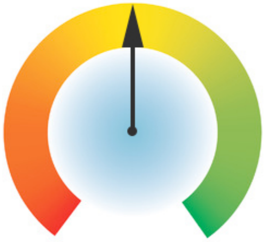
This sample report demonstrates the type of analysis your organization will receive from an Atlas Services remote analysis report.

Annotations provided in this document highlight features of the report.

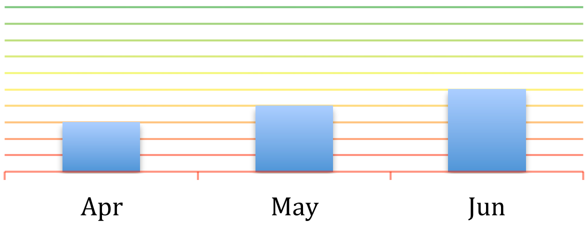
ExtraHop ATLAS SERVICES

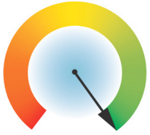
Remote Analysis Report

Enabling Continual Service Improvement in Critical Systems

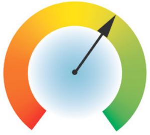


Overall Health

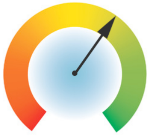




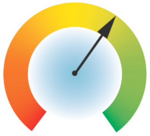
Web Application



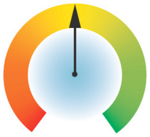
Database



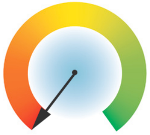
Middleware



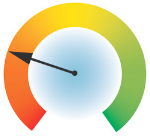
Citrix



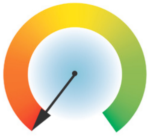
Storage



Supporting Application Infrastructure



Application Communication



Security

PREPARATION

Month: June 2016

Report: Sample

Prepared for:
Customer

Analyst:
Analyst
ExtraHop Networks

Configuration:
EDA9100

Firmware: 5.2

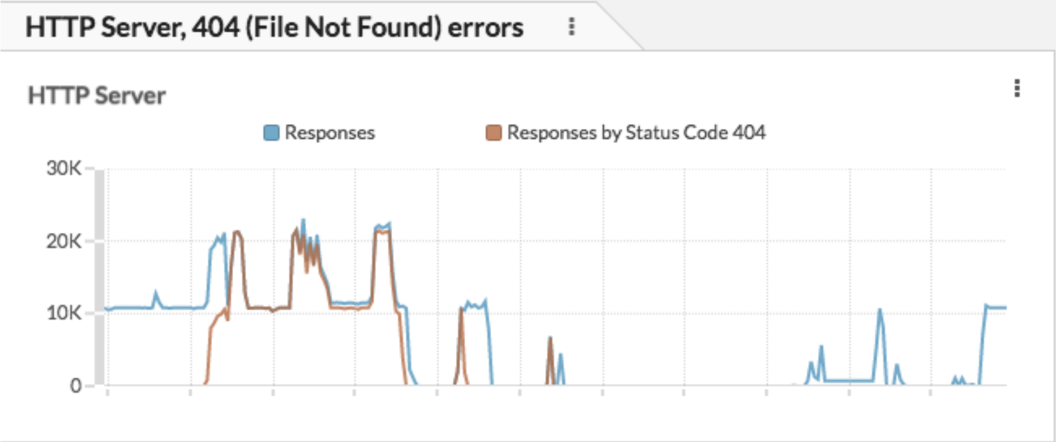
ID: XXXXX

Web Application

A review of the web application protocols including HTTP and HTTPS. More information regarding presentation of the HTTP protocol in the ExtraHop UI is available here.

Findings:

File Not Found errors (HTTP status code 404) on `device1` have significantly decreased. (Trend: Resolved)	



HTTP Server, 404 (File Not Found) errors

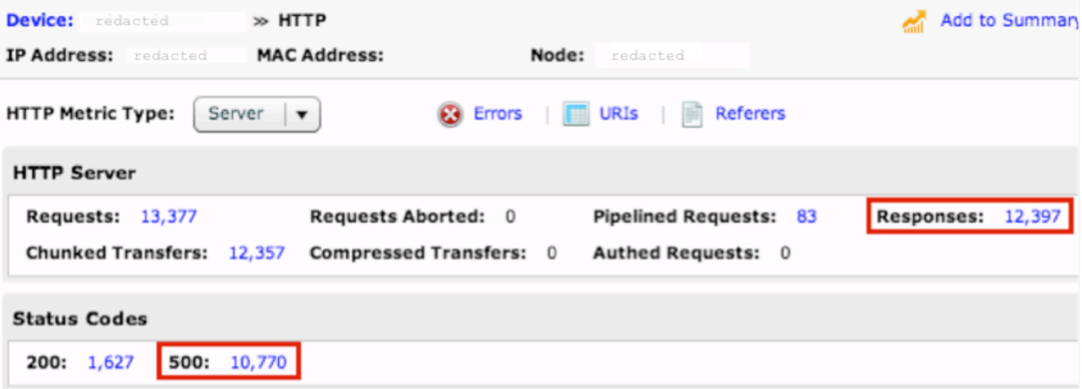
Investigate Internal Server errors (HTTP status code 500) that occurred on the ~~AAAAA~~ server and were associated with a single URI. Internal Server errors were not previously noted on this server. (New finding)	☀

Investigate improvements that can be made to the ~~ZZZZZ~~ server that experienced lengthy processing time on average. Processing time on this server has become less severe since the previous analysis period. (Trend: Improvement)	↗

Each piece of analysis comes with an indicator of how it compares with the previous report. An up-and-to-the-right arrow indicates improvement, a down arrow indicates degradation, and a star symbolizes a new finding.

CRITICAL CONCERNS:

86.9% of HTTP responses on the ~~AAAAA~~ server were Internal Server errors (HTTP status codes 500). Internal Server errors indicate that HTTP server encountered an unexpected condition that prevented it from fulfilling the request.



Device: redacted » HTTP — Add to Summary

IP Address: redacted **MAC Address:** **Node:** redacted

HTTP Metric Type: Server ▾ — Errors | URIs | Referers

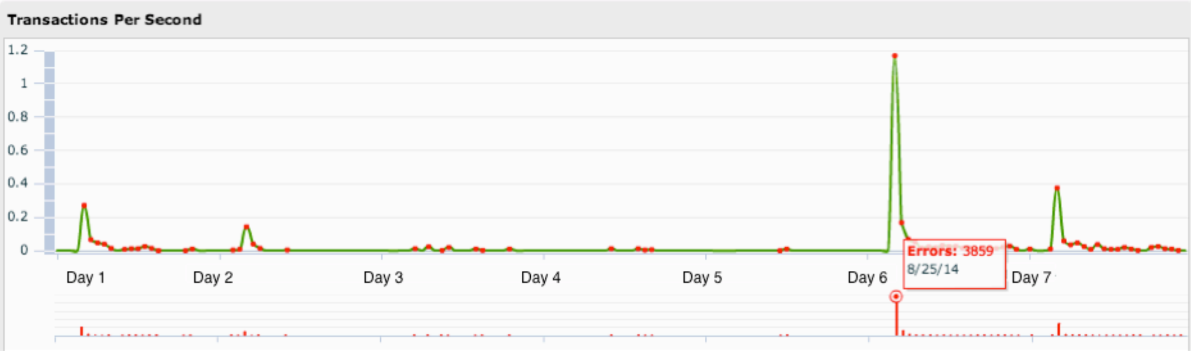
HTTP Server

Requests: 13,377	Requests Aborted: 0	Pipelined Requests: 83	Responses: 12,397
Chunked Transfers: 12,357	Compressed Transfers: 0	Authed Requests: 0	

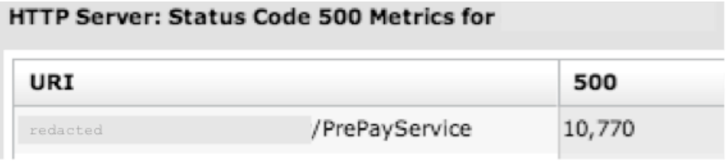
Status Codes

200: 1,627	500: 10,770

Internal Server errors on ~~AAAAA~~ (indicated by the vertical red bars) appeared to correlate with the HTTP transaction rate (indicated by the green line). At peak, 3,859 Internal Server errors occurred on this device in a single hour.



100% of Internal Server errors on ~~AAAAA~~ occurred while attempting to access a single URI resource, ~~xxxx.xxxxxxxx~~/PrePayService.



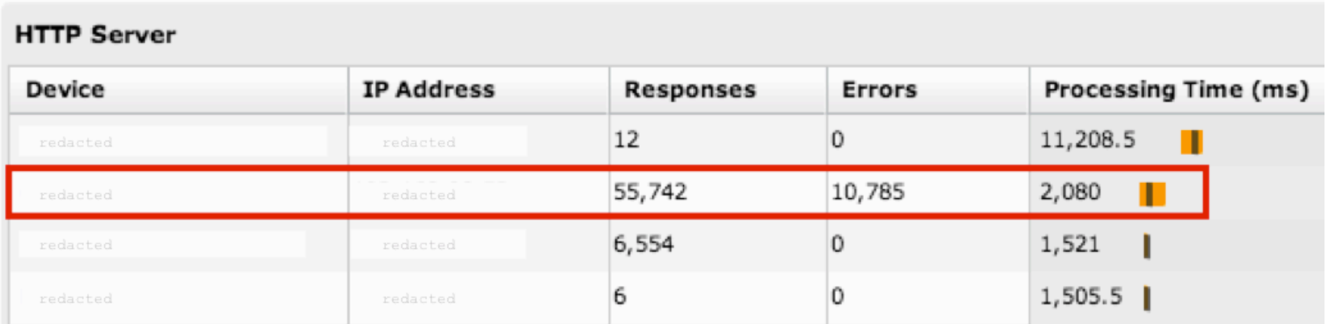
HTTP Server: Status Code 500 Metrics for

URI	500
redacted /PrePayService	10,770

Trend graphs make it easy to determine if errors occur during acute events or if they are part of a chronic problem.

IMPROVEMENT OPPORTUNITIES:

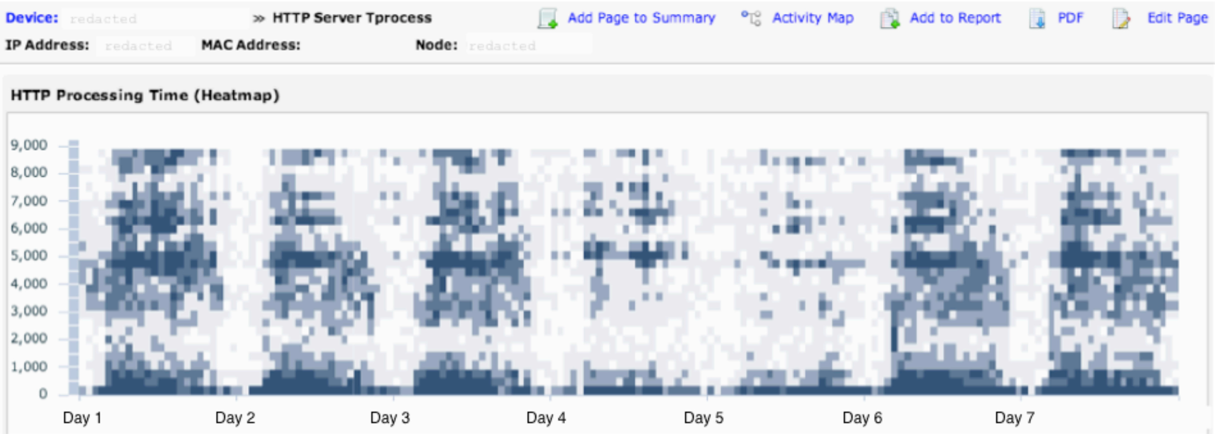
Several HTTP servers are experiencing lengthy processing time on average. Notice that the ~~zzzzz~~ server accounted for 55,742 responses and experienced an average processing time of over 2 seconds.



