



ForeScout App for Splunk

How-to Guide

Version 1.0.1



About the ForeScout App for Splunk

The ForeScout app for Splunk provides a dashboard of key metrics for endpoints monitored and managed by ForeScout CounterACT, including:

- Patterns of network access over time
- Device types in the network
- Registered corporate users vs. guests
- Endpoint compliance status summaries
- And more

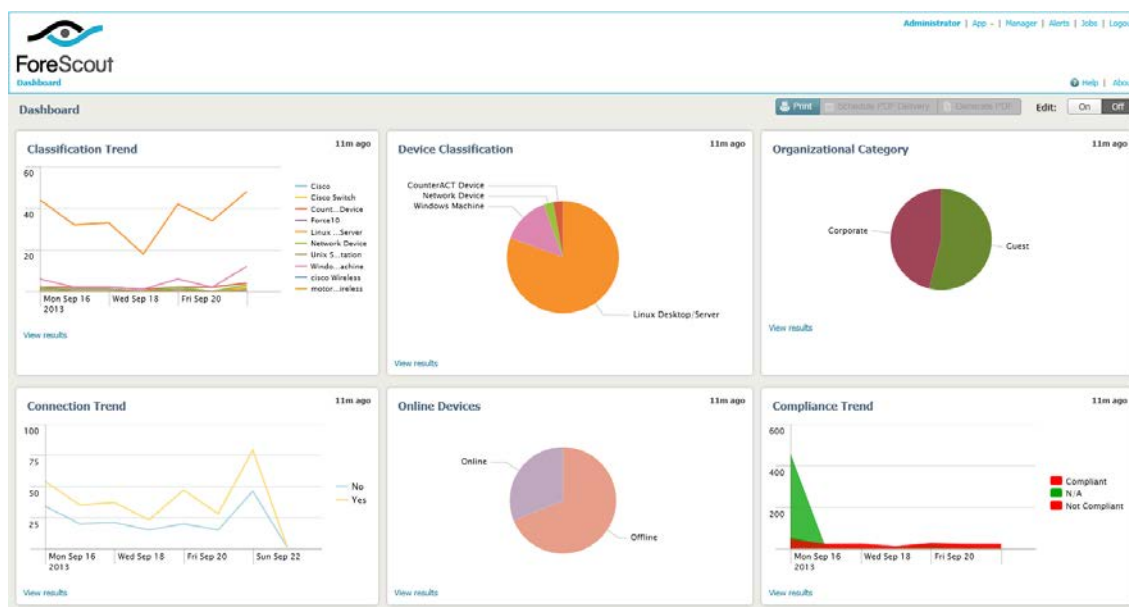
You can determine the network scope CounterACT reports to Splunk, for example:

- Report on all endpoints
- Report for a specific network segment or IP range
- Report by a specific user group or device type

You can control the volume and frequency of CounterACT reports to Splunk, for example:

- Schedule recheck and repeat behaviors for policies and actions that report data to Splunk.
- Use endpoint discovery/admission events to trigger data reporting to Splunk.

By default, the dashboard includes events from the past week. Some panels are based on hourly data. You can use standard Splunk tools to modify this default time frame.



Before You Begin


Perform the following steps to work with the dashboard:

- Verify that you are running CounterACT version 7.0.0 with the most recent Hotfix.
- Verify that the following template policies are active:
 - Classification
 - Corporate/Guest Control
 - Compliance

Host information determined by these policies is reported to Splunk. Similarly, host information determined by other policies categorized as *Classification*, *Corporate/Guest Control*, or *Compliance* policies is reported to Splunk.

Verify that version 3.0.0 or higher of the Data Exchange Plugin is installed on CounterACT. This plugin provides the DEX Send Web Service Request action, which is the preferred method for CounterACT to send data to Splunk. For information about accessing the plugin, navigate to:

<http://updates.forescout.com/support/files/plugins/splunk-app/Updates.pdf>

 *If the Data Exchange Plugin is not installed, you can use Syslog messaging to submit data to Splunk.*

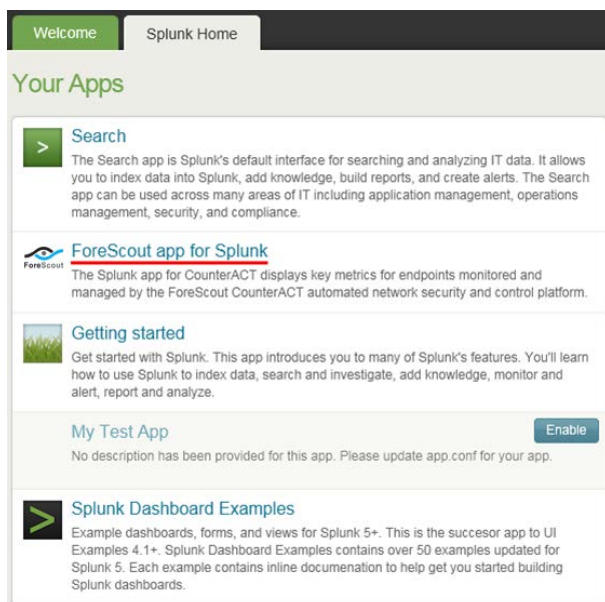
- Download and install the app from the Splunk app store. See [Download and Install the ForeScout App for Splunk](#)
- Create a CounterACT policy that sends endpoint information to Splunk. See [Create a CounterACT Policy that Sends Data to Splunk](#).

