Symantec. Security Analytics

Risk and Visibility Report

Report Timespan:
June 21, 2017 10:00AM GMT-0500 to
June 30, 2017 10:15AM GMT-0500

Report Generated: June 30, 2017 10:19AM GMT-0500
Generated by: Administrator

Executive Summary

Key Findings

2
Malicious files detected by FRS

10
Malicious URLs detected by WRS

4
Systems Impacted

11
Systems Impacted

4
Malicious Files detected by MA

28.34 GB
High Risk Traffic

14
Systems Impacted

Potential risk of data loss or policy compliance issues

60.13%
Encrypted Traffic

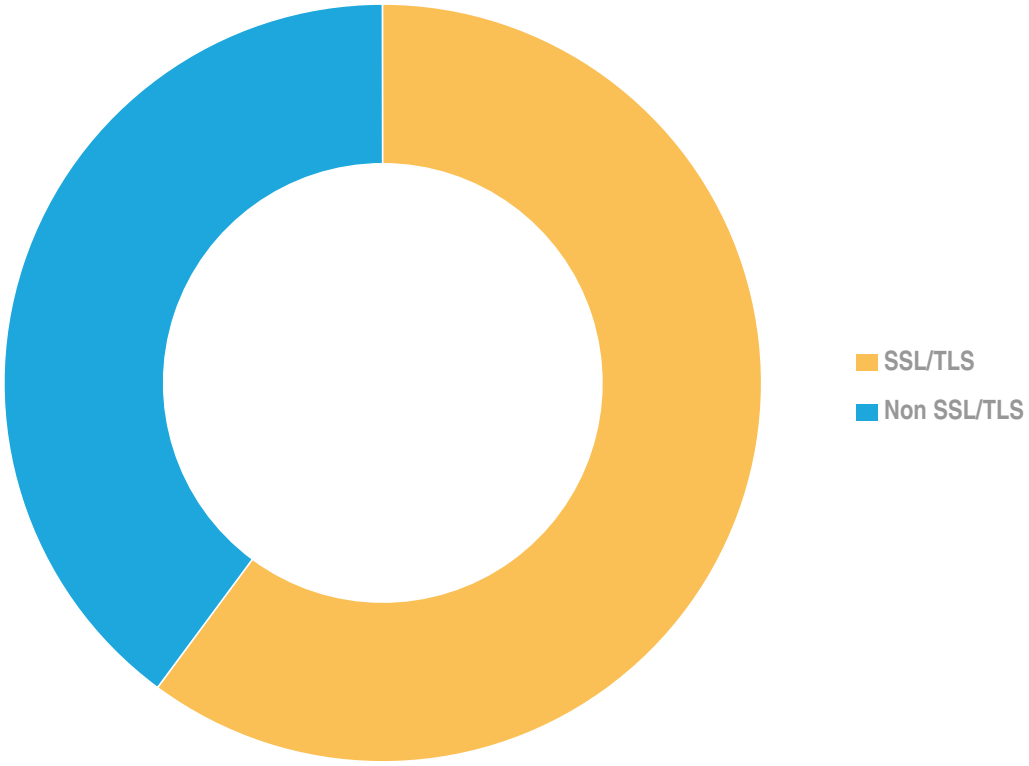
668
Predicted Files Hidden in Encrypted Traffic

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.



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.