HTTP Server

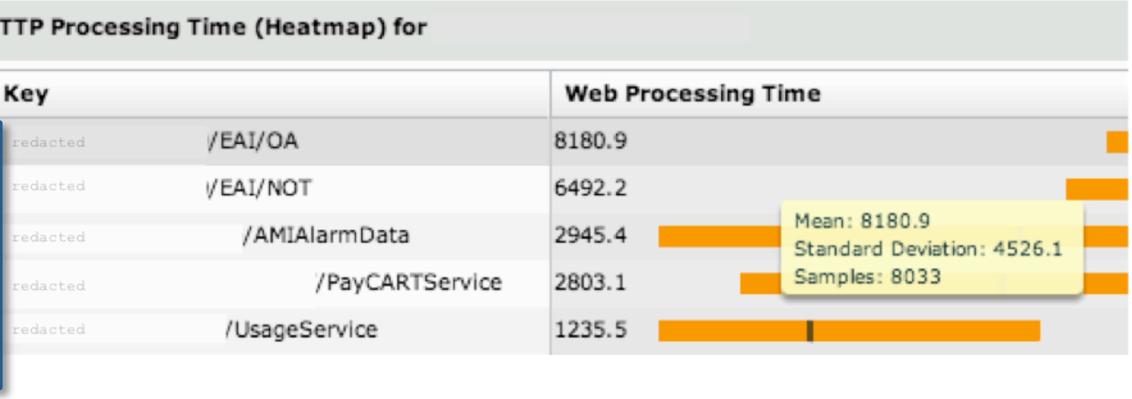
Device	IP Address	Responses	Errors	Processing Time (ms)
redacted	redacted	12	0	11,208.5
redacted	redacted	55,742	10,785	2,080
redacted	redacted	6,554	0	1,521
redacted	redacted	6	0	1,505.5

Utilizing the ExtraHop Heatmaps feature, we see that a high concentration of transactions on ~~zzzzz~~ experienced approximately 5 seconds of processing time. A darker area on the graph below indicates a high concentration of transactions.



Device: redacted » HTTP Server Tprocess
IP Address: redacted MAC Address: Node: redacted

Note the large standard deviation tied to processing time for the `xxx.xxx.xxx.xx:xxxx/EAI/OA` URI. This indicates that the processing times experienced for this URI were very "dispersed" and had a large amount of variation, meaning that much larger processing times were also observed. Using these standard deviation and mean measurements, we can conclude that approximately 1,277 transactions experienced processing times of approximately 12.7 seconds.



HTTP Processing Time (Heatmap) for

Key	Web Processing Time
redacted /EAI/OA	8180.9
redacted /EAI/NOT	6492.2
redacted /AMIAlarmData	2945.4
redacted /PayCARTService	2803.1
redacted /UsageService	1235.5

Mean: 8180.9
Standard Deviation: 4526.1
Samples: 8033

Each report includes different types of visualizations, optimized for the type of data being shown.

DATABASE

A review of all parsed database protocol traffic, regardless of the type of database. Protocols include (if licensed): TNS (Oracle), TDS (MS SQL), DB2, Informix, Sybase, PostgreSQL, and MySQL. More information regarding presentation of database protocols in the ExtraHop UI is available here.

FINDINGS:

Investigate database errors on the ~~BBBBB~~ server that occurred constantly; these errors were related to failed logins for the ZZZ_ZZZZZ database. (New finding)	☀

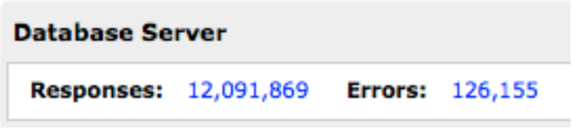
CRITICAL CONCERNS:

None noted.

Where appropriate, the Atlas report provides percentage calculations so that you can easily understand the relative impact of the findings.

IMPROVEMENT OPPORTUNITIES:

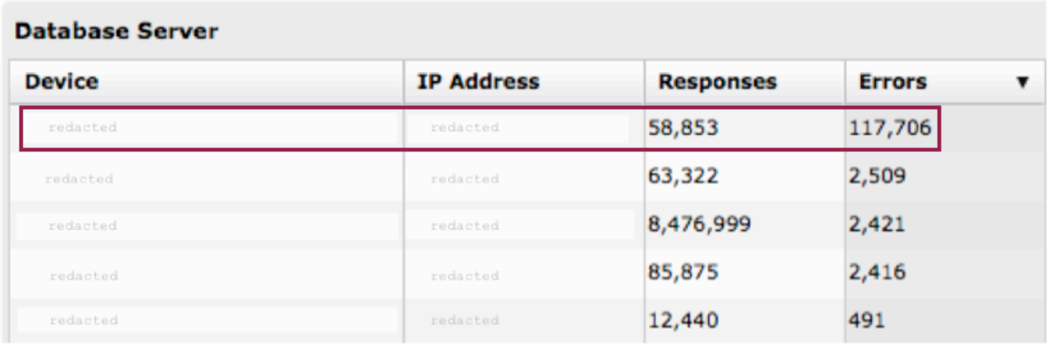
1.0% of all database responses were errors.



Database Server

Responses: 12,091,869 **Errors:** 126,155

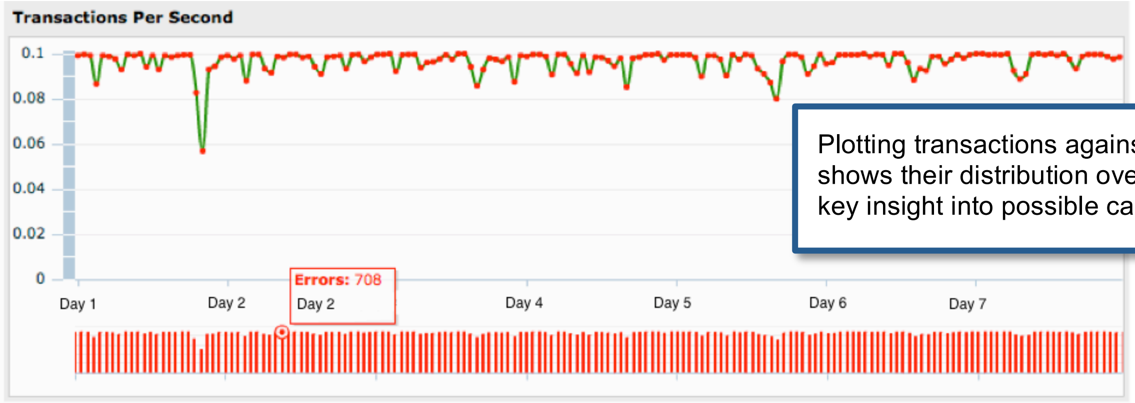
93.3% of database errors were concentrated on the ~~BBBBB~~ server. Also note that there were approximately twice as many errors on this server than there were responses, indicating that each response sent from this server corresponded to two error messages.



Database Server

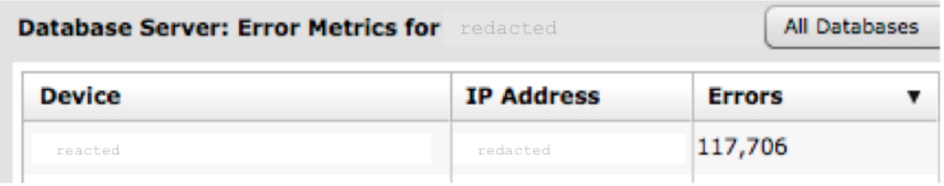
Device	IP Address	Responses	Errors ▼
redacted	redacted	58,853	117,706
redacted	redacted	63,322	2,509
redacted	redacted	8,476,999	2,421
redacted	redacted	85,875	2,416
redacted	redacted	12,440	491

Database error rate (indicated by the vertical red bars) on ~~BBBBB~~ directly correlated with overall database transaction rate (indicated by the green line). Both of these metrics remained approximately constant for the duration of the observation period. For the majority of the analysis period more than 700 database errors were sent from this server each hour.



Plotting transactions against errors shows their distribution over time—a key insight into possible causes.

100% of database errors from ~~BBBBB~~ were returned to the ~~YYYYYY~~ client.

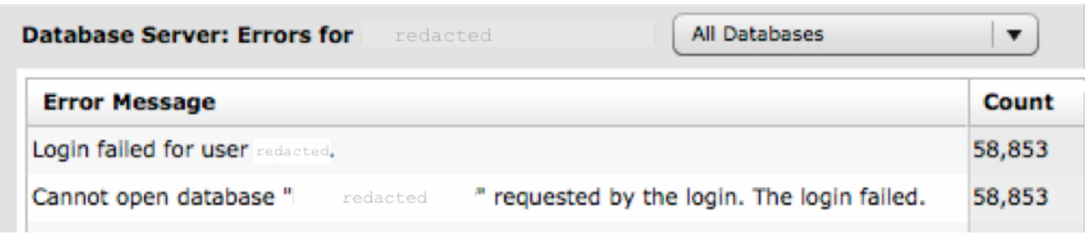


Database Server: Error Metrics for redacted

All Databases

Device	IP Address	Errors ▼
reacted	redacted	117,706

Database errors from ~~BBBBB~~ had two error messages. These error messages suggest that 100% of errors on ~~BBBBB~~ result from the ~~YYYYYY~~ client attempting to log on to ~~BBBBB~~ and open a ZZZ_ZZZZZ database. 100% of these login and open attempts are failing. Investigate scheduled tasks that may be causing these errors.

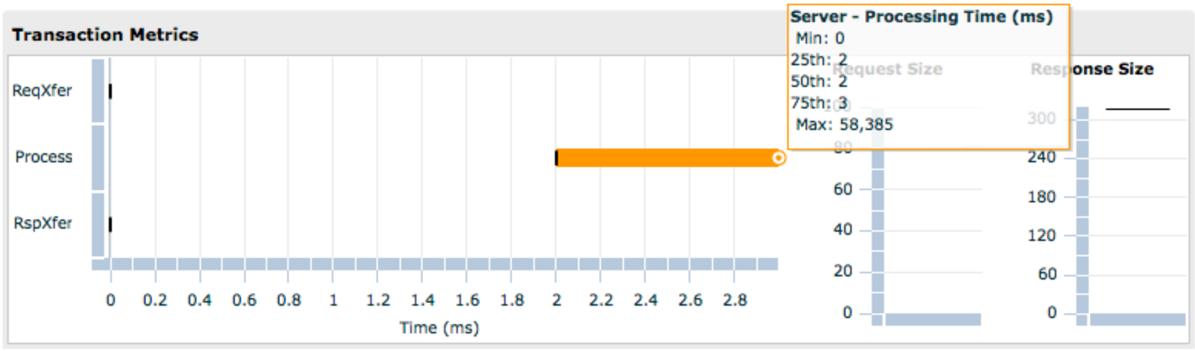


Database Server: Errors for redacted

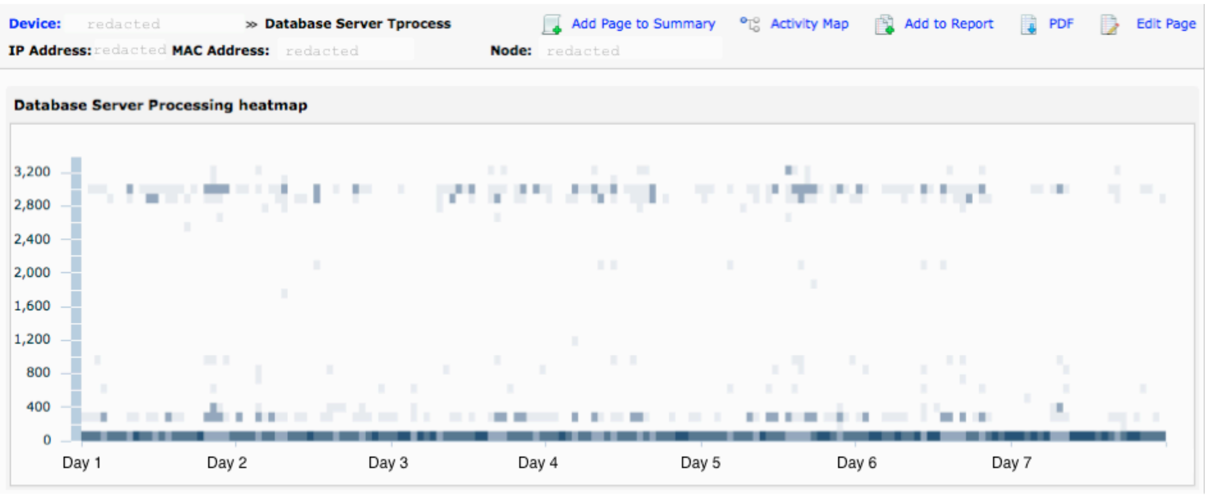
All Databases ▼

Error Message	Count
Login failed for user redacted.	58,853
Cannot open database " redacted " requested by the login. The login failed.	58,853

Also worth noting are the processing times observed on this database server. While a majority of transactions were non-concerning (75% of all database transactions took, at most, 3 milliseconds of processing time), note that database transactions on ~~BBBBB~~ experienced as much as a minute of processing time.



