MANAGED SECURITY SERVICE

Portal User Guide - Cisco
# Table of contents

**Introduction**..................................................................................................................3
**Sign in to Managed Security portal**..................................................................................3
**Detailed Security Metrics**..................................................................................................5
  **Overview tab – Summary dashboard**...............................................................................5  
    Network subtab...................................................................................................................6  
    Threats subtab....................................................................................................................11  
    Intrusion Events subtab.......................................................................................................13  
    Geolocation subtab............................................................................................................18  
  **Overview tab – Application Statistics dashboard**..............................................................20  
    Connections subtab............................................................................................................20  
    Intrusion Events subtab.......................................................................................................23  
  **Overview tab – Connections Summary dashboard**...........................................................27  
    Connections subtab............................................................................................................27  
    Traffic subtab.....................................................................................................................29  
    Geolocation subtab............................................................................................................32  
    URL subtab.........................................................................................................................36  
  **Overview tab – Detailed dashboard**.................................................................................40  
    Intrusion Events subtab.......................................................................................................40  
    Context subtab....................................................................................................................43  
  **Overview tab – Files dashboard**.......................................................................................46  
    Malware subtab..................................................................................................................46  
    Files subtab.........................................................................................................................51  
**Analysis tab**.......................................................................................................................55  
  **Context Explorer tab**.......................................................................................................55  
    Traffic and Intrusion Events over Time.............................................................................56  
    Indications of Compromise...............................................................................................56  
    Network Information..........................................................................................................57  
    Application Protocol Information......................................................................................60  
    Intrusion Information.........................................................................................................62  
    File Information................................................................................................................65  
    Geolocation Information....................................................................................................68  
    URL Information.................................................................................................................70  
    Intelligence Feeds.............................................................................................................73
Introduction

Sign In to the Managed Security Portal

Supported browsers
The Managed Security portal is best viewed in the following browsers:

- Chrome®
- Firefox®
- Internet Explorer® (PC only)
- Safari® (MAC only)

Account access
The Managed Services portal provides access to the Managed Security Services and Managed Router Services reporting tools. The Managed Services portal is located at https://ms.spectrumenterprise.net.

Access your account by logging in with your username and password. If you have forgotten your password, click the “Forgot Password?” link.

When you click on the “Forgot Password” link and fill out the information below, the system will send you an email to reset your password. If the email doesn’t show in your inbox, please check your Spam or Junk File in case your network doesn’t recognize the sender.
The following page will appear with instructions on resetting your password:

Once you have logged into the Managed Services portal, the Managed Services landing page will appear:

Click on the “Radio Button”; this will bring you to the portal login page:
Username: E-Mail address
Password:

• The very first time a user logs in to the portal they’ll have to change their password. The password the Spectrum portal shows the first time they click the icon is the password they use the first time.

• When a user logs in with these credentials, the system will ask them to change their password.

Once you create your new password and log into the portal, it will bring you to the landing page.

**Detailed security metrics**

When you Log in, you will see two tabs — the Overview tab and the Analysis tab. Within each tab there are subtabs that contain graphs that provide different information about your managed devices.

**Overview tab — Summary dashboard**

Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

The first tab you see in the Managed Security portal is the Overview — Summary Dashboard tab, which contains widgets and graphs that together offer a complete overview of Managed Security data on your monitored network.

There are four subtabs that give you an at-a-glance picture of recent trends in your network’s activity. The four subtabs are:

• Network
• Threats
• Intrusion Events
• Geolocation
Network subtab
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

Unique Applications over Time
Displays a graph of total unique applications detected on your monitored network over the dashboard time range.

Traffic by Application Risk
Displays estimated risk levels of applications on your monitored network, based on total kilobytes of data transmitted on your monitored network by applications at each level for the selected time period.

Risk is determined by how likely it is that the application will be used for purposes that violate your organization’s security policy.
Traffic by Business Relevance
Displays estimated business relevance levels of applications on your monitored network, based on total kilobytes of data transmitted on your monitored network by applications at each level over the dashboard time range.

Business Relevance is the likelihood that the application is being used within the context of your organization's business operations, as opposed to recreationally. Example: Gaming applications tend to have a very low business relevance.

Traffic by Application Category
Displays application categories on your monitored network, based on total kilobytes of data transmitted on your monitored network by applications in each category over the dashboard time range.
Top Web Applications Seen
Displays web applications on your monitored network, based on total kilobytes of data transmitted by the web application itself.

Top Server Applications Seen
Displays server applications on your monitored network, based on the number of hosts running the service.
Risky Applications with Low Business Relevance
Displays all application connections on your monitored network that have both high application risk level and low estimated business relevance.

