Zscaler and Bitglass

Cloud Access Security Broker Deployment Guide

Deployment Guide

August 2020
Contents

SOLUTION OVERVIEW .......................................................... 3
ARCHITECTURE ........................................................................ 4
SOLUTION PREREQUISITES ......................................................... 5
  Document Audience .................................................................. 5
  Software Revisions ................................................................... 5
  Document Prerequisites ............................................................ 5
CLOUD DATA VISIBILITY REPORT .................................................. 6
  Create a Nanolog Streaming Server ........................................... 6
  Deploy Nanolog Streaming Service (NSS) Virtual Appliance ....... 8
  Create a Nanolog Streaming Feed ............................................. 9
  Deploy Bitglass Syslog Server .................................................. 10
  Discovery Dashboard ............................................................... 11
CONTROL BITGLASS DISCOVERED APPS WITH ZSCALER ............... 13
  Setup ....................................................................................... 13
  Actions ..................................................................................... 16
CLOUD ACCESS CONTROLS .......................................................... 20
  Bitglass Unmanaged Device Control Overview ................................ 20
  Define Zscaler networks in Bitglass .......................................... 21
CLOUD DATA CONTROLS ............................................................. 24
  Adding a Cloud Condition ....................................................... 24
  Cloud Dashboard ...................................................................... 26
COMPANY OVERVIEW ................................................................. 27
SOLUTION OVERVIEW

Most organizations are rapidly adopting cloud services, unaware of the long-term pitfalls associated with a lack of data visibility and inconsistent security controls. Without a comprehensive cloud security platform, they lack what they need to manage this risk. It is impossible to know which cloud apps contain your sensitive data and who it’s being shared with if you don’t have the tools to detect it. The adoption of sanctioned cloud apps provides an ongoing and ever-changing challenge for security teams. The cloud application landscape is changing so rapidly that security teams need to apply consistent security policies across all apps adopted by their businesses.

The average organization now uses hundreds of cloud services, often with inadequate security controls that can put them at risk of breaches. As people access and share sensitive company data in authorized cloud apps and unauthorized services, unmanaged device security becomes a critical concern. Data can be moved from corporate systems to unknown cloud apps without your existing security systems detecting it. On-premises security solutions lack the ability to monitor and protect data in the cloud and enforce corporate and regulatory compliance policies.

Zscaler has a very sophisticated array of cloud services, with AV inspection, Next-Gen Firewall, Sandbox, Advanced Threat Protection, URL Filters, SSL Inspection, DLP, and more, in a unified platform. It provides airtight security without the cost and complexity of stacks of appliances, and it delivers a fast, secure user experience. Zscaler provides this comprehensive security using a combination of GRP tunneling, PAC files, and Zscaler App to forward traffic to the Zscaler service. This provides great coverage for all your managed networks and managed devices.

The ubiquitous nature of cloud apps and the fast adoption of bring-your-own-device is a huge concern for CISOs. Bitglass' revolutionary reverse proxy technology protects and controls cloud data access from both managed and unmanaged devices. Bitglass provides data loss prevention (DLP), advanced threat protection (ATP), and sensitive data sharing detection in one simple console. Whether users connect from a coffee shop, the airport, at home, or abroad, Bitglass is there to protect you.
ARCHITECTURE

As data moves beyond the firewall, the traditional security solutions lack the ability to monitor data usage and enforce security controls, in the cloud. The Zscaler and Bitglass joint solution enables customers to securely adopt cloud services by enforcing security controls across any cloud app from managed and unmanaged, BYO devices.

- Web Browsing logs are sent from Zscaler to Bitglass to produce a Bitglass Cloud Visibility Report
- Managed device and network traffic are sent through Zscaler
- Unmanaged device traffic is redirected through Bitglass
SOLUTION PREREQUISITES

Document Audience

This document was designed for Security Architects and Engineers. For additional product and company resources, please refer to the Appendix section.

Software Revisions

This document was written using Zscaler Internet Access v5.6 and Bitglass v181114 or later.