The ExtraHop Heatmaps feature reveals that a “concentration” of transactions experienced around 3 seconds (3,000 milliseconds) of processing time. A darker area on the graph below indicates a higher concentration of transactions so while a large volume of transactions experienced less than 400 milliseconds of processing time, it may be worth researching what is causing some of the previously discussed failed logins to experience such lengthy processing times.



Device: redacted » **Database Server Tprocess**

IP Address: redacted **MAC Address:** redacted **Node:** redacted

Database Server Processing heatmap

MIDDLEWARE

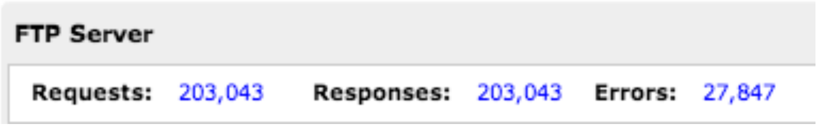
A review of all parsed middleware protocol traffic (if licensed): FTP, MQSeries, and Memcache. More information regarding presentation of the FTP protocol in the ExtraHop UI is available here.

FINDINGS:

Investigate FTP errors that occurred on the ~~ccccc~~ server that appeared to correlate with `SITE` method calls. Overall FTP error rate has decreased since the previous analysis period. (Trend: Improvement)	↗

CRITICAL CONCERNS:

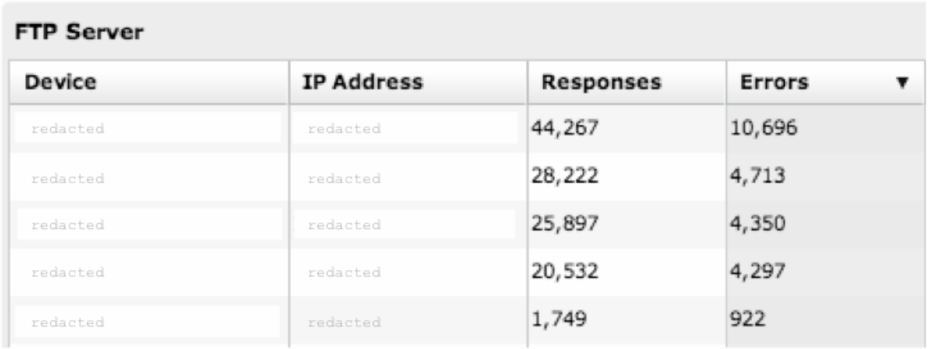
16.8% of FTP responses resulted in an error. This is a decrease from the 25.4% FTP error rate noted in the previous report.



FTP Server

Requests:	203,043	Responses:	203,043	Errors:	27,847

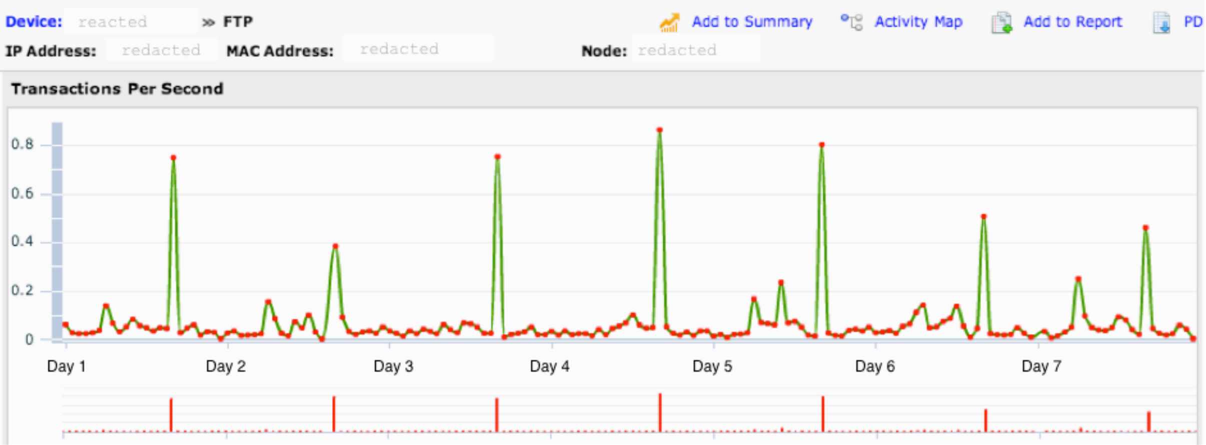
38.4% of FTP errors occurred on the ~~ccccc~~ server.



FTP Server

Device	IP Address	Responses	Errors ▼
redacted	redacted	44,267	10,696
redacted	redacted	28,222	4,713
redacted	redacted	25,897	4,350
redacted	redacted	20,532	4,297
redacted	redacted	1,749	922

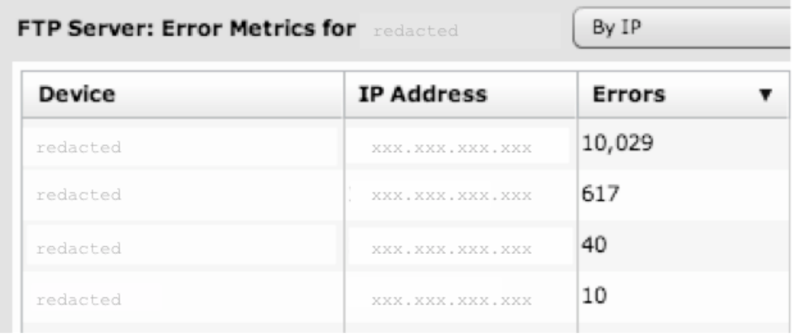
Spikes, in both FTP error rate (indicated by the vertical red bars) and transaction rate (indicated by the green line) on ~~ccccc~~, occurred at the same time each day. The nightly spike is highly suggestive of an automated FTP process that is broken or otherwise misconfigured.



Device: reacted » FTP

IP Address: redacted MAC Address: redacted Node: redacted

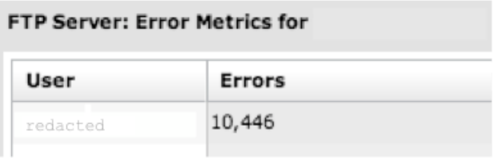
93.8% of FTP errors from ~~ccccc~~ were returned to the ~~device2~~ client.



FTP Server: Error Metrics for redacted

Device	IP Address	Errors ▼
redacted	xxx.xxx.xxx.xxx	10,029
redacted	xxx.xxx.xxx.xxx	617
redacted	xxx.xxx.xxx.xxx	40
redacted	xxx.xxx.xxx.xxx	10

100% of FTP errors from ~~ccccc~~ affected FTP transactions for the ~~xxx_xxx~~ user.

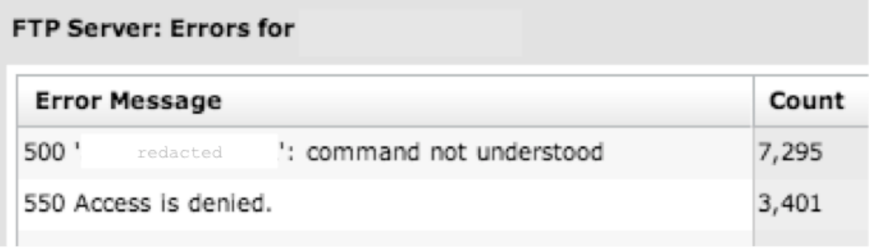


FTP Server: Error Metrics for

User	Errors
redacted	10,446

68.2% of FTP errors from ~~ccccc~~ had a single error message, “`500 '    redacted    ': command not understood`”. FTP 500 errors are indicative of failures related to invalid syntax.

Additionally, another 31.8% of FTP errors from ~~ccccc~~ had the “`550 Access is denied.`” error message. FTP 550 errors imply that a file is not available because it was not found or there was some other error related to invalid use of the file system.

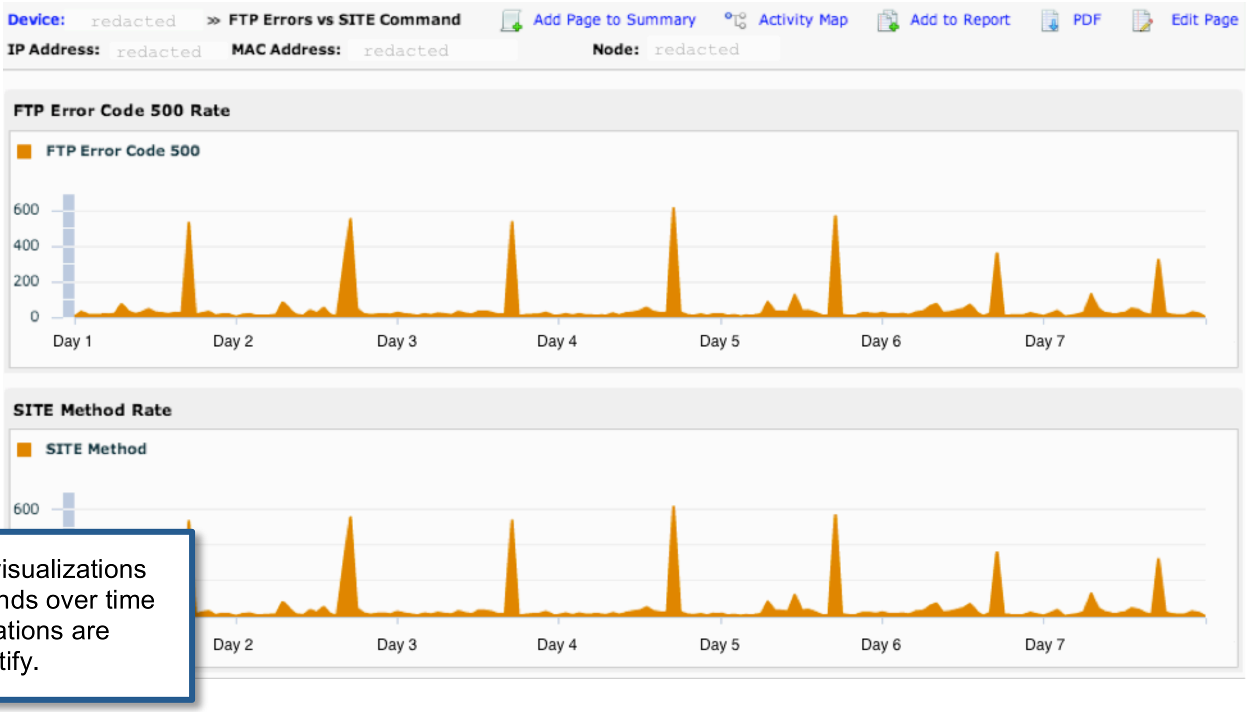


FTP Server: Errors for

Error Message	Count
500 ' redacted ': command not understood	7,295
550 Access is denied.	3,401

Further analysis of FTP errors suggests that there is a relationship between FTP 500 errors and the use of the FTP `SITE` method. FTP 500 errors are indicative of erroneous syntax resulting in an unrecognized action that, as a result, could not take place.