Business Relevance is the likelihood that the application is being used within the context of your organization’s business operations, as opposed to recreationally. Example: Gaming applications tend to have a very low business relevance.

Connections by URL Reputation
Displays all application connections on your monitored network, grouped by URL reputation.

URL reputation is determined by how likely a web site is to be used for purposes that might be against your organization’s security policy. Managed Security provides feeds which contain IP addresses, domain names, and URLs with poor reputation, as determined by security intelligence. The two feeds are:

- **Intelligence Feed** which contains several regularly updated collections of IP addresses
- **DNS and URL Intelligence Feed** which contains several regularly updated collections of domain names and URLs

Intelligence Feeds
Because malicious IP addresses, domain names, and URLs that represent security threats (malware, spam, botnets, and phishing) can appear and disappear faster than you can update and deploy new policies, the Intelligence Feeds keep track of open relays, known attackers, bogus IP addresses, and so on. Spectrum Enterprise continually updates its threat intelligence feeds with new URLs, domain names, and IP addresses, as well as new categories and risks for existing URLs, to ensure that our system uses the most up-to-date threat information to filter your network traffic.
Top Client Applications Seen

Displays operating systems on your monitored network, based on the number of network hosts with the operating system.
Connections by URL Category
Displays all application connections on your monitored network, grouped by URL category.

Threats subtab
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

Indications of Compromise by Host
Displays the hosts on your network that are the most likely to be compromised, grouped by associated host IP address. Indicators of Compromise are a quick and easy way to identify which hosts might have been exploited.
**Malware Threats**
Displays the number of malware threats detected in network traffic by the system and grouped by threat name.

**New Indications of Compromise over Time**
Displays a graph of new indications of compromise detected over the dashboard time range.

**Intrusion Events**
The Intrusion Events widget shows the intrusion events that occurred over the time period specified on the Dashboard, organized by priority from most severe to least severe. This includes statistics on intrusion events with dropped packets. On managed devices, the widget can display statistics for dropped (or, on passively deployed devices, would have dropped) intrusion events, all intrusion events, or both.
Note: All events trigger a notification to technical support to investigate and resolve the event.

- Impact 0: Neither the source or the destination host is on a monitored network
- Impact 1: The host is vulnerable. The source or destination host is potentially compromised by a virus, Trojan, or other piece of malicious software
- Impact 2: The host is potentially vulnerable
- Impact 3: The host is currently not vulnerable
- Impact 4: The source or the host is on a monitored network, but there is no entry for the host in the network map

**Intrusion Events subtab**

Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Top Attackers**

Displays attacking host IP addresses on your monitored network, based on the number of intrusion events where the listed IP address was the attacker in the connection that caused the event.
**Top Targets**
Displays destination host IP addresses (where your traffic is going to) on your monitored network, based on the number of intrusion events where the destination host IP address was targeted in the connection that caused the event.

![Top Targets Table]

**Dropped Intrusion Events**
Displays counts for intrusion events, by classification, where the packet was dropped.

![Dropped Intrusion Events Table]
All Intrusion Events
Displays a graph of the total number of intrusion events on your monitored network over the dashboard time range.

Intrusion Events
The Intrusion Events widget shows the intrusion events that occurred over the time period specified on the Dashboard, organized by priority from least severe to most severe. This includes statistics on intrusion events with dropped packets. On managed devices, the widget can display statistics for dropped (or, on passively deployed devices, would have dropped) intrusion events, all intrusion events, or both.

Note: All events trigger a notification to technical support to investigate and resolve the event.

- **Impact 0**: Neither the source or the destination host is on a monitored network.
- **Impact 1**: The host is vulnerable. The source or destination host is potentially compromised by a virus, Trojan, or other piece of malicious software.
- **Impact 2**: The host is potentially vulnerable.
- **Impact 3**: The host is currently not vulnerable.
- **Impact 4**: The source or the host is on a monitored network, but there is no entry for the host in the network map.
**Total Events by Application Protocol**
Displays application protocols on your monitored network, based on the number of intrusion events associated with the application protocol.
Impact 1 Events by Application Protocol
The number of events that indicate that the host is vulnerable (impact 1). The source or destination host is potentially compromised by a virus, trojan, or other piece of malicious software.

Impact 2 Events by Application Protocol
The number of events that indicate the host is potentially vulnerable (not as serious as impact 1) grouped by application protocol.
Geolocation subtab
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

Intrusion Events by Source Country
Displays countries where intrusion events originated, based on the number of events originating from each country. The +1 and -1 indicate an increase and a decrease in ranking, respectively.

