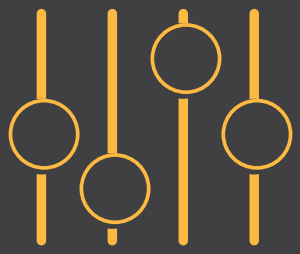


PROTECT

TECH NOTE

Elastica Integration with Cisco pxGrid

elastica

Cloud Security

Symantec + BLUE COAT

Defining the Future of Cyber Security

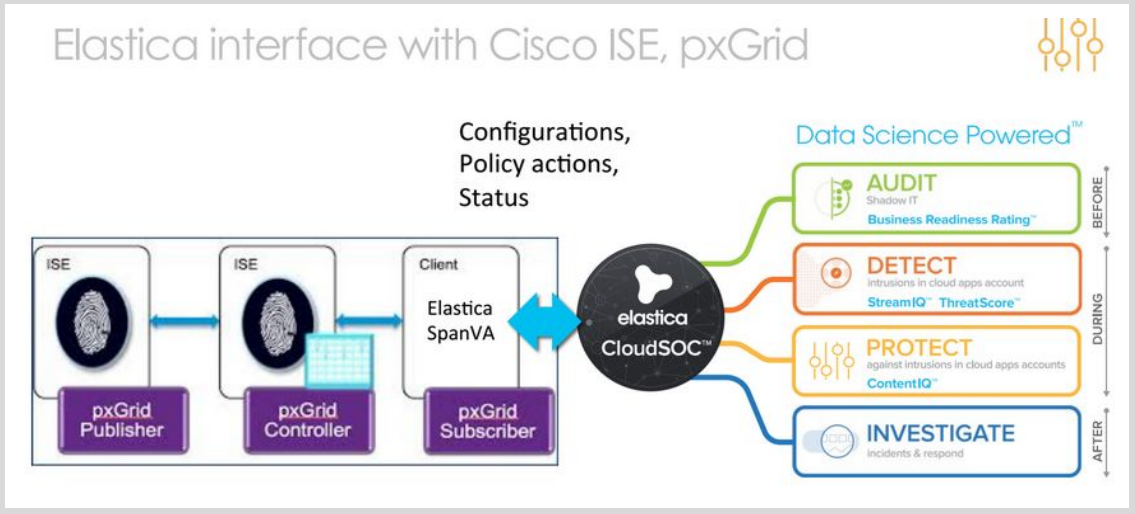
Table of Contents

Introduction

This Tech Note describes how to integrate Elastica CloudSOC with Platform Exchange Grid (pxGrid) so that you can quarantine and unquarantine any network user based on policies that you create using the Elastica Protect app.

Cisco Platform Exchange Grid (pxGrid) is a framework that enables sharing of user and device information between various IT systems and Cisco platforms. This framework consists of two parts, as shown in the figure below:

- The pxGrid controller: A function provided by the Cisco Identity Services Engine (ISE), which orchestrates and authorizes sharing of information between platforms.
- The pxGrid client: a Cisco partner that subscribes and/or publishes information to the pxGrid controller. In the installation described here, Elastica CloudSOC serves as a pxGrid client.



Subscribe to pxGrid integration support

You must subscribe to the pxGrid integration feature before you can enable it on your CloudSOC account. Contact your Elastica representative to request this feature for your account.

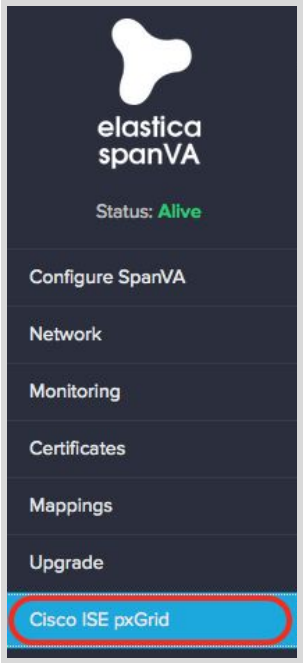
Install and configure SpanVA

SpanVA is a virtual appliance that serves as the on-premises portion of the CloudSOC-pxGrid integration. SpanVA operates as a pxGrid subscriber, and maintains communication between the pxGrid controller and CloudSOC.