Looking at the busiest FTP server (~~ccccc~~), we see an almost 1:1 relationship between the use of the `SITE` method and FTP error code 500.



Device: redacted » FTP Errors vs SITE Command
IP Address: redacted MAC Address: redacted Node: redacted

The report’s visualizations also show trends over time so that correlations are easier to identify.

IMPROVEMENT OPPORTUNITIES:

Not evaluated.

CITRIX

A review of Citrix performance.

Citrix analysis can reveal whether poor user experience is due to the Citrix infrastructure or slow applications.

FINDINGS:

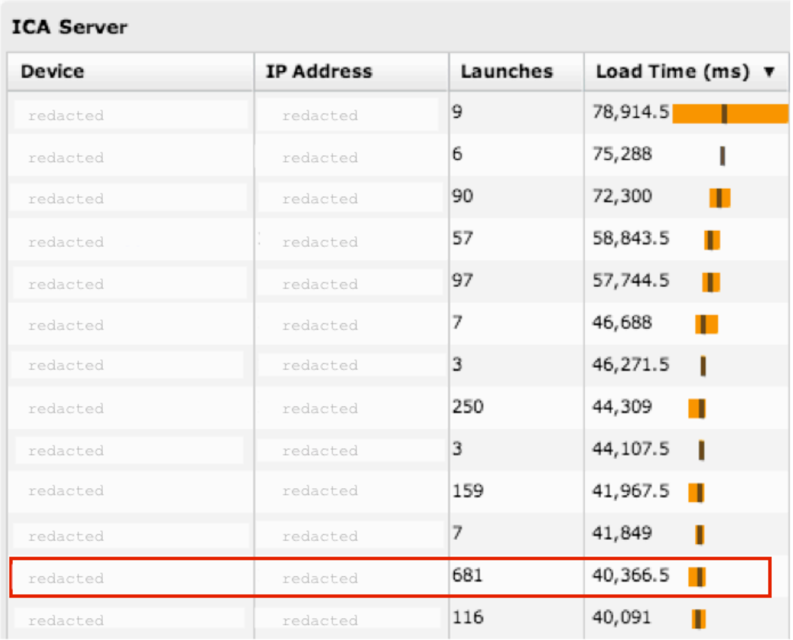
Investigate lengthy session load times on the ~~DDDDD~~ device that primarily affected two clients and were related to a single application. Citrix load times have slightly decreased since the previous observation period. (Trend: Improvement)	↗

CRITICAL CONCERNS:

None noted.

IMPROVEMENT OPPORTUNITIES:

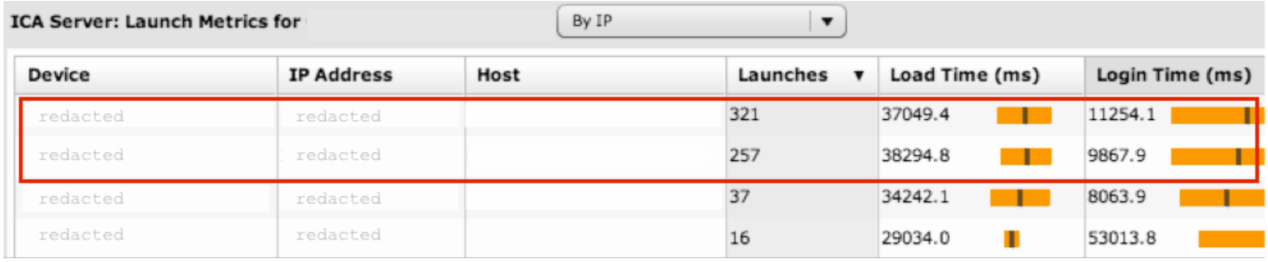
Several ICA servers are experiencing lengthy load times in excess of 40 seconds per session launch. When launching an ICA session, lengthy load times will delay the start of the ICA session and cause latency in overall application processing. ICA session launches transiting the ~~DDDDD~~ device experienced a high number of launches with long load times.



ICA Server

Device	IP Address	Launches	Load Time (ms) ▼
redacted	redacted	9	78,914.5
redacted	redacted	6	75,288
redacted	redacted	90	72,300
redacted	redacted	57	58,843.5
redacted	redacted	97	57,744.5
redacted	redacted	7	46,688
redacted	redacted	3	46,271.5
redacted	redacted	250	44,309
redacted	redacted	3	44,107.5
redacted	redacted	159	41,967.5
redacted	redacted	7	41,849
redacted	redacted	681	40,366.5
redacted	redacted	116	40,091

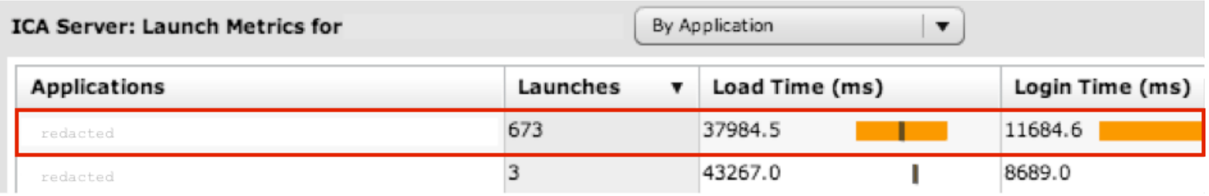
Drilling into ~~DDDDD~~, we can see that session launches transiting two Cisco devices are primarily affecting two clients: ~~FFFFF~~ and ~~GGGGGG~~.



ICA Server: Launch Metrics for

Device	IP Address	Host	Launches ▼	Load Time (ms)	Login Time (ms)
redacted	redacted		321	37049.4	11254.1
redacted	redacted		257	38294.8	9867.9
redacted	redacted		37	34242.1	8063.9
redacted	redacted		16	29034.0	53013.8

Three #~~MMMMMM~~ application was most impacted by lengthy load times. Investigate transactions that may be impacted by lengthy load times for this application.



ICA Server: Launch Metrics for

Applications	Launches ▼	Load Time (ms)	Login Time (ms)
redacted	673	37984.5	11684.6
redacted	3	43267.0	8689.0

STORAGE

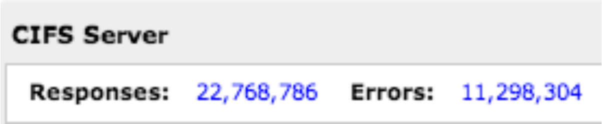
A review of all parsed storage protocol traffic. Protocols include (if licensed): CIFS, NFS, and iSCSI. More information regarding presentation of storage protocols in the ExtraHop UI is available here.

FINDINGS:

Investigate `STATUS_ACCESS_DENIED` CIFS errors that transited the ~~NNNNN~~ device and appeared to have originated at ~~`yy.yy.yy.yy`~~. The volume of CIFS errors significantly increased since the previous observation period. (Trend: Worse)	↓

CRITICAL CONCERNS:

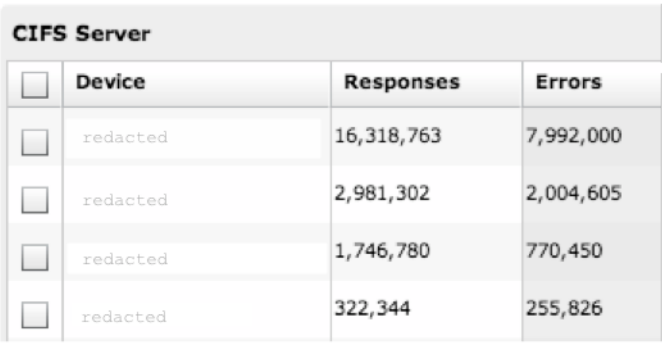
49.6% of CIFS responses were errors. This is an increase from the 3.4% CIFS error rate noted in the previous report. High volumes of errors should be investigated to determine if action is required to fix or if changes can be made to reduce unnecessary processing time.



CIFS Server

Responses: 22,768,786 **Errors:** 11,298,304

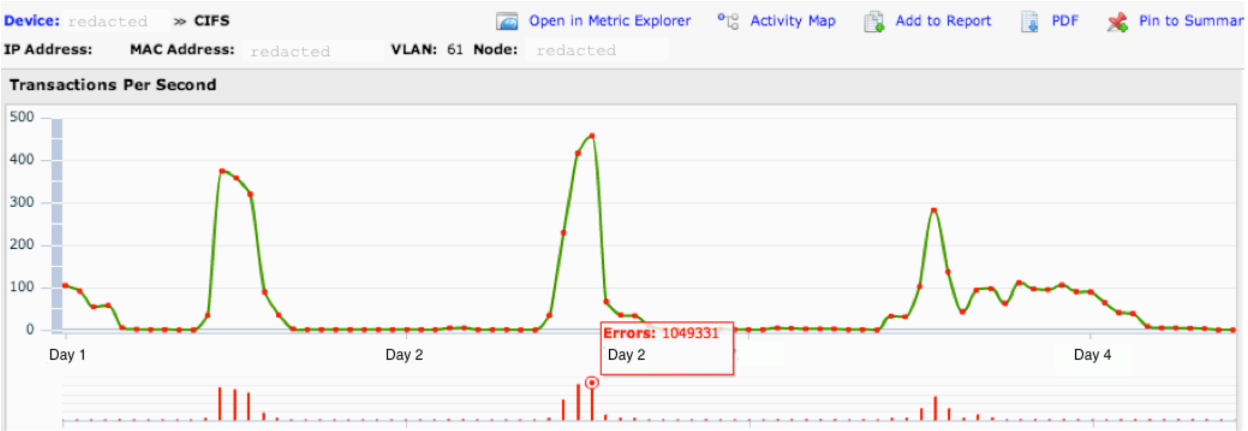
70.7% of CIFS errors transited the ~~NNNNN~~ device. Additionally, note that 49.0% of CIFS responses that transited this device were errors.



CIFS Server

□	Device	Responses	Errors
□	redacted	16,318,763	7,992,000
□	redacted	2,981,302	2,004,605
□	redacted	1,746,780	770,450
□	redacted	322,344	255,826

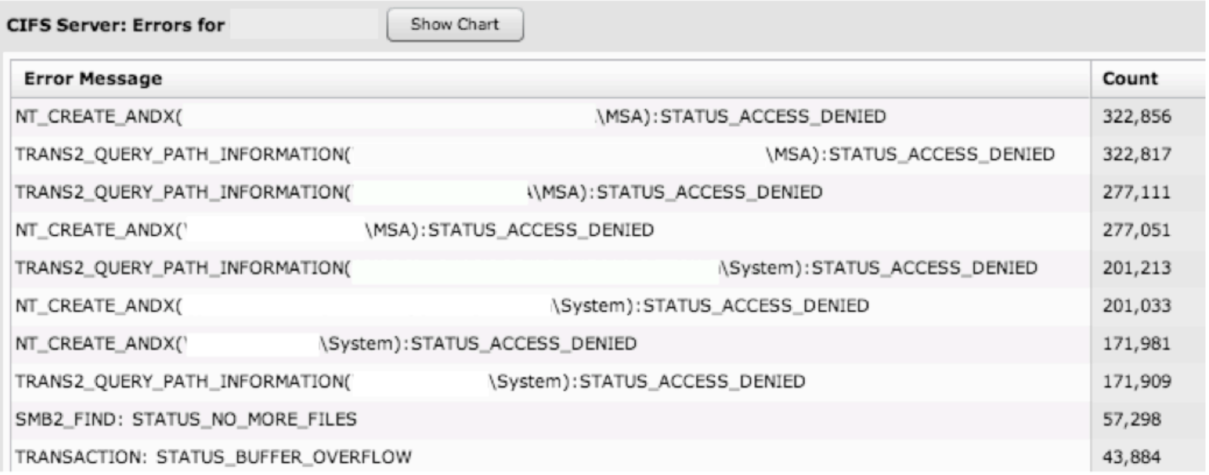
CIFS error rate (indicated by the vertical red bars) on ~~NNNNN~~ directly correlates with overall CIFS transaction rate (indicated by the green line). Both of these metrics increased each afternoon. At peak, this device experienced 1,049,331 errors over the course of a single hour, or **more than 291 errors every second**. Note that this server was only active for the first four days of the observation period.