Intrusion Events by Destination Country
Displays destination countries (where the traffic from your network is going to) targeted by intrusion events. Countries are listed based on the amount of destination traffic where intrusion events were detected.
Intrusion Events by Source Continent
Displays continents where intrusion events originated (the traffic came to your network), based on the number of events originating from each continent.

<table>
<thead>
<tr>
<th>Source Continent</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>552</td>
</tr>
<tr>
<td>Europe</td>
<td>31</td>
</tr>
<tr>
<td>Asia</td>
<td>26</td>
</tr>
<tr>
<td>South America</td>
<td>10</td>
</tr>
</tbody>
</table>

Last updated 1 hour, 42 minutes ago

Intrusion Events by Destination Continent
Displays destination continents (where the traffic from your network is going to) targeted by intrusion events. Continents are listed based on the amount of destination traffic where intrusion events were detected.

<table>
<thead>
<tr>
<th>Destination Continent</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>420</td>
</tr>
<tr>
<td>Europe</td>
<td>145</td>
</tr>
<tr>
<td>Asia</td>
<td>57</td>
</tr>
<tr>
<td>South America</td>
<td>3</td>
</tr>
</tbody>
</table>

Last updated 1 hour, 42 minutes ago
Overview tab – application statistics dashboard

Connections subtab
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

Allowed Connections by Application
Displays allowed application connections on your monitored network, grouped by application.

Denied Connections by Application
Displays denied connections on your monitored network, grouped by application.
Unique Applications over Time
Displays a graph of total unique applications detected on your monitored network over the dashboard time range.

Allowed Connections by Application Risk
Displays allowed application connections on your monitored network, grouped by application risk level.

Risk is determined by how likely it is that the application will be used for purposes that violate your organization's security policy.
Allowed Connections by Business Relevance
Displays allowed application connections on your monitored network, grouped by estimated relevance to business activity.

Business Relevance is the likelihood that the application is being used within the context of your organization’s business operations, as opposed to recreationally. Example: Gaming applications tend to have a very low business relevance.

Traffic by Application
Displays applications on your monitored network, based on total kilobytes of data transmitted on your monitored network by the application over the dashboard time range.
Traffic by Application Category
Displays application categories on your monitored network, based on total kilobytes of data transmitted on your monitored network by applications in each category over the dashboard time range.

Intrusion Events subtab
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

Dropped Events by Application
Displays dropped intrusion events, grouped by application.
**Impact 3 Events by Application**
Displays number of events where the host is not vulnerable (impact 3) grouped by application.

![Impact 3 Events by Application]

**Impact 1 Events by Application**
Displays number of events where the host is vulnerable (impact 1) grouped by application. The source or destination host is potentially compromised by a virus, trojan, or other piece of malicious software.

![Impact 1 Events by Application]
**Impact 4 Events by Application**
Displays number of events of estimated impact level 4 grouped by application.

Impact 4 means either the source or destination host is on a monitored network, but there is no entry for the host in the network map.

![Impact 4 Events by Application](image)

**Total Events by Application Protocol**
Displays applications on your monitored network, based on the number of intrusion events generated by the application.

![Total Events by Application Protocol](image)
**Impact 2 Events by Application**
Displays number of events where the host is potentially vulnerable (impact 2) grouped by application.

**Impact 0 Events by Application**
Displays number of events of estimated impact level 0 grouped by application. Impact 0 means neither the source nor the destination host is on a network that is monitored by network discovery.
Overview tab – Connections summary dashboard

Connections subtab
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

Connections by Initiator IP
Displays host IP addresses on your monitored network, based on the number of connections where that IP address on a host initiated the session.

Connections by Responder IP
Displays host IP addresses on your monitored network, based on the number of connections where the responder in that session was that IP address on a host. The output of this widget varies when there is an increase in connections from a specific responder IP.
Connections over Time
Displays a graph of the total number of connections on your monitored network, over the dashboard time range.

![Connections over Time Graph](image)

Connections by Port
Displays ports on your monitored network, based on the number of detected connections.

<table>
<thead>
<tr>
<th>Responder Port</th>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>53 (domain) / udp</td>
<td>852</td>
</tr>
<tr>
<td>80 (http) / tcp</td>
<td>436</td>
</tr>
<tr>
<td>123 (ftp) / udp</td>
<td>5</td>
</tr>
</tbody>
</table>

Last updated 5 minutes ago
Connections by Applications
Displays applications on your monitored network, based on the number of detected connections.

Traffic subtab
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

Traffic by Initiator IP
Displays host IP addresses on your monitored network, based on total kilobytes of data transmitted on your monitored network from the IP address over the dashboard time range.
Traffic by Responder IP
Displays IP addresses on your monitored network, based on total kilobytes of data received by the IP addresses (on hosts) over the dashboard time range. The output of this widget varies when there is an increase in connections from a specific responder IP.