You install and run this virtual appliance inside your NAT, and assign it a local IP address from your network. In some use cases, SpanVA might also need credentials to access to other specific servers and perimeter devices like firewalls.

For detailed installation procedures, see the Elastica Tech Note *Installing and Configuring SpanVA*.

After installing SpanVA, check the tabs on the left side of the SpanVA web interface and make sure that there is a tab for Cisco ISE pxGrid as shown in the following figure.



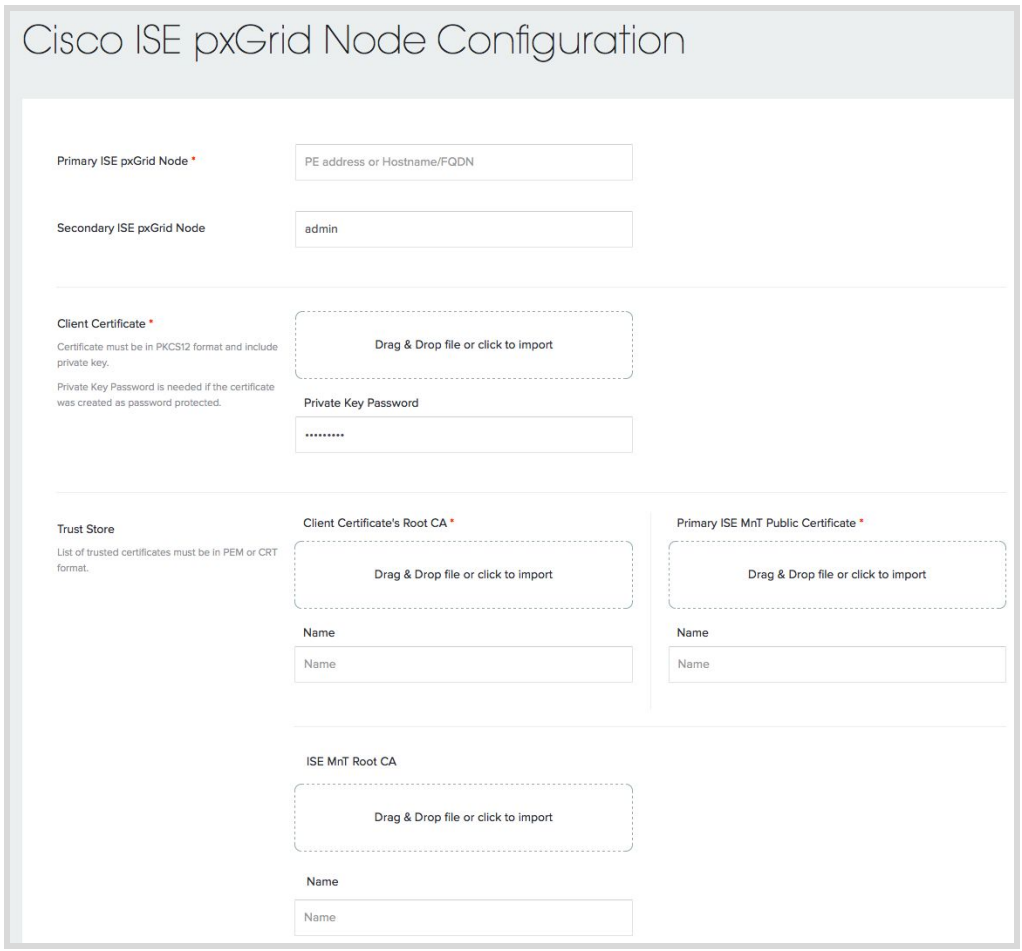
If the pxGrid tab is absent, it means that your CloudSOC account has not been configured for pxGrid integration. Contact your Elastica representative to address this issue.

