Symantec. Security Analytics

Risk and Visibility Report

Report Timespan:
July 18, 2018 12:00AM GMT+0900 to
July 24, 2018 09:15AM GMT+0900

Report Generated: July 24, 2018 10:05AM GMT+0900
Generated by:

Executive Summary

Key Findings

1.28M
Malicious files
detected by FRS

1585
Systems Impacted

3.06M
unknown/unrated
files not scanned for
novel threats and
zero-day malware

49.05%
Encrypted Traffic

5.22K
Predicted Files
Hidden in Encrypted
Traffic

3.74K
Malicious URLs
detected by WRS

337
Systems Impacted

228.46 GB
High Risk Traffic

Potential risk of data loss
or policy compliance issues

Threat Analysis

Detect breaches and integrate context

Encrypted Traffic Visibility

As of 2015, most enterprise network traffic averages 40-50% SSL/TLS traffic. In almost all cases, current security tools cannot examine this traffic, and this lack of visibility into SSL can make it difficult or impossible for network and security teams to stop intrusions and malware before they compromise their targets.

- SSL/TLS
- Non SSL/TLS
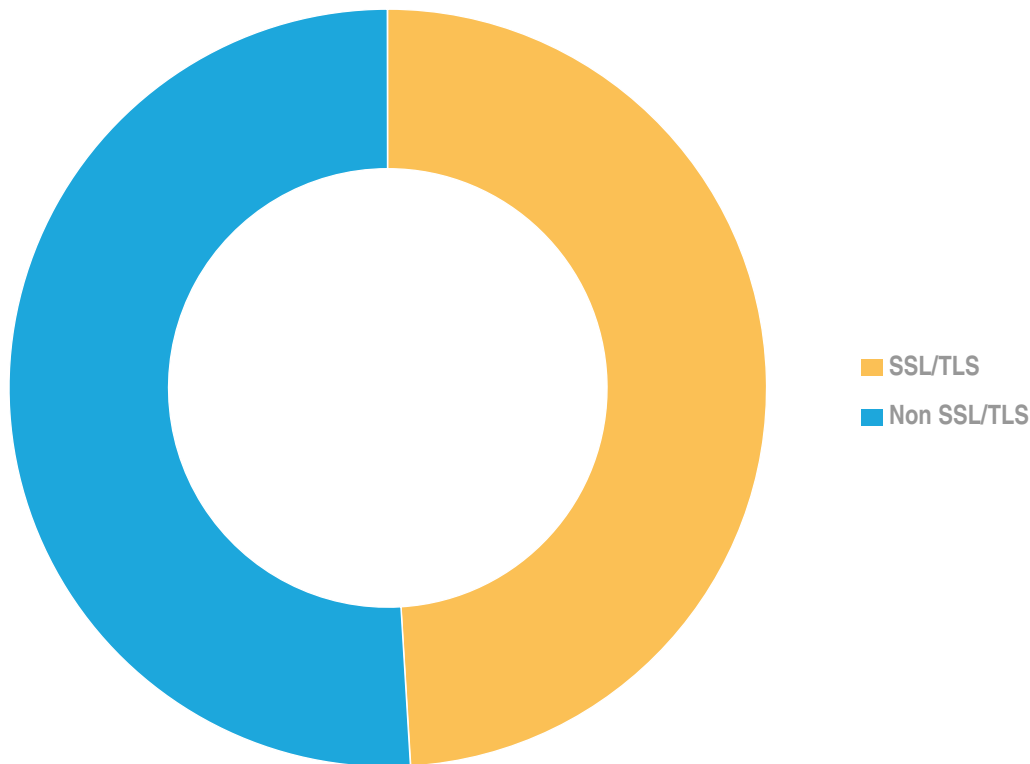
Predicted File Count Hidden in Encrypted Traffic

These predicted values assume a 1:1 ratio of files being delivered over HTTP and HTTPs. In reality most video streaming, CDN, and performance monitoring happens over HTTP, whereas files are typically delivered over HTTPs (Google Services, malware hiding in SSL) so it's expected the hidden file count is actually higher than predicted here.

2.00K PDF Files   **1.46K** ZIP Files

1.27K PE (exe) Files   **317** FLASH (swf) Files

176 7ZIP Files

Application Groups using SSL

Without the ability to inspect SSL content, sensitive or critical information can easily be accidentally leaked or worse: stolen. Network security appliances can usually inspect only plaintext traffic and so are unable to inspect SSL-encrypted communications for malware, hidden threats, or exfiltrated data. They therefore become less and less effective as the volume of encrypted SSL traffic grows.

