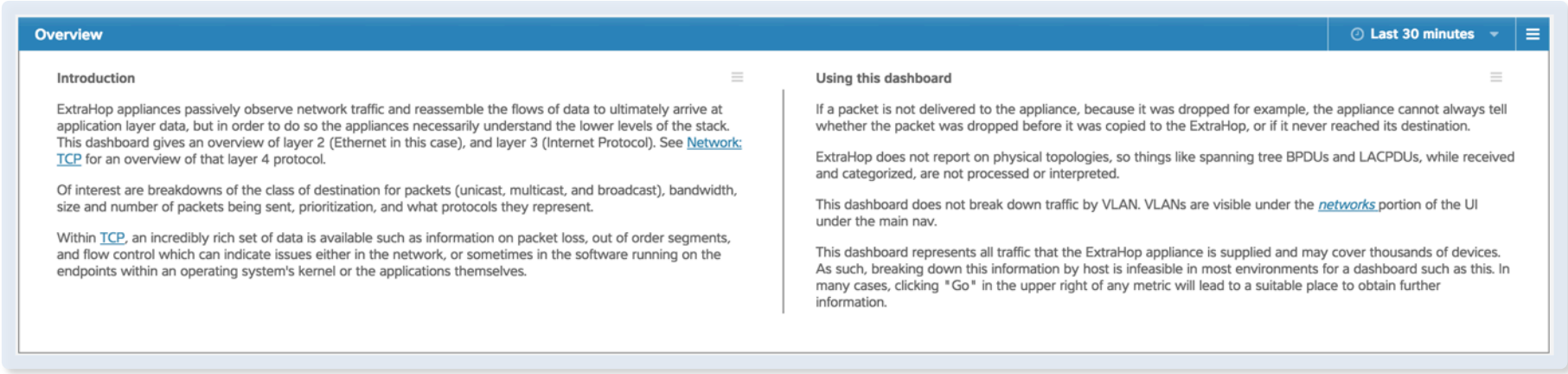
The section of the dashboard below tracks high-severity exploit attempts that could represent serious compromises to security. The security team should be aware of these attempts as they may not be recorded elsewhere or available in a timely manner. Once they have compromised a machine, malicious actors will often turn off logging to hide their activity.



NETWORK HEALTH AND UTILIZATION DASHBOARDS

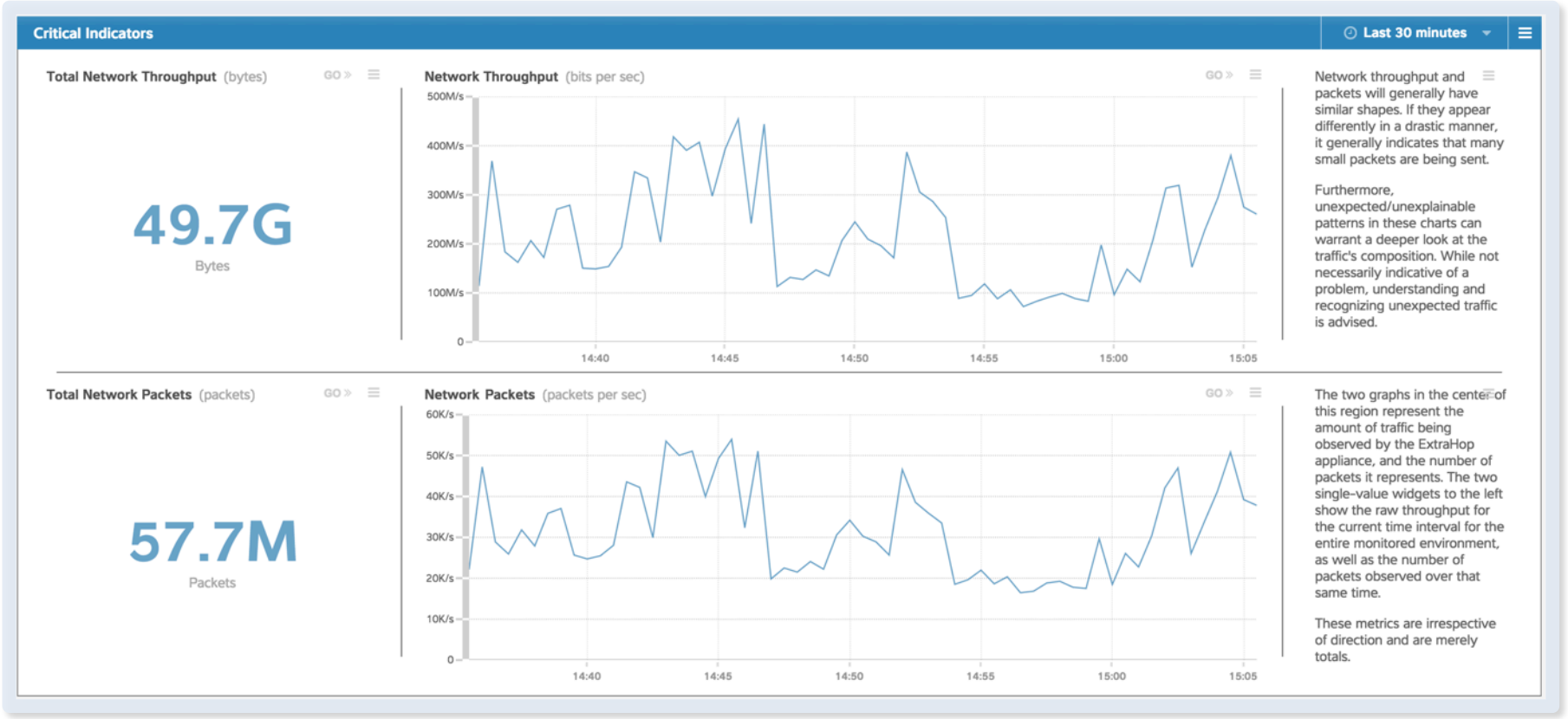
Network teams frequently lack an up-to-date understanding of the health and utilization of their entire network. While traditional technologies such as SNMP, NetFlow, and packet sniffing can provide some visibility into specific network links and devices, obtaining a holistic and real-time view of the entire network is nearly impossible with those technologies. The Network Health and Utilization dashboards provide this missing overview, with the ability to drill down into specific protocol activity and devices.