Document Prerequisites

Zscaler Internet Access (ZIA)
● A working instance of ZIA 5.6 (or newer)
● An active subscription to Nanolog Streaming Service (NSS).
● Administrator login credentials to ZIA

Bitglass Cloud Access Security
● A working instance of Bitglass Cloud Discovery Reports
● Administrator login credentials to Bitglass

Cloud Application (Office365, G Suite, Salesforce etc.)
● A working instance of the cloud application federated to Bitglass for authentication.
CLOUD DATA VISIBILITY REPORT

Note: If you already have a set up NSS server and deployed the NSS Virtual Appliance, then please skip to the section Create a Nanolog Streaming Feed.

Create a Nanolog Streaming Server

Before you set up an NSS server on the Admin Portal, you're required to enter information about your traffic and users so the Zscaler service can compute the appropriate resources for your NSS. The NSS buffers logs for at least one hour. If the BitGlass Rsyslog service goes offline for maintenance or if the connection between the NSS and the Rsyslog server is disrupted, the NSS buffers the logs and sends them once the connection is reestablished. The amount of memory required to buffer the logs is incorporated into the VM spec computation. The buffer size increases proportionally to the amount of RAM allocated to the NSS.

1. Launch your browser
2. Navigate to https://www.zcaler.com/ and log in to your tenant:

3. Enter your credentials and log in to the Zscaler service.
1. Go to Administration > Settings > Nanolog Streaming Service.

2. From the Nanolog Streaming Service page, click Add NSS Server.

3. In the Add NSS Server dialog,
   - Enter a name ‘Bitglass Shadow IT’
   - Choose ‘NSS for Web’

4. Click Save

5. Click Download in the SSL Certificate column of the NSS that you are configuring, and then save the certificate. You will upload the certificate to the virtual appliance.
Deploy Nanolog Streaming Service (NSS) Virtual Appliance

There are many options for deploying NSS Virtual Appliances. Here, we are showing the VMware deployment, which is like other hypervisors. For a full list of deployment options please visit: https://help.zscaler.com/zia/deploying-nss-virtual-appliances

To deploy the VMWare NSS Virtual Appliance, follow the instructions below.

1. Go to Administration > Settings > Nanolog Streaming Service.
2. Click Deploy NSS Virtual Appliance to enter data that the Zscaler service needs to compute the appropriate resources for your NSS.
4. Choose the VMWare platform, and then click Compute
5. Click Download NSS Virtual Appliance to download the NSS OVA file.
6. Click Close to exit the dialog.

Now that you have the NSS Virtual Appliance, you can follow the instructions to set passwords, install certificates, and update binaries here:

Create a Nanolog Streaming Feed

1. Go to Administration > Cloud Configuration > Nanolog Streaming Service > NSS Feeds
2. Click Add NSS Feed to create a feed that will be sent to Bitglass.

Add a new NSS Feed with the following options:

Feed Name: **Bitglass Shadow IT**
NSS Server: **Bitglass Shadow IT**
SIEM IP Address: Enter the Local IP Address of Bitglass Syslog Server (e.g. 192.168.1.90)
SIEM TCP Port: **514**
Log Type: **Web Log**
Status: **Enabled**
Feed Output Type: **Tab-Separated**

Feed Output Format:

```
%d{yy}-%02d{mth}-%02d{dd}
%02d{hh}:%02d{mm}:%02d{ss}\thostname=%s{ehost}\tClientIP=%s{cip}\ntserverip=%s{sip}\ntuser=%s{login}\ntappname=%s{appname}\ntrequest
size=%d{reqsize}\ntresponse\size=%d{respsize}\tuseragent=%s{ua}\tvendor=Zscaler
```

**Note:** Make sure the Feed Output Format field doesn’t contain any special characters.
Deploy Bitglass Syslog Server

The Discovery Dashboard is where you can upload firewall/proxy logs or set up syslog streaming to be analyzed. Bitglass Discovery provides a detailed report to identify the Shadow IT cloud applications your users are interacting with and allows you to identify possible data leakage. Bitglass utilizes machine learning to scour the web for information about cloud applications so that our cloud app database is always up to date. This means any time a new app is created, or an application’s attribute changes (have they been breached, did they add new features meeting a prior requirement, etc.) Bitglass will see that information, immediately auto-categorize the app, and incorporate it into our database. App risk scores are computed with a proprietary algorithm that analyzes the reputation of the application relative to other apps in a category, which map to an associated risk level (e.g. High, Medium, Low). When an app is a member of multiple categories the median value across categories is reported.