1 Download and Install the ForeScout App for Splunk

To download and install the app:

1. Download the app from the Splunkbase website at:
<http://updates.forescout.com/support/files/plugins/splunk-app/1.0.1/build/5/CounterACT.spl>
2. Within your Splunk console window, select **Apps>Manage apps>install from file**. Browse to the app package you downloaded, and upload the package to your Splunk instance.

The ForeScout app appears in your Splunk console homepage view, and is listed under the Apps menu.



2 Create a CounterACT Policy that Sends Data to Splunk

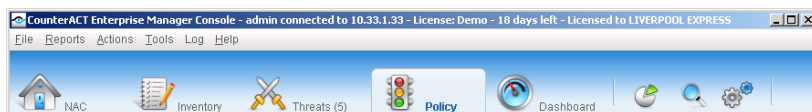
The ForeScout app for Splunk displays a dashboard of status information for endpoints monitored and managed by CounterACT. To populate this dashboard with data, you create a CounterACT policy that uses the **DEX Send Web Service Request** action to submit host property values to a web service exposed by Splunk. You should use the action schedule option to determine how frequently CounterACT updates Splunk. Tune the frequency based on your network conditions and the volume of data you want to work with in Splunk.

For each endpoint selected by the policy, CounterACT replaces property tags in the request message with actual host property values, and submits the request to the Splunk web service.

The policy described here sends Splunk information for all endpoints and network devices discovered by CounterACT. You can add filtering conditions if you wish – for example, you may want to exclude certain types of network devices. Similarly, you can use standard Scope settings to limit the range of endpoints for which data is reported to Splunk.

To run the template:


1. Select the Policy tab from the Console.




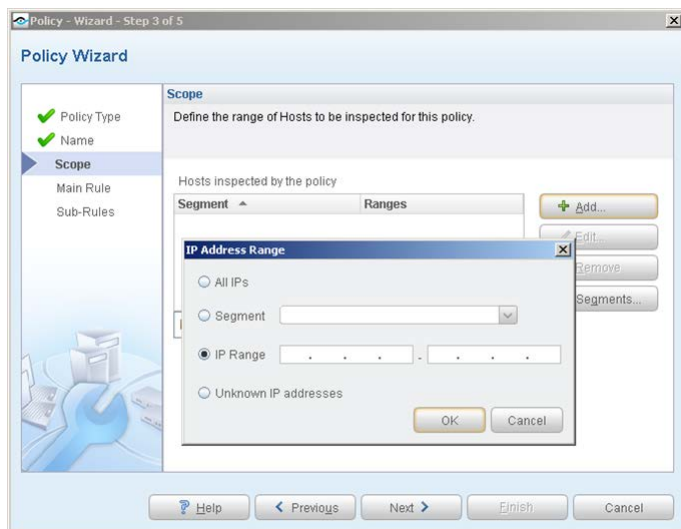
2. Select **Add**. The Policy Wizard opens.
3. Select **Custom**.



4. Select **Next**. The Name page opens. Define a unique name for the policy you are creating based on this template.
5. Select **Next**. The Scope page opens. Use the IP Address Range dialog box to define which endpoints will be inspected. Data for these endpoints will be reported to Splunk. The following options are available for defining a scope:
 - **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
 - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** to close the IP Address Range dialog box, and select **Segments** from the Scope page.
 - **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.

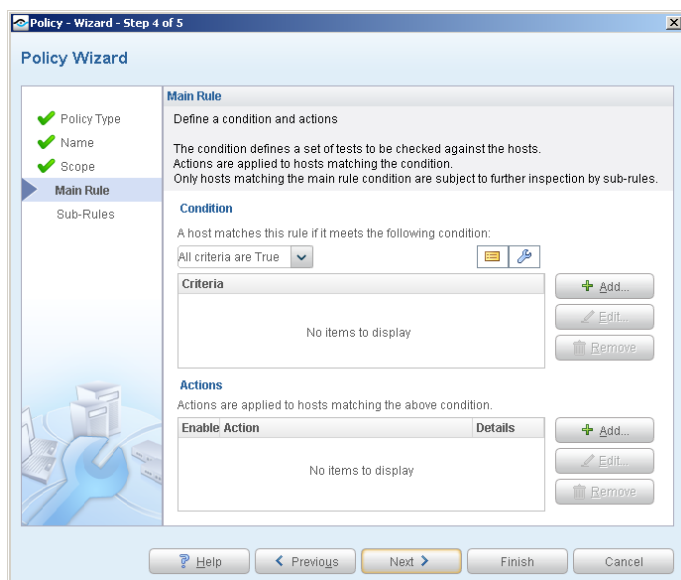
 *Do not use the **Unknown IP addresses** option in this policy. Splunk indexes data by IP address. Data reported to Splunk must include an IP address for the endpoint.*

 *See Creating Custom Policies in the Console User Manual for additional advanced scope features.*
6. Select **OK**. The added range appears in the Scope page.



