RESEARCH

HOW ADASSESSOR BRINGS VISIBILITY TO AD ATTACK SURFACES

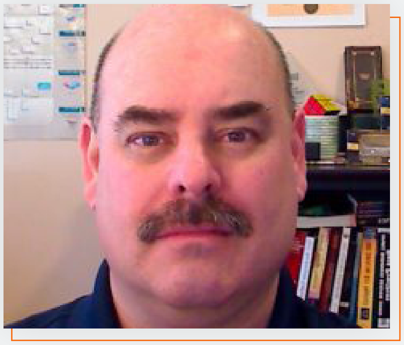
eWEEK

ADSecure intercepts unauthorized AD queries and then returns false information to the attacker, which security teams could further use to trap an attacker and gather information on the attack.

RESEARCHER'S BIO

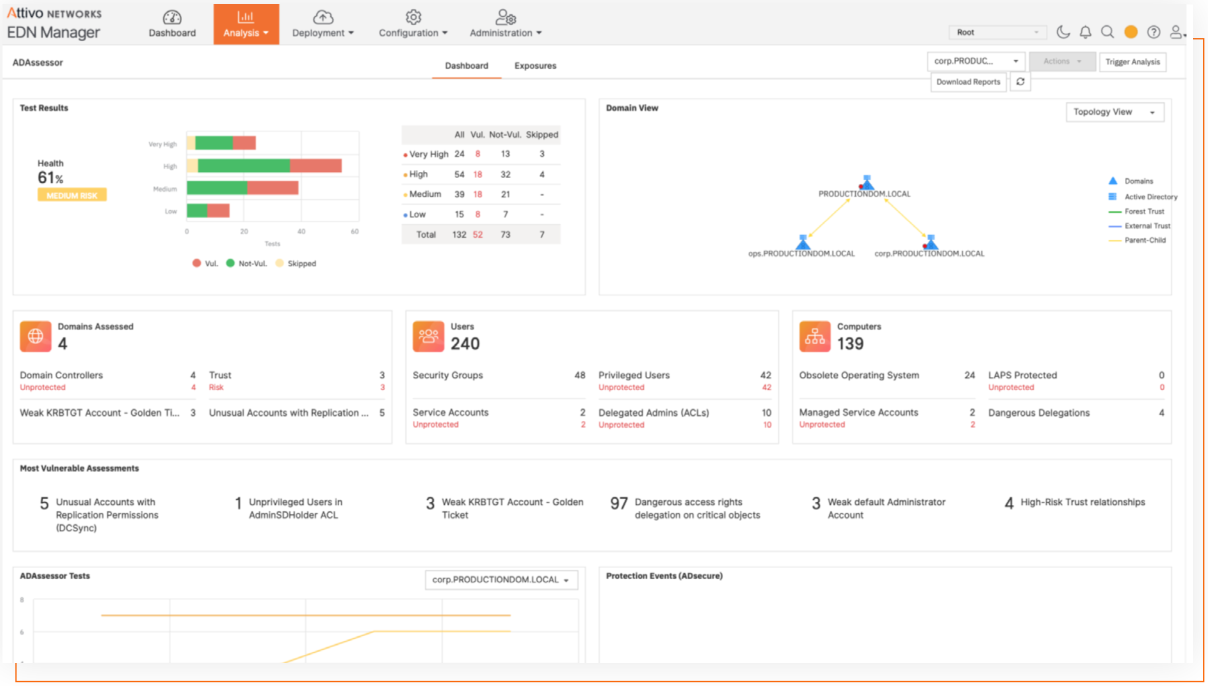
FRANK J. OHLHORST

Frank Ohlhorst is an award-winning technology journalist and IT industry analyst, with extensive experience as a business consultant, editor, author, and blogger. Frank works with both technology startups and established technology ventures, helping them to build channel programs, launch products, validate product quality, create marketing materials, author case studies, eBooks and white papers.



By Frank J. Ohlhorst - August 6, 2021 Effectively securing and protecting Active Directory (AD) is an undeniable best practice for businesses today. Especially since some 90% of the world's enterprise organizations are using AD as their primary method for authentication and authorization.

AD's enormous market share has made it a prime target for attackers. In fact, cyberattacks on AD are so prevalent that Microsoft warns that some 95 million AD accounts are the target of cyberattacks every day.



Health
61%
MEDIUM RISK

	All	Vul.	Not-Vul.	Skipped
● Very High	24	8	13	3
● High	54	18	32	4
● Medium	39	18	21	-
● Low	15	8	7	-
Total	132	52	73	7

Domains Assessed
4

Domain Controllers Unprotected	4 4	Trust Risk	3 3
Weak KRBTGT Account - Golden Ti...	3	Unusual Accounts with Replication ...	5

Users
240

Security Groups	48	Privileged Users Unprotected	42 42
Service Accounts Unprotected	2 2	Delegated Admins (ACLs) Unprotected	10 10

Computers
139

Obsolete Operating System	24	LAPS Protected Unprotected	0 0
Managed Service Accounts Unprotected	2 2	Dangerous Delegations	4

Most Vulnerable Assessments

5 Unusual Accounts with Replication Permissions (DCSync)

1 Unprivileged Users in AdminSDHolder ACL

3 Weak KRBTGT Account - Golden Ticket

97 Dangerous access rights delegation on critical objects

3 Weak default Administrator Account

4 High-Risk Trust relationships

ADAssessor Tests

corp.PRODUCTIONDOM.LOCAL

Protection Events (ADsecure)

AD houses a myriad of sensitive information, such as user account information, enterprise resources, ACLs, and so on, making it an extremely attractive target for cybercriminals. Simply put, if an attacker can exploit the information contained within AD, they can do pretty much as they please with an organization, including stealing information, compromising applications, planting malicious software, or even just simply locking every user out of all applications.