Application Group	Bytes
Web	3.71 TB
Audio/Video	146.32 GB
Application Service	76.99 GB
Webmail	40.25 GB
Standard	32.66 GB
Instant Messaging	14.85 GB
Mail	10.94 GB
Encrypted	7.95 GB
Forum	4.08 GB
Thin Client	1.48 GB
Network Service	1.36 GB
Game	1.33 GB
Network Management	235.41 MB
Security Service	234.89 MB
Antivirus	868.86 KB
Tunneling	811.48 KB
Peer to Peer	112.93 KB
File Server	52.14 KB

Malicious Files

Detected by File Reputation Service

File Reputation Service extracts and analyzes key file types such as Microsoft Office documents, Adobe Flash, PDFs, Java, EXE files, email attachments, Android APK files, web objects and more. It alerts security analysts to the presence of known malicious activity across many network transports including web sessions, file-transfer mechanisms, email protocols, and raw TCP connections.

- ■ Malicious Files
- ■ Non-malicious Files
- ■ Unknown/Unrated Files
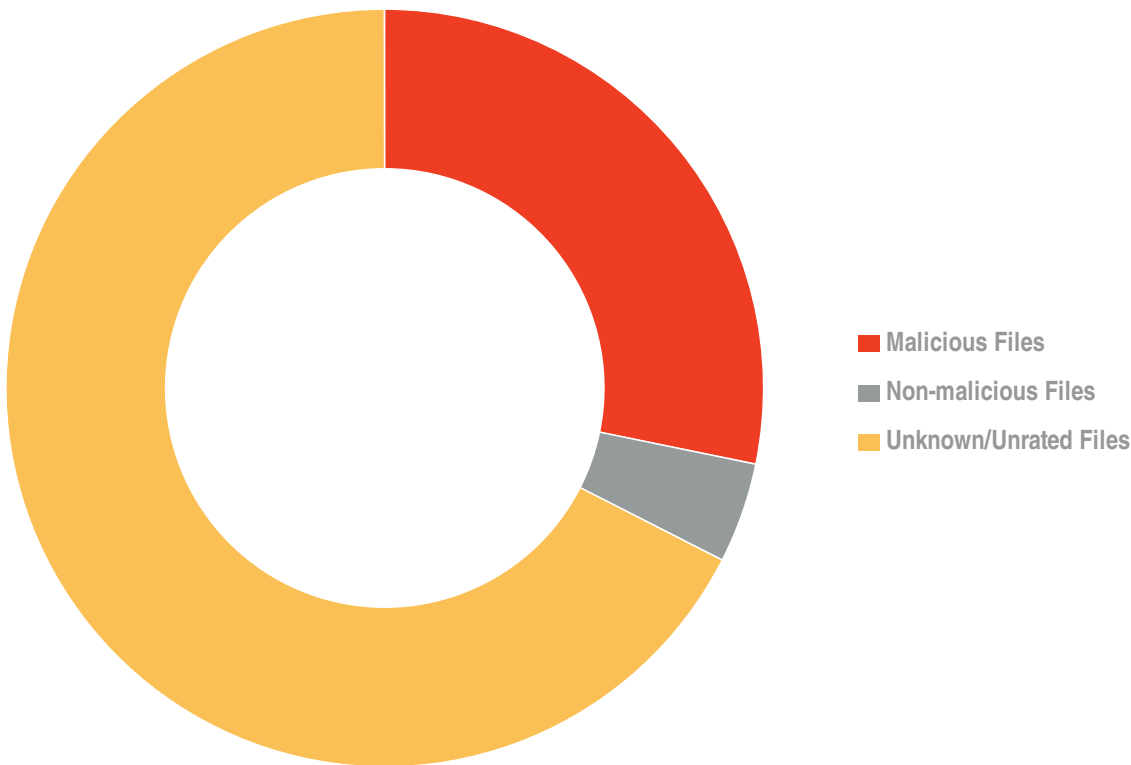
1.28M (28.23%) Malicious Files

193.58K (4.28%) Non-malicious Files

3.06M (67.49%) Unknown/Unrated Files

4.53M Total Files Analyzed

1585 Systems Impacted

Malicious URLs

Detected by Web Reputation Service

Web Reputation Service detects and reports suspicious web sites and network activity in more than 100 different categories and uses reputation data on URLs and IP addresses to identify network traffic originating from known bots, spammers, phishing sites, malware sources, and compromised websites.