7. Select **Next**. The Main Rule page opens.

In the example policy described here, no further conditions are defined – CounterACT reports host information for all endpoints in the policy scope. The main rule contains only an action.



8. Select **Add** from the **Actions** section of the Main Rule dialog box. In the Actions tree, open the Audit group. Select the **DEX Send Web Service Request** action.

9. In the Parameters tab, do the following:

- Specify a **Name** for the request message
- In the **HTTP Request Method** drop-down, select **POST**.
- In the **URL** field, enter the following HTTP message request text:

```
https://{splunkIP}:8089/services/receivers/simple?source=CounterACT&sourcetype=web_event
```

Where

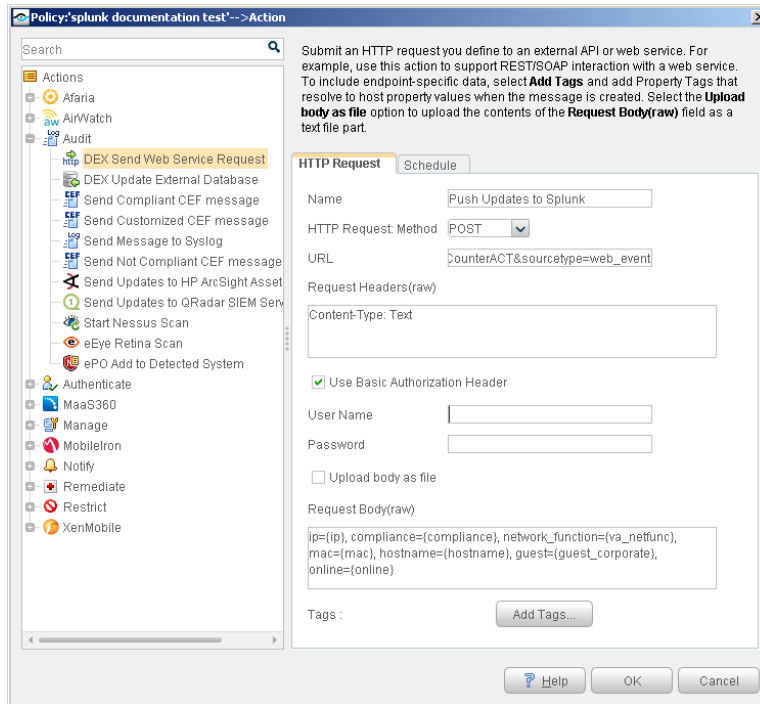
{splunkIP} is the IP address of your Splunk service.

This URL addresses the web service exposed by Splunk to receive web event updates. The term **source=CounterACT**

Indicates to Splunk that the data is coming from CounterACT, and relevant to the CounterACT app.

- In the **Request Headers(raw)** – enter the following message header:
Content-Type: Text

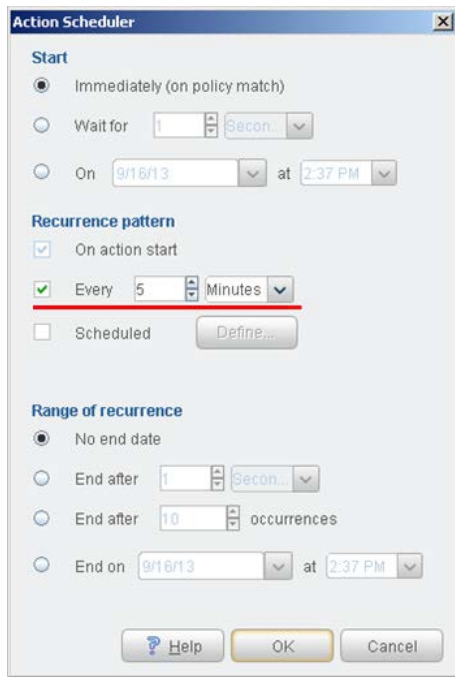
- Select the **Use Basic Authentication Header** option. In the **User Name** and **Password** fields, enter authorization credentials for the request message. Use the login credentials for your Splunk account.
- Clear the **Upload body as file** option.
- In the **Request Body (raw)** field, enter the body of the request message as follows:
`ip={ip}, compliance={compliance}, network_function={va_netfunc}, mac={mac},
hostname={hostname}, guest={guest_corporate}, online={online}`



The following table lists key-value pairs that are included in the body of the message.