Device: redacted » CIFS

IP Address: MAC Address: redacted VLAN: 61 Node: redacted

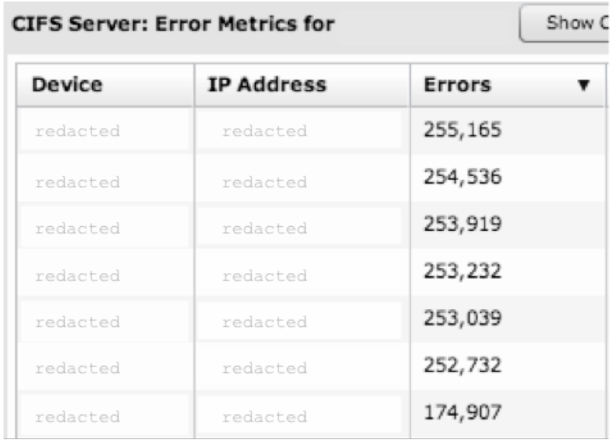
CIFS errors from ~~NNNNN~~ have variations of `STATUS_ACCESS_DENIED` error messages. This error indicates that a method, in this case `NT_CREATE_ANDX`, was unable to complete due to invalid credentials.



CIFS Server: Errors for

Error Message	Count
NT_CREATE_ANDX(\MSA):STATUS_ACCESS_DENIED	322,856
TRANS2_QUERY_PATH_INFORMATION(\MSA):STATUS_ACCESS_DENIED	322,817
TRANS2_QUERY_PATH_INFORMATION(\\MSA):STATUS_ACCESS_DENIED	277,111
NT_CREATE_ANDX(' \MSA):STATUS_ACCESS_DENIED	277,051
TRANS2_QUERY_PATH_INFORMATION(\System):STATUS_ACCESS_DENIED	201,213
NT_CREATE_ANDX(\System):STATUS_ACCESS_DENIED	201,033
NT_CREATE_ANDX(' \System):STATUS_ACCESS_DENIED	171,981
TRANS2_QUERY_PATH_INFORMATION(\System):STATUS_ACCESS_DENIED	171,909
SMB2_FIND: STATUS_NO_MORE_FILES	57,298
TRANSACTION: STATUS_BUFFER_OVERFLOW	43,884

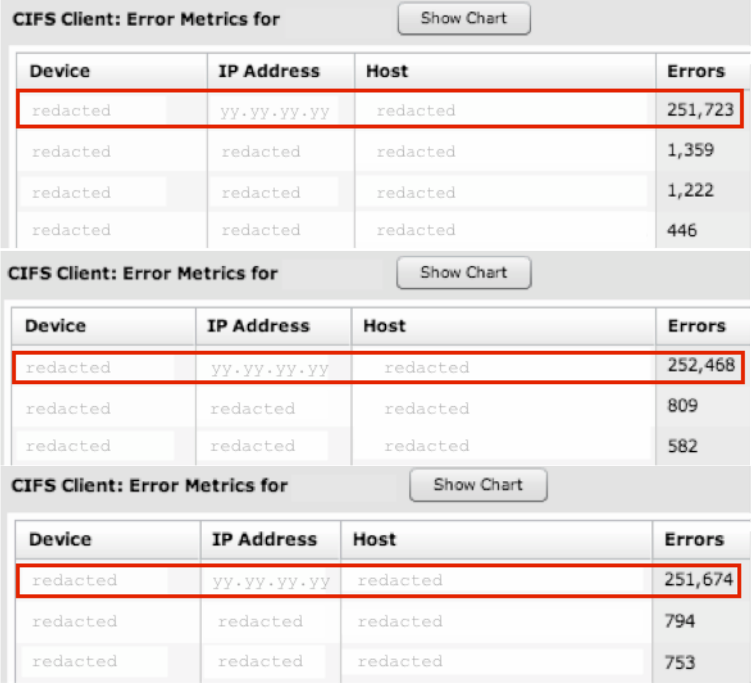
CIFS errors from ~~NNNNN~~ were returned to a wide variety of clients.



CIFS Server: Error Metrics for

Device	IP Address	Errors ▼
redacted	redacted	255,165
redacted	redacted	254,536
redacted	redacted	253,919
redacted	redacted	253,232
redacted	redacted	253,039
redacted	redacted	252,732
redacted	redacted	174,907

Looking at client-side CIFS metrics for some of these clients, we see that a large portion of CIFS errors that transited ~~NNNNN~~ originated on the ~~SSSSS~~ server at ~~yy.yy.yy.yy~~.



CIFS Client: Error Metrics for

Device	IP Address	Host	Errors
redacted	yy.yy.yy.yy	redacted	251,723
redacted	redacted	redacted	1,359
redacted	redacted	redacted	1,222
redacted	redacted	redacted	446

CIFS Client: Error Metrics for

Device	IP Address	Host	Errors
redacted	yy.yy.yy.yy	redacted	252,468
redacted	redacted	redacted	809
redacted	redacted	redacted	582

CIFS Client: Error Metrics for

Device	IP Address	Host	Errors
redacted	yy.yy.yy.yy	redacted	251,674
redacted	redacted	redacted	794
redacted	redacted	redacted	753

Improvement Opportunities:

Not evaluated.

Supporting Application Infrastructure

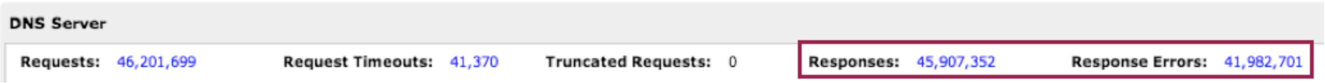
A review of protocol traffic related to supporting application infrastructure, including DNS, SMTP, LDAP and Kerberos. More information regarding presentation of the DNS and LDAP protocols in the ExtraHop UI is available via the previous links.

Findings:

Investigate the high volume of DNS response errors concentrated on the ~~HHHHH~~ device that were related to reverse IP lookups. (New finding)	☼

Critical Concerns:

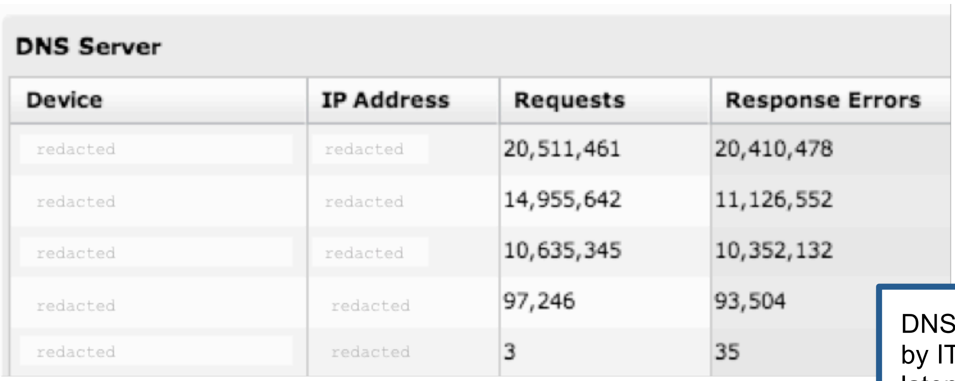
91.4% of all DNS responses were errors. A DNS response error occurs when a client makes a DNS lookup and the DNS server responds with some sort of error. These errors may not break an application, but they add latency to application transactions and cause unnecessary processing on the DNS server.



DNS Server

Requests:	Request Timeouts:	Truncated Requests:	Responses:	Response Errors:
46,201,699	41,370	0	45,907,352	41,982,701

48.6% of DNS response errors occurred on the ~~HHHHH~~ server. Note that 99.5% of DNS requests made to this server resulted in response errors.

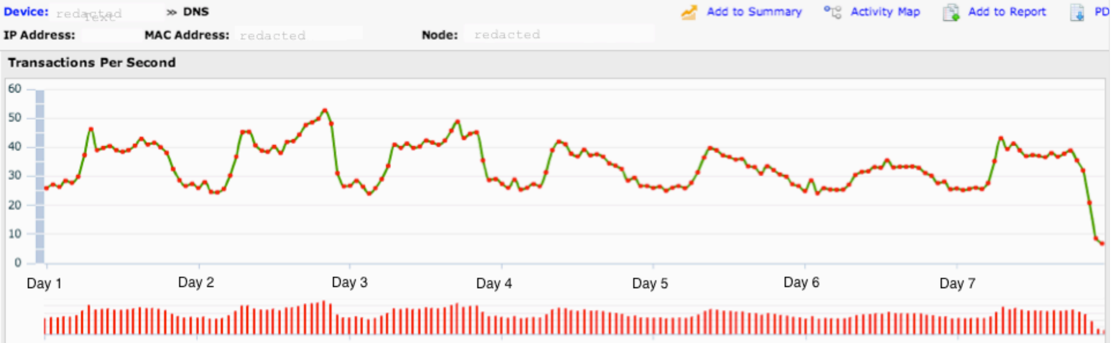


DNS Server

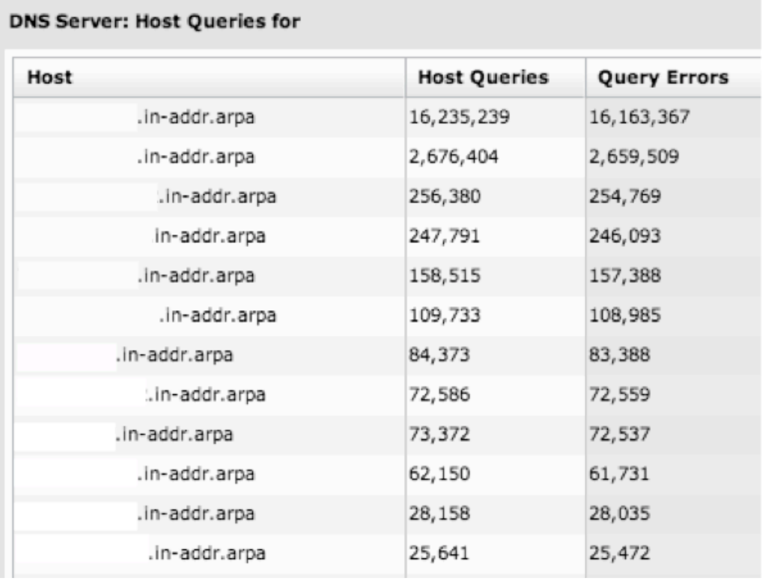
Device	IP Address	Requests	Response Errors
redacted	redacted	20,511,461	20,410,478
redacted	redacted	14,955,642	11,126,552
redacted	redacted	10,635,345	10,352,132
redacted	redacted	97,246	93,504
redacted	redacted	3	35

DNS problems often go unnoticed by IT staff, but contribute to overall latency and can be fixed with minimal effort.

DNS response error rate (indicated by the vertical red bars) on HHHHH directly correlated with transaction rate (indicated by the green line). Both of these metrics fluctuated over the course of the analysis period but generally increased during daytime hours.



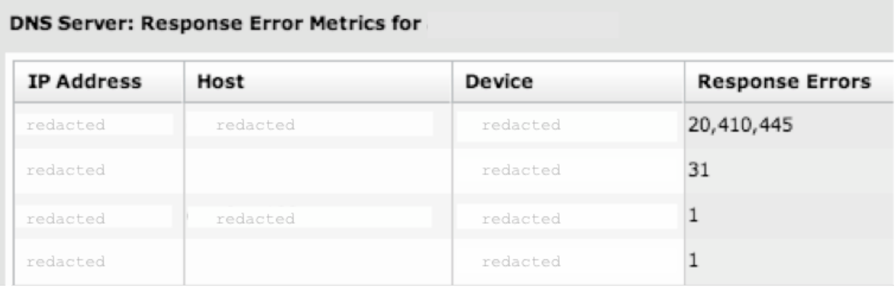
DNS response errors from HHHHH occurred in association with what appear to be a variety of reverse DNS lookups, when the client feeds the server an IP address looking for a hostname. Note that these queries are erring nearly 100% of the time they are called.