Traffic over Time
Displays a graph of total kilobytes of data transmitted on your monitored network over the dashboard time range.
Traffic by Port
Displays responder ports on your monitored network, based on total kilobytes of data transmitted on your monitored network via each port over the dashboard time range. The output of this widget varies according to your connection logging configuration.

Traffic by Application
Displays applications on your monitored network, based on total kilobytes of data transmitted on your monitored network by the application over the dashboard time range.
Geolocation subtab
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

Connections by Source Country
Displays countries communicating with your monitored network, based on the number of connections initiated from each country.

<table>
<thead>
<tr>
<th>Initiator Country</th>
<th>Total Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA (United States)</td>
<td>88,635</td>
</tr>
<tr>
<td>BRA (Brazil)</td>
<td>5,277</td>
</tr>
<tr>
<td>GBR (United Kingdom)</td>
<td>43</td>
</tr>
<tr>
<td>AUS (Australia)</td>
<td>31</td>
</tr>
<tr>
<td>EUR (Europe (unknown Country))</td>
<td>31</td>
</tr>
<tr>
<td>IRL (Ireland)</td>
<td>30</td>
</tr>
<tr>
<td>CHN (China)</td>
<td>24</td>
</tr>
<tr>
<td>CZE (Czech Republic)</td>
<td>12</td>
</tr>
<tr>
<td>NLD (Netherlands)</td>
<td>9</td>
</tr>
<tr>
<td>ITA (Italy)</td>
<td>6</td>
</tr>
</tbody>
</table>

Last updated 3 minutes ago

Connections by Destination Country
Displays countries communicating with your monitored network (traffic is coming to you), based on the number of connections.

<table>
<thead>
<tr>
<th>Responder Country</th>
<th>Total Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA (United States)</td>
<td>2,758</td>
</tr>
<tr>
<td>GBR (United Kingdom)</td>
<td>5</td>
</tr>
</tbody>
</table>

Last updated 3 minutes ago
Connections by Source Continent
Displays continents your monitored network is communicating with (you are sending traffic), based on the number of connections initiated from each continent.

Connections by Destination Continent
Displays continents that sent connections to your monitored network (traffic is coming to you), based on the number of connections.
Traffic by Source Continent
Displays continents sending data to your monitored network, based on total kilobytes of data transmitted from each continent during the selected time range.

Note: When a graph contains no data, it means that the device did not send any information to Managed Security portal for the time range selected; it does not indicate a problem with the device itself.

Traffic by Destination Continent
Displays continents contacted from your monitored network (you sent traffic), based on total kilobytes of data transmitted to each continent during the selected time range.
**Traffic by Source Country**
Displays countries transmitting data to your monitored network (traffic is coming to you), based on total kilobytes of data transmitted from each country during the selected time range.

![Traffic by Source Country Table]

**Traffic by Destination Country**
Displays countries contacted from your monitored network, based on total kilobytes of data transmitted on your monitored network to each country over the dashboard time range.

![Traffic by Destination Country Table]
**URL subtab**
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Allowed Connections by URL Category**
Displays allowed application connections on your monitored network, grouped by URL category.

**Denied Connections by URL Category**
Displays denied connections on your monitored network, grouped by URL category.
Traffic by URL Category
Displays application URL categories on your monitored network, based on total kilobytes of data exchanged with URLs of each category over the dashboard time range.

Traffic by URL Reputation
Displays application URL reputation types on your monitored network, based on total kilobytes of data exchanged with URLs of each reputation over the dashboard time range.

URL reputation is determined by how likely a web site is to be used for purposes that might be against your organization's security policy. Spectrum Enterprise provides feeds which contain IP addresses, domain names, and URLs with poor reputation, as determined by security intelligence. The two feeds are:

- Intelligence Feed, which contains several regularly updated collections of IP addresses
- DNS and URL Intelligence Feed, which contains several regularly updated collections of domain names and URLs

Intelligence Feeds
Because malicious IP addresses, domain names, and URLs that represent security threats (malware, spam, botnets, and phishing) can appear and disappear faster than you can update and deploy new policies, the Intelligence Feeds keep track of open relays, known attackers, bogus IP addresses, and so on. Cisco continually updates its threat intelligence feeds with new URLs, domain names, and IP addresses, as well as new categories and risks for existing URLs, to ensure that our system uses the most up-to-date threat information to filter your network traffic.
Allowed connections by URL Reputation
Displays allowed application connections on your monitored network, grouped by URL reputation.