The Network Overview dashboard starts off with an introduction to the metrics covered, which follow the OSI model for computer-to-computer communications, along with instructions on how to use the dashboard for daily monitoring of network health and utilization.



NETWORK HEALTH AND UTILIZATION DASHBOARDS

The Network Overview dashboard features critical indicators for network health and utilization. The time period covered can be controlled with the drop-down selector in the top right corner and can include time-period comparisons.

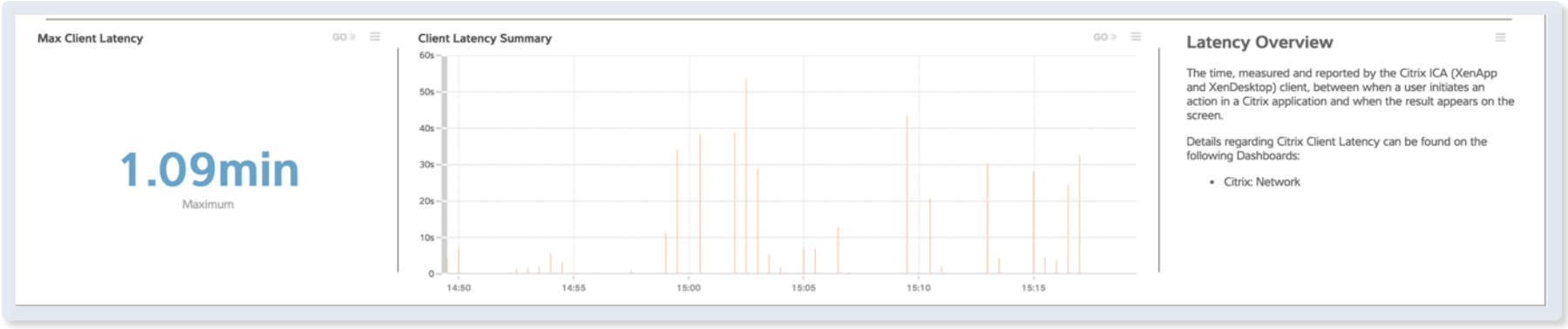


CITRIX MONITORING DASHBOARDS

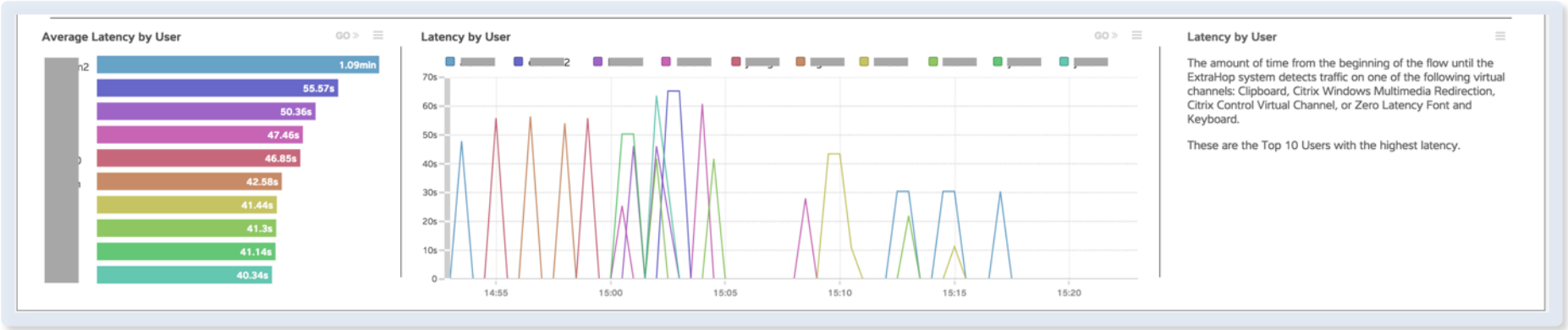
Citrix affects the productivity of a huge number of workers in your organization. Performance troubles like slow logins and application loading can create a negative user experience and reduced productivity across the whole business. This dashboard shows the number of times someone in your organization has launched a Citrix session for a given window of time, as well as the number of times they aborted a launch, and the maximum load time a launch experienced.

CITRIX MONITORING DASHBOARDS

Client latency is a measure of how quickly a client, usually a user's computer, is communicating with the Citrix servers. High client latency numbers mean that someone in your organization is having to wait a long time between when they take an action, and when the result appears on their screen.