DNS Server: Host Queries for

Host	Host Queries	Query Errors
[redacted].in-addr.arpa	16,235,239	16,163,367
[redacted].in-addr.arpa	2,676,404	2,659,509
[redacted].in-addr.arpa	256,380	254,769
[redacted]in-addr.arpa	247,791	246,093
[redacted].in-addr.arpa	158,515	157,388
[redacted].in-addr.arpa	109,733	108,985
[redacted].in-addr.arpa	84,373	83,388
[redacted].in-addr.arpa	72,586	72,559
[redacted].in-addr.arpa	73,372	72,537
[redacted].in-addr.arpa	62,150	61,731
[redacted].in-addr.arpa	28,158	28,035
[redacted].in-addr.arpa	25,641	25,472

Nearly 100% of DNS response errors from HHHHH were returned the LLLLL client via a Cisco device.



DNS Server: Response Error Metrics for

IP Address	Host	Device	Response Errors
redacted	redacted	redacted	20,410,445
redacted		redacted	31
redacted	redacted	redacted	1
redacted		redacted	1

IMPROVEMENT OPPORTUNITIES:

Not evaluated.

APPLICATION COMMUNICATION

Review of lower levels (L2, L3, L4/TCP) in the TCP stack, and L7 metric overview. More information regarding presentation of the Transmission Control Protocol (TCP) in the ExtraHop UI is available here.

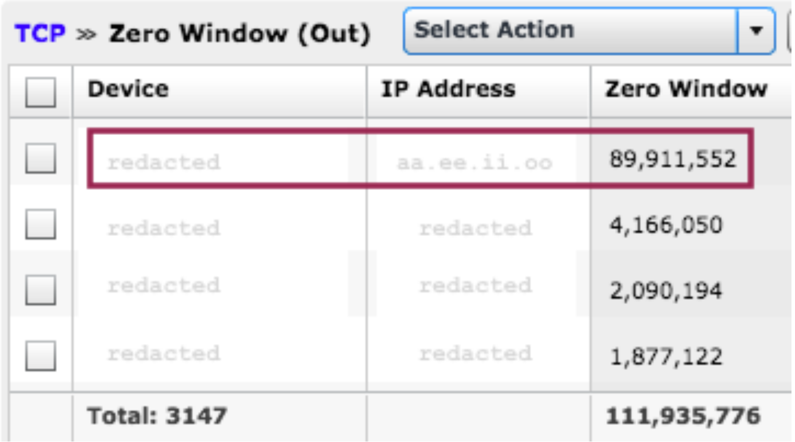
FINDINGS:

Investigate Zero Windows sent from the ~~RRRR~~ device that impacted HTTP transactions. The overall volume of Zero Windows increased 223% (more than tripled) since the previous analysis period. (Trend: Worse)	↓

Investigate IP fragmentation on the ~~UUUUU~~ device. (New finding)	☀

CRITICAL CONCERNS:

More than 111,000,000 Zero Windows were observed on the Customer network over the course of the seven-day observation period. This is an increase from the 34,600,000 Zero Windows noted in the previous report. A Zero Window indicates that the connection between two devices has stalled and that the device sending the Zero Window is unable to keep up with the rate of data that a peer is sending. In effect, the device sending the Zero Window is saying, "send no data until further notice." 80.3% of Zero Windows were sent from the ~~RRRR~~ device at aa.ee.ii.oo.

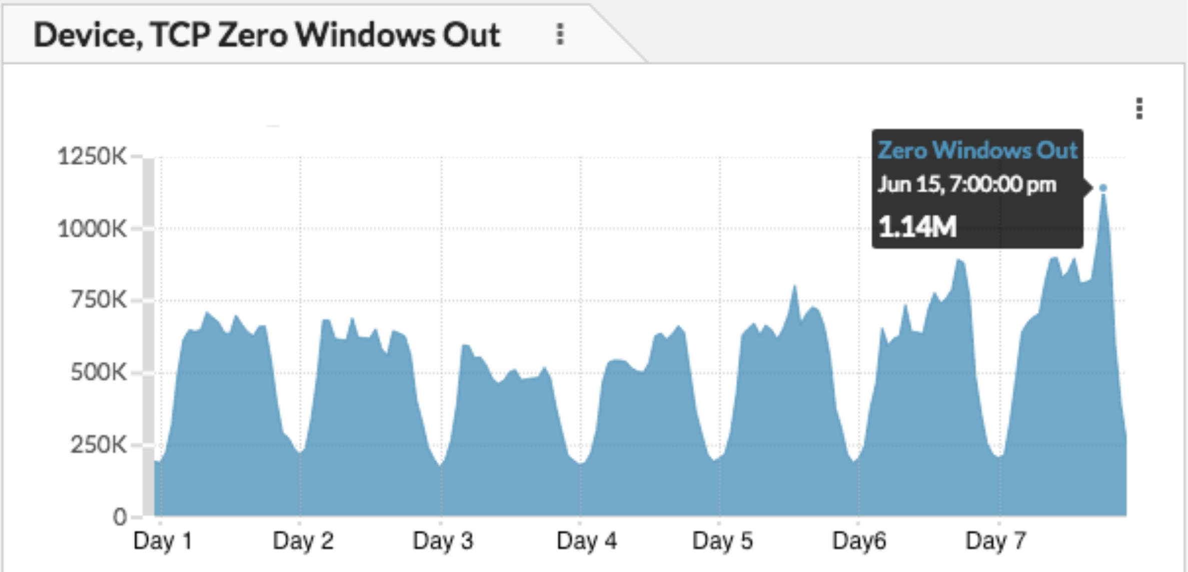


TCP » Zero Window (Out)

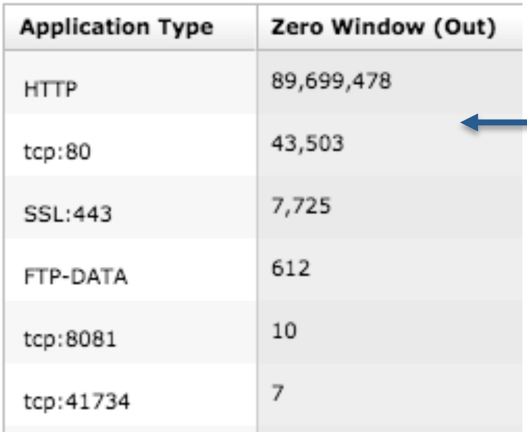
□	Device	IP Address	Zero Window
□	redacted	aa.ee.ii.oo	89,911,552
□	redacted	redacted	4,166,050
□	redacted	redacted	2,090,194
□	redacted	redacted	1,877,122
	Total: 3147		111,935,776

TCP analysis offers insight into a commonly overlooked area. The Atlas report's TCP analysis reveals how well applications and the network interact.

The rate of Zero Windows sent from ~~RRRR~~ increased during daytime hours. At peak, 1,140,000 Zero Windows were sent from this device over the course of a single hour, or **more than 316 Zero Windows every second.**



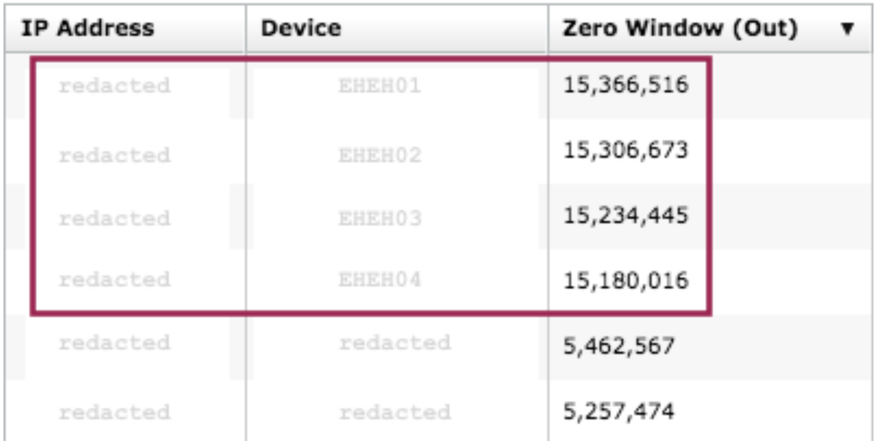
99.8% of Zero Windows sent from ~~RRRR~~ impacted HTTP transactions.



Application Type	Zero Window (Out)
HTTP	89,699,478
tcp:80	43,503
SSL:443	7,725
FTP-DATA	612
tcp:8081	10
tcp:41734	7

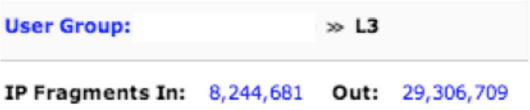
Tying TCP metrics with Layer 7 protocols helps staff to diagnose underlying communication problems.

67.9% of Zero Windows sent from ~~RRRR~~ impacted communication with four similarly named EHEH0# devices.



IP Address	Device	Zero Window (Out) ▼
redacted	EHEH01	15,366,516
redacted	EHEH02	15,306,673
redacted	EHEH03	15,234,445
redacted	EHEH04	15,180,016
redacted	redacted	5,462,567
redacted	redacted	5,257,474

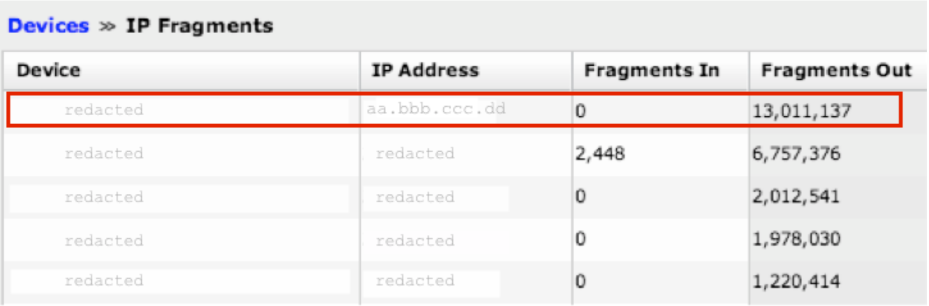
More than 29,300,000 IP fragments were sent onto the Customer network over the course of the seven-day observation period. IP fragmentation may be caused by an MTU mismatch between devices on the network. This results in high volumes of segments being sent across the network, which can overwhelm both the network as well as devices.



User Group: » L3

IP Fragments In: 8,244,681 Out: 29,306,709

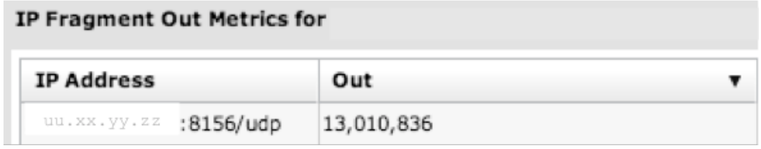
44.4% of IP fragments were outbound from the ~~UUUUU~~ device. Note that there were no IP fragments inbound to ~~UUUUU~~. This indicates that all IP fragmentation originated on ~~UUUUU~~ (rather than ~~UUUUU~~ simply transferring IP fragments from other transactions).



Devices » IP Fragments

Device	IP Address	Fragments In	Fragments Out
redacted	aa.bbb.ccc.dd	0	13,011,137
redacted	redacted	2,448	6,757,376
redacted	redacted	0	2,012,541
redacted	redacted	0	1,978,030
redacted	redacted	0	1,220,414

100% IP fragments from ~~UUUUU~~ were sent to `uu.xx.yy.zz` via broadcast traffic on UDP port 8156.



IP Fragment Out Metrics for

IP Address	Out ▼
uu.xx.yy.zz :8156/udp	13,010,836

Improvement Opportunities:

Not evaluated.

SECURITY

Review of SSL sessions that may be insecure, transactions involving suspicious foreign IPs, and other L7 protocol activity that may be easily compromised. More information regarding presentation of the SSL protocol in the ExtraHop UI is available here.

