Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response

Published 20 October 2022 - ID G00765882 - 21 min read

By Analyst(s): Henrique Teixeira, Peter Firstbrook, Ant Allan, Rebecca Archambault

Initiatives: Identity and Access Management and Fraud Detection

Conventional identity and access management and security preventive controls are insufficient to protect identity systems from attack. To enhance cyberattack preparedness, security and risk management leaders must add ITDR capabilities to their security infrastructure.

Overview

Key Findings

- Credential misuse was involved in 40% of security breaches in 2021. Modern identity threats can subvert traditional identity and access management (IAM) preventive controls, such as multifactor authentication (MFA). This makes identity threat detection and response (ITDR) a top cybersecurity priority for 2022 and beyond.
- There are major detection gaps between IAM and infrastructure security controls. IAM is traditionally used mainly as a preventive control, whereas infrastructure security is used broadly but has limited depth when it comes to detecting identity-specific threats.
- As ITDR capabilities are new, there are few predefined identity-threat-specific playbooks to cover identity breaches and other types of attack on identity infrastructure.
- Identity threats are multifaceted. Misconfigurations of, and vulnerabilities in, identity infrastructure can be exploited. Attackers can also use social engineering against organizations and identity providers' employees in order to steal or misuse credentials, or they can simply buy credentials from initial access brokers (IABs) in the dark web.

Recommendations

Security and risk management leaders focused on identity and access management should:

- Prepare for ITDR with hygiene measures by inventorying their existing prevention controls and auditing their IAM infrastructure for misconfigurations, vulnerabilities and exposures.
- Enhance detection controls by choosing a focal point for identity alert correlation and detection logic that prioritizes identity tactics, techniques and procedures (TTPs) above other detection mechanisms.
- Master the response phase by building or updating playbooks and automation to include IAM enforcement within the steps taken to eradicate, recover from, report and remediate identity threats. Integrate IAM incidents into response and threat-hunting processes using existing security controls in the security operations center (SOC).
- Fill gaps in ITDR by assessing the full range of attack vectors and telemetry covered. Plan to use a mosaic of tools that complement each other, and may overlap, to meet the requirements for a comprehensive ITDR initiative.