Host Property	Exported Data Key	Property Tag
IP Address	IP	{ip}
Compliance	compliance	{compliance}
Corporate/Guest Control	guest	{guest_corporate}
DNS Name	hostname	{hostname}
MAC Address	mac	{mac}
Network_function	function	{va_netfunc}
Host is Online	online	{online}

- 10.** By default, the action runs only the first time that an endpoint matches the policy. To report data to Splunk more frequently, select the **Schedule** tab. Select the **Customize action start time** option and select **Define**. In the **Recurrence pattern** section, Select **Every** to repeat the action at regular intervals. To avoid overloading Splunk with irrelevant data, change the time interval to a value greater than the default (1 second). Schedule the action to repeat based on your network conditions and the volume of data you want to work with in Splunk.



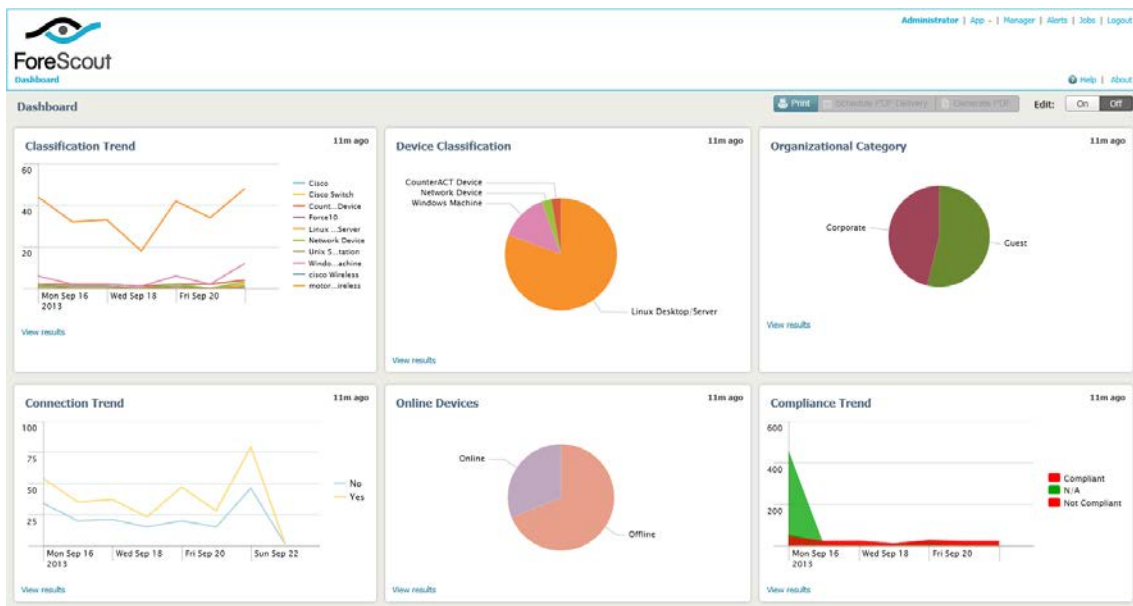
11. Select **OK**. Select **Finish** to save the policy.

12. Select **Apply** to activate the policy.

3 Working with the Dashboard

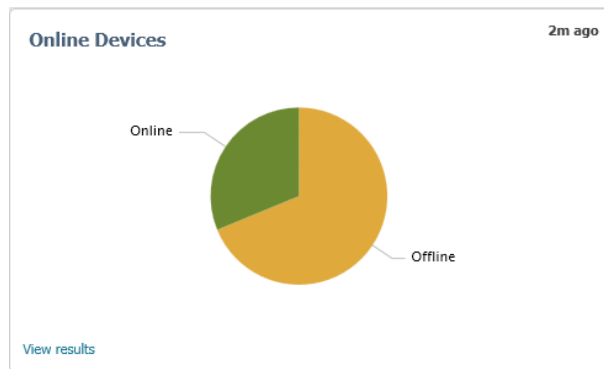
The ForeScout app for Splunk presents a dashboard of six basic status charts based on endpoint properties reported by CounterACT.

- *Online Devices*
- *Connection Trend*
- *Device Classification*
- *Classification Trend*
- *Organizational Category*
- *Compliance Trend*



Online Devices

This panel shows the relative frequency of online and offline status during the time period of the chart, for all endpoints within the reporting scope. By default, the graph is based on data reported over the past week.



