Cayosoft®

Solution Brief

Protect Hybrid Active Directory Before, During, and After a Cyberattack with Cayosoft ITDR & IGA Solutions

Steps to Achieve Hybrid AD Identity Resilience and Avoid Costly Outages

BACKGROUND

Identity threat detection and response (ITDR) was recently defined by Gartner as a set of practices and software solutions that analyze and defend identity systems to better protect organizations user identities from compromise. The most popular identity system is Microsoft Active Directory (AD) and its popular cloud counterpart: Azure AD. According to Microsoft, AD is used by 86% of enterprises around the world, making it the obvious target for cyberattacks. This can include ransomware, wiperware, and other malware deployed with the intent to cause a costly AD outage. Cayosoft is recognized by Gartner as an ITDR solution provider and delivers solutions that make identities more resilient to attacks and allow organizations to guarantee a fast forest recovery, if needed.

WHY IS ITDR IMPORTANT

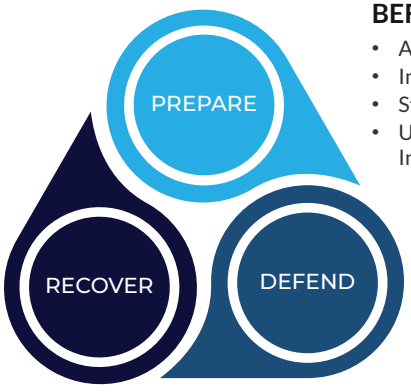
When an AD outage occurs, employees are denied the ability perform their jobs, crippling the entire organization and resulting in a business shutdown. To prevent detrimental business interruptions like these, extra care must be given to protect on-premises and cloud Active Directory identities. Organizations must prioritize the protection of Active Directory and Azure AD by taking proactive measures to prevent attacks, detect and defend against active attacks, and to guarantee an instant full forest AD recovery, should an attacker succeed.

STEPS TO ACHIEVE IDENTITY RESILIENCE

Understanding what should be done before, during, and after an attack may not be immediately clear. Below are some of the required steps to achieve hybrid AD identity resilience, avoid costly outages, and, when needed, ensure the fastest recovery possible.

ACHIEVE HYBRID AD IDENTITY RESILIENCE

Steps to Achieve Hybrid AD Identity Resilience, Avoid Costly Outages, & Guarantee Instant AD Recovery



BEFORE ATTACK

- Adopt the Zero-Trust Framework
- Implement Identity Governance & Administration *
- Start Continuous Change Auditing & Alerting *
- Use Threat Detection to Uncover & Resolve Indicators of Exposure *

DURING ATTACK

- Quickly Isolate Suspect Changes for Analysis *
- Implement Automatic Countermeasures *
- Use Threat Detection to Uncover & Resolve Indicators of Compromise (Attacks) *

AFTER ATTACK

- Guarantee & Recover AD Forest Instantly *
- Automatically Deploy Isolated Recovery Sites *
- Post-Recovery Analysis & Forensics *

* Indicates a Cayosoft Solution

Learn more at cayosoft.com

BEFORE ATTACK

Adopt a Zero-Trust Framework

Zero trust is a modern approach to security design and implementation for IT systems. The core principle is to use strong verification for everyone, and anything, connected to or attempting to access an organization's resources.

Implement Identity Governance and Administration (IGA)

Identity governance and administration (IGA) is one way to implement a Zero-Trust Administration and is a critical solution to preventing insider threats. While both IGA and ITDR fall within identity management, they are fundamentally different. To understand the difference, think of IGA as management controls, while ITDR is finding and fixing threats to the environment on an ongoing basis. IGA and ITDR are directly complimentary and arguably should be implemented together.

Institute Continuous Change Monitoring and Auditing

Native event logs are often the first target for attackers, causing the organization to be blind to changes they are making. Understanding what is changing across AD and Azure AD is a serious challenge for all Microsoft customers. On top of that, they must then be able to quickly identify mistakes or malicious changes to the AD data, configuration, or security policies. Continuous change monitoring and auditing goes beyond event log collection to identify all changes, including those that would be missed by security and risk management (SIEM) tools, to deliver the critical visibility needed to identify and understand a single change or a series of changes.