436 ZIP Files

117 PE (exe) Files

61 7ZIP Files

35 PDF Files

19 FLASH (swf) Files

Application Groups using SSL

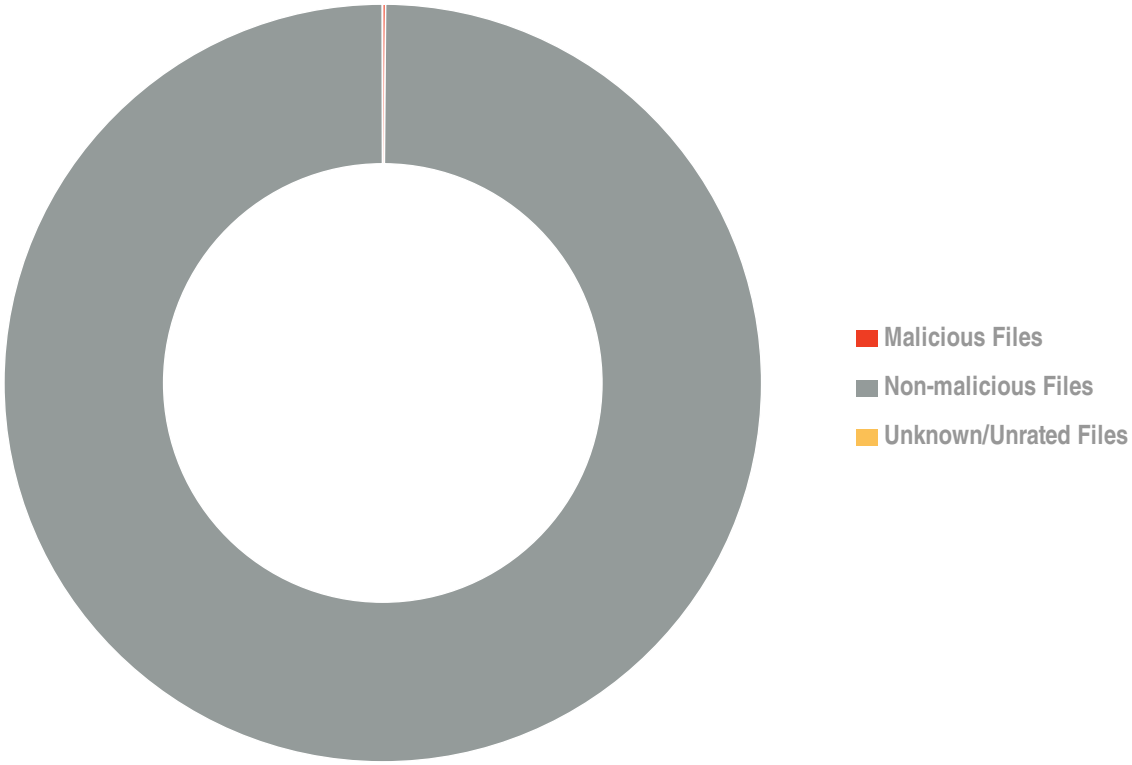
Without the ability to inspect SSL content, sensitive or critical information can easily be accidentally leaked or worse: stolen. Network security appliances can usually inspect only plaintext traffic and so are unable to inspect SSL-encrypted communications for malware, hidden threats, or exfiltrated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

Application Group	Bytes
Web	117.10 GB
Standard	16.45 GB
Audio/Video	15.59 GB
Mail	9.10 GB
Application Service	1.13 GB
Forum	273.79 MB
Instant Messaging	261.67 MB
Encrypted	158.80 MB
Webmail	78.95 MB
Network Service	35.89 MB
Game	32.77 MB
Security Service	13.19 MB
Antivirus	1.12 MB
Peer to Peer	751.11 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.