Data is drawn from the following CounterACT host properties:

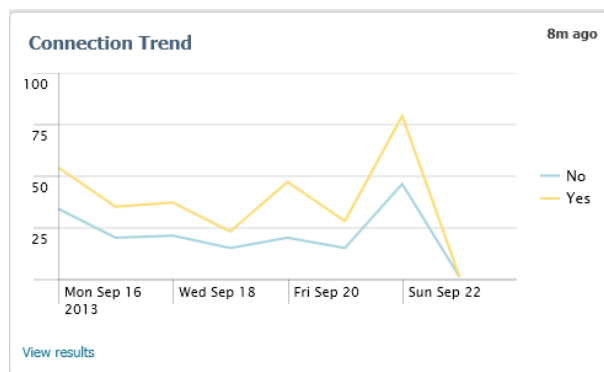
Host Property	Exported Data Key	Property Tag
IP Address	IP	{ip}
Host is Online	online	{online}

Hover over the graph to view details and percentages.

Select **View results** to view the Splunk search used to generate the graph, to modify the time period of the graph, and to view web events reported by CounterACT.

Connection Trend

This panel tracks the online or offline status of endpoints within the reporting scope over time. The graph shows the variation in the total number of endpoints that are online or offline during the specified time period. By default, the graph is based on data reported over the past week.



Data is drawn from the following CounterACT host properties:

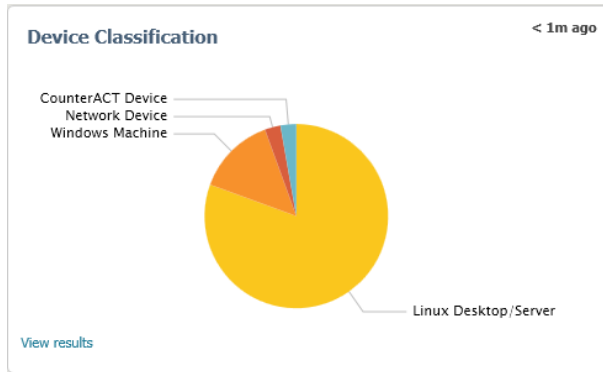
Host Property	Exported Data Key	Property Tag
Host is Online	online	{online}

Hover over the graph to view details and percentages.

Select **View results** to view the Splunk search used to generate the graph, to modify the time period of the graph, and to view web events reported by CounterACT.

Device Classification

This panel shows the overall results of endpoint classification policies. The graph shows the relative prevalence of different types of endpoint during the charted period, as a percentage of all endpoints within the reporting scope. By default, the graph is based on data reported over the past week.



Data is drawn from the following CounterACT host properties:

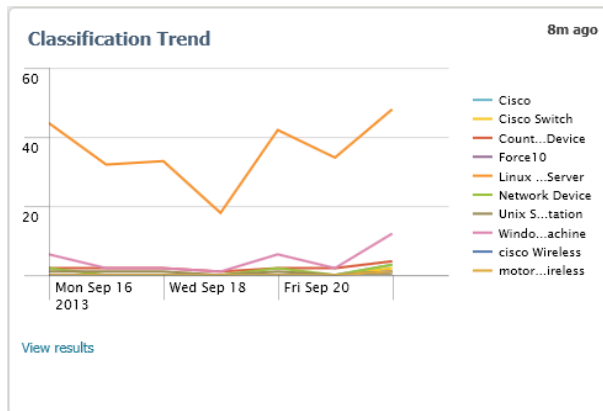
Host Property	Exported Data Key	Property Tag
IP Address	IP	{ip}
Network_function	function	{va_netfunc}

Hover over the graph to view details and percentages.

Select **View results** to view the Splunk search used to generate the graph, to modify the time period of the graph, and to view web events reported by CounterACT.

Classification Trend

This panel tracks the results of endpoint classification policies over time. The graph shows changes in the relative number of different endpoint types in the network over the specified time period. By default, the graph is based on data reported over the past week.



Data is drawn from the following CounterACT host properties:

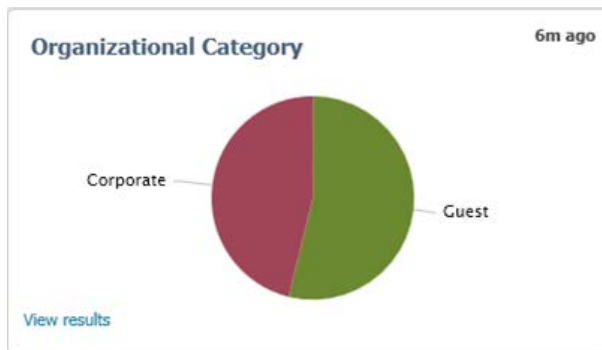
Host Property	Exported Data Key	Property Tag
IP Address	IP	{ip}
Network_function	function	{va_netfunc}

Hover over the graph to view details and percentages.

Select **View results** to view the Splunk search used to generate the graph, to modify the time period of the graph, and to view web events reported by CounterACT.

Organizational Category

This panel displays the results of corporate/guest handling policies. The graph shows the relative prevalence of different user registration results during the charted period, as a percentage of all endpoints within the reporting scope. By default, the graph is based on data reported over the past week.