URL reputation is determined by how likely a web site is to be used for purposes that might be against your organization’s security policy. Cisco provides feeds which contain IP addresses, domain names, and URLs with poor reputation, as determined by Cisco’s Security Intelligence. The two feeds are:

• Intelligence Feed, which contains several regularly updated collections of IP addresses
• DNS and URL Intelligence Feed, which contains several regularly updated collections of domain names and URLs

Intelligence Feeds
Because malicious IP addresses, domain names, and URLs that represent security threats (malware, spam, botnets, and phishing) can appear and disappear faster than you can update and deploy new policies, the Intelligence Feeds keep track of open relays, known attackers, bogus IP addresses, and so on. Cisco continually updates its threat intelligence feeds with new URLs, domain names, and IP addresses, as well as new categories and risks for existing URLs, to ensure that our system uses the most up-to-date threat information to filter your network traffic.
Denied Connections by URL Reputation
Displays denied connections on your monitored network, grouped by URL reputation. URL reputation is determined by how likely a web site is to be used for purposes that might be against your organization’s security policy. Managed Security provides feeds which contain IP addresses, domain names, and URLs with poor reputation, as determined by security intelligence. The two feeds are:

- Intelligence Feed which contains several regularly updated collections of IP addresses
- DNS and URL Intelligence Feed which contains several regularly updated collections of domain names and URLs

Intelligence Feeds
Because malicious IP addresses, domain names, and URLs that represent security threats (malware, spam, botnets, and phishing) can appear and disappear faster than you can update and deploy new policies, the Intelligence Feeds keep track of open relays, known attackers, bogus IP addresses, and so on. Cisco continually updates its threat intelligence feeds with new URLs, domain names, and IP addresses, as well as new categories and risks for existing URLs, to ensure that our system uses the most up-to-date threat information to filter your network traffic.
Overview tab – Detailed dashboard

Intrusion Events subtab
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

Intrusion Events
The Intrusion Events widget shows the intrusion events that occurred over the time period specified on the Dashboard, organized by priority from least severe to most severe. This includes statistics on intrusion events with dropped packets. On managed devices, the widget can display statistics for dropped (or, on passively deployed devices, would have dropped) intrusion events, all intrusion events, or both.

Note: All events trigger a notification to technical support to investigate and resolve the event.

- Impact 0: Neither the source or the destination host is on a monitored network.
- Impact 1: The host is vulnerable. The source or destination host is potentially compromised by a virus, Trojan, or other piece of malicious software.
- Impact 2: The host is potentially vulnerable.
- Impact 3: The host is currently not vulnerable.
- Impact 4: The source or the host is on a monitored network, but there is no entry for the host in the network map.
**All Intrusion Events**
Displays a graph of the total number of intrusion events on your monitored network over the dashboard time range.

![All Intrusion Events Graph](image)

Last updated 2 hours, 7 minutes ago.

**All Intrusion Events (Not Dropped)**
Displays the most frequently occurring types of intrusion events, by classification, where the packet was not dropped as part of the event.

![All Intrusion Events (Not Dropped) Table](image)

Last updated 2 hours, 7 minutes ago.
**Dropped Intrusion Events**
Displays counts for intrusion events, by classification, where the packet was dropped.

![Dropped Intrusion Events]

**Intrusion Events Requiring Analysis**
Displays a count of intrusion events requiring analysis, based on event classification.

Note: When a graph contains no data, it means that the device did not send any information to Managed Security portal for the time range selected; it does not indicate a problem with the device itself.

![Intrusion Events Requiring Analysis]
**Context subtab**
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Servers**
Displays servers, by number of hosts.

![Server Graph]

**Operating Systems**
Displays operating systems, based on the number of hosts running each operating system within your network.

![Operating System Graph]
**Clients**
Displays clients on your monitored network, by type.

**Traffic by Application**
Displays applications on your monitored network, based on total kilobytes of data transmitted on your monitored network by the application over the dashboard time range.
**Traffic by Initiator IP**
Displays host IP addresses on your monitored network, based on total kilobytes of data transmitted on your monitored network from the IP address over the dashboard time range.

**Traffic by Responder IP**
Displays IP addresses on your monitored network, based on total kilobytes of data received by the IP addresses (on hosts) over the dashboard time range. The output of this widget varies when there is an increase in connections from a specific responder IP.
Traffic over Time
Displays a graph of total kilobytes of data transmitted on your monitored network over the dashboard time range.

Overview tab — Files dashboard
Malware subtab
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

Hosts Receiving Malware
Displays the number of malware files received by host IP addresses on your network, grouped by IP address.
**Hosts Sending Malware**
Displays the number of malware files sent from host IP addresses on your network, grouped by IP address.

**Application Protocols Introducing Malware**
Displays the number of malware files transmitted over your network, grouped by the application protocol used to transmit the files.

