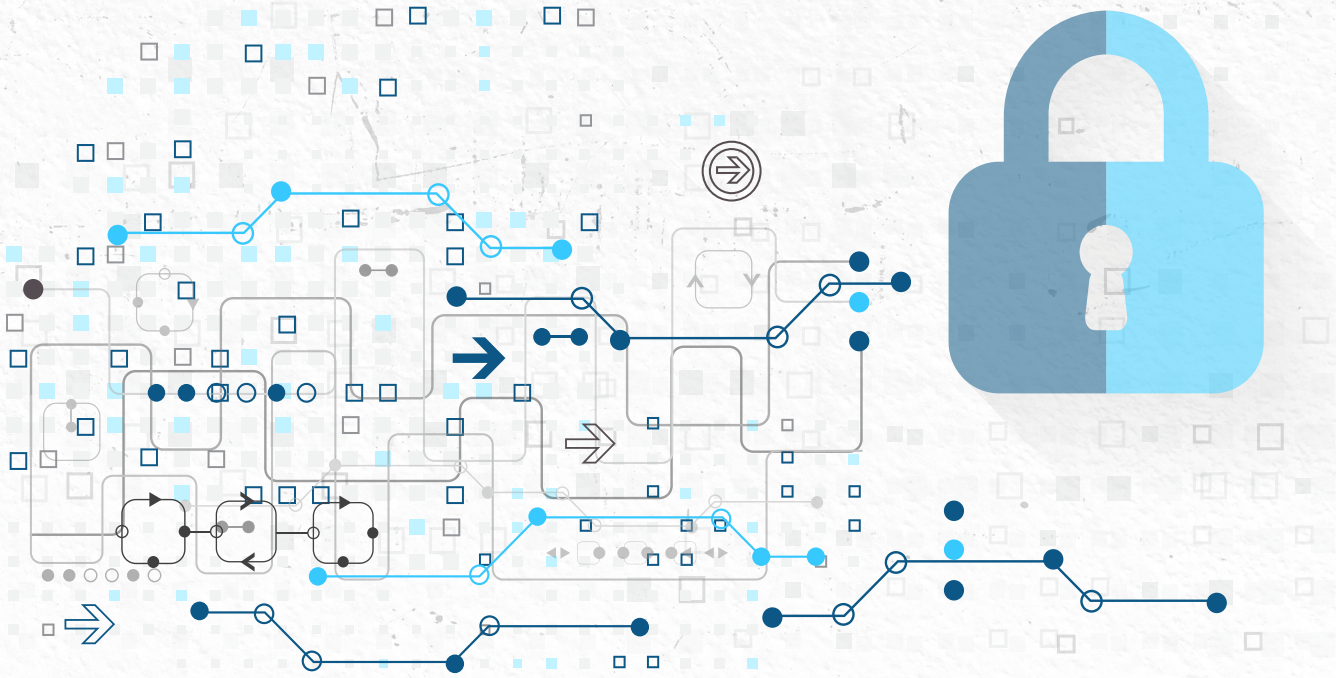
An Essential Buyer's Guide to AD Threat Detection & Response

By Sarah Pavlak, Industry Principal, Security

FROST & SULLIVAN VISUAL WHITEPAPER

BONUS RESOURCE:
2023 AD Threat Detection and Response Vendor Scorecard Template

CONTENTS



Introduction to Active Directory (AD) Security Challenges

AD Is Critical to Organizations, but AD Security Is Often Overlooked

WHY IS AD IMPORTANT?

If AD is not secure, nothing is

- AD is the core identity store for 90% of organizations worldwide—if AD is breached, an attacker gets virtually unrestrained access to the organization's entire network and resources.
- AD underpins cloud identity infrastructure—if a breach occurs in AD, it causes a ripple effect.
- Hybrid identity environments with on-premises AD and Azure AD are complex and difficult to secure—and are increasingly targeted by cyber adversaries.

WHY IS AD SUCH A PROMINENT ATTACK VECTOR?

AD controls access to assets

- AD is a lucrative target because it controls access to critical assets that adversaries can successfully hold for ransom, including sensitive data, customer information, and access to controls that can disrupt operations.
- AD is difficult to secure because of risky configurations that accumulate over time; difficulty in detecting malicious changes, especially in complex AD environments; and constantly expanding threat landscapes.
- Once attackers gain access to the identity system, they can move laterally to achieve domain dominance within AD—at that point, they have access to the entire network and resources.

WHAT IS THE IMPACT OF AN AD ATTACK?

AD attacks are a widespread problem

- The impact of an AD attack is devastating to an organization because the foundation of IT systems has been compromised, which then prevents users from logging into systems and accessing necessary resources.
- Nine out of 10 attacks involve AD exploitation, including SolarWinds, Colonial Pipeline, Maersk, and Hafnium attacks on Microsoft Exchange.
- For sophisticated ransomware-as-a-service (RaaS) groups such as Conti and LockBit 2.0, AD exploits are core to their methodology.
- AD forest recovery is complicated, requiring AD expertise that many organizations don't have.