- Malicious URLs
- Non-malicious URLs
- Unrated/Unknown Urls
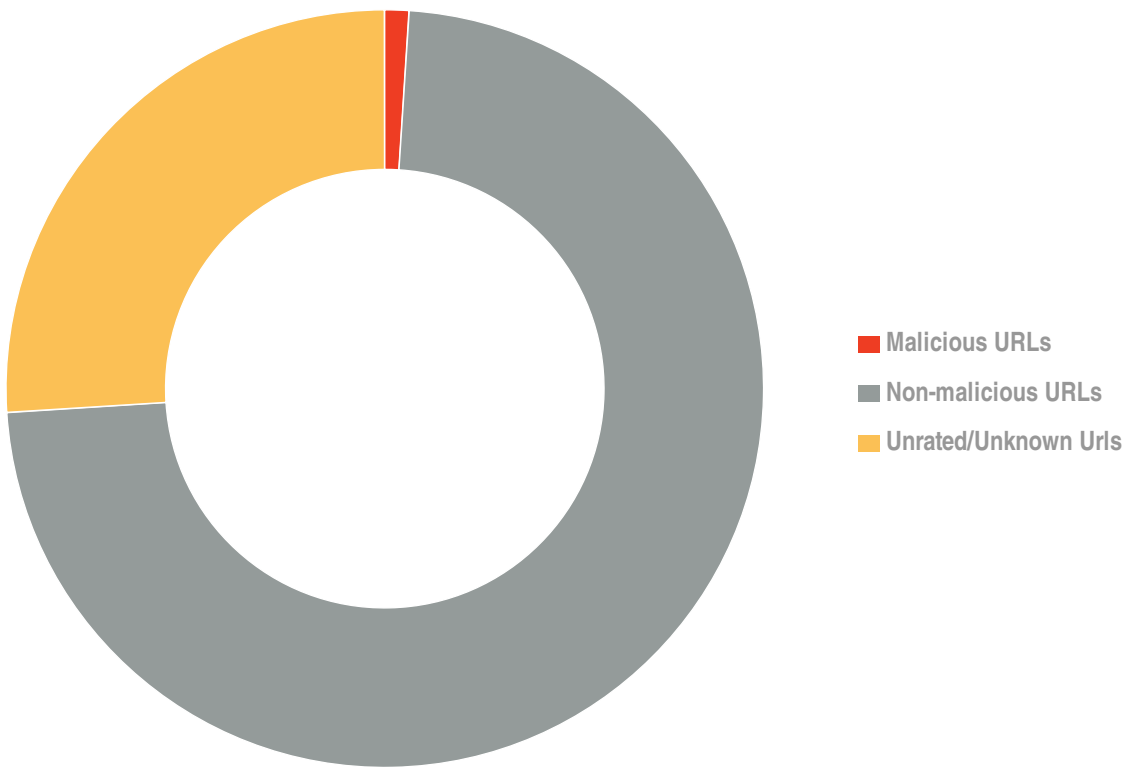
3.74K (1.02%) Malicious URLs

266.68K (72.98%) Non-malicious URLs

**95.02K** (26.00%) Unrated/Unknown Urls

365.44K Total URLs Analyzed

337 Systems Impacted

Malicious Files

Detected by Malware Analysis

For novel threats, zero-day malware, and targeted attacks not previously seen by the File Reputation Service, comprehensive static and dynamic behavioral analysis is performed in real time by the Malware Analysis appliance.


