DATA SHEET

Contact us - Business Security Consultants, Inc.

Symantec Endpoint Threat Defense for Active Directory

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 – servers, endpoints, applications, and users[1]. 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.

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 admins 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.

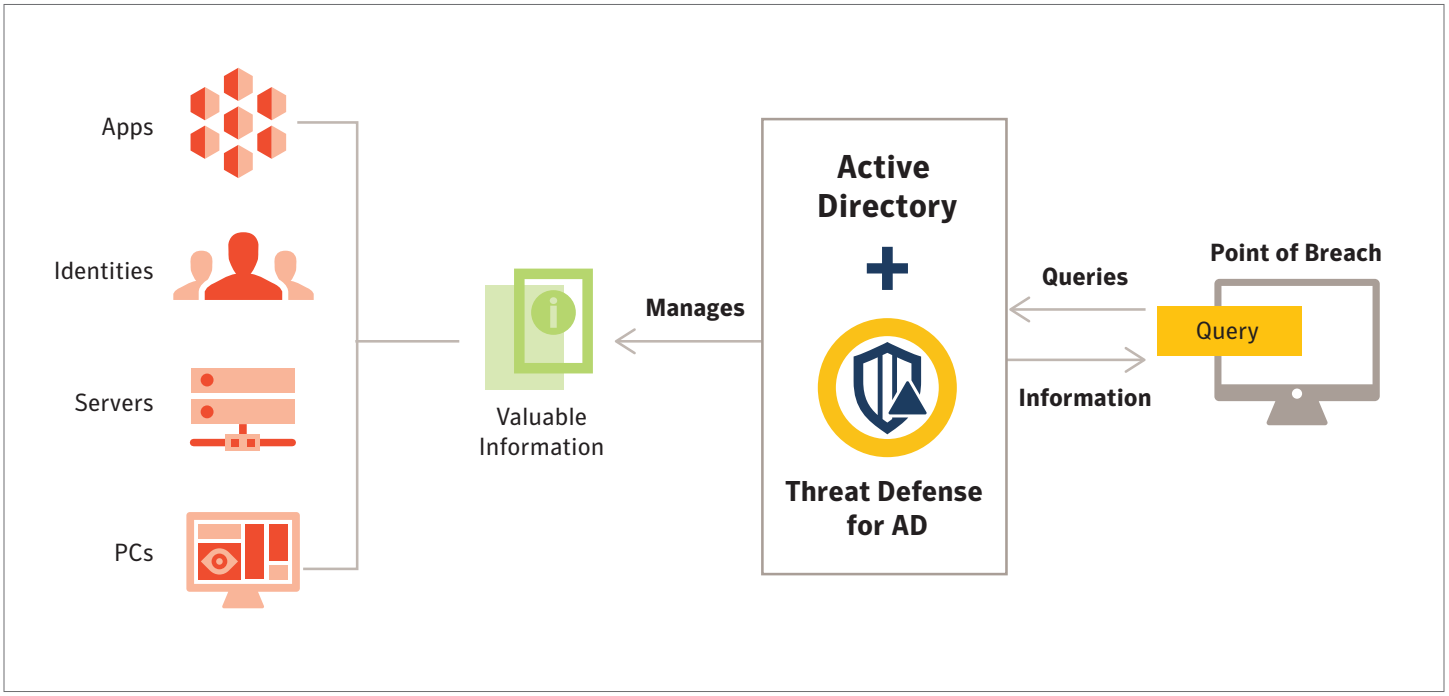
Contain APTs by Hardening Active Directory

Symantec Endpoint Threat Defense for Active Directory (Endpoint Threat Defense for AD) advances Symantec's endpoint security solution for addressing stealthy attacks or APTs with effective Active Directory 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 compromise of an endpoint, but before they can persist on the domain. It disrupts reconnaissance activity and prevents them from utilizing Active Directory to move laterally to other assets. Threat Defense for AD addresses the least path of resistance in today's networks, 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.

[1] An Overview of Active Directory, Philippe Beraud, Microsoft Corporation, 2016



Defend Active Directory Against Attacks with Obfuscation

Threat Defense for AD effectively controls the attacker's perception of the organization's internal resources—all endpoints, servers, users, applications, and locally stored credentials—right at the point of breach. Symantec's solution autonomously learns the organization's Active Directory structure in its entirety (servers, endpoints, applications, users, branches, naming conventions, configurations, attributes etc.) and uses this data to create an authentic and unlimited obfuscation. On the endpoint, runtime evaluation of processes, context and Active Directory activity is evaluated to determine if activation of obfuscation is needed. With obfuscation, a perspective of the domain-connected assets compromised is projected to the attacker; the attacker gives themselves away while interacting with assets or attempting use of domain admin credentials on Threat Defense for AD's perception. At this point a high-fidelity alert is triggered and the attack is automatically blocked.

Real-Time Breach Visibility and Automated Attack Containment

The moment an attack is detected, and an alert is triggered from the endpoint, and an on-demand scan gathers specific forensic information related to the attack. Automating the forensic process and scanning for the right information, only when an attack is detected, guarantees only high priority, legitimate alerts get surfaced, reducing alert fatigue.

Using unique incident response methodologies specifically designed for a corporate AD domain environment, this solution provides real-time forensics reporting that captures actual reconnaissance, credential theft, and lateral movement phases that were performed by the attacker. The attack chain is documented all the way back to patient zero to identify where the attack originated and assesses if the attack is a local incident or part of a bigger effort. Automatic mitigation stops the malicious process on the endpoint to contain the breach in real- time, removing its ability to spawn another process, overwrite another part of memory, run reconnaissance commands, or communicate out to the network.

Continuous Active Directory Assessment to Reduce Attack Surface

As organizations' implementation of Active Directory evolves, configuration settings may not be properly maintained, security enhancements may not be implemented, and vulnerabilities may begin to appear on the domain and Active Directory service, which may be used against them by attackers. Additionally, attackers leave behind backdoors 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 Active Directory Administrator their 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. Next, it autonomously analyzes every component of the domain and Active Directory structure for misconfigurations and backdoors attackers may have left behind. It's important to identify these misconfigurations and back doors on an ongoing basis to reduce risk on the domain. Once a misconfiguration or backdoor is identified, an alert is sent to the central console with prescriptive recommendations on remediation.

To learn more about Symantec Endpoint Threat Defense for Active Directory, visit http://www.go.symantec.com/threat-defense-for-ad

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

19C199995_DS_SEP_THREAT_DEFENSE_AD_EN