Configure pxGrid certificates

Follow this procedure to configure the SpanVA virtual appliance with the information and certificates it needs to communicate with the pxGrid controller.

1. If you have not already done so, browse to the SpanVA URL to open the SpanVA configuration page in your web browser.

2. On the left side of the page, click the **Cisco ISE pxGrid** tab to bring it to the front, as shown in the following figure.



3. On the Cisco ISE pxGrid Node Configuration page, configure the following settings:

    - For Primary ISE pxGrid Node, enter the hostname or IP address for the node.
    - For Client Certificate and Client Certificate's Root CA, click to import or drag-and-drop the appropriate certificates. Also enter the client certificate's private key password if the certificate is password protected. Creating these certificates is outside the scope of this Tech Note.
    - For Primary ISE MnT Public Certificate and ISE MnT Root CA, click to import or drag-and-drop the appropriate certificates from your pxGrid implementation. For more information about these certificates, see Configuring pxGrid in an ISE Distributed Environment.

4. Click **Save**.

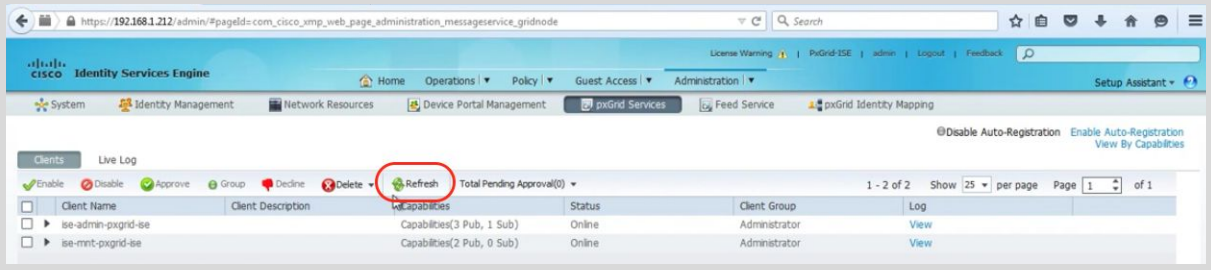
   SpanVA saves the pxGrid configuration and shows a green banner near the upper right corner of the page, as shown in the following figure.

5. Near the upper right corner of the tab, move the Connect to pxGrid Server slider to the right so that its label reads **Connected**, as shown in the following figure.

Configure pxGrid to recognize SpanVA as an ISE client

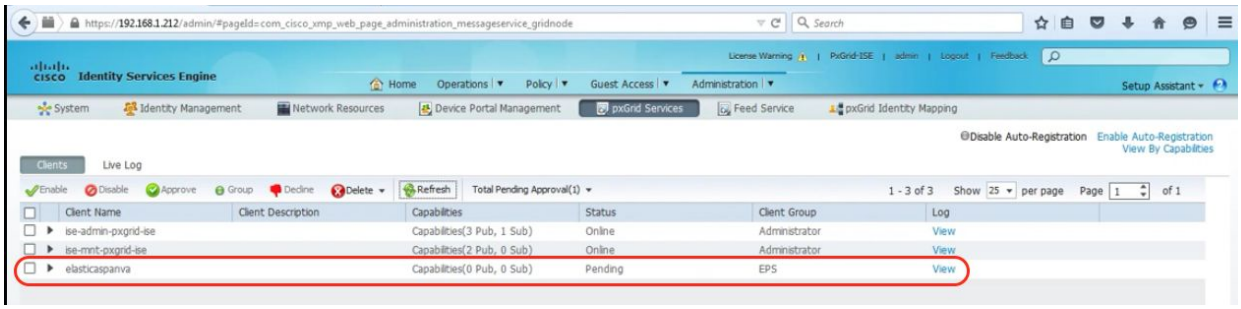
Follow this procedure to use the ISE console to configure pxGrid so that it recognizes the SpanVA virtual appliance as an ISE client:

1. Open your pxGrid ISE console and navigate to **Administration** > **pxGrid Services** > **Clients** as shown in the following figure.

