ManageEngine
ADAudit Plus

Securing your Azure AD:

A comprehensive guide to safeguarding your cloud environment.

When asked about adopting an enterprise cloud computing platform, 66 percent of IT professionals say security is their greatest concern. The substantial benefits of cloud platforms are matched by great risks. If you're planning on or have already migrated your Active Directory (AD) to Azure AD, cloud security concerns are bound to cross your mind more often than not.

Where native Azure AD auditing falls behind in cloud security

Despite Microsoft taking every step possible to ensure safety of users, they are bound to vulnerabilities. Some of these vulnerabilities that could pave way to an attack are:

Paywalls

Microsoft provides an array of sophisticated auditing and security solutions, but it reserves them for its high-tier plans. For instance, advanced threat intelligence is only available for E5 subscriptions and above, although any organization that's entrusted Azure AD with its data could greatly benefit from this feature. Because Microsoft has restricted its security solutions using paywalls, the average Azure AD customer is less equipped to face various security risks.

Limited data-retention period

Azure AD stores activity reports for a maximum of 30 days, and security signals for a maximum of 90 days (for Azure AD Premium P2). This is not nearly enough time to clearly identify threats. The Ponemon Institute's 2017 Cost of a Data Breach Study found that it takes an average of 191 days to detect a data breach.

Moreover, most compliance standards require companies to store their audit logs for a much longer period. For example, PCI DSS requires organizations to store logs for one year, while HIPAA requires a minimum of six years of logs. For compliance audits and investigations, the short data retention period offered by Microsoft is insufficient, unless IT admins periodically save the logs manually.

Lack of support for hybrid auditing

Despite cloud deployments witnessing a boom in the past decade, Gartner estimates that 72 percent of organizations opt for a hybrid environment. Azure AD has made it difficult to integrate cloud-based reports with data from on-premises reports. When making a change in a hybrid AD environment, it's impossible to know whether a change was made from the cloud or on-premises.

What you can do to secure your Azure AD

Here's what you'll need to do to achieve optimum security for your cloud environment.

Gain insight on logons and logoffs

Azure AD is the gatekeeper for all Microsoft cloud solutions, so the first step toward securing your Microsoft cloud is monitoring users' logon activity. Brute force and identity hijacking attacks depend on vulnerabilities in the authentication process; once hackers have stolen the credentials they need, they can gain access to cloud environments. Keeping an eye on who's accessing what in your cloud environment via Azure AD will help you detect and respond to attacks that utilize stolen credentials.

Monitor all domain activities

According to Forcepoint, only seven percent of businesses have good visibility of all their critical data. To ensure complete safety, you need to keep up with the changes and activities happening in various devices and applications across your domain.

Misconfigurations in resource access and role assignments could open up opportunities for rogue insiders. Having a keen eye on every change made and permission granted could give you the upper hand in detecting and hopefully preventing any malicious behavior.

Detect anomalous behavior

Among the multitude of occurrences happening throughout the day, a few key abnormalities can indicate a security threat. These could include abnormal resource access, a threshold breach in the volume or number of activities, unusual remote sessions, irregular file activity, and much more. These telltale signs, if detected and investigated, have the potential to immediately stop a large-scale attack in its tracks.

Respond to threats immediately

Cloud providers are getting better at securing their offerings. A 2018 Gartner study shows that by 2022, at least 95 percent of cloud security failures are predicted to be the customer's fault. The responsibility for keeping your cloud resources secure lands on you, so you need to always be on the lookout for potential security infringements. Giving a seemingly harmless situation the benefit of the doubt could drive you towards big losses. Always have a safety net to fall back on in case your organization ever faces a security breach.

Third-party solutions for securing Azure AD

The above tips will help you secure your Azure AD environment, but accomplishing them with Azure AD's native event logging tools proves difficult. Security professionals like you need third-party solutions to spot threats and investigate incidents across your entire IT infrastructure.

An ideal solution provides comprehensive analysis of all your logs and centralized access to audit data for all your systems. According to Crowd Research Partners, 84 percent of organizations say traditional security solutions don't work in cloud environments. Take a look at what ADAudit Plus has to offer to overcome the shortcomings of Azure AD auditing.

How ADAudit Plus helps

Complete change monitoring across hybrid environments

ADAudit Plus offers a correlated view of all changes happening across your AD, be it on-premises or in the cloud. Pull up reports with complete details about who made a change, when it happened, where it originated, and what the old and new values are. Information like the on-premises SAM, GUID, SID, and DN of the user who made the change, along with the tenant and application name, are included.

These customizable reports also include information like the devices from which events have been logged, those devices' geolocation, and their IP address. License management and application management reports keep you updated on the status of license changes and applications in your environment. Each of these reports can be exported in the format of your choice.

Limitless data logging and archiving

Unlike Azure AD's native auditing tool, ADAudit Plus' audit logs and reports are stored for an indefinite amount of time. They can be archived and restored whenever you want. Logon and logoff details of all users are categorized by application and type of logon. You can pull up complete logon activity, along with logon failures, and the reason for each.

ADAudit Plus also includes preconfigured reports that are tailored to meet industry standards like SOX, HIPAA, PCI DSS, FISMA, and GLBA to ensure that your organization always stays compliant.

User behavior analytics for accelerated threat response

Insider threats often occur by malicious users misusing their privilege or committing out-of-the-ordinary activities. Start detecting anomalous behavior with ADAudit Plus' analytics engine, which uses machine learning techniques to separate normal activities from abnormal happenings.

Things like irregular logons, critical resource accesses, and high-volume activity breaches are all potential indicators of threats. By detecting these indicators as quickly as possible, you're getting a head-start on investigating suspicious behavior.

Real-time alerts and automated response

With all the detection and prevention out of the way, get down to responding to these threats. ADAudit Plus sends you real-time notifications of alarming events occurring in your domains. These alarms can be sent straight to your inbox or phone, so you'll never miss a critical notification.

Take your threat mitigation a notch further and configure automated responses to events that execute scripts whenever a specific alert is triggered. With automated responses in place, you can be sure that risky situations don't get worse while you try to determine the source of an issue.

With the above features and more, ADAudit Plus ensures that your domain is as safe as it can get by providing you a complete audit overview of your hybrid network