Introduction

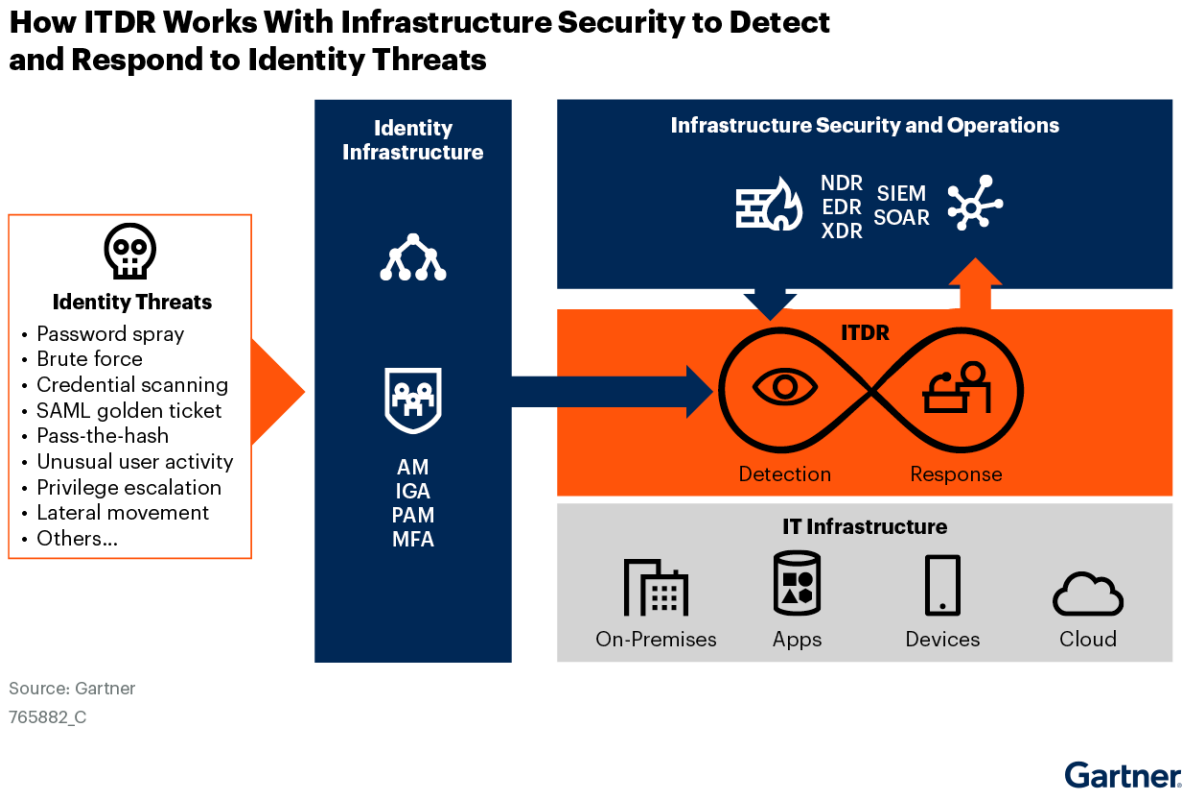
ITDR is a security discipline that encompasses threat intelligence, best practices, a knowledge base, tools and processes to protect identity systems. It works by implementing detection mechanisms, investigating suspect posture changes and activities, and responding to attacks to restore the integrity of the identity infrastructure.

ITDR is similar in focus to existing solutions, such as those used for network detection and response (NDR) and endpoint detection and response (EDR), which perform similar functions to protect this critical infrastructure.

Identity is a foundational aspect of cybersecurity (see Predicts 2022: Identity-First Security Demands Decentralized Enforcement and Centralized Control). A zero trust approach to security demands that only approved end users, devices and services should have access to systems. ITDR unifies tools and best practices to protect the integrity of identity systems, which is necessary even for mature IAM and infrastructure security deployments.

Identity is also fundamental to business. Organizations' reliance on their identity infrastructure to enable collaboration, remote work and customer access to services has transformed identity systems into prime targets for threat actors, with credential misuse being the most popular path to security breaches in 2021. [1] There is an active IAB marketplace for stolen credentials. [2] There are well-known attacks against multifactor authentication (MFA; see Note 1). [3] And sophisticated attackers are now targeting IAM infrastructure itself (see Figure 1). [4]

Figure 1: How ITDR Works With Infrastructure Security to Detect and Respond to Identity Threats



How should SRM leaders prepare to deal with such attacks? They should collaborate with IAM and other cybersecurity leaders to protect their organization's identity infrastructure, as set out in this research.

Analysis

Prepare for ITDR by Defining What Is (and Is Not) ITDR

An identity threat is a potential cyberattack related to identity infrastructure, such as access management (AM) tools, directory servers, certificate authorities, and other IAM systems and stores. An identity threat focuses on circumventing, bypassing or abusing identity systems in order to enable a cyberattack.

Prevention should be a foundational part of every cyberattack preparedness plan. SRM leaders must document key elements of their identity infrastructure and assess whether proper preventive controls are in place. They should use both traditional IAM controls and new ITDR-specific controls to ensure that the security posture (configuration hygiene) of these elements aligns with their enterprise's risk appetite and business goals.

Good preventive controls assist identity security posture management in order to avoid:

- **Misconfiguration,** by ensuring IAM controls are properly configured, that the IAM configuration is continuously monitored for suspicious changes, and that appropriate steps are taken to investigate and, if necessary, resolve issues.
- **Vulnerabilities,** by addressing commonly exploited vulnerabilities in the identity infrastructure via patching or compensating controls.
- **Exposure,** by reducing the attack surface by removing unnecessary or excessive privileges, for example.