■ **Unrated/Unknown Files**
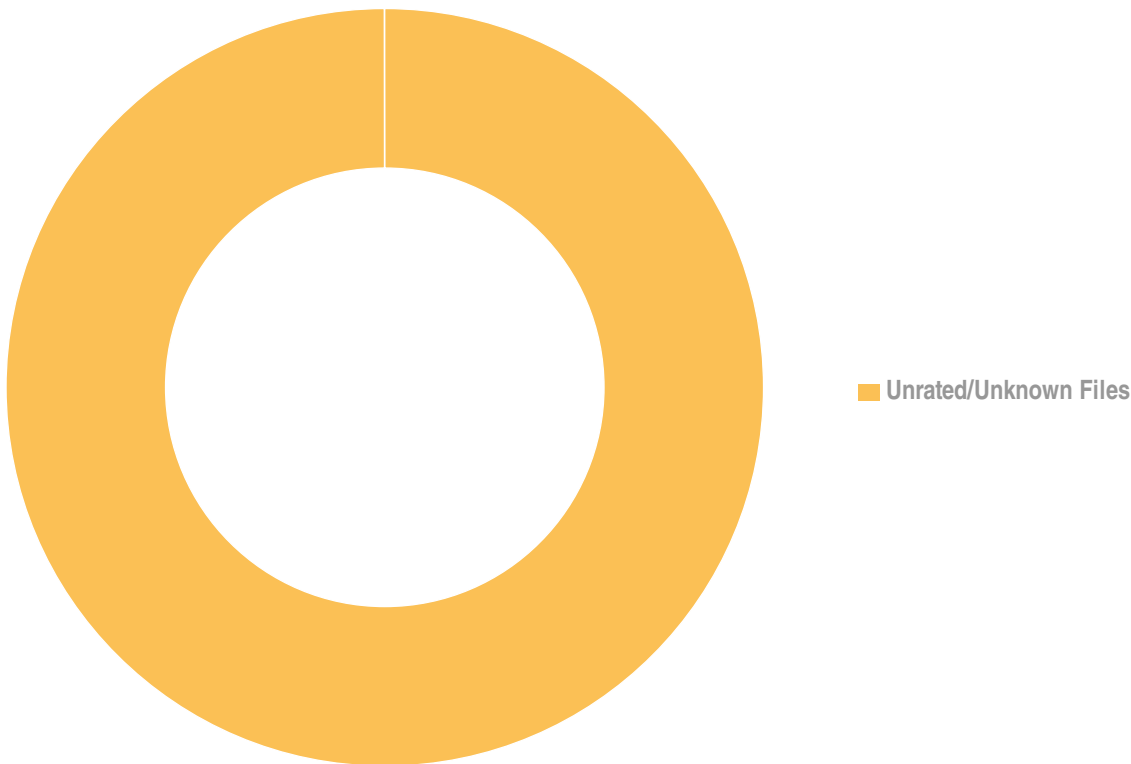
3055413 Unrated/Unknown Files

Alerts

Alerts Over Time

Indicators and rules allow security professionals to automate the notification of events in real time. Indicators can be created for suspicious, malicious, or prohibited behavior, and then rules automatically generate alerts to notify analysts of suspicious activity and violations. A sudden increase in the number of alerts could be an indication of a malicious attack.
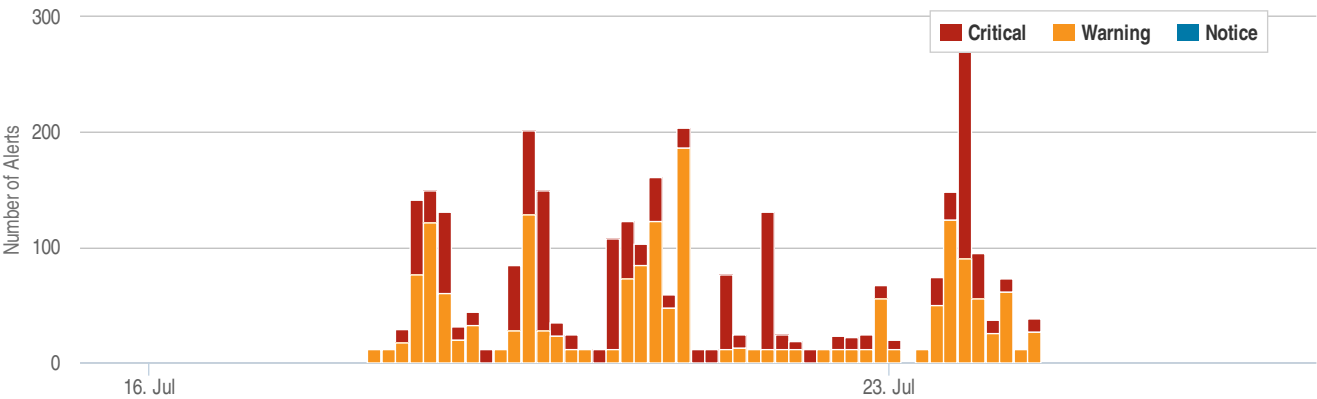
Top 5 Rules