Data is drawn from the following CounterACT host properties:

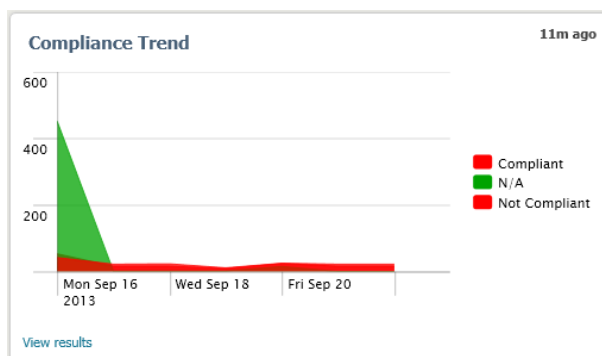
Host Property	Exported Data Key	Property Tag
IP Address	IP	{ip}
Corporate/Guest Control	guest	{guest_corporate}

Hover over the graph to view details and percentages.

Select **View results** to view the Splunk search used to generate the graph, to modify the time period of the graph, and to view web events reported by CounterACT.

Compliance Trend

This panel tracks the results of compliance policies over time. The graph shows the number of endpoints that were compliant and non-compliant over the specified time period. By default, the graph is based on data reported over the past week.



Data is drawn from the following CounterACT host properties:

Host Property	Exported Data Key	Property Tag
IP Address	IP	{ip}
Compliance	compliance	{compliance}

Hover over the graph to view details and percentages.

Select **View results** to view the Splunk search used to generate the graph, to modify the time period of the graph, and to view web events reported by CounterACT.

Early Availability End User License Agreement

IMPORTANT NOTICE – THIS AGREEMENT IS A CONTRACT BETWEEN YOU AND FORESCOUT WHICH COVERS YOUR USE OF THE FORESCOUT EARLY AVAILABILITY PRODUCT(S) THAT ACCOMPANY THIS AGREEMENT, WHICH MAY INCLUDE ASSOCIATED PRINTED MATERIALS, AND ONLINE OR ELECTRONIC DOCUMENTATION. ALL SUCH PRODUCTS AND MATERIALS ARE REFERRED TO HEREIN AS THE “EARLY AVAILABILITY PRODUCT(S).” PLEASE CAREFULLY READ THIS AGREEMENT BEFORE YOU DOWNLOAD, INSTALL OR ACCESS THE EARLY AVAILABILITY PRODUCTS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, THEN DO NOT INSTALL OR USE THE EARLY AVAILABILITY PRODUCTS. BY INSTALLING, DOWNLOADING, ACCESSING OR OTHERWISE USING THE EARLY AVAILABILITY PRODUCTS, YOU ARE ACKNOWLEDGING AND AGREEING TO BE BOUND BY THE FOLLOWING TERMS.

1. DEFINITIONS

- (a) "**Documentation**" shall mean the printed or online written reference material furnished to Licensee in conjunction with the Early Availability Products, including, without limitation, instructions, beta testing guidelines, and end user guides.
- (b) "**Early Availability Product(s)**" shall mean the early release version of certain ForeScout software products (including any Updates thereto) and Documentation provided by ForeScout to Licensee, for non-production, evaluation purposes pursuant to this Agreement.
- (c) "**Intellectual Property Rights**" shall mean all intellectual property rights, including, without limitation, patent, copyright, trademark, and trade secret.
- (d) "**Open Source Software**" means various open source software components of the Early Availability Products that are licensed to you under the terms of the applicable license agreements included with such open source software components or other materials for the Early Availability Products.
- (e) "**Updates**" shall mean a modification, error correction, bug fix, new release, or other update to or for any Early Availability Product.

2. LICENSE GRANT, USE AND OWNERSHIP

- (a) **Limited License.** Subject to the terms and conditions of this Agreement, ForeScout grants to Licensee a non-exclusive, nontransferable license (without the right to sublicense) (i) to use the Early Availability Product in accordance with the Documentation solely for purposes of advance release use; for purposes of clarification the use of the Early Availability Products is intended non-production use only; (ii) to use the Documentation provided with the Early Availability Product in support of Licensee's authorized use of the Early Availability Product; and (iii) to copy the software included with the Early Availability Product for archival or backup purposes, provided that all titles and trademarks, copyright, and restricted rights notices are reproduced on such copies. Nothing in this limited license permits Licensee to modify the Early Availability Products.
- (b) **Feedback.** The purpose of this license is the limited use and evaluation of the Early Availability Product(s). Any feedback and other information which is provided by Licensee to ForeScout in connection with the Early Availability Products or this Agreement may be used by ForeScout to improve or enhance its products and, accordingly, Licensee grants ForeScout a non-exclusive, perpetual, irrevocable, royalty-free, worldwide right and license to use, reproduce, disclose, sublicense, distribute, modify, and otherwise exploit such feedback and information without restriction.
- (c) **Restrictions.** Licensee shall not copy or use the Early Availability (including the Documentation) or disseminate Confidential Information, as defined below, to any third party except as expressly permitted in this Agreement. Licensee will not, and will not permit any third party to, sublicense, rent, copy, modify, create derivative works of, translate, reverse engineer, decompile, disassemble, or otherwise reduce to human perceivable form any Software or accompanying Documentation. In no event shall Licensee use the Early Availability Products for Licensee's product development or any other commercial purpose. The Early Availability Products and all performance data and test results, including without limitation, benchmark test results (collectively "Performance Data"), relating to the Early Availability Products are the Confidential Information of ForeScout, and will be treated in accordance with the terms of Section 4 of this Agreement. Accordingly, Licensee shall not publish or disclose to any third party any Performance Data relating to the Early Availability Products.