Primary Challenges

FALSE ASSUMPTIONS

- Many organizations falsely assume that AD security is covered by other security solutions—but without AD-specific protection, they are vulnerable to cyberattacks.

LACK OF AD EXPERTISE

- Lack of AD expertise—combined with reluctance to address risky settings for fear of negative unforeseen consequences in complex environments—increases attack risk.

SILOED OPERATIONS

- Without collaboration between IT and security teams, AD security is not a focus area—despite AD being a prime target for cyberattackers.

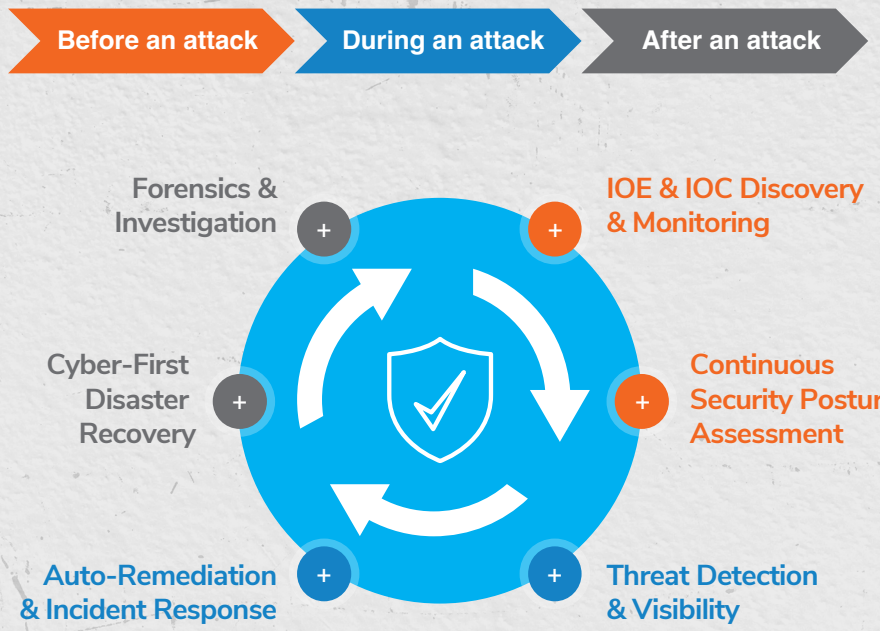
PROLIFERATION OF ATTACKER TOOLS

- Innovative cyberattackers continue to develop new AD exploits, expanding on groundwork laid by successful attacks such as DCShadow, Golden Ticket, and Kerberoasting.

HYBRID IDENTITY ENVIRONMENTS

- Complex hybrid identity environments make it difficult for IT operations and security teams to detect and correlate malicious changes across on-prem AD and Azure AD that could signal an attack.

A LAYERED DEFENSE STRATEGY THAT PROTECTS AD BEFORE, DURING, AND AFTER ATTACK IS KEY TO CYBER RESILIENCE.



No organization can be 100% safe from cyberattacks, but every organization can improve its cyber resilience by identifying and closing security gaps, continuously monitoring for attacks, and implementing a tested AD recovery plan.

Organizations Need AD-specific Security and Recovery Solutions

PREVENTION

Uncover security vulnerabilities

Legacy AD environments are prone to risky misconfigurations and vulnerabilities that accumulate over time. Attackers constantly devise new ways to exploit identity system vulnerabilities. Lack of AD expertise hinders efforts to make substantive security improvements.

AD attack prevention solutions should provide:

- Frequently updated AD security assessments to uncover indicators of compromise (IOCs) and indicators of exposure (IOEs)
- Continuously updated security indicators to address emerging AD exploits
- Expert guidance to prioritize remediation to quickly improve the overall security posture

MITIGATION

Detect advanced attacks

Many AD attacks bypass traditional log- or event-based solutions, such as SIEM products. Lack of visibility into attacks that move vertically in a hybrid environment thwart efforts to stop cloud identity exploits. Detected attacks often spread too quickly to be contained by human intervention.

AD monitoring solutions should:

- Use multiple data sources, including the AD replication stream, to detect advanced attacks
- Automatically remediate malicious changes to stop fast-spreading attacks
- Provide visibility and correlation of changes that originate in on-prem AD and move to Azure AD (or vice versa)
- Provide ability to correlate changes across on-prem AD and Azure AD

RECOVERY

Automate AD forest recovery

Manual AD forest recovery is cumbersome, time-consuming, and error-prone. Traditional backup solutions do not guard against malware reintroduction, and restoring large backups is a slow process that prolongs recovery.

AD recovery solutions should:

- Provide automated, full AD forest recovery to a known-secure state
- Be optimized for speed with small backup size, easy OS provisioning, and ability to restore to any hardware
- Include post-breach forensics to prevent follow-on attacks
- Enable test environment setup to simplify full AD disaster recovery drills

Can you afford for your business to be down for weeks if AD gets attacked?