Rule	Alert Count
finename	1651
Blue Coat Web Reputation Service	1064
Alert - Heartbleed Attack Attempt	202
Blue Coat File Reputation Service	10
Local File Analysis	5

Top 5 Indicators

Indicator	Alert Count
Filename	1651
Blue Coat Web Reputation Service	1064
Heartbleed Attack Attempt	202
Blue Coat File Reputation Service Presented File Extensions	8
Local File Analysis	5

Systems Impacted by Alerts

Alerts are generated for suspicious, malicious, or prohibited behavior. Systems with a high number of alerts should be investigated, especially if they are part of the critical company infrastructure or are known to contain confidential company information.

Top 10 Source IPs

Source IP Address	Alert Count
177.1	202
.146.77	159
.18.181	109
.20.20	103
.49.251	87
.17.130	81
.17.201	79
51.101	64
.80.124	58
.24.44	56

Top 10 Destination IPs

Destination IP Address	Alert Count
.33.53	109
.248.58	81
.149.29	79
.75.214	79
.75.202	69
.130.24	60
.75.204	57
.75.208	51
.175.42	51
.26.24	51

Network Visibility

See All. Know More. Respond Faster.

Applications Identified by Risk

A variety of applications - most commonly web applications - are used to penetrate and carry out attacks. Applications that provide file transfer and communication exchange usually pose a greater risk to business as they are the easy means of data loss, exfiltration, and in the event of a compromise, are often used for command and control. Application visibility is a key to measuring risk and protecting assets.

| Application	Bytes	Risk
tcp > ssl > https > tor	4.61 KB	10 ⚠
udp > utp > bittorrent	7.52 GB	9 ⚠
tcp > ssl > https > vector	1.74 GB	9 ⚠
tcp > bittorrent	1.32 GB	9 ⚠
tcp > uusee	408.47 MB	9 ⚠
udp > bittorrent	186.76 MB	9 ⚠
udp > kazaa	111.83 MB	9 ⚠
tcp > edonkey	6.99 MB	9 ⚠
tcp > gnutella	1.06 MB	9 ⚠
tcp > http > bittorrent	1.00 MB	9 ⚠

Considerations for Risk Classification

- Can it be used for data exfiltration?
- Does the app encrypt/obfuscate data rendering analysis difficult or impossible?
- Does it have a propensity to sharing questionable content such as copyright material, illegal, etc.?
- Is it adult oriented?
- Can it be or has it been associated with malicious activity/intent?
- Does it generally have no practical use in most corporate networks (e.g. gaming)?
- Does it provide some type of remote console/system control (e.g. RDP, SSH)?
- Does it transmit sensitive data in clear text (e.g. telnet, POP3, FTP)?

Capture Summary

Capture Rate by Interface

Advanced threat detection, prevention, and effective preparedness have become urgent priorities as organizations accept the inevitably of successful security breaches. Security operation centers need to rely on security technologies that allow them to gain real-time situational awareness, context, intelligence, and visibility.
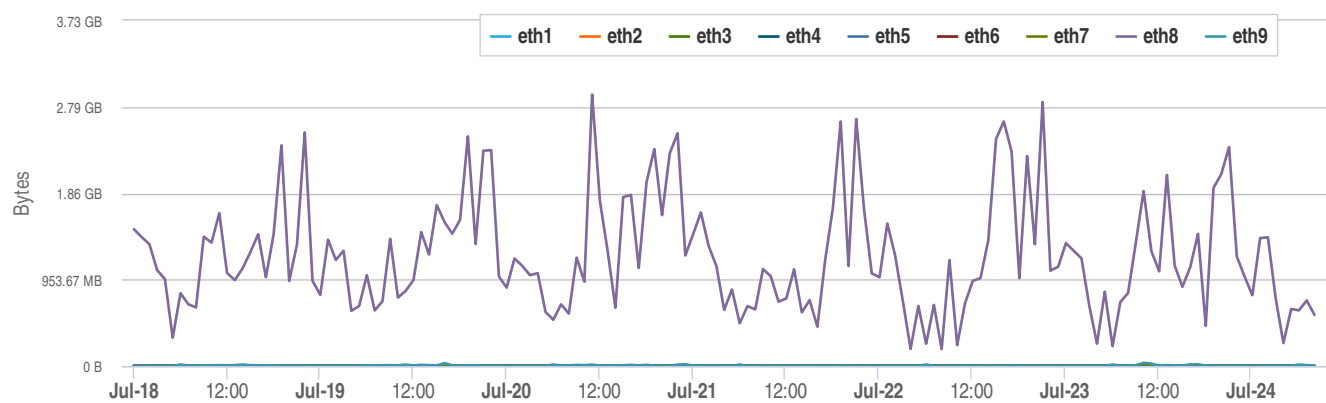
Active Interfaces

