Fast 360 Assessment Report

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 OF FAST 360 ASSESSMENT FINDINGS

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

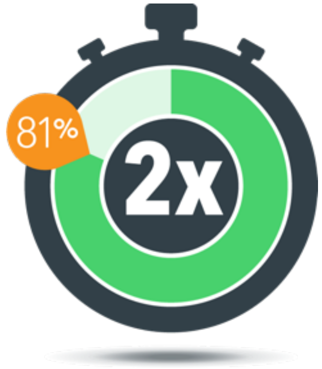
There were no FTP requests originating outside of corporate headquarters, which is expected.

WHAT EXTRAHOP CUSTOMERS ARE SAYING

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

TechValidate

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

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

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

- **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

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

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

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

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.

See the Appendix for Web Optimization dashboards

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

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

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

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

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

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

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.

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

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