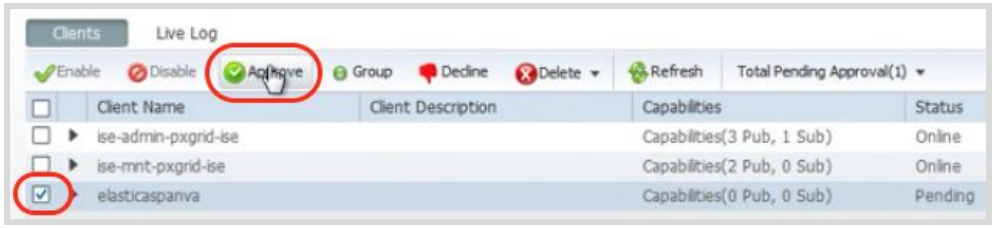


2. Click **Refresh**.

3. The console displays SpanVA as a new client as shown below.

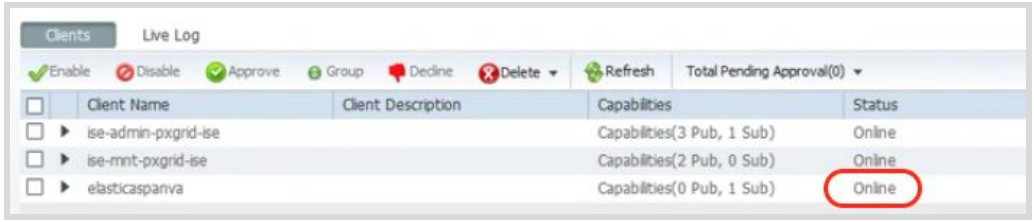


4. Mark the checkbox next to the entry for the SpanVA client, and then click **Approve** as shown in the following figure.



5. The ISE console asks you to confirm the approval. Click **Yes**.

6. Check to make sure that the Status for SpanVA is “Online” as shown in the following figure.



7. Browse to the SpanVA URL to open the SpanVA configuration page in your web browser.

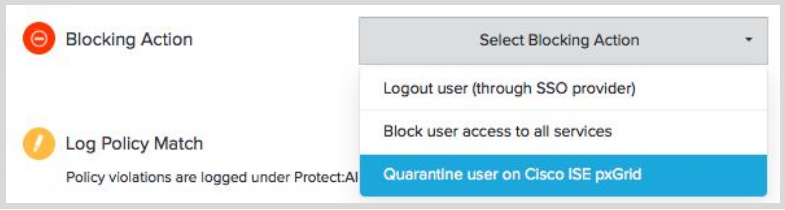
8. On the left side of the page, click the **Cisco ISE pxGrid** tab to bring it to the front.

9. Near the upper right corner of the tab, make sure that the Registration Status is “Registered” as shown in the following figure.

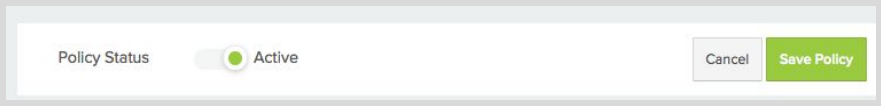
Create quarantine policies in Protect

Follow this procedure to create a Protect policy that uses pxGrid to quarantine a user.