eth8
Max Capture Rate: 694.93 MB/s
Total Captured: 65.12 TB
Total Filtered: 34.98 GB

eth9
Max Capture Rate: 14.40 MB/s
Total Captured: 76.35 GB
Total Filtered: 97.33 MB

Inactive Interfaces

eth1
Max Capture Rate: 0 B/s
Total Captured: 0 B
Total Filtered: 0 B

eth2
Max Capture Rate: 0 B/s
Total Captured: 0 B
Total Filtered: 0 B

eth3
Max Capture Rate: 0 B/s
Total Captured: 0 B
Total Filtered: 0 B

eth4
Max Capture Rate: 0 B/s
Total Captured: 0 B
Total Filtered: 0 B

eth5
Max Capture Rate: 0 B/s
Total Captured: 0 B
Total Filtered: 0 B

eth6
Max Capture Rate: 0 B/s
Total Captured: 0 B
Total Filtered: 0 B

eth7
Max Capture Rate: 0 B/s
Total Captured: 0 B
Total Filtered: 0 B

Anomalies

Preventing known threats is not enough.
Detect and prepare for the unknown.
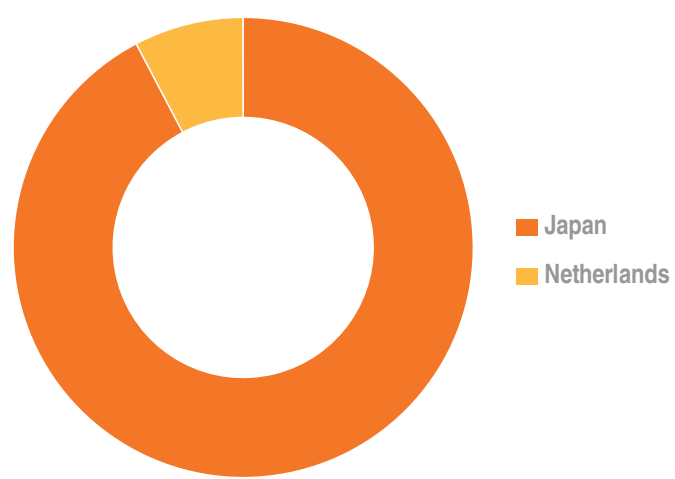
Anomalies