Utilize Threat Detection to Uncover and Resolve Indicators of Exposure (IOE)

Indicators of exposure (IOE) are weaknesses that can be exploited by an attacker to compromise an organization's security. Threat detection can reveal misconfigurations and vulnerabilities in AD and Azure AD, allowing administrators to mitigate these risks and close the door on attackers. Like antivirus for computers, identity threat detection is the antivirus for AD.

DURING ATTACK

Quickly Isolate Suspect Changes for Analysis

Visibility into changes made, as part of an attack, are crucial in an effort to slow down or stop the attack entirely. Because an attacker may make changes to on-premises AD and use those changes to move the attack to Azure AD, it is critical that the changes be presented in a single place. The defender can then isolate those changes quickly and easily for additional action.

Implement Automatic Countermeasures

In most environments, unwanted or forbidden changes (changes that should have never been made) can be identified ahead of time. Unfortunately, the native permissions typically used to control changes may have been compromised by an attacker, so additional measures are needed. The ability to easily identify forbidden changes and then automatically rollback those changes when they are detected may stop an attack or at least slow down an attack, providing critical time for additional countermeasures to be enacted.

Utilize Threat Detection to Uncover Indicators of Compromise (IOC)

Indicators of compromise (IOC) and indicators of attack (IOA) are artifacts or other evidence that an attack has already occurred, or an attack is in progress. Threat detection can uncover indicators that AD is compromised and, based on the indicators, detail the likely method used and potential remediation steps. By uncovering these indicators, administrators may gain insight into additional steps they can take to stop or slow down the attack or future attacks.

AFTER ATTACK

Guarantee & Recover AD Forest Instantly

If an attack is successful and an AD outage occurs, it will be highly visible to both users and executive management. The longer the outage lasts, the higher the costs, placing pressure on IT to resolve the problem – fast. To minimize the recovery time and the possibility of a failed recovery, a standby recovery directory can be used. Standby directories eliminate the problems of legacy recovery solutions, with the same or lower costs to the organization. Standby directories also have additional advantages over legacy directory backup and recovery solutions.

Automatically Deploy Isolated Recovery Sites

Unlike legacy directory backup and recovery tools, which require prebuilt servers to wait idle in case a recovery is attempted, standby directories use automatically created isolated recovery sites. These sites are built automatically in Azure or Amazon AWS and represent an exact clone of the production AD. When the production AD goes down, the recovery only requires an administrator to change one or two lines in a network routing table. Then the isolated recovery site takes over. The routing change will take effect in a matter of seconds and results in an instant recovery of the services AD provides. Also, unlike legacy AD backup and recovery solutions, with standby directories the isolated recovery labs are created in advance and the servers in them created and started. This means they have demonstrated a successful recovery and are ready when needed. Legacy solutions can't guarantee success until after a recovery is attempted.

Post-Recovery Analysis and Forensics

After an AD recovery it is important to understand the cause of the problem, so that it does not reoccur. Continuous change auditing, mentioned above, is also useful in a post-attack investigation as it will show what happened before, during, and after an attack.

ABOUT CAYOSOFT

Cayosoft delivers the only unified solution enabling organizations to securely manage, continuously monitor for threats or suspect changes, and instantly recover their Microsoft platforms, including on-premises Active Directory, hybrid AD, Azure AD, Office 365, and more.

Cayosoft Guardian Forest Recovery is the industry's only solution combining all critical AD recovery scenarios into a single, unified platform. Cayosoft Guardian Forest Recovery's capabilities include: hybrid change monitoring, instant rollback of unwanted changes to objects and attributes, instant rollback of unwanted changes to AD group policies, antivirus-like threat protection for hybrid AD, recovery of domain controllers, partitions, and Instant Forest Recovery, using the standby directory architecture discussed in this solution brief.

To learn more, visit cayosoft.com and be sure to follow @cayosoft on LinkedIn, Twitter, and Facebook.

For more information about Cayosoft Guardian Forest Recovery, visit cayosoft.com/gfr.