Before you proceed in configuring Bitglass Syslog Server, you will need to make sure you meet the following requirements:

- The Bitglass Syslog Server must be able to send logs to syslog.bitglass.com
- Logs must be sent to syslog.bitglass.com over TCP port 1999
- Logs must be sent utilizing TLS 1.2 with client authentication as a primary method of tenant identification.
- The configuration provided in this document is based upon Rsyslog 8.x and CentOS 7.

Make sure to install & update Rsyslog to the latest version including the required TLS modules.

1. Create a Virtual Machine, install CentOS 7 and apply security patches.
2. Run `sudo yum install rsyslog rsyslog-gnutls rsyslog-gssapi`
3. Run `sudo yum info rsyslog` to ensure you have the latest version.
4. Configure Bitglass Syslog Server [link]
5. Restart Syslog, run `sudo service rsyslog restart`
6. Once the Bitglass Syslog server receives logs from NSS it will forward them to Bitglass
7. Bitglass support will analyzes these log files and create log parsing rules.
8. Bitglass support will configure log parsing rules on the customers tenant.
9. Bitglass will now produce a Cloud Discovery Report.
10. Customers can review these reports in the Bitglass Console.
Discovery Dashboard

The Discovery Dashboard analyzes your Zscaler logs to report on Shadow IT applications being accessed and used by your users. The Dashboard provides information on the trust levels of applications and can help surface risky or suspicious activity from your users (e.g. uploading large amounts of data to untrustworthy apps or shadow IT applications that are not sanctioned by your company). The Discovery Dashboard is separated into two primary pages to provide an overview of the activity occurring as well as detailed information about each application.

Discovery Page

The Discovery page provides a summary overview of your users’ Shadow IT usage. It includes a breakdown of total events and numbers of applications accessed broken down by trust rating. This allows admins to quickly review the riskiest activity within their network at a quick glance. The page is divided into three sections, the "Cloud Risk Assessment" summary box, summary graphs, and a volume bar chart. Click Dashboards > Discovery to access the dashboard.
Investigate Page

The Investigate page will list out all the applications and domains discovered. Here you can see them listed with high level information such as uploaded data and trust rating. Clicking into an application will allow you to view greater details about the application and allow you to manage the application as an unlicensed app. This page also allows you to search through your report if you are looking to see if an application was being accessed by your users.

<table>
<thead>
<tr>
<th>APP</th>
<th>SOURCES</th>
<th>EVENTS</th>
<th>UPLOAD</th>
<th>TRUST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>1,683</td>
<td>235,241</td>
<td>23,292,192,219</td>
<td>★★★★</td>
</tr>
<tr>
<td>Apple</td>
<td>749</td>
<td>9,015</td>
<td>13,890,433,232</td>
<td>★★★★</td>
</tr>
<tr>
<td>Amazon AWS</td>
<td>1,340</td>
<td>204,983</td>
<td>8,742,899,069</td>
<td>★★★★</td>
</tr>
<tr>
<td>Yahoo</td>
<td>566</td>
<td>16,657</td>
<td>1,742,584,327</td>
<td>★★★★</td>
</tr>
<tr>
<td>Canonical</td>
<td>73</td>
<td>744</td>
<td>1,322,795,935</td>
<td>★★★★</td>
</tr>
<tr>
<td>Facebook</td>
<td>364</td>
<td>2,365</td>
<td>1,042,757,563</td>
<td>★★★★</td>
</tr>
<tr>
<td>Netflix</td>
<td>2</td>
<td>91</td>
<td>972,621,477</td>
<td>★★★★</td>
</tr>
</tbody>
</table>

There are three primary views for this page. You can view the page sorted by the application, by the sources (or users), or by new domains that were discovered. This can be changed by clicking the dropdown in the top left corner above the search bar.
CONTROL BITGLASS DISCOVERED APPS WITH ZSCALER

Bitglass can integrate directly with Zcaler to send applications in Discovery Shadow IT reports to Zcaler for policy controls. This guide page will walk you through how to configure the integration with Zcaler.

Setup

To begin, login to the Bitglass admin portal and navigate to Protect > Integrations > Zcaler. Here is where you will configure your Zcaler information for integration. You should also have another tab open and logged in to your Zcaler admin portal so you can acquire the API key needed for integration.
1. On the Zscaler portal page select "Administration" in the left column and then under the Authentication section and select "API Key Management".