2 (0.12%) Malicious Files

1.72K (99.88%) Non-malicious Files

0 (0.00%) Unknown/Unrated Files

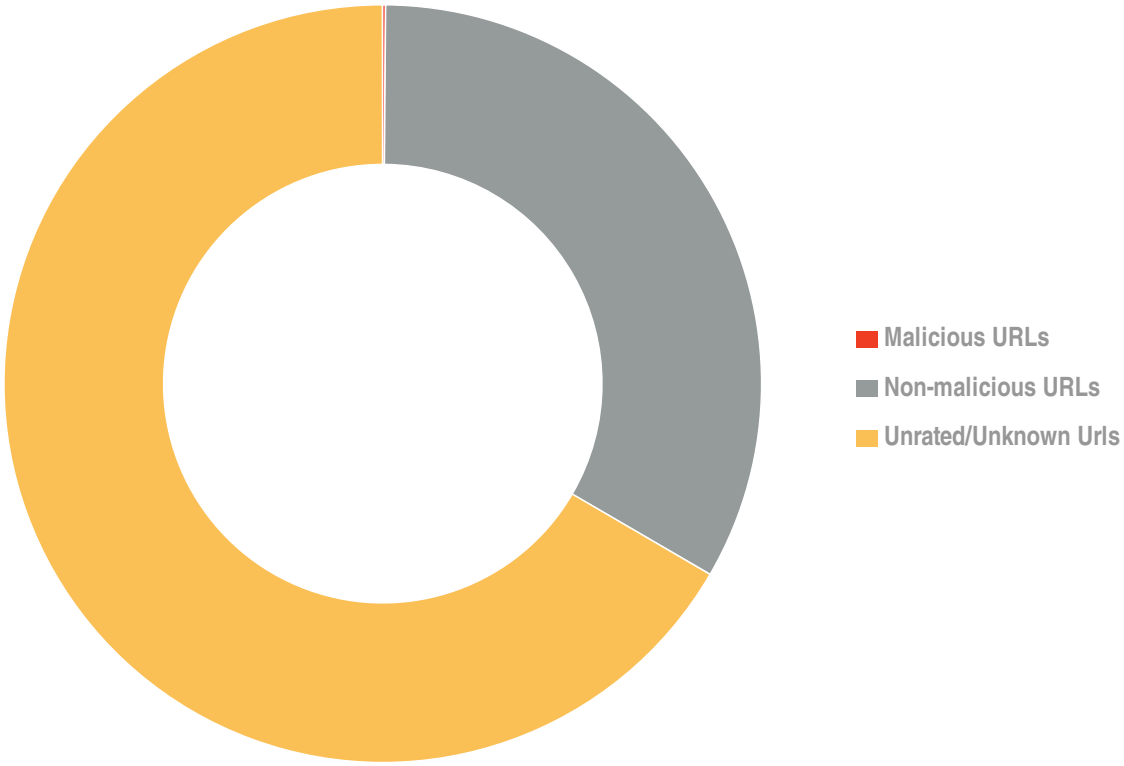
1.72K Total Files Analyzed

4 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.