Anomalies Over Time

Anomaly detection is about enabling proactive incident response by giving the incident response team the ability to hunt for potential risks proactively. By utilizing analysis to hunt intelligently, the incident response team can focus attention on anomalies that most likely represent actual threats. An important step towards achieving a comprehensive information security and incident response program is to establish a baseline of normal behavior in the data. This tells you what network activity looks normal so you can identify abnormal activity.
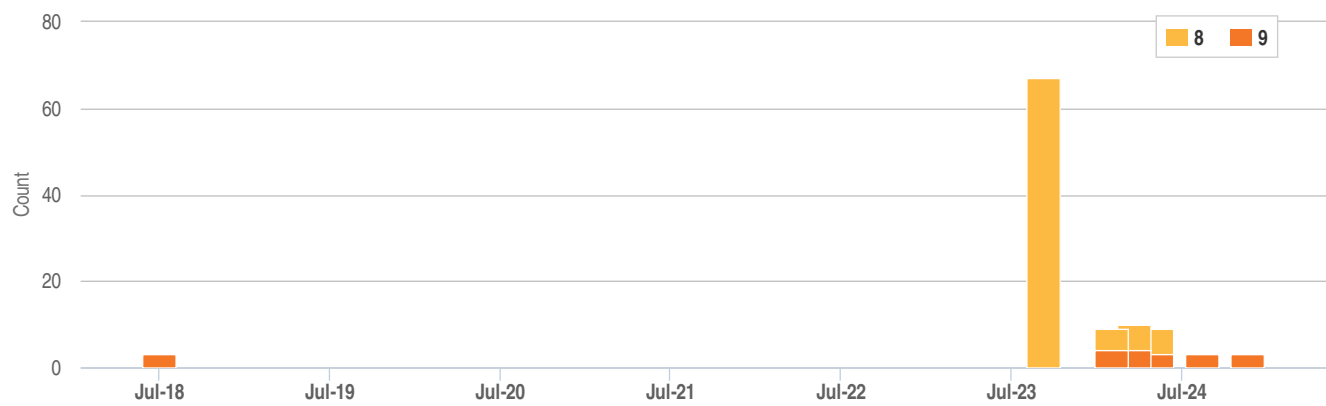
Anomalies by Score
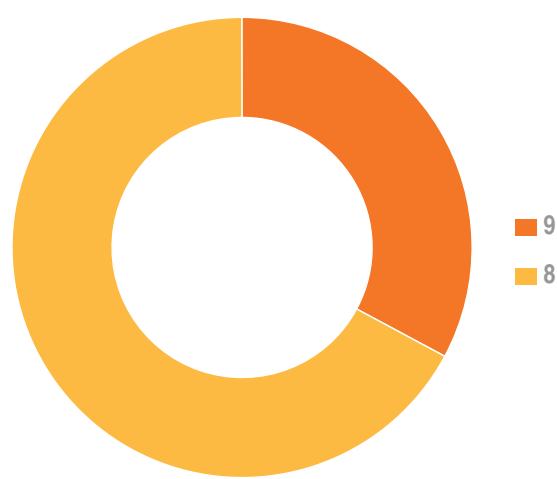
Anomalies by Location

Anomalies

An automated anomaly detection solution allows your security and incident response teams to understand normal baseline activity. The team can then be alerted on abnormal activity that may be a sign of an attack or security breach. While one anomaly detection indicator may not be suspicious, multiple indicators could mean your response team needs to quickly investigate.

IP Initiators with Anomalies

IP Initiator	Anomaly Count
6.177.1	87
.16.62	29
.19.65	15
.36.91	4
.27.124	4
.27.125	3
.36.15	3
.16.242	2
.177.206	2
16.241	2

IP Responders with Anomalies

IP Responder	Anomaly Count
.177.1	49
.26.35	39
.137.36	22
.11.15	11
8.11.5	11
.1.3	11
.16.62	10
.32.16	10
.34.64	10
.15.254	10

Appendix

Symantec Security Analytics - a cornerstone
of effective security incident response.

Network Visibility

Detect breaches and integrate context

- Complete, lossless packet capture on high-speed network (24/7 – all ports/all traffic)
- Comprehensive DPI with layers 2-7 indexing (over 2,800 applications classified)
- Actionable intelligence, anomaly detection and event reconstruction (full packet, flow, session & file)
- Chronological display of all network events validates compliance and acceptable use policies
- Scalable deployment as either appliance/software/virtual appliance for days/weeks/months of traffic

Reconstruct Incidents & Extract Evidence

- Know what happened before, during and after an alert, with complete, clear supporting evidence
- Multiple sources for real-time integrity & reputation of URL, IP address, file hash or email address
- Trace back and discover Tactics, Techniques & Procedures and identify Indicators of Compromise
- Integrated workflows with leading network and endpoint security tools to add context and improve effectiveness

Remediate & Fortify - Increased Time to Action

- Retrospective forensics analysis on any attack
- Answer critical "post-breach" questions that plague CISOs - how? what? who? when? ...
- Root Cause Explorer quickly identifies the source of attack, reducing time-to-resolution
- Faster time-to-identification/action/reaction with Security Analytics allows up to 85% faster resolution
- Global Intelligence Network updated with newly-discovered threat intelligence

Threat Analysis

Intelligence Services

The Global Intelligence Network (GIN) is one of the world's largest threat-intelligence knowledge bases. The GIN is a massive clearing house of known-good and known-bad content, fed by over 15,000 enterprise organizations and 75 million users. With service points to more than 50 antivirus knowledge bases, the GIN provides attribution of content and web activity on an unprecedented scale. The software-based Symantec Intelligence Services harness this incredible power for real-time network threat detection.