Privileged access management (PAM) and identity governance and administration (IGA) offer foundational preventive controls to limit exposure of excessive privileges if a credential is compromised.

Cloud infrastructure entitlement management (CIEM) tools can also help prevent identity threats from materializing by reducing the attack surface created by excessive and unnecessary cloud identity privileges. This helps to restrict lateral movement.

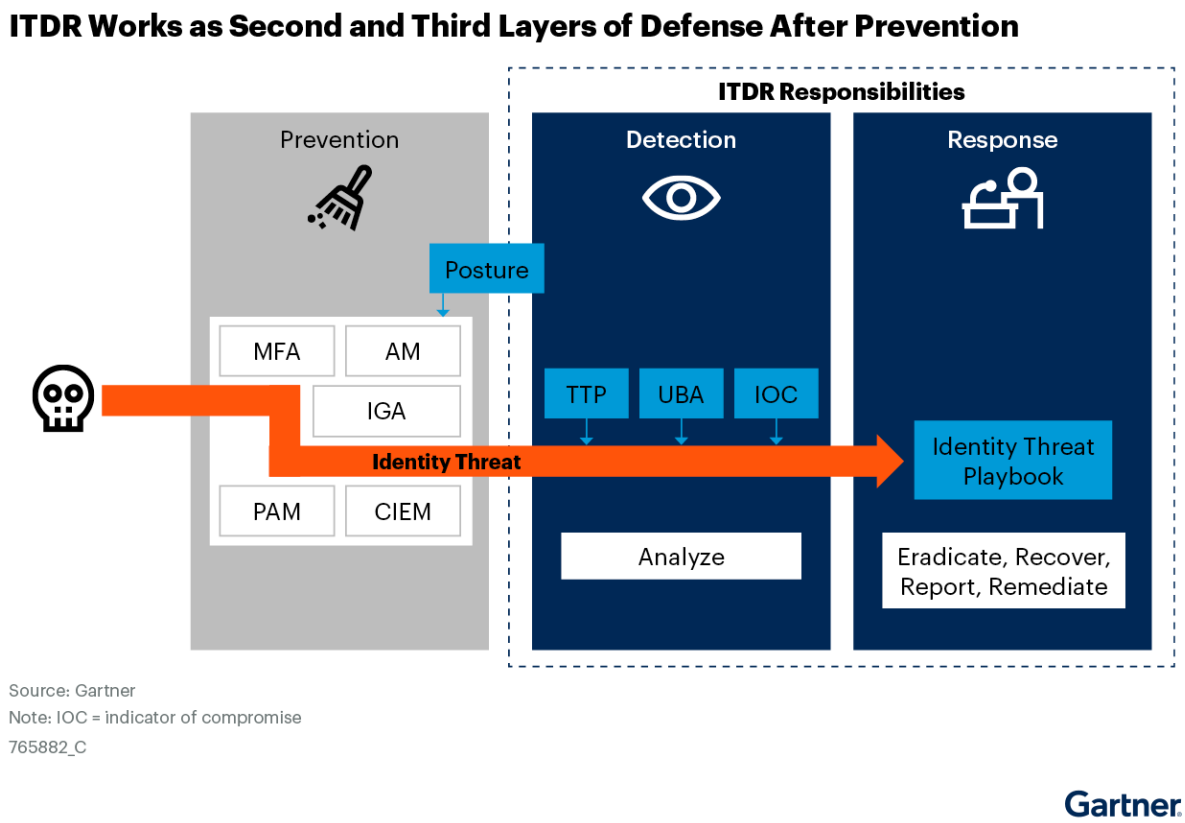
Proper configuration of MFA and enforcement of remote desktop protocol (RDP) session termination also helps prevent administrator accounts from being compromised.