10 (0.12%) Malicious URLs

2.77K (33.29%) Non-malicious URLs

5.55K (66.59%) Unrated/Unknown Urls

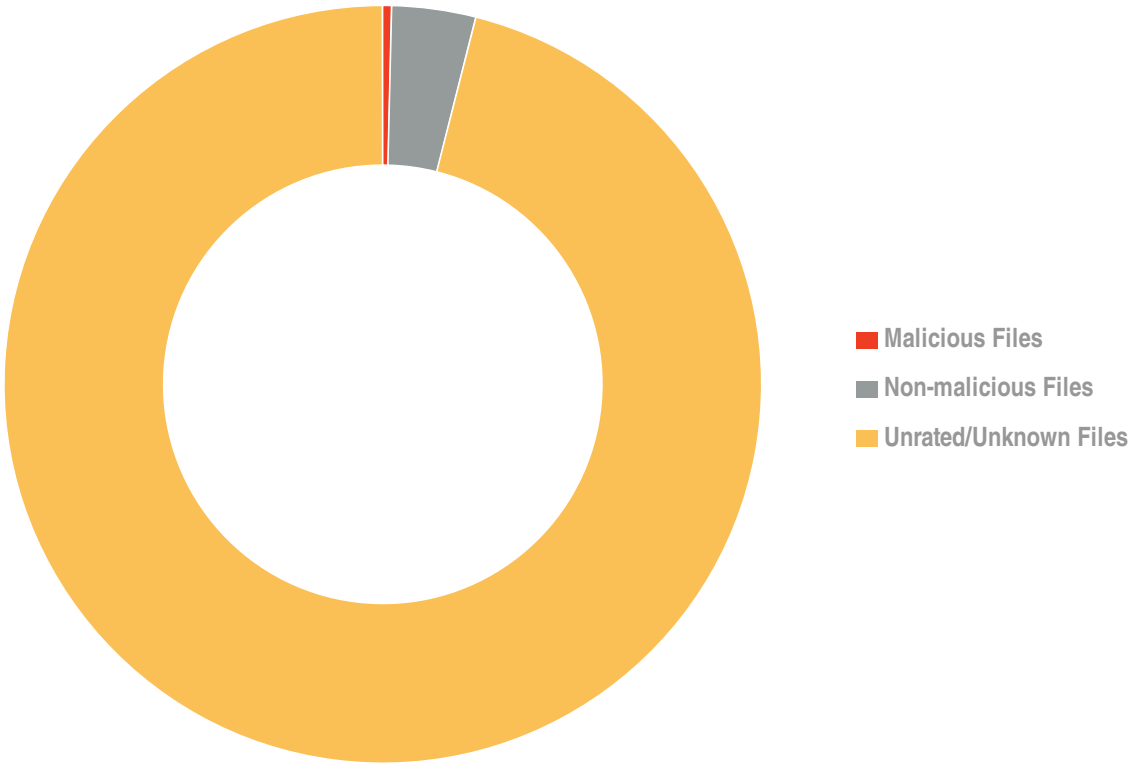
8.33K Total URLs Analyzed

11 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.



4 (0.38%) Malicious Files

38 (3.58%) Non-malicious Files

1.02K (96.04%) Unrated/Unknown Files

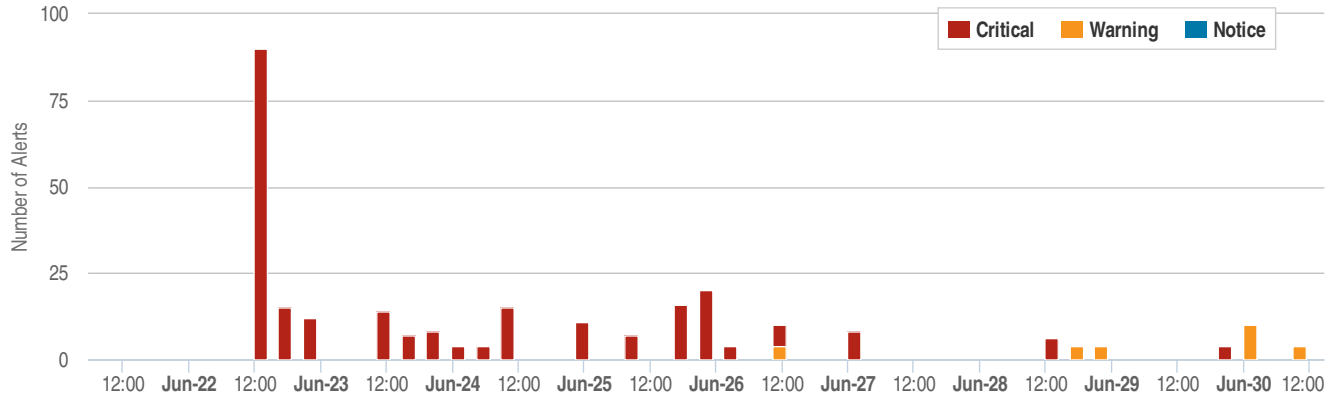
1.06K Total Files Analyzed

14 Systems Impacted

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
Blue Coat Web Reputation Service	228
Symantec Malware Analysis Service	34
Local File Analysis - Live Exploits	2
Local File Analysis	2

Top 5 Indicators

Indicator	Alert Count
Blue Coat Web Reputation Service	228
Blue Coat File Reputation Service Presented MIME Types	16
Blue Coat File Reputation Service File Types	9
Blue Coat File Reputation Service Presented File Extensions	9
Local File Analysis - Live Exploits	2

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
10.1.1.106	120
192.168.8.128	90
172.18.1.4	24
10.1.1.102	12
192.168.4.6	7
10.1.1.175	6
10.1.1.112	3
172.18.1.6	2
2602:30a:2c51:b73f:f666:6de8:6cba:ac4e	2