It is a threat made even more dramatic by how AD is now used with Azure and Office 365, extending threats to the enterprise beyond just on premise and into the cloud. Making due diligence even more critical for cybersecurity professionals. Basic chores such as regular audits and defining policies to protect AD must become the norm. However, those traditional best practices have been proven to be insufficient, since organizations still fall prey to attacks on AD.

It is a problem best defined by a lack of visibility. In other words, cybersecurity pros lack complete visibility into AD to detect attack surfaces, as well as suspicious objects, or activities. Audits prove only useful as a snapshot of AD's status at a given time, while activity monitors cannot often lack the ability to detect anomalous actions.

ADAssessor from Attivo Networks aims to bring real-time visibility to AD solving one of the biggest challenges faced by administrators, the ability to fully understand what is happening behind the scenes in AD, discover attack surfaces, and detect active attacks.

A CLOSER LOOK AT ADASSESSOR

ADAssessor is all about detection, visibility, and response for AD environments. In other words, the product is designed to bring cyber hygiene to AD by continuously scanning AD for exposures, misconfigurations, and anomalous activity in AD. What's more, ADAssessor provides real-time alerting for activities that signify that AD is under attack. Capabilities that are akin to continuous penetration testing for AD.

ADAssessor can be deployed on-premise or as a cloud hosted platform, either of which links to Windows Domain Controllers to monitor AD events, such as change notifications, and detect misconfigurations, scan for potential attack vectors, or identify attacks in progress.

The product establishes the link between the cloud service and the domain controller by installing a software client onto a domain controlled PC, which also acts as an endpoint that enables the product to detect endpoint based attacks on the domain controller.

ADAssessor uses a combination of detection and automation to drive response and alerting, which in turn acts on immediate threats, while also informing administrators of needed actions.

HANDS ON WITH ADASSESSOR

ADAssessor connects to a domain using what could be best described as a hybrid model. Administrators will need to install software on a local PC endpoint, which acts as an ersatz connection between the domain controller and the ADAssessor's services engine. There are several advantages to that method of integration.

For example, there is no disruption in operations, meaning that the domain controller does not need to be shutdown or rebooted. What's more, the installation methodology helps keep deployment very simple, while also creating the opportunity to secure the host endpoint.

However, there are a couple of considerations when using that type of installation, such as that dedicated endpoint can become a single point of failure for ADAssessor, and that PC must also be secured, maintained, and managed. Those concerns aside, a hybrid deployment model would seem to be a preferred method for integrating a product such as ADAssessor.

Once installed, ADAssessor goes about its business of assessing the domain controller(s) to discover misconfigurations and weaknesses across AD domains and forests. As the product finds those potential security flaws, it surfaces the information so cybersecurity pros can eliminate those potential attack vectors.

One particular area of interest is how the product helps to reduce attack surfaces by identifying exposures and misconfigurations that leave AD vulnerable to attack. Here the product analyzes active directory information to provide visibility to account risks, privilege exposures, and policy weaknesses, which in turn is used to create something akin to risk metrics that are surfaced to the administrator.

WHERE ATTACKS ON AD USUALLY START

That proves very important for the ongoing battle against attackers. Attacks on AD usually start with an attacker searching an AD controller for exposures and misconfigurations. While attackers may have different goals, most attacks start with attempts at lateral movement, where attackers can attempt to gain privileged access to seize control of the domain. Those types of attacks create recognizable patterns, but only if the activity is being continually monitored and classified.

Here, ADAssessor provides the visibility and the necessary analytics to detect attacks in progress, in real time. What's more, ADAssessor can restrict suspicious activity from impacting AD, and prevents attackers from gaining granular access to the security settings (or entitlements) , derailing an attack before any damage is done.

ADAssessor continuously monitors identities, as well as privileged account risks. That monitoring creates an active baseline, identifying risks created by AD objects, such as stale credentials, service accounts, shared credentials, and the paths commonly used for attacks on AD identities. The product derails many of those types of attacks by flagging suspicious activities on the AD controller that indicate an attack is underway. .

Typically, attackers will query AD to discover high-value privileged accounts and gather as much data as possible to create a potential attack surface. ADAssessor works well with another Attivo solution called ADSecure, which detects attackers' attempts to make unauthorized queries and then obfuscates the data that an AD query normally returns.

Simply put, ADSecure intercepts unauthorized AD queries and then returns false information to the attacker, which security teams could further use to trap an attacker and gather information on the attack. ADSecure detections can appear on the ADAssessor dashboard.

The combination of continuous monitoring, paired with real-time analysis improves AD's cyber hygiene, with the added benefits of reducing potential attack surfaces, and preventing attackers from gaining a foothold on an AD domain.

CLOSING THOUGHTS

ADAssessor solves many of the security pain points those administrators encounter on large across Active Directory implementations. That said, it should not be considered a replacement for a competent administrator, but a tool that lessens the burden on administrators. The product also aids security teams by allowing them to go deeper, broader, and wider in their assessments, while gaining continuous visibility to exposures.

ADAssessor offers immediate value by identifying and remediating Active Directory security hygiene issues. That value is further extended by the ease of implementation, which eliminates disruption and gives access to an innovative management console, where analysis and data for remediation assistance is readily available.

ADAssesor also brings real-time attack detection to the table, backed by visibility into critical domain, computer, and user-level exposures. Those insights reveal identities and service account risk related to credentials, privileged accounts, stale accounts, shared credentials, and AD attack paths.

As businesses leverage AD across domains, and implement hybrid solutions, tools that can surface threats and give visibility into complex AD implementations will prove to be even more critical. Attivo seems to have a head start in the world of securing AD, and ADAssessor appears seems to be the primary reason for that head start.