The Intelligence Services, embedded in Security Analytics, analyze and classify file content, network activity, URLs, and IP addresses in real time to find malware, malicious activity, botnet activity, phishing, and other indicators of compromise. By extracting and analyzing key file types such as Microsoft Office documents, Adobe Flash and PDFs, Java, EXE files, email attachments, Android APK files, web objects and more, Intelligence Services alert security analysts to the presence of known malicious activity across many network transports including web sessions, file-transfer mechanisms, email protocols, and raw TCP connections. They detect and report suspicious web sites and network activity in more than 100 different categories and use reputation data on URLs and IP addresses to identify network traffic originating from known bots, spammers, phishing sites, malware sources, and compromised websites. For novel threats, zero-day malware, and targeted attacks not previously seen by the GIN, comprehensive static and dynamic behavioral analysis is performed in real time by the Malware Analysis appliance.

Threat Analysis

Advanced Malware Analysis

Tightly integrated with Symantec Security Analytics and File Reputation Service, Malware Analysis provides a highly scalable solution for detecting and analyzing unknown, advanced, and targeted malware in near-real time. Uncovering sophisticated attacks requires sophisticated approaches to detection, which are core capabilities provided by Malware Analysis. This adaptive and customizable sandbox solution delivers enterprise-class, comprehensive malware detonation and analysis using a unique, dual-detection approach based on emulation and virtualization. It quickly analyzes suspicious files and URLs, interacts with running malware to reveal its complete behavior, and exposes zero-day threats.

Malware Analysis provides broader coverage than typical consolidated single-sandbox solutions by supporting custom-tailored Windows execution environments, as well as Android and iOS malware analysis all on a single platform. Unlike some "black box" approaches, the system is fully extensible, supporting customizable behavioral-detection patterns and customizable YARA analysis. With the fully exposed Windows environments, robust configurations and customizations can be made to closely match corporate "gold" images. As unknown, advanced, or targeted malware and zero-day threats are exposed, the new threat intelligence is continuously shared across the security infrastructure and with the Symantec Global Intelligence Network.

Network Visibility

Encrypted Traffic Visibility

As of 2015, most enterprise network traffic averages 40-50% SSL/TLS traffic. In almost all cases, current security tools cannot examine this traffic, and this lack of visibility into SSL can make it difficult or impossible for network and security teams to stop intrusions and malware before they compromise their targets. For example, Symantec research labs has observed that the Dyre banking Trojan uses SSL over multiple non-standard TCP ports for its command & control activity and data exfiltration capabilities. Without the ability to inspect SSL content, sensitive or critical information can easily be accidentally leaked or worse: stolen.

Network and security professionals already deploy an array of network security appliances to protect their organizations, enforce acceptable-use policies, and satisfy government regulations. These devices can control network applications and provide intrusion detection and prevention (IDS/IPS), antivirus protection, data-loss prevention, network forensics, and more. Unfortunately, these network security appliances can usually inspect only plaintext traffic and so are unable to inspect SSL-encrypted communications for malware, hidden threats, or exfiltrated data. They therefore become less and less effective as the volume of encrypted SSL traffic grows. Further, organizations easily miss half of the ROI and value from their existing network security solutions if they are unable to see and inspect decrypted SSL traffic.

SSL Visibility, coupled with Security Analytics, allows security teams to see what they've been missing. Incident Response is easier with 100% visibility into all of the traffic. Hidden threats are uncovered, analyzed, and classified in real time. Data-loss analysis is exponentially simpler with access to content that normally would be encrypted on the wire. Security Analytics implements role-based access control to provide assurances that only authorized individuals and systems can access decrypted content.

Network Visibility

Applications Identified

Securing business critical applications should be a top priority for any security organization. Most enterprises have hundreds or even thousands of applications running over their networks. A variety of applications—most commonly web applications—are used to penetrate and carry out attacks. Applications that provide file transfer and communication exchange usually pose a greater risk to business as they are the easy means of data loss, exfiltration, and in the event of comprommise, are often used for command and control. The basic step of having visibility into the activity of all the applications in a network is an important one for measuring risk and protecting the assets and information that is vital to any enterprise.

Symantec Security Analytics has the unique capability to identify and classify thousands of applications—and extensive metadata for each application—using a powerful deep packet inspection engine. This ability empowers security teams to have information on all of the applications running on their network, regardless of application port or protocol. Security Analytics delivers comprehensive application intelligence, which enables security organizations to regain application control on their networks.