(d) **Ownership.** ForeScout shall own and retain all right, title and interest in and to the Intellectual Property Rights in the Early Availability Products and any derivative works thereof, subject only to the limited license expressly set forth in Section 2(a) hereof. Licensee does not acquire any other rights, express or implied, in the Early Availability Products. ALL RIGHTS NOT EXPRESSLY GRANTED HEREUNDER ARE RESERVED TO FORESCOUT.

(e) **Support for Early Availability Products.** ForeScout will use reasonable commercial efforts to provide telephone and email support for the Early Availability Products during normal business hours. If Licensee is an existing ForeScout customer, support for the Early Availability Products is *not* covered by any existing paid product support agreement between ForeScout and Licensee. In the event ForeScout, in its sole discretion, supplies any Update to Licensee, such Update shall be deemed an Early Availability Product hereunder and shall be subject to the terms and conditions of this Agreement.

(f) **Open Source Software.** The terms and conditions of this Agreement shall not apply to any Open Source Software accompanying the Early Availability Products. Any such Open Source Software is provided under the terms of the open source license agreement or copyright notice accompanying such Open Source Software.

(g) **Production Use of Early Availability Products.** Licensee acknowledges that the Early Availability Products are advance release products that have been made available to the Licensee without ForeScout completing ForeScout's customary testing or evaluation.. The Early Availability Products are not designed for use in a production environment. Any use by Licensee of the Early Availability Products in a production environment are at Licensee's sole risk.

3. TERM AND TERMINATION

(a) **Early Availability Products.** Unless otherwise terminated as specified under this Agreement, Licensee's rights with respect to the Early Availability Products will terminate upon the earlier of (a) the initial release by ForeScout of the generally available version of the Beta Product, or (b) one year after the effective date set forth below.

(b) **This Agreement.** This Agreement shall remain in effect until the earlier of (i) the date Licensee ceases to be a licensee of ForeScout's commercially available CounterACT product, or (ii) the date this Agreement is terminated by either party with thirty (30) days notice to the other party, or (iii) the date on which ForeScout immediately terminates this Agreement in the event of Licensee's breach of Section 4 (Confidentiality) below. While in effect, this Agreement governs the terms of any Early Availability Products provided by ForeScout to Licensee.

(c) **Effect of Termination.** Upon any expiration or termination of this Agreement, the rights and licenses granted to Licensee under this Agreement shall immediately terminate, and Licensee shall immediately cease using, and will return to ForeScout (or, at ForeScout's request, destroy), the Early Availability Products, Documentation, and all other tangible items in Licensee's possession or control that are proprietary to ForeScout or contain ForeScout Confidential Information. The rights and obligations of the parties set forth in Sections 2(b) 2(c), 2(d), 2(e), 2(f), 4, 5, 6 and 7 shall survive termination or expiration of this Agreement for any reason.

4. CONFIDENTIALITY

(a) "Confidential Information" shall mean all non-public information of either party ("Discloser") that is disclosed to the other party ("Recipient") and that, if disclosed in written form, is labeled as "confidential" or "proprietary" at the time of disclosure or, if disclosed orally or by inspection, is stated to be confidential at the time of disclosure and is summarized in a written memo to Recipient indicating the confidential nature of the material disclosed that is delivered to Recipient within ten (10) days of the date of disclosure. Notwithstanding the foregoing, Early Availability Products, the Feedback, the Performance Data and any Updates shall be considered the Confidential Information of ForeScout without any requirement to mark them as such. Confidential Information does not include information which Recipient can demonstrate (i) was already known to Recipient, other than under an obligation of confidentiality, at the time of disclosure; (ii) was generally available in the public domain at the time of disclosure to Recipient; (iii) became generally available in the public domain after disclosure other than through any act or omission of Recipient; (iv) was subsequently lawfully disclosed to Recipient by a third party without any obligation of confidentiality; or (v) was independently developed by Recipient without use of or reference to any information or materials disclosed by Discloser or its suppliers. Recipient shall not use any Confidential Information for any purpose other than as expressly authorized under this Agreement. In no event shall Licensee use the Early Availability Products or any ForeScout Confidential Information to develop, manufacture, market, sell, or distribute any product or service. In no event shall Recipient disclose any Confidential Information to any third party. Without limiting the foregoing, Recipient shall use at least the same degree of care that it uses to prevent the disclosure of its own confidential information of like importance, but in no event less than reasonable care, to prevent the disclosure of such Confidential Information.

