iboss Integration with Microsoft® Azure AD

The Challenge

Organizations using Azure Active Directory via SAML improve their security posture for access to cloud applications. But what about legacy applications that they have on premises or may have moved to hosting in the public cloud? Many of those applications do not support SAML based identity. They often rely on legacy NTLM or Kerberos authorization for user access. These methods authorize access for an extended period of time and do not enable Zero Trust access where authorization needs to be done on a least privileged basis.

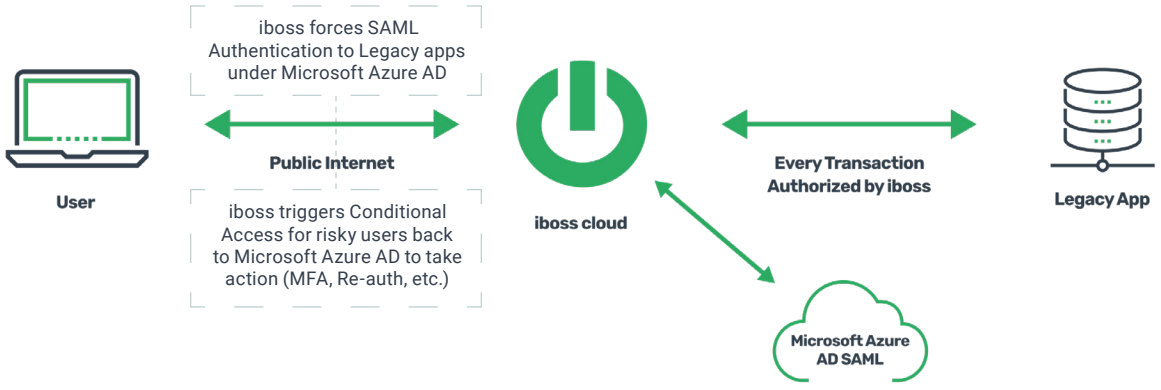
Organizations also want to be able to apply conditional access policies for resource access based on device risk posture or threat level and take action on each request.

The challenge and solution look like this:

iboss Extends SAML Authorization to Legacy Applications

Before iboss

After iboss



The Solution

iboss forces SAML authentication to any non-SAML aware app resource by applying Azure AD authorization on a per-request basis in compliance with Zero Trust principles.

iboss can apply different levels of authentication requirements for different resources

- iboss can perform SAML authentication (SAML/OIDC) on legacy applications and services that do not support SAML authentication.
- iboss can force SAML authentication for resources that require different identity providers.
- iboss can associate each resource policy with a different Identity Provider (IdP) that can be used for authenticating users.

Because access is granted to resources through the iboss Zero Trust Edge, iboss can force SAML authentication even in cases where the protected resources have no ability to do so. This is because the SAML authentication is performed between the user and the iboss Zero Trust Edge before the connection is granted to the resource. This allows legacy applications and services to be protected by SAML authentication and comply with Zero Trust principles.

Resource policies can also be configured to require that multi factor authentication (MFA) be used before access to a resource is granted. If the resource policy requires MFA, the iboss Zero Trust Edge confirms that MFA was validated during the login process.

Benefits of Microsoft Azure AD and iboss for Authorization to Legacy Applications

- Eliminates the need for legacy firewalls with shift to iboss Zero Trust Edge.
- Eliminates reliance on Kerberos authentication, with shift to SAML authentication.
- Lowers risk from reliance on legacy authorization's lengthy session time outs which can result in high risk impact from unauthorized access.
- Enables Zero Trust compliance from forced authentication on every packet, regardless of application.
- Avoids the need to lift and shift legacy resources immediately in order to support Zero Trust Architecture.
- Provides granular per resource control around applications.
- Provides visibility into risk profile beyond just legacy user authentication.

About iboss®

iboss is a cloud security company that enables organizations to reduce cyber risk by delivering a Zero Trust service designed to protect resources and users in the modern distributed world. Applications, data and services have moved to the cloud and are located everywhere while users needing access to those resources are working from anywhere. Built on a containerized cloud architecture, iboss delivers security capabilities such as SWG, malware defense, browser isolation, CASB and data loss prevention to protect all resources, via the cloud, instantaneously and at scale. This shifts the focus from protecting buildings to protecting people and resources wherever they are located. Leveraging a purpose-built cloud architecture backed by 230+ issued and pending patents and more than 100 points of presence globally, iboss processes over 150 billion transactions daily, blocking 4 billion threats per day. More than 4,000 global enterprises trust the iboss Cloud Platform to support their modern workforces, including a large number of Fortune 50 companies. iboss was named one of the Top 25 Cybersecurity Companies by The Software Report, one of the 25 highest-rated Private Cloud Computing Companies to work for by Battery Ventures, and CRN's top 20 Coolest Cloud Security Companies of 2022. To learn more, visit www.iboss.com

+1 877.742.6832
sales@iboss.com

101 Federal St
Boston, MA 02110