Top 10 Destination IPs

Destination IP Address	Alert Count
107.154.108.7	108
46.105.131.124	27
96.44.136.154	27
149.174.97.123	12
188.40.61.79	10
149.174.144.10	8
212.129.9.221	7
10.1.1.175	6
62.210.112.171	6
94.102.158.162	6

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 > tor	102.94 MB	10
tcp > ssl > https > tor	32.15 MB	10
udp > utp > bittorrent	9.99 GB	9
tcp > bittorrent	5.59 GB	9
bittorrent	560.85 MB	9
udp > bittorrent	531.02 MB	9
tcp > http > bittorrent > vuze	49.22 MB	9
tcp > http > vuze	1.25 MB	9
tcp > ssl > https > vuze	751.11 KB	9
udp > dns > vpnoverdns	711.07 KB	9

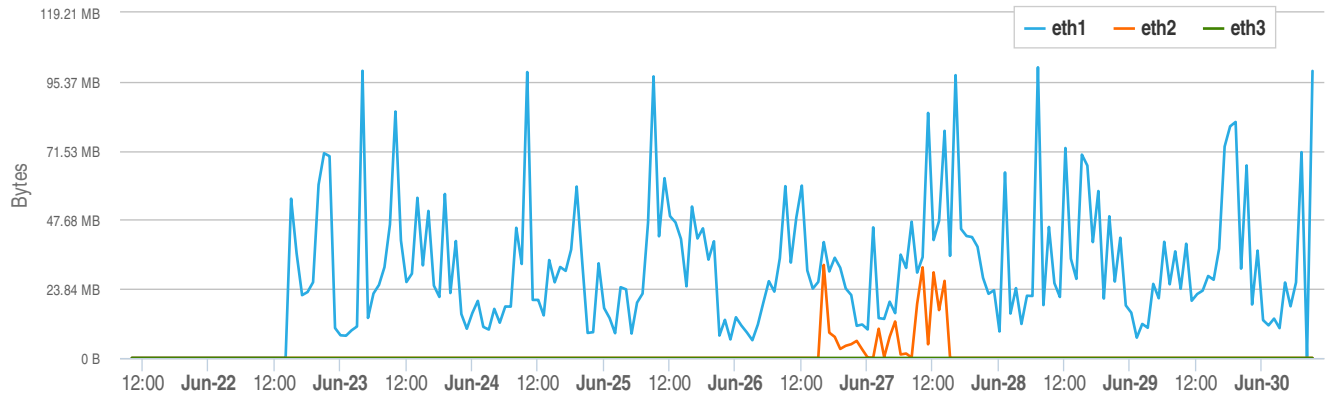
Considerations for Risk Classification

- 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

eth1

Max Capture Rate: 1.18 GB/s
Total Captured: 116.66 GB
Total Filtered: 0 B

eth2

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

Inactive Interfaces

eth3

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

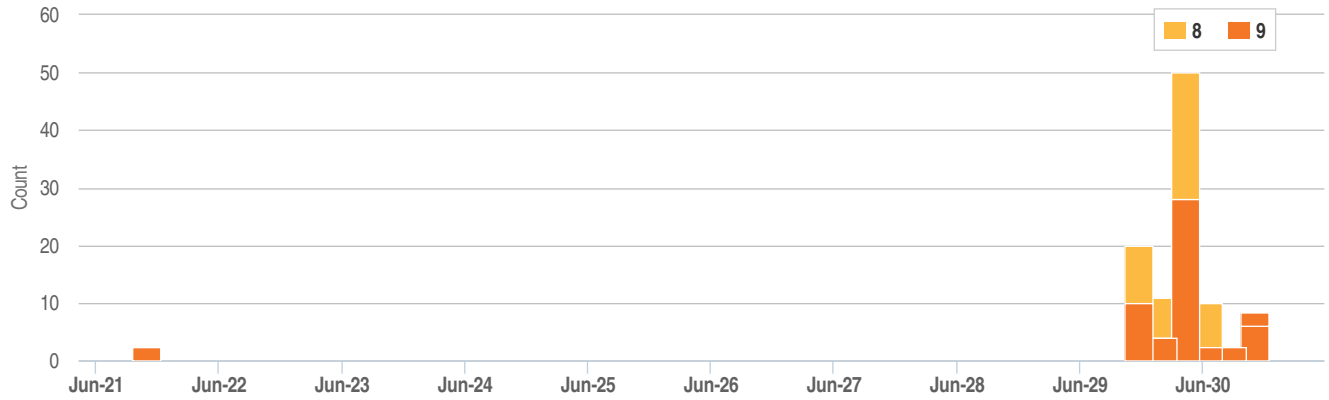
Anomalies

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