5. LIMITATION OF LIABILITY

IT IS UNDERSTOOD THAT THE EARLY AVAILABILITY PRODUCTS ARE PROVIDED WITHOUT CHARGE FOR LIMITED TESTING AND EVALUATION PURPOSES. ACCORDINGLY, THE TOTAL LIABILITY OF FORESCOUT AND ITS SUPPLIERS ARISING OUT OF OR RELATED TO THIS AGREEMENT SHALL NOT EXCEED \$100. IN NO EVENT SHALL FORESCOUT OR ITS SUPPLIERS HAVE LIABILITY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, EVEN IF FORESCOUT AND ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

6. WARRANTY DISCLAIMER

IT IS UNDERSTOOD THAT THE EARLY AVAILABILITY PRODUCTS, DOCUMENTATION, AND ANY UPDATES MAY CONTAIN ERRORS AND ARE PROVIDED FOR LIMITED TESTING AND EVALUATION ONLY. THE EARLY AVAILABILITY PRODUCTS AND ANY UPDATES ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. FORESCOUT AND ITS SUPPLIERS SPECIFICALLY DISCLAIM ALL IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. Licensee acknowledges that ForeScout may not have publicly announced the availability of the Early Availability Products, that ForeScout has not promised or guaranteed to Licensee that such Early Availability Products will be made available to anyone in the future, that ForeScout has no express or implied obligation to Licensee to announce or introduce the Early Availability Products, and that ForeScout may not introduce a product similar or compatible with the Early Availability Products. Accordingly, Licensee acknowledges that any research or development that it performs regarding the Early Availability Products or any product associated with the Early Availability Products is done entirely at its own risk. Specifically, the Early Availability Products may contain features, functionality or modules that may change or will not be included in the production version of the Early Availability Products, if released, or that will be marketed separately for additional fees.

7. OTHER PROVISIONS

- (a) **Governing Law.** This Agreement, and all disputes arising out of or related thereto, shall be governed by and construed under the laws of the State of California without reference to conflict of laws principles. All such disputes shall be subject to the exclusive jurisdiction of the state and federal courts located in Santa Clara County, California, and the parties agree and submit to the personal and exclusive jurisdiction and venue of these courts.
- (b) **Assignment.** Licensee shall not assign this Agreement or any rights or obligations hereunder, directly or indirectly, by operation of law, merger, acquisition of stock or assets, or otherwise, without the prior written consent of ForeScout. Subject to the foregoing, this Agreement shall inure to the benefit of and be binding upon the parties and their respective successors and permitted assigns.
- (c) **Export Regulations.** Licensee understands that ForeScout is subject to regulation by U.S. and foreign governments and agencies, which prohibit export or diversion of certain technical products and information to certain countries and individuals. Licensee warrants that it will comply in all respects with all export and re-export restrictions applicable to the technology and documentation provided hereunder.
- (d) **Modification.** This is the entire agreement between the parties relating to the subject matter hereof and all other terms are rejected. No waiver or modification of this Agreement shall be valid unless in writing signed by each party. The waiver of a breach of any term hereof shall in no way be construed as a waiver of any term or other breach hereof. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law the remaining provisions of this Agreement shall remain in full force and effect.
- (e) **Counterparts.** This Agreement may be executed in two (2) counterparts, both of which taken together shall constitute one (1) single agreement between the parties. The parties hereto agree that a version of this Agreement transmitted by means of electronic message or electronic record (electronic mail, electronic data interchange, or facsimile), once duly signed by the authorized representatives of each party, shall constitute a binding agreement and shall have the same force and effect as a document bearing original signatures.

8. CONTACT INFORMATION

If you have any questions about this Beta Test Agreement, or if you want to contact ForeScout for any reason, please direct all correspondence to: ForeScout Technologies, Inc., 900 E. Hamilton Avenue, Suite 300, Campbell, CA 95008, United States of America.

ForeScout® is a trademark and/or registered trademark of ForeScout Technologies, Inc.

Legal Notice

Copyright © ForeScout Technologies, 2000-2013. All rights reserved.

The copyright and proprietary rights in the guide belong to ForeScout Technologies. It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this guide in any way, shape or form without the prior consent of ForeScout Technologies.

This product is based on software developed by ForeScout Technologies. The products described in this document are protected by U.S. Patent number 6,363,489 and 8,254,286, issued March 2002 and may be protected by other U.S. Patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use, acknowledge that the software was developed by ForeScout Technologies.

THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

All other trademarks used in this document are the property of their respective owners.

Send comments and questions regarding documentation to: documentation@forescout.com

10/1/13