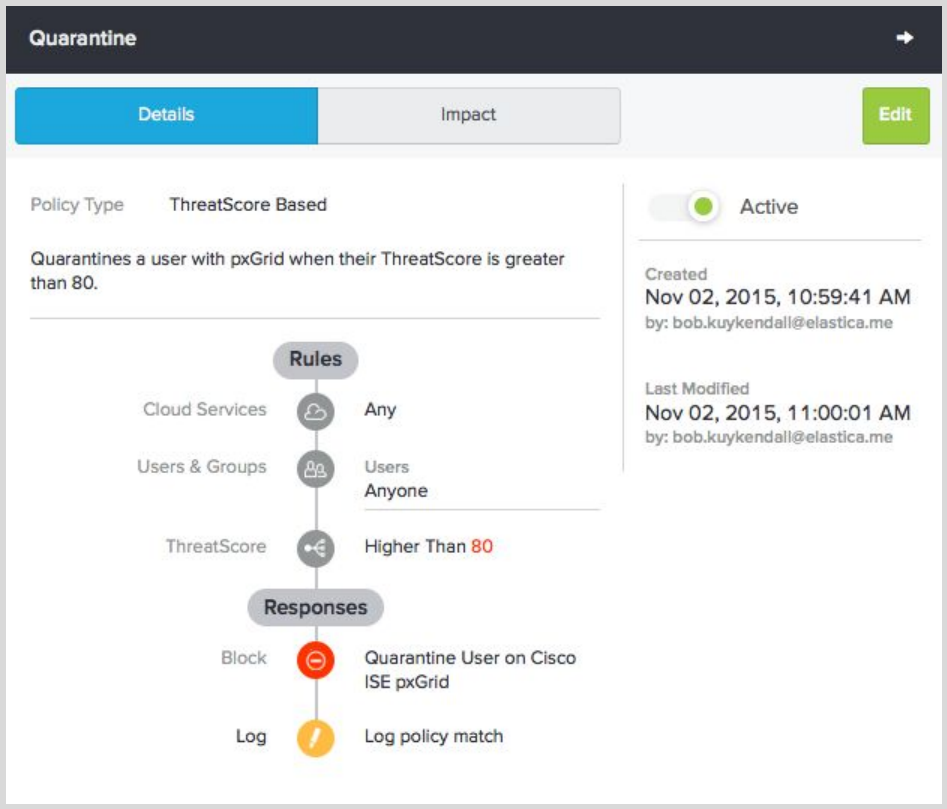
1. In the CloudSOC left side navigation bar, click **Protect**.
2. Near the upper right corner of the Protect page, choose **New > Policy**.
3. In the Policy Details area, give the policy a name and description.
4. For Policy Type, choose **Threatscore Based**.
5. In the Define Rules area, choose the users and cloud service to which the policy applies, and set the ThreatScore value that triggers the policy.
6. In the Define Response area, click Select Blocking action and choose **Quarantine user on Cisco ISE pxGrid** as shown in the following figure.



7. At the top of the page, move the Policy Status slider to Active and click **Save Policy**.



8. Protect creates the policy as shown in the following example schematic.



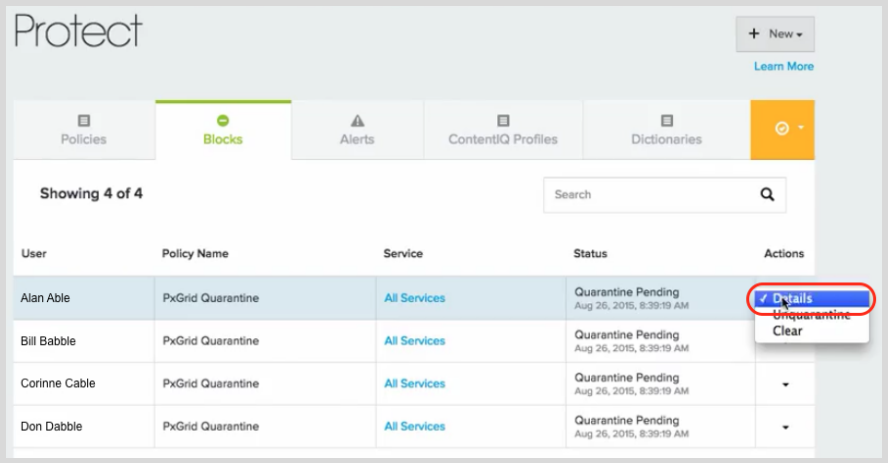
For more information on creating policies, see the Elastica Tech Note *Creating and enforcing security policies for Cloud Services*.