**Client Applications Introducing Malware**
Displays the applications, or parent files, that accessed or created malware detected by the Advanced Malware protection tool.
**Web Applications Introducing Malware**
Displays web applications on your monitored network that accessed or created malware detected by the Advanced Malware protection tool.

![Web Applications Introducing Malware](image1)

**Possible Zero Day Malware**
Displays the captured files most likely to be zero-day malware, with a file disposition of unknown and either High or Very High threat scores, based on the number of times the file was seen.

![Possible Zero Day Malware](image2)

**Malware Threats**
Displays the number of malware threats detected either in network traffic by the system or by Spectrum Enterprise, grouped by threat name.

![Malware Threats](image3)
**Threat Detections over Time**
Displays a graph of the total number of malware threats detected either in network traffic by the system or by Spectrum Enterprise, over the dashboard time range.

![Threat Detections over Time](image)

**Top Threats**
Displays the distribution of threat scores, based on the number of stored files with that threat score.

Note: When a graph contains no data, it means that the device did not send any information to Managed Security portal for the time range selected; it does not indicate a problem with the device itself.
Malware Intrusions
Displays intrusion events, based on the number of intrusion events occurring in connections transmitting malware.

Note: When a graph contains no data, it means that the device did not send any information to Managed Security portal for the time range selected; it does not indicate a problem with the device itself.

File Types Infected with Malware
Displays the number of malware detected either in network traffic by the system or by Spectrum Enterprise, grouped by file type.
**Processes Introducing Malware**
Displays the system processes that accessed or created malware detected by Spectrum Enterprise.

Note: When a graph contains no data, it means that the device did not send any information to Managed Security portal for the time range selected; it does not indicate a problem with the device itself.

**Files subtab**
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Hosts Receiving Files**
Displays the number of files received (downloaded) by host IP addresses on your network, grouped by IP address.
Hosts Sending Files
Displays the number of files sent (uploaded) from host IP addresses on your network, grouped by IP address.

Applications Protocols Transferring File
Displays the number of files transmitted over your network, grouped by the application protocol used to transmit the files.

Client Applications Transferring files
Displays the applications, or parent files, that transmitted files over your network.
Web Applications Transferring Files
Displays the number of files transmitted over your network, grouped by the web application used to transmit the files.

File Transfers over Time
Displays a graph of the total number of file transfers detected in network traffic by the system, over the dashboard time range.

File Dispositions
Displays the number of files detected in network traffic as a result of Malware Cloud Lookup file rules, grouped by malware disposition. A local lookup is performed first; then for any unknown files, Spectrum Enterprise performs a cloud lookup and stores the information locally.
File Actions
Displays the number of files transmitted over your network, grouped by the file rule actions used to handle the files.

File Categories
Displays the number of files transmitted over your network, grouped by file category.

File Types
Displays the number of files transmitted over your network, grouped by file type.
File Names
Displays the number of files transmitted over your network, grouped by file name.

Analysis tab
The Analysis tab in the Managed Security portal is divided into sections that show you even more details about events and trends you might see on the dashboards on the Overview tab.

The Analysis tab includes the following subtabs:

- Context Explorer
- Connections
- Intrusions
- Files
- Host

Context Explorer tab
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

The Context Explorer tab contains details that help you to understand more information and gather data to determine the best needs for your company. This section explains the parts of the Context Explorer and the graphs contained in each section.
Traffic and Intrusion Events over Time
At the top of the Context Explorer is a line chart of traffic and intrusion events over time. The X-axis (horizontal line) plots time intervals, which range from five minutes to one month, depending on the selected time window. The Y-axis (vertical line) plots traffic in kilobytes (blue line) and intrusion event counts (red line).

By default, this section shows all network traffic and all generated intrusion events for the selected time range. If you apply filters, the chart changes to display only traffic and intrusion events associated with the specified filters.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Indications of Compromise
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

Hosts by Indication
The Hosts by Indication pie chart displays a proportional view of the Indications of Compromise triggered by hosts on your monitored network.

• The inner ring divides by category (such as Command and Control Connected or Malware Detected).
• The outer ring divides data by specific event type.

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.
**Indications by Host**
Indications by Host bar graph displays the IP addresses and counts of unique Indications of Compromise triggered by the top 15 most active users on your monitored network.

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.

The other sections are sets of interactive graphs that you can click to see lists that provide greater detail for indications of compromise, network, application, intrusion, file, geolocation, and URL data.

Note: All the sections on the Analysis tab combined together are called the Context Explorer.

**Network information**
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

This section contains interactive graphs on monitored network information.