Additionally, SRM leaders should continue to modernize their IAM infrastructure to prevent vulnerabilities by using current and emerging standards, such as OAuth 2.0 and Continuous Access Evaluation Protocol (CAEP). They should also avoid using unsafe legacy protocols, such as Post Office Protocol (POP) and Internet Message Access Protocol (IMAP).

The focus of ITDR, however, is to work as second and third layers of defense (see Figure 2), after the foundational preventive mechanisms identified above are in place. ITDR is necessary for two reasons:

- First, one must never assume basic preventive controls alone are sufficient to stop a cyberattack (see Maverick* Research: You Will Be Hacked, So Embrace the Breach).
- Secondly, attacks can damage identity infrastructure itself.

Figure 2: ITDR Works as Second and Third Layers of Defense After Prevention



Source: Gartner
Note: IOC = indicator of compromise
765882_C

Identity threats can bypass or neutralize IAM preventive controls. It is therefore important to understand the separation of prevention (hygiene and identity security posture activities undertaken before an attack) from detection and response (monitoring for attacks and stopping them once they are in progress). By understanding this separation, SRM leaders can make better plans to implement "defense in depth," with a focus on identity. They should also assess the risks inherent in having a single point of failure, if they adopt a single tool that claims to offer prevention, detection and response, rather than a multivendor approach (see Note 2).

What ITDR Is Not

ITDR is not:

- **A single group's responsibility:** ITDR is a responsibility shared by IAM and infrastructure security teams. SRM leaders must choose a sponsor who can initiate, identify stakeholders and spearhead this collaborative initiative.
- **Only about Active Directory (AD):** The ITDR discipline includes AD threat detection and response (TDR), but it is more than that. Whereas AD TDR focuses on AD threats only, ITDR also includes detection of, and response to, a broader set of identity threats to other kinds of IAM systems and tools, including those used for AM, IGA, authentication and PAM. However, whereas AD TDR has been adopted by roughly one-third of organizations, [5] adoption of ITDR is only just emerging.
- **Only a SOC tool:** Security information and event management (SIEM), security orchestration, automation and response (SOAR), and extended detection and response (XDR) are active parts of a cohesive ITDR strategy, and are fundamental to the concentration of signals and logs, and to the response layer. However, most vendors in those markets lack identity threat detection capabilities, which are mostly based on user behavior, instead of TTPs. SOC tools do not provide the necessary depth to counter identity attacks, but building a successful strategy for ITDR requires integration with those SOC tools.

- **Just a collection of IAM and fraud prevention controls:** ITDR should always be complemented by other prevention controls to avoid misconfiguration, exposure and vulnerability. But although prevention is important, and is addressed by different kinds of IAM tools (IGA, AM, PAM, authentication and CIEM), detecting and responding to threats requires runtime threat intelligence analysis. It also requires expansion of protection layers beyond the prevention features of IAM tools by:
  - Enabling more runtime analysis in the IAM tools that organizations already have.
  - Introducing detection and response capabilities independent of those IAM tools, in case they are compromised.

Enhance Detection and Analysis Controls

Attack techniques are diverse, with attackers probing all aspects of identity infrastructure and using multiple techniques. These range from highly technical exploits like zero day attacks to popular "info stealer" malware, [6] to social engineering.

The key for defenders is to be as agile in detecting new techniques as the attackers are in developing TTPs. SRM leaders need, for example, to be able to detect multiple SSO sessions from the same user on multiple nonmobile operating systems. This requires the ability to collect the right signals and to use detection logic to elevate and analyze suspicious events. TTP detection may be harder to implement, but it is more durable, proactive, and can be used to detect multiple threat actors and malicious tools, which are typical of multifaceted identity-based attacks.

For identity threat detection, the foundational step for most organizations is to monitor their identity infrastructure for unauthorized changes or changes outside normal channels.