Viewing quarantine details

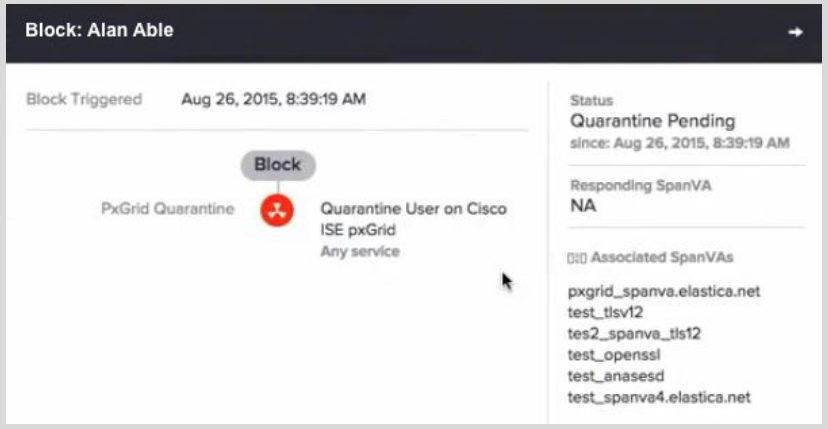
To view details for users quarantined with pxGrid:

1. In Elastica Protect, click the Blocks tab to bring it to the front.

2. On the Blocks tab, click in the Actions column in the row for a blocked user and choose **Details**, as shown in the following figure.



Protect shows you details for the block, as shown in the following figure.



The following table describes the details panel fields:

Field	Description	
Block Triggered	The date and time the block was triggered by the Protect policy	
Status	The status of the block attempt. Typical statuses are:	
	Quarantine Pending	Request was sent to the SpanVA appliances but no response received yet
	Quarantine Done	Response was received from a SpanVA confirming quarantine completed successfully
	Quarantine Failed	Request timed out (after 60 seconds) or Response received from a SpanVA confirming quarantine action failed
	Unquarantine Pending	Request was sent to the SpanVA appliances but no response received yet
	Unquarantine Done	Response received from a SpanVA confirming unquarantine completed successfully
	Unquarantine Failed	Request timed out (after 60 seconds) or Response received from a SpanVA confirming quarantine failed
Responding SpanVA	Name of the SpanVA virtual appliance that responded to the block/unblock request from CloudSOC	