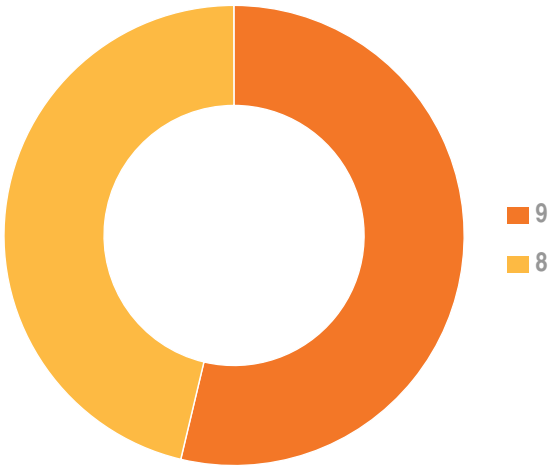
Anomalies

Anomalies Over Time

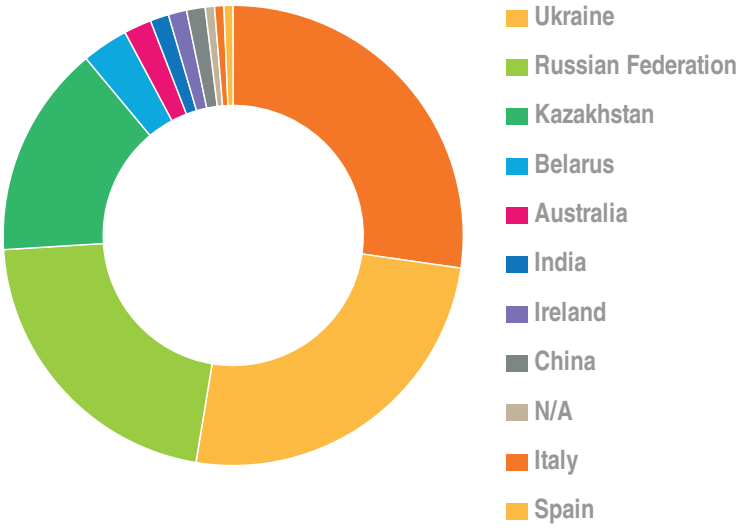
Anomaly detection is about enabling proactive incident response by giving the incident response team the ability to hunt for potential risks proactively. By utilizing analysis to hunt intelligently, the incident response team can focus attention on anomalies that most likely represent actual threats. 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
2602:30a:2c51:b73f:58f1:d9e5:1da3:852	12
192.168.2.233	11
217.197.250.146	10
192.168.4.6	9
10.1.1.100	9
172.28.195.1	8
2602:30a:2c51:b73f:6e:beb:fd46:7285	8
93.80.249.145	7
172.68.195.1	7
192.168.3.7	7

IP Responders with Anomalies

IP Responder	Anomaly Count
192.31.80.30	23
81.163.111.2	23
81.163.100.2	23
192.42.93.30	22
185.113.38.81	19
83.143.236.147	18
192.26.92.30	17
192.55.83.30	16
192.33.14.30	16
192.5.6.30	15

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 compromise, 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.