Expert Buyer's Tip:

Ensure your AD backup solution does not risk reintroducing malware during the recovery process and provides the ability to uncover backdoors that attackers might have left in the environment after recovery.

Watchlist for Hybrid AD Defense Solutions

1

Solutions that offer only partial coverage of the AD attack life cycle will require acquiring, installing, and managing multiple products—increasing total cost of ownership.

2

Solutions not purpose-built for AD protection will fail to address the most common attack vectors cyberattackers routinely use to successfully breach AD environments.

3

In a hybrid environment (common in most organizations), beware of important security challenges in identity environments that use both on-prem AD and Azure AD. It is not enough to track changes in each environment: Organizations need the ability to see across both environments and make critical connections to threats that might otherwise be missed because of siloed data, tools, and teams.

4

Solutions that do not provide full AD forest recovery or rely on bare-metal recovery or system-state backups will prolong recovery, risk re-introducing malware, and fail to provide post-breach forensics to protect against follow-on attacks.

5

Solutions such as Microsoft Defender for Identity (MDI) are an essential element of identity security and complement identity protection solutions but do not specifically address AD security and recovery—MDI monitors and alerts on user behaviors that fit into known attack models but not malicious changes within AD itself. MDI will complement your AD identity system defense.

Beware of common misconceptions about identity security and recovery.

Do you have a fully tested AD disaster recovery plan?

Expert Buyer's Tip:

Ensure your AD recovery solution makes it easy to conduct frequent disaster recovery drills to prepare for a cyber disaster and ensure compliance with security regulations—and get expert help if you don't have an incident response team with identity security experience.

Hybrid AD Protection Vendor Evaluation Criteria - Before an Attack

Before an attack | During an attack | After an attack

BONUS RESOURCE:

Download the 2023 AD Threat Detection and Response Vendor Scorecard Template for a visual comparison of solution providers.

IOE & IOC Discovery

- Scans for indicators of exposure
- Scans for indicators of compromise
- Provides overall security posture score
- Provides remediation guidance
- Supports industry standards such as MITRE ATT&CK, MITRE D3FEND, ANSSI
- Includes Azure AD and hybrid AD indicators
- Incorporates threat intelligence from dedicated research team

Continuous Security Posture Assessment

- Provides real-time IOE monitoring
- Provides real-time IOC monitoring
- Provides continuous security posture assessment
- Detects dangerous operator errors
- Identifies and prioritizes attack paths that lead to Tier 0 assets
- Includes Azure AD and hybrid AD indicators

Hybrid AD Protection Vendor Evaluation Criteria - During an Attack

Before an attack | During an attack | After an attack

BONUS RESOURCE:

Download the 2023 AD Threat Detection and Response Vendor Scorecard Template for a visual comparison of solution providers.

Threat Detection & Visibility

- Detects real-time attacks
- Discovers attacks that bypass event- or log-based monitoring by using replication stream data
- Not dependent on a single agent—provides extended coverage with multidimensional monitoring
- Provides tamperproof tracking
- Integrates with third-party SIEM & SOAR solutions
- Provides contextualized notifications
- Provides prioritized remediation guidance
- Identifies threats across the hybrid AD environment that might otherwise be missed due to siloed data, tools, and teams

Auto-remediation & Incident Response

- Provides automated rollback of unwanted changes
- Supports granular rollback of malicious changes
- Change tracking and rollback in single console
- Provides visibility into exactly who made malicious changes
- Provides hybrid AD threat prevention, detection, and response in a single console
- Includes script-enabled integration capabilities (PowerShell, etc.)

Hybrid AD Protection Vendor Evaluation Criteria - After an Attack

Before an attack | During an attack | **After an attack**

BONUS RESOURCE:

Download the 2023 AD Threat Detection and Response Vendor Scorecard Template for a visual comparison of solution providers.

Cyber-first Disaster Recovery

- Provides automated AD forest recovery
- Provides optimized recovery with multiple processes running in parallel
- Uses small backups for speedy recovery
- Provides clean, malware-free recovery by keeping AD backup separate from OS
- Recovers AD to any hardware, virtual or physical
- Facilitates isolated recovery environment
- Supports disabling all executables on restore to eradicate malware
- Provides post-recovery scan to eliminate backdoors & trust environment again
- Supports Azure AD backup and recovery of objects, groups, users, roles

Forensics & Investigation

- Provides post-breach forensic analysis
- Analyzes malicious changes across hybrid AD environment
- Offers expert breach preparedness and response services
- Provides 24/7 incident response from identity security experts

BONUS RESOURCE:

Download the 2023 AD Threat Detection and Response Vendor Scorecard Template for a visual comparison of solution providers.

GROWTH IS A JOURNEY. WE ARE YOUR GUIDE.

For over six decades, Frost & Sullivan has provided actionable insights to corporations, governments and investors, resulting in a stream of innovative growth opportunities that allow them to maximize their economic potential, navigate emerging Mega Trends and shape a future based on sustainable growth.