FINDINGS:

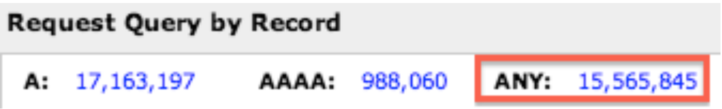
Investigate excessive use of the `ANY` method by the ~~PPPPP~~ server; a significant volume of `ANY` method calls originated in Australia. The volume of `ANY` method calls has slightly decreased since the previous analysis period. (Trend: Improvement)	↗

Reduce use of the `TLS_DH_anon_WITH_AES_256_GCM_SHA384` cipher suite associated with connections involving the ~~LLLLL~~ client. Overall usage of the `TLS_DH_anon_WITH_AES_256_GCM_SHA384` cipher suite has not significantly changed since the previous analysis period. (Trend: No change)	→

Reduce FTP 530 errors that occurred on the ~~PPPPP~~ server and were primarily returned to clients in China. (New finding)	☀

CRITICAL CONCERNS:

Over 15,500,000 instances of the DNS "`ANY`" method occurred during the observation period. This is a decrease from the volume of `ANY` method requests noted in the previous report, however, this is still a concerning volume. Use of the `ANY` method returns all known information about a DNS zone in a single request, and high volumes of these method calls is usually indicative of a DNS Amplification Attack. More information available here: http://www.us-cert.gov/ncas/alerts/TA13-088A.

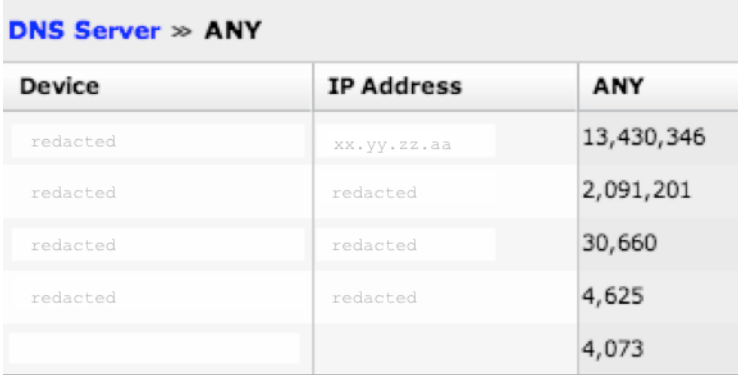


Request Query by Record

A:	17,163,197	AAAA:	988,060	ANY:	15,565,845

The Atlas report's security section frequently uncovers user and system behavior that represents risk to your organization.

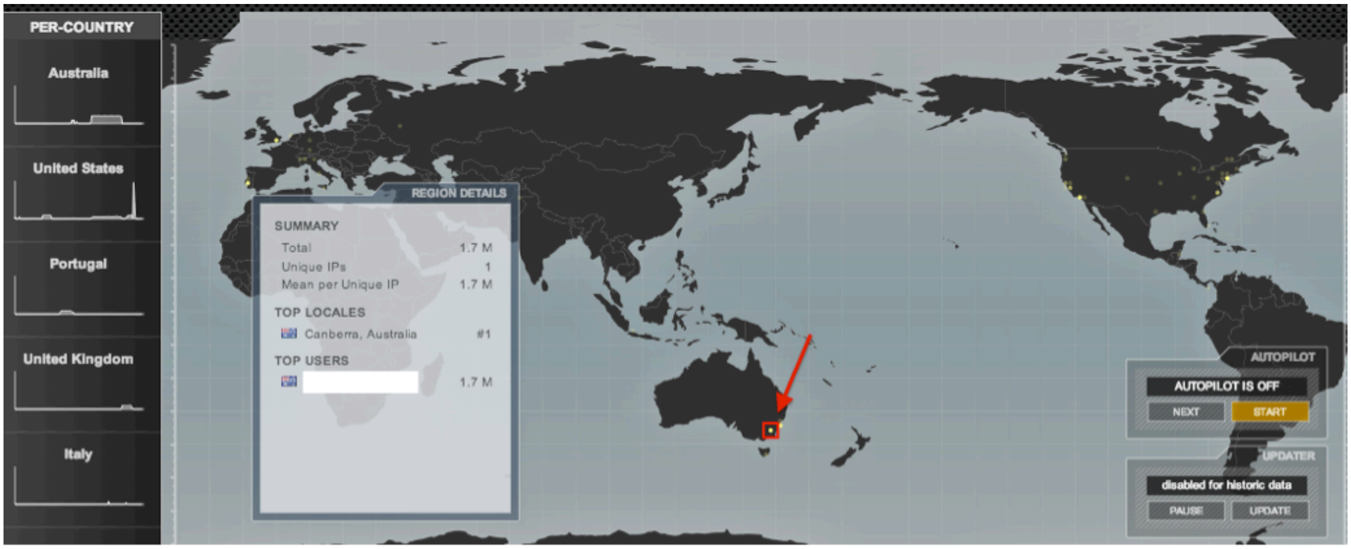
86.3% of `ANY` method calls occurred on the ~~PPPPP~~ DNS server at `xx.yy.zz.aa`.



DNS Server » ANY

Device	IP Address	ANY
redacted	xx.yy.zz.aa	13,430,346
redacted	redacted	2,091,201
redacted	redacted	30,660
redacted	redacted	4,625
		4,073

The following Geomap identifies the physical location of IPs that sent `ANY` requests to the server at `xx.yy.zz.aa`. A denser dot indicates a higher volume of transactions. Note that the `AAA.BB.XXX.ZZ` IP located in Canberra, Australia accounts for a large portion of these `ANY` method requests. Investigate if transactions with this IP are expected behavior on the Customer network, or indicative of a larger issue.



SUMMARY

Total	1.7 M
Unique IPs	1
Mean per Unique IP	1.7 M

TOP LOCALES

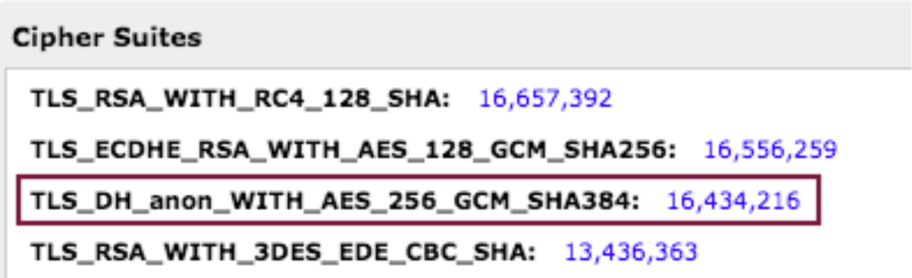
Canberra, Australia	#1

TOP USERS

	1.7 M

Where appropriate, geomaps from the ExtraHop UI enable you to quickly determine the geographic origin of application communications.

11.7% of encrypted traffic on the Customer network used the `TLS_DH_anon_WITH_AES_256_GCM_SHA384` cipher suite. This is not a significant change from the 10.5% of encrypted traffic using this cipher suite noted in the previous report. Note that this was the fourth most commonly used cipher suite. A server that supports a cipher suite containing “anon” does not require key authentication, which allows clients to establish encrypted connections with the server anonymously. As such, ciphers of this type are vulnerable to man-in-the-middle attacks.

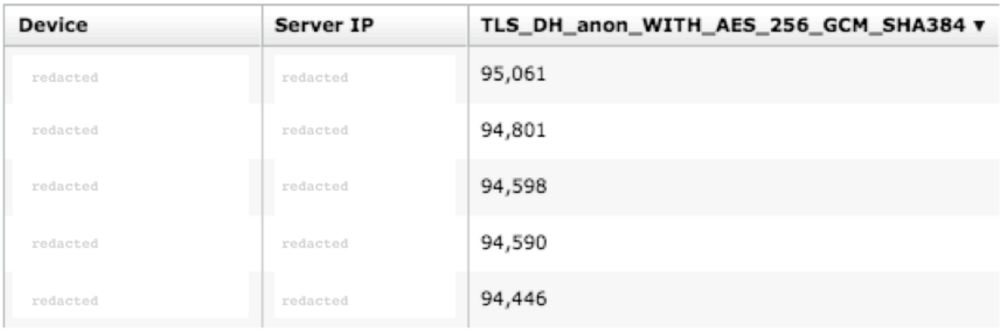


Cipher Suites

TLS_RSA_WITH_RC4_128_SHA: 16,657,392
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256: 16,556,259
TLS_DH_anon_WITH_AES_256_GCM_SHA384: 16,434,216
TLS_RSA_WITH_3DES_EDE_CBC_SHA: 13,436,363

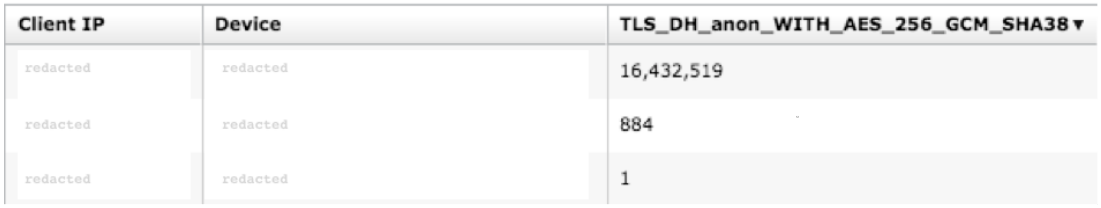
The security section includes a detailed review of the types of encryption used on your network.

A variety of servers established encrypted connections using the `TLS_DH_anon_WITH_AES_256_GCM_SHA384` cipher suite.



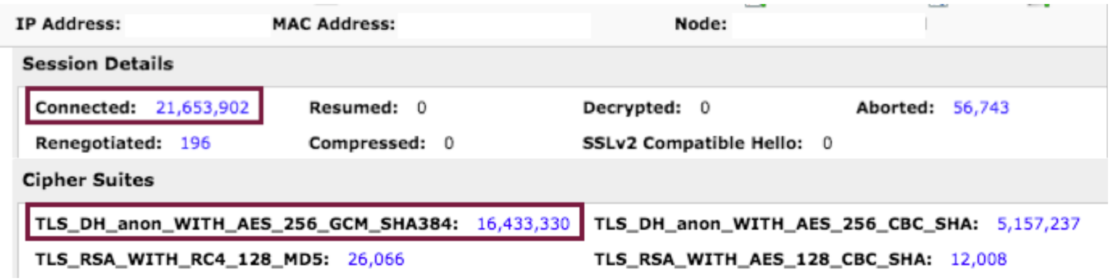
Device	Server IP	TLS_DH_anon_WITH_AES_256_GCM_SHA384 ▾
redacted	redacted	95,061
redacted	redacted	94,801
redacted	redacted	94,598
redacted	redacted	94,590
redacted	redacted	94,446

Nearly 100% of connections using the `TLS_DH_anon_WITH_AES_256_GCM_SHA384` cipher suite were associated with SSL sessions involving the ~~LLLLL~~ client. This behavior was also noted in the previous report.



Client IP	Device	TLS_DH_anon_WITH_AES_256_GCM_SHA38 ▾
redacted	redacted	16,432,519
redacted	redacted	884
redacted	redacted	1

Additionally, note that 75.9% of SSL sessions involving the ~~LLLLL~~ client used the `TLS_DH_anon_WITH_AES_256_GCM_SHA384` cipher suite. Additionally, note that the second most commonly used cipher suite by this client, `TLS_DH_anon_WITH_AES_256_CDC_SHA`, is also vulnerable to the same pitfalls.