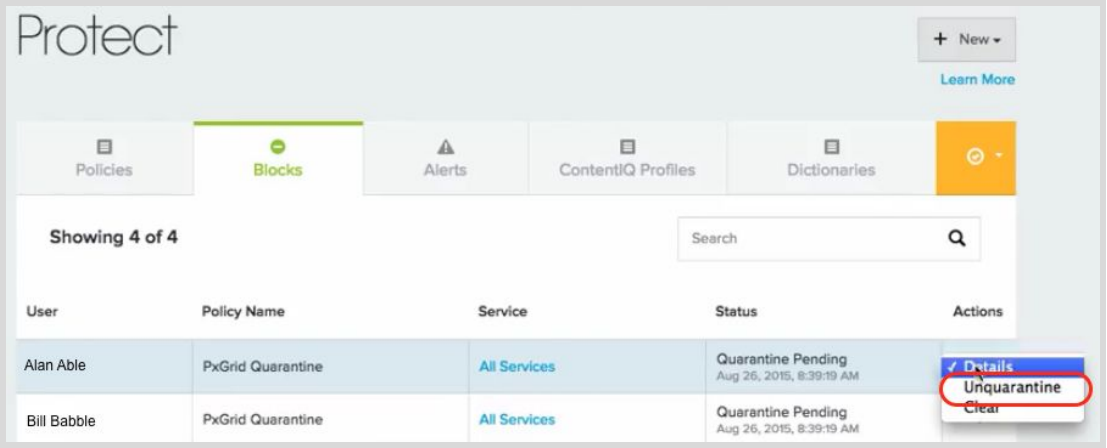
Unblocking quarantined users

Whenever a user is quarantined by the Elastica Protect app, unblock the user using only the Elastica Protect application. Doing so prevents status inconsistencies between CloudSOC and pxGrid.

To unblock a quarantined user:

1. In Elastica Protect, click the Blocks tab to bring it to the front.

2. On the Blocks tab, click in the Actions column in the row for a blocked user and choose **Unquarantine**, as shown in the following figure.



Protect unquarantines the selected user.

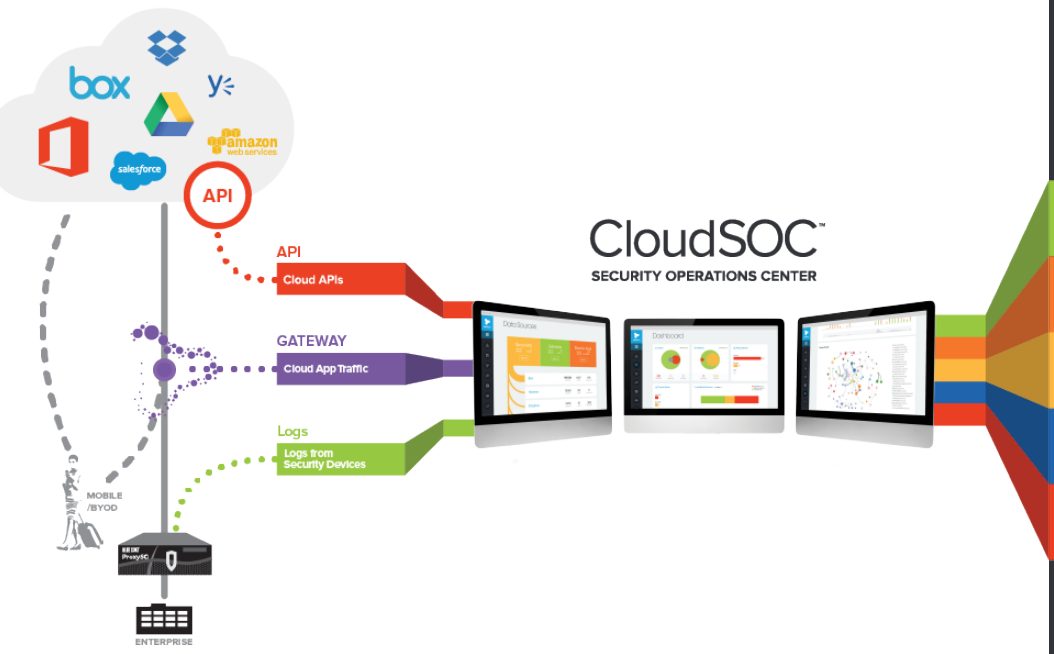
Revision history

Date	Version	Description
2 November 2015	1.0	Initial release
9 December 2016	1.1	Fix typo

Symantec + BLUE COAT
Defining the Future of Cyber Security

elastica

Cloud Security



Blue Coat is a leader in advanced enterprise security. Its Elastica cloud security solution provides granular visibility and controls for cloud applications to audit Shadow IT, control application usage, protect data, detect threats, and enable post-incident analysis.

Learn more about the Elastica data-science powered CASB solution at elastica.net.

Follow us on Twitter
@ElasticaInc

If you need any further assistance please contact support@elastica.net