Such changes may include alterations to Windows registry keys, or the creation of unusual accounts, or the registering of new authentication devices.

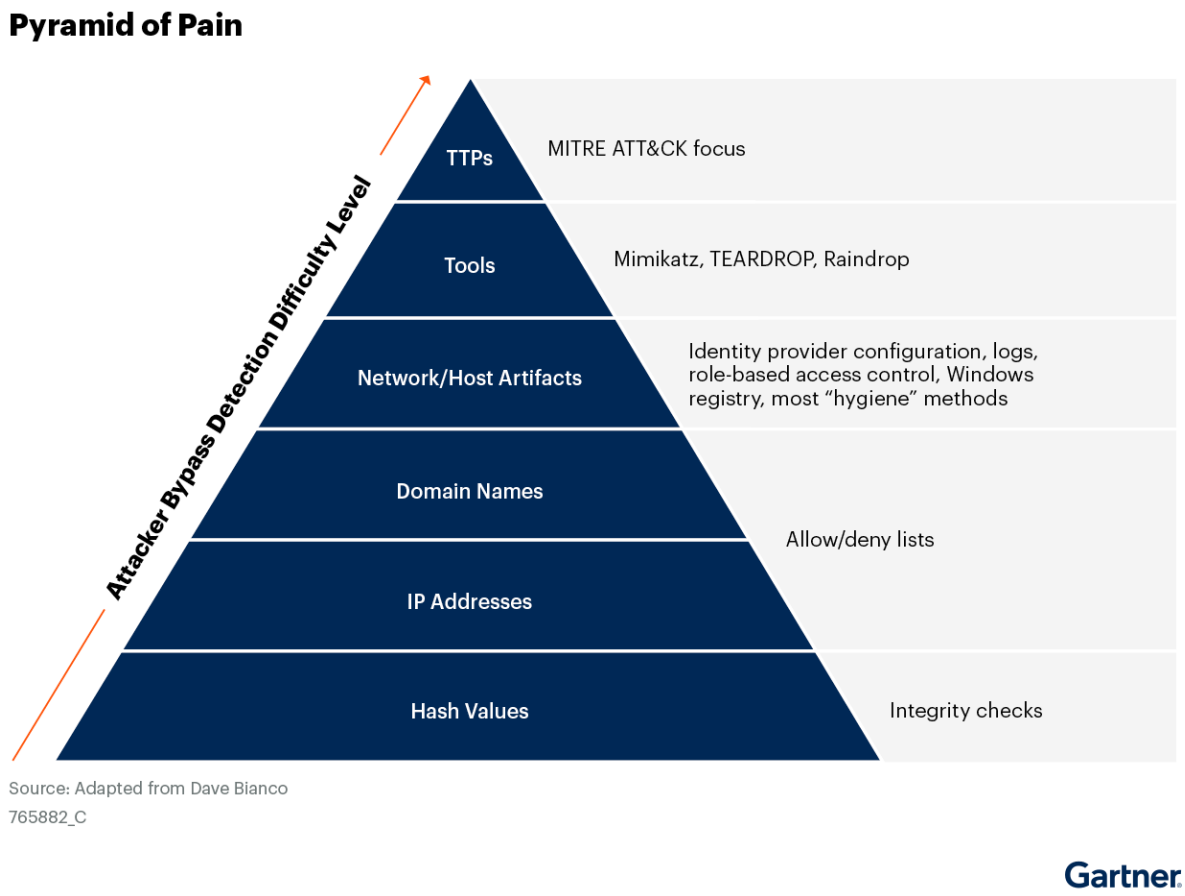
Security service edge (SSE) and cloud access security broker (CASB) technology could be used "in line" for users of an administration console, for example, to ensure their devices are fully managed and have endpoint protection enabled.

PAM and IGA, combined with MFA, can be used to ensure that only strongly authenticated users, using fully managed/secure devices, can make changes to