**Operating Systems**
The Operating Systems pie graph shows you the operating systems running on your network.

- Inner ring shows groups of operating systems, such as Windows
- Outer ring shows details about versions of the operating systems, such as Windows XP
Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.

**Traffic by Source IP**

The Traffic by Source IP bar graph shows you the IP addresses of the users on your network who generate the most traffic. Blue bars represent source IP address and red bars represent connection data.

Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.
**Traffic by Destination IP**
The Traffic by Destination IP bar graph shows you the top destination addresses for traffic leaving your network. Blue bars represent the destination IP address and red bars represent connection data.

Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.

![Traffic by Destination IP](image1)

**Connections by Access Control Action**
The Connections by Access Control Action pie graph displays a proportional view of the access control actions (determined when the security policy is defined) taken the most regarding your network traffic.

Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.

![Connections by Access Control Action](image2)
Traffic by Source User
The Traffic by Source User graph, in bar form, displays counts of network traffic (in kilobytes per second) and unique connections for the top 15 most active source users on your monitored network. For each source IP address listed, blue bars represent traffic data and red bars represent connection data.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Application Protocol Information
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

The Application Protocol Information section displays application groups together by type. Charts are color-coded to indicate the risk level and business relevance for each type of application.

For example, there can be traffic that is exposing your network to risk, but has little or no business relevance. This could lead to policies and decisions about what types of traffic to keep out of your network.

Intrusion Events by Risk and Application
The Intrusion Events by Risk and Application donut graph displays the applications by intrusion events and is arranged by the applications’ estimated risk (default) or by estimated business relevance.

• The inner ring represents estimated risk- or business-relevance level (such as Medium or High)

• The outer ring shows you the actual applications that represent the risk

Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.
Business Relevance is the likelihood that the application is being used within the context of your organization’s business operations, as opposed to recreationally. Example: Gaming applications tend to have a very low business relevance.

Note: The assignment of risk and business relevance are maintained by security intelligence.

Hosts by Risk and Application

The Hosts by Risk and Application donut graph displays the applications used most by your users and is arranged by the applications’ estimated risk (default) or by estimated business relevance.

- The inner ring represents estimated risk- or business-relevance level (such as Medium or High)
- The outer ring shows you the actual applications that represent the risk

Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.

Business Relevance is the likelihood that the application is being used within the context of your organization’s business operations, as opposed to recreationally. Example: Gaming applications tend to have a very low business relevance.

Note: The assignment of risk and business relevance are maintained by security intelligence.
**Application Details List**

The Application Detail List displays below the Risk and Application graphs. In this list you can see all the identified applications from each graph with the application’s name, Risk, Business Relevance, Category, and numbers of hosts.

---

**Intrusion information**

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Risk</th>
<th>Business Relevance</th>
<th>Category</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>High</td>
<td>Business</td>
<td>Web browser</td>
<td>54</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>Medium</td>
<td>Medium</td>
<td>Web browser</td>
<td>25</td>
</tr>
<tr>
<td>Google Search</td>
<td>Very high</td>
<td>Medium</td>
<td>Web service provider</td>
<td>15</td>
</tr>
<tr>
<td>MySQL</td>
<td>Very high</td>
<td>High</td>
<td>Web service provider</td>
<td>5</td>
</tr>
<tr>
<td>Microsoft Outlook</td>
<td>Medium</td>
<td>Medium</td>
<td>Web service provider</td>
<td>9</td>
</tr>
<tr>
<td>VMware Horizon</td>
<td>Low</td>
<td>Low</td>
<td>Web service provider</td>
<td>9</td>
</tr>
<tr>
<td>Adobe Flash Player</td>
<td>High</td>
<td>High</td>
<td>Browser plugin, business, software update</td>
<td>7</td>
</tr>
<tr>
<td>Firefox</td>
<td>Very high</td>
<td>Low</td>
<td>Email, gaming, instant messaging, media player</td>
<td>7</td>
</tr>
</tbody>
</table>

Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Intrusion Events by Impact**

The Intrusion Events by Impact pie chart displays a proportional view of intrusion events on your monitored network, grouped by estimated impact level; 0 is the least impactful and 4 is the most impactful.

- **Impact 0**: Neither the source or the destination host is on a monitored network
- **Impact 1**: The host is vulnerable. The source or destination host is potentially compromised by a virus
- **Trojan, or other piece of malicious software**
- **Impact 2**: The host is potentially vulnerable
- **Impact 3**: The host is currently not vulnerable
- **Impact 4**: The source or the host is on a monitored network, but there is no entry for the host in the network map
Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

**Top Attackers graph**
The Top Attackers bar graph shows the IP addresses sorted by the number of intrusion events (targeted in the connections causing those events) on your monitored network.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
Intrusion Events by Priority
The Intrusion Events by Priority graph, in pie form, displays a proportional view of intrusion events on your monitored network, grouped by estimated priority level (such as High, Medium, or Low).

