PRODUCT BRIEF

Endpoint Threat Defense for Active Directory

DOMAIN COMPROMISE

It only takes one compromised endpoint connected to a corporate domain to jeopardize the entire organization:

- Want to know where the sensitive data lives?
- Want to know where the administrators are?
- Want to know how to own the target environment?

Ask Microsoft Active Directory

Once a foothold on a domain-connected endpoint is achieved, attackers perform reconnaissance to the AD database to gain visibility into all organizational resources. The next step is to steal domain credentials stored locally on the endpoint or remotely on other resources. With stolen credentials, attackers are granted full and stealth access to all servers, applications, and computers in the organization - with the end goal of stealing or encrypting data.

Attackers utilize trusted applications and built-in tools in their post-exploitation efforts; the use of trusted applications and built-in protocols, as opposed to malicious binaries, makes the detection, forensic tracing as well as hunting of these stealthy attacks nearly an impossible task.

Active Directory: The Root of Domain Compromise

Microsoft Active Directory is a network domain service used globally by nine out of ten companies to manage and control their internal resources, including servers, endpoints, applications, and users. By design, Active Directory (AD) is open to any domain-connected user, meaning all identities and resources on a corporate network are visibly exposed, making AD the number one target for attackers.

Contain APTs by Hardening AD

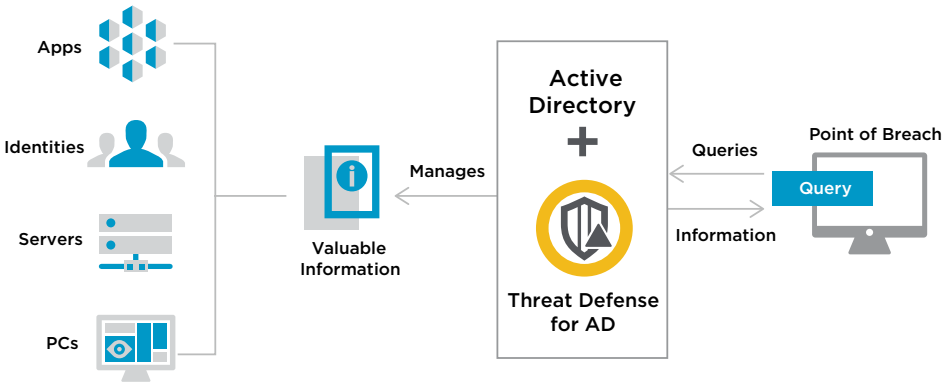
Symantec® Endpoint Threat Defense for Active Directory (AD) provides effective AD defense from the endpoint to provide autonomous breach containment, incident response, and domain security assessment. It's the only security solution that immediately contains attackers after endpoint compromise but before attackers can persist on the domain. It disrupts reconnaissance activity and prevents attackers from utilizing AD to move laterally to other assets. Threat Defense for AD addresses the network path of least resistance, greatly reducing the time, effort, and error involved in detecting and containing a breach where it starts: the endpoint. Threat Defense for AD applies AI-driven native-language processing, sophisticated obfuscation techniques, and advanced forensics methodologies to quickly discover and contain a breach.

Defend AD Against Attacks with Obfuscation

Threat Defense for AD aims to alter the attacker's perception of the organization's internal resources—all endpoints, servers, users, applications, and locally stored credentials—at the point of breach. This solution autonomously learns the organization's AD structure in its entirety—servers, endpoints, applications, users, branches, naming conventions, configurations, attributes—and uses this data to create an authentic and unlimited obfuscation.

On the endpoint, AD activities are evaluated, including runtime processes and context. These actions determine if obfuscation needs to be activated, helping project the compromised domain-connected assets to the attacker. Memory is manipulated on each endpoint, and the obfuscation is presented to the attacker when it interacts with the native and open AD APIs, providing a view of the environment that differs from reality. With these elements in place, the attacker gives itself away while interacting with assets or attempting use of domain administrator credentials. At the same time, a high-fidelity alert is triggered and the attack is automatically blocked.

Figure 1: Endpoint Threat Defense for AD Addresses Stealthy Attacks



Continuous AD Assessment to Reduce Attack Surface

As an organization's implementation of AD evolves, configuration settings may not be properly maintained, security enhancements may not be implemented, and vulnerabilities may begin to appear on the domain and AD service, which may be used against them by attackers. Additionally, attackers leave behind back doors and persistence hooks that allow them to come back at any time. Threat Defense for AD continuously probes for domain misconfigurations, vulnerabilities, and persistence, and presents the AD administrator the domain from the attacker's perspective, allowing for immediate risk mitigation to reduce the attack surface.

An automated assessment process uses attack simulations to gather in-depth information about the configuration of the domain, privileged accounts, security settings, GPO, endpoints, domain controller, and Kerberos. It autonomously analyzes every component of the domain and AD structure for misconfigurations and back doors attackers may have left behind. It is important to identify these misconfigurations and back doors on an ongoing basis to reduce risk on the domain. Once a misconfiguration or back door is identified, an alert is sent to the central console with prescriptive recommendations on remediation.

Learn more about Symantec Endpoint Threat Defense for AD at broadcom.com/info/endpoint-security/threat-defense-for-active-directory.

BROADCOM
connecting everything®

For more information, visit our website at: www.broadcom.com

SED-ETD-AD-PB102 March 18, 2025