IP Address: MAC Address: Node:

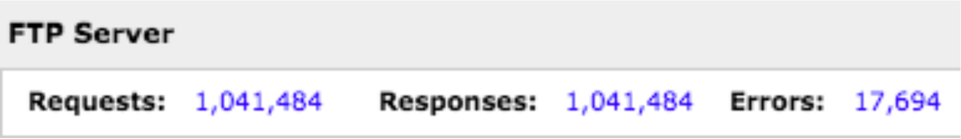
Session Details

Connected: 21,653,902 Resumed: 0 Decrypted: 0 Aborted: 56,743
Renegotiated: 196 Compressed: 0 SSLv2 Compatible Hello: 0

Cipher Suites

TLS_DH_anon_WITH_AES_256_GCM_SHA384: 16,433,330 TLS_DH_anon_WITH_AES_256_CBC_SHA: 5,157,237
TLS_RSA_WITH_RC4_128_MD5: 26,066 TLS_RSA_WITH_AES_128_CBC_SHA: 12,008

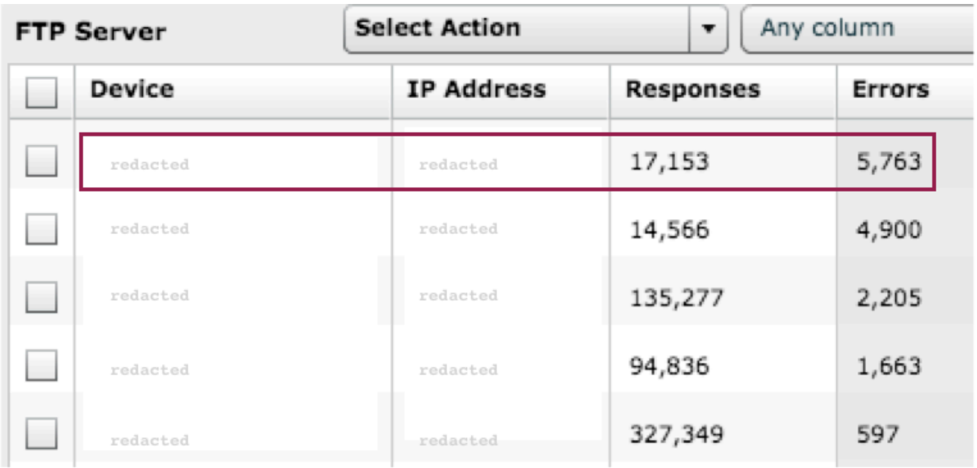
1.7% of FTP responses were errors.



FTP Server

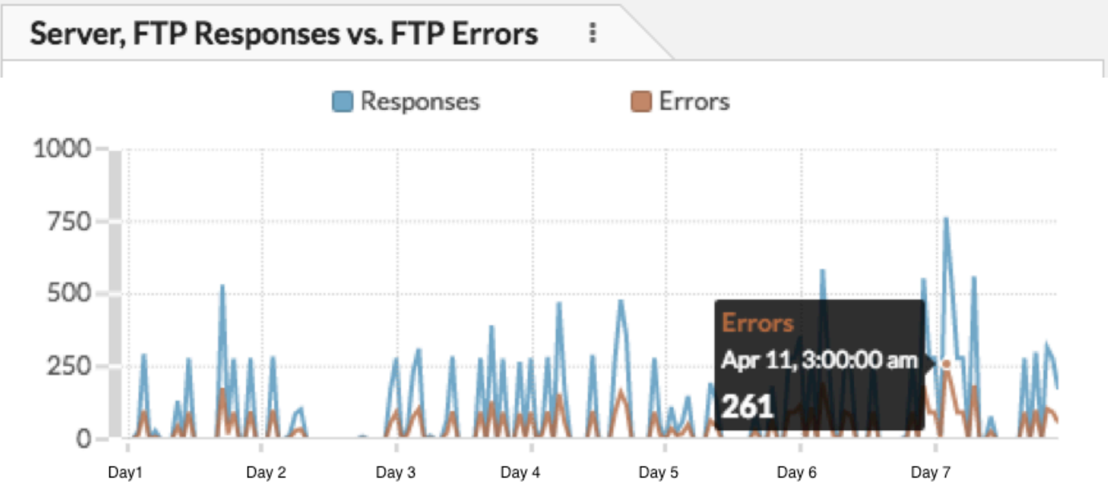
Requests:	1,041,484	Responses:	1,041,484	Errors:	17,694

32.6% of FTP errors occurred on the ~~PPPPP~~ server. Additionally, note that 33.6% of FTP responses sent from this server were errors.

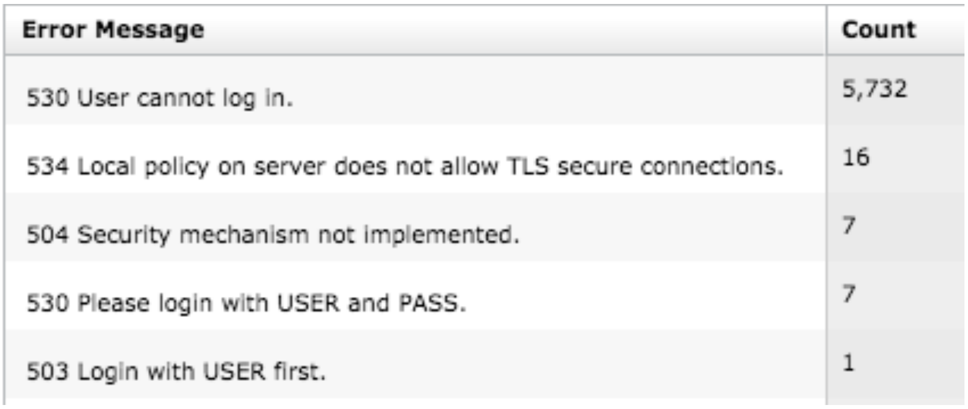


□	Device	IP Address	Responses	Errors
□	redacted	redacted	17,153	5,763
□	redacted	redacted	14,566	4,900
□	redacted	redacted	135,277	2,205
□	redacted	redacted	94,836	1,663
□	redacted	redacted	327,349	597

FTP error rate (indicated by the orange line) on ~~PPPPP~~ directly correlated with overall FTP response rate (indicated by the blue line). Both of these metrics fluctuated over the course of the observation period and did not appear to follow a particular pattern. At peak, 261 FTP errors were sent over the course of a single hour.

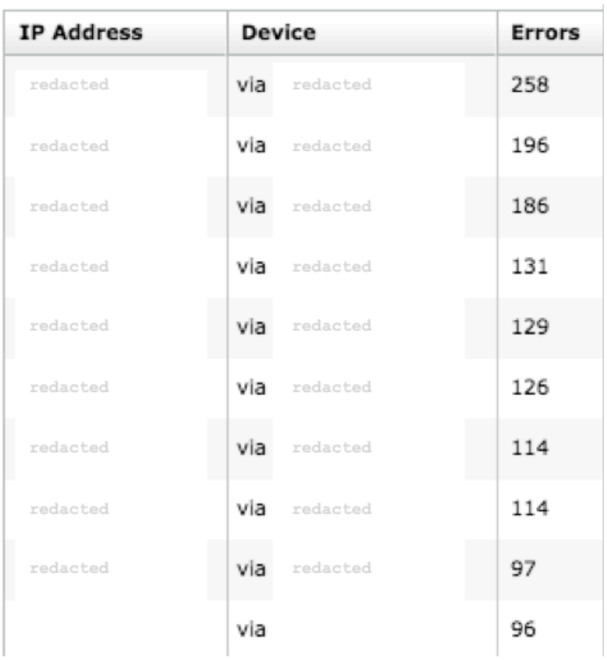


99.5% of FTP errors sent from ~~PPPPP~~ had a single error message, "`530 User cannot log in.`". FTP 530 errors occur due to invalid usernames and/or passwords provided during login, or other authentication and accounting errors. This was also the most common error message during the previous analysis period.



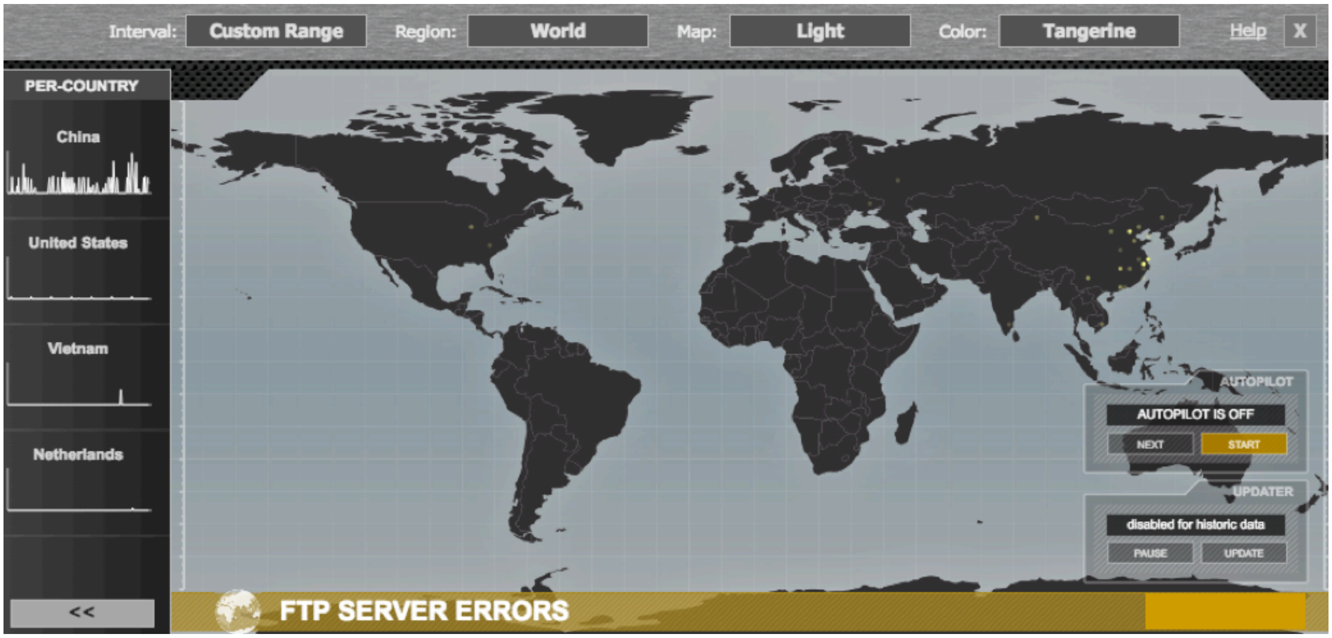
Error Message	Count
530 User cannot log in.	5,732
534 Local policy on server does not allow TLS secure connections.	16
504 Security mechanism not implemented.	7
530 Please login with USER and PASS.	7
503 Login with USER first.	1

FTP errors sent from ~~PPPPP~~ were returned to a variety of what appear to be external client IPs via a Cisco device.



IP Address	Device	Errors
redacted	via redacted	258
redacted	via redacted	196
redacted	via redacted	186
redacted	via redacted	131
redacted	via redacted	129
redacted	via redacted	126
redacted	via redacted	114
redacted	via redacted	114
redacted	via redacted	97
	via	96

Utilizing the ExtraHop Geomap feature, we can physically locate the clients that received FTP errors from ~~PPPPP~~. Note that FTP errors from ~~PPPPP~~ were primarily returned to clients across China. FTP errors with these IPs are likely not by design, and should be further investigated and eliminated so as to reduce potential malicious behavior on the Customer network.



Interval: Custom Range
Region: World
Map: Light
Color: Tangerine

AUTOPILOT IS OFF

disabled for historic data

Improvement Opportunities:

Deferred due to critical concerns.

METRICS CHECKLIST

Atlas Remote Analysis reports include analysis of more than 20 protocols and look into problems regarding 70+ metrics that commonly impact network performance. For a complete overview of the protocols included and a detailed list of items analyzed in this report, please visit the following:

https://www.extrahop.com/platform/services/atlas-remote-analysis/checklist/

The findings in Atlas reports are based off of common issues seen across IT infrastructures in many different verticals, and with network configurations utilizing a wide swath of tools. If, however, some of the findings included in this report are expected behavior in your network, **please send a note to atlas@extrahop.com outlining these items**. ExtraHop Atlas analysts will keep note of the expected and/or excluded behavior seen in your infrastructure, and eliminate these findings from future report composition.