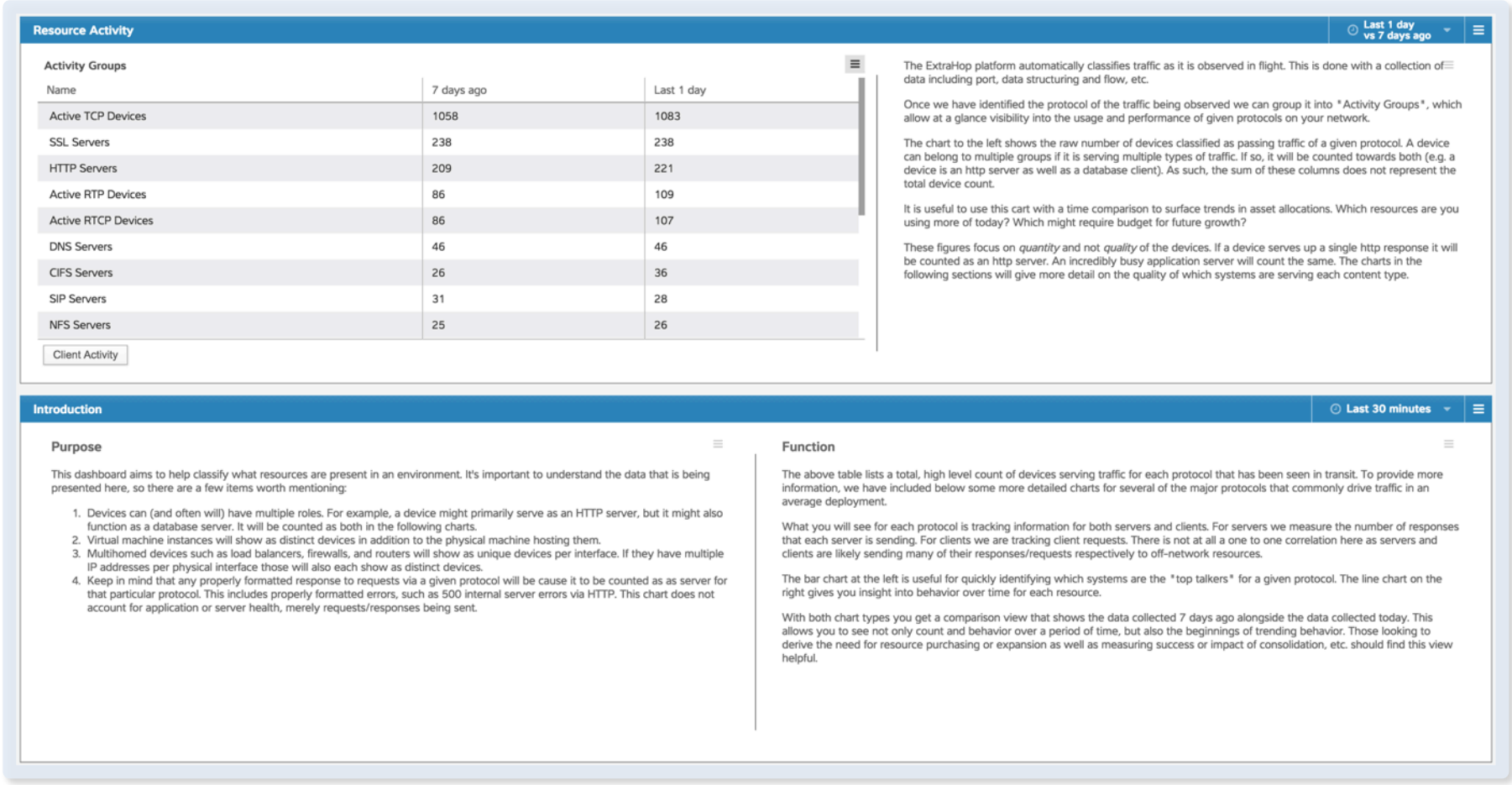


Average latency by user is exactly what it sounds like. Which users are getting the most latency when they use their Citrix applications. High latency indicates poor performance, so these users are probably frustrated and would appreciate remediation.



ASSET CLASSIFICATION DASHBOARDS

The Asset classification dashboards provide a central view of all devices on your network. ExtraHop makes it easy to discover and catalogue the functions of your devices to support better manageability of your environment. With this visibility you can identify rogue systems, protocols that shouldn't be used, capacity plan, and decommission/consolidate assets.



Resource Activity — Last 1 day vs 7 days ago

Activity Groups

Name	7 days ago	Last 1 day
Active TCP Devices	1058	1083
SSL Servers	238	238
HTTP Servers	209	221
Active RTP Devices	86	109
Active RTCP Devices	86	107
DNS Servers	46	46
CIFS Servers	26	36
SIP Servers	31	28
NFS Servers	25	26

Client Activity

The ExtraHop platform automatically classifies traffic as it is observed in flight. This is done with a collection of data including port, data structuring and flow, etc.

Once we have identified the protocol of the traffic being observed we can group it into *Activity Groups*, which allow at a glance visibility into the usage and performance of given protocols on your network.

The chart to the left shows the raw number of devices classified as passing traffic of a given protocol. A device can belong to multiple groups if it is serving multiple types of traffic. If so, it will be counted towards both (e.g. a device is an http server as well as a database client). As such, the sum of these columns does not represent the total device count.

It is useful to use this cart with a time comparison to surface trends in asset allocations. Which resources are you using more of today? Which might require budget for future growth?

These figures focus on *quantity* and not *quality* of the devices. If a device serves up a single http response it will be counted as an http server. An incredibly busy application server will count the same. The charts in the following sections will give more detail on the quality of which systems are serving each content type.

Introduction — Last 30 minutes

Purpose

This dashboard aims to help classify what resources are present in an environment. It's important to understand the data that is being presented here, so there are a few items worth mentioning:

1. Devices can (and often will) have multiple roles. For example, a device might primarily serve as an HTTP server, but it might also function as a database server. It will be counted as both in the following charts.
2. Virtual machine instances will show as distinct devices in addition to the physical machine hosting them.
3. Multihomed devices such as load balancers, firewalls, and routers will show as unique devices per interface. If they have multiple IP addresses per physical interface those will also each show as distinct devices.
4. Keep in mind that any properly formatted response to requests via a given protocol will be cause it to be counted as as server for that particular protocol. This includes properly formatted errors, such as 500 internal server errors via HTTP. This chart does not account for application or server health, merely requests/responses being sent.

Function

The above table lists a total, high level count of devices serving traffic for each protocol that has been seen in transit. To provide more information, we have included below some more detailed charts for several of the major protocols that commonly drive traffic in an average deployment.

What you will see for each protocol is tracking information for both servers and clients. For servers we measure the number of responses that each server is sending. For clients we are tracking client requests. There is not at all a one to one correlation here as servers and clients are likely sending many of their responses/requests respectively to off-network resources.

The bar chart at the left is useful for quickly identifying which systems are the *top talkers* for a given protocol. The line chart on the right gives you insight into behavior over time for each resource.

With both chart types you get a comparison view that shows the data collected 7 days ago alongside the data collected today. This allows you to see not only count and behavior over a period of time, but also the beginnings of trending behavior. Those looking to derive the need for resource purchasing or expansion as well as measuring success or impact of consolidation, etc. should find this view helpful.

ASSET CLASSIFICATION DASHBOARDS

This dashboard shows the most active HTTP and HTTPS Servers that have been identified in the period specified, as well as their activity over time. You can also discover the least active servers as well during the time period by clicking into the details and setting sort to least active.