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

This graph draws data primarily from the Intrusion Events table.

---

Top Targets graph
The Top Targets bar graph shows the top 10 target host IP addresses sorted by number of intrusion events (targeted in the connections causing those events) on your monitored network.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
File Information
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

Top File Types
The Top File Types donut graph displays a view of detected file types associated with malware.

- The outer ring shows file types detected in network traffic
- The inner ring shows the file types grouped by category

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on information.

Top Hosts Sending Files
The Top Hosts Sending Files or Malware graph shows the top IP addresses of users sending malware or the top users sending files across your network.

To switch between the number of files and the number of files containing malware, point to the graph and select the option that shows what you want to see.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
Top File Names
The Top File Names bar graph shows the names of the files affected by malware that were detected in network traffic.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Top Hosts Receiving Files
The Top Hosts Receiving Files graph shows the IP addresses of the users who receive the most files.

To switch between the number of files and the number of files containing malware, point to the graph and select the option that shows what you want to see.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
Files by Disposition
Shows the status of the files that were detected by the network.

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.

Top Malware Detections
Shows the Point to a bar in the graph to see detailed information about the malware, such as the threat name and the number of files that contain the selected malware.
Geolocation Information

Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

Geolocation Information section contains three interactive donut graphs that display an overall picture of countries with which hosts on your monitored network are exchanging data: unique connections by initiator or responder country, intrusion events by source or destination country, and file events by sending or receiving country.

Connections by Initiator Country

The Connections by Initiator/Responder Country donut graph displays a proportional view of the countries involved in connections on your network as either the initiator (the default) or the responder.

- The inner ring groups the connections by continent
- The outer ring groups the connections by country

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
Intrusion Events by Source Country

The Intrusion Events by Source Country donut graph displays countries targeted by intrusion events, based on the number of events associated with each country.

- The inner ring groups the connections by continent
- The outer ring groups the connections by country

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
**File Events by Sending Country**
The File Events by Sending/Receiving Country donut graph displays a proportional view of the countries detected in file events on your network as either sending (the default) or receiving files.

- The inner ring groups the connections by continent
- The outer ring groups the connections by country

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

![File Events by Sending Country](image)

**URL Information**
Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

The URL Information section contains three interactive bar graphs that display an overall picture of the URLs that the hosts on your monitored network use to exchange data.

These graphs show you traffic and unique connections associated with URLs, sorted by:

- Separate URLs
- URL category
- URL reputation

Note: You must have enable URL Filtering for these graphs to include URL category and URL reputation data. Contact Spectrum Enterprise to set up these filtering options for you.
Traffic by URL
The Traffic by URL bar graph shows network traffic in kilobytes per second and unique connections for most-requested URLs on your monitored network. For each URL listed, blue bars represent traffic data and red bars represent connection data.

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.

Traffic by URL Category
The Traffic by URL Category bar graph shows network traffic in kilobytes per second and unique connections for the most-requested URL categories on your monitored network. For each URL category listed, blue bars represent traffic data and red bars represent connection data.

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.
Traffic by URL Reputation
The Traffic by URL Reputation bar graph shows network traffic in kilobytes per second and unique connections for the most requested URL reputation groups on your monitored network. For each URL reputation listed, blue bars represent traffic data and red bars represent connection data.

The URL reputations are:
- Well known
- Benign site
- Benign with Security Risk
- Suspicious Site
- High Risk

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.

URL reputation is determined by how likely a web site is to be used for purposes that might be against your organization’s security policy. Managed Security provides feeds which contain IP addresses, domain names, and URLs with poor reputation, as determined by security intelligence. The two feeds are:

- Intelligence Feed which contains several regularly updated collections of IP addresses
- DNS and URL Intelligence Feed which contains several regularly updated collections of domain names and URLs
**Intelligence Feeds**

Because malicious IP addresses, domain names, and URLs that represent security threats (malware, spam, botnets, and phishing) can appear and disappear faster than you can update and deploy new policies, the Intelligence Feeds keep track of open relays, known attackers, bogus IP addresses, and so on. Spectrum Enterprise continually updates its threat intelligence feeds with new URLs, domain names, and IP addresses, as well as new categories and risks for existing URLs, to ensure that our system uses the most up-to-date threat information to filter your network traffic.

---

**About Spectrum Enterprise**

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. Spectrum Enterprise’s industry-leading team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. More information about Spectrum Enterprise can be found at [enterprise.spectrum.com](http://enterprise.spectrum.com).