2. On the API Key Management page copy your API key or keep this window open so you can copy/reference this later.
3. Now switch back to your Bitglass admin portal tab for your Zscaler integration page and fill out the info in the fields with your info. This will include your admin account and password you are using for the integration, the API key we copied in step 2 above, the category you want to send apps to (category must already exist in Zscaler), and then the URL for your Zscaler instance. Click "Connect to Zscaler" when you are ready.

4. Once you have saved, you should see the card change to indicate a healthy connection and display the last sync time.
Actions

Once you have setup your integration with Zscaler you can now send applications from Shadow IT reports or found within Bitglass's cloud app database to Zscaler for control.

1. Navigate to Dashboards > Discovery and examine one of your Shadow IT reports or search for an app. When you click on an application to view the details you should see 3 dots in the top right corner. Clicking on those will expand options to control the app via Bitglass or Zscaler.

2. When you selected one of the options you will see an icon display in the top right to indicate how that app is being controlled:
3. Now you can navigate back to your Zscaler admin portal page and create rules for the Category that you defined on the Bitglass Zscaler integration setup. To do so start by reviewing the apps that have been added by navigating to the Administration tab and selecting "URL Categories". On the URL Categories page, you can locate your category name or filter by it to see which apps have been added.
4. Now navigate to the Policy tab and select "URL & Cloud App Control". Create your URL filtering rule how you want and ensure you are selecting the category you created for the apps sent from Bitglass.
CLOUD ACCESS CONTROLS

Bitglass Unmanaged Device Control Overview

Zscaler and Bitglass have partnered to provide a joint solution that enables enterprises to secure cloud services by enforcing security and governance controls to managed and unmanaged devices.

Zscaler has a very sophisticated array of cloud services, with AV inspection, Next-Gen Firewall, Sandbox, Advanced Threat Protection, URL Filters, SSL Inspection, and more, in a unified platform. It provides airtight security without the cost and complexity of stacks of appliances, and it delivers a fast, secure user experience. Zscaler provides this comprehensive security using a combination of GRE or IPsec tunneling, PAC files, and Zscaler App to forward traffic to the Zscaler service. This provides great coverage for all your managed networks and managed devices.

The ubiquitous nature of cloud apps and the fast adoption of bring-your-own-device is a huge concern for CISOs. Bitglass' revolutionary reverse proxy technology protects and controls cloud data access from unmanaged devices. Bitglass provides data loss prevention (DLP), advanced threat protection (ATP), and sensitive data sharing detection in one simple console. Whether users connect from a coffee shop, the airport, at home, or abroad, Bitglass is there to protect you.

Custom objects are created within Bitglass to define the Zscaler Public Service Edge nodes:

- zscloud
- zscaler
- zscalerone
- zscalertwo
- zscallerthree
- zscalerbeta

These objects can be used within Bitglass to determine if the cloud application traffic is coming from a Zscaler Node. This allows us to make policy decision on who the user is, what device they're using, and whether they are protected by Zscaler. For example, a policy is created within Bitglass to allow devices that are protected by Zscaler to access cloud applications with very little or no Bitglass DLP applied. The traffic has already been processed by Zscaler, so the traffic is secure and compliant. If the traffic is not coming from a Zscaler service, then Bitglass may apply a strict DLP policy or even block the connection, especially if it is coming from an unsanctioned location or is included in a banned countries list. This can mitigate a whole category of attacks, as well as sophisticated campaigns like password stuffing.
This integration also allows Zscaler and Bitglass customers to scan cloud data at rest and check for inappropriate data sharing. Cloud data visibility is one of the fastest growing issues within the CISO community because of tighter cloud data privacy regulations. Administrators and security staff can no longer access all data, therefore it's impossible to know whether a user has any sensitive information.

Define Zscaler networks in Bitglass

1. Open a new tab in your browser
2. Go to the Bitglass web site [https://portal.bitglass.com](https://portal.bitglass.com) and login

3. Go to Apps > Objects

4. Click on the green square + next to Customer Locations to create an object.

5. Give the Location a name and specify the range of Zscaler addresses, Click OK.

Zscaler Cloud Enforcement Node Ranges: [link]
6. Add as many Custom Locations as you want, as shown below:

Define Bitglass Policies

1. Go to Admin > Policies
2. Find that App you want to manage and click the green cross [+].

<table>
<thead>
<tr>
<th>Access</th>
<th>Action</th>
<th>Location</th>
<th>Device</th>
<th>Access Method</th>
<th>Web App</th>
<th>Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure App Access</td>
<td>Direct App Access</td>
<td>United States</td>
<td>Any</td>
<td>Modern Auth Apps</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>Secure App Access</td>
<td>Direct App Access</td>
<td>Australia</td>
<td>Any</td>
<td>Modern Auth Apps</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>Secure App Access</td>
<td>Direct App Access</td>
<td>United States</td>
<td>Any</td>
<td>ActiveSync</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>Secure App Access</td>
<td>Direct App Access</td>
<td>Banned Countries</td>
<td>Any</td>
<td>Web</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>Secure App Access</td>
<td>Direct App Access</td>
<td>Anonymizers</td>
<td>Any</td>
<td>Web</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>Secure App Access</td>
<td>Direct App Access</td>
<td>IaaS Provider IPs</td>
<td>Any</td>
<td>Web</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>

3. Change the new policy line to match Zscaler and Direct App Access:
4. The policies match from the top down. Move the new policy to the correct place and save:

<table>
<thead>
<tr>
<th>Access</th>
<th>Web App</th>
<th>Access Method</th>
<th>Device</th>
<th>Location</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Web</td>
<td>Any</td>
<td>Anonymizes IaaS Provider IPs</td>
<td>Deny</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td>Web</td>
<td>Any</td>
<td>Banned Countries</td>
<td>Deny</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td>Web</td>
<td>Any</td>
<td>Zscaler US, Zscaler Asia, Zscaler Europe, Zscaler Latin, Zscaler Africa</td>
<td>Direct App Access</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td>Web</td>
<td>Any</td>
<td>Any</td>
<td>Secure App Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DLP Download</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DLP Upload</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td>Activesync</td>
<td>Any</td>
<td>Any</td>
<td>Secure App Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DLP Download</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DLP Upload</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td>Modern Auth Apps</td>
<td>Any</td>
<td>United States Australia</td>
<td>Direct App Access</td>
</tr>
</tbody>
</table>

CLOUD DATA CONTROLS

Bitglass leverages cloud app APIs for additional visibility and control over data stored in cloud apps. Bitglass can analyze the data-at-rest to identify its sensitivity, classification, and malware, across any app that provides API access. In turn, this informs the placement of controls around data so that organizations can govern sharing and access more effectively. Advanced data protection capabilities can also be implemented via API; for example, DLP actions like quarantining and encryption can be taken on cloud data-at-rest.

This integration allows Zscaler and Bitglass customers to scan cloud data at rest and check for inappropriate data sharing. Cloud data visibility is one of the fastest growing issues within the CISO community, because of tighter cloud data privacy regulations. Administrators and security staff can no longer access all data, therefore it's impossible to know whether a user has any sensitive data. Bitglass visualizes your data across all your apps in a Cloud Dashboard, while retaining user privacy.

Adding a Cloud Condition

Now you can configure the API Cloud Condition to scan data at rest

1. Create a new Cloud Condition by clicking the 🔃 icon
2. Open the new Cloud Condition by clicking on it

3. Click **Add Column** and check for Credit Cards

4. Click **Add Group** and check for External Sharing

5. Click **Add Column** and check for Public Sharing, and change the operator to **OR**

6. Modify the Action to **Remove All Sharing** and tick **Alert Admin**
7. Click **OK**, and **Save** the Policy

Every time you try and Share one of the documents in OneDrive that contain Credit Cards, the Sharing will be turned off automatically and the Admin will be notified.

**Cloud Dashboard**

Once Bitglass scans the data, it presents the data and sharing status in a Cloud Dashboard.

1. **Click Dashboards > Discovery** to access the dashboard.
COMPANY OVERVIEW

Zscaler Overview
Zscaler enables the world’s leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access and Zscaler Private Access, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. For more information on Zscaler, please visit www.zscaler.com or follow them on Twitter @zscaler.

Bitglass Overview
Bitglass, the Next-Gen CASB company, is based in Silicon Valley with offices worldwide. The company’s cloud security solutions deliver zero-day, agentless, data and threat protection for any app, any device, anywhere. Bitglass is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution. For more information on Bitglass, please visit www.bitglass.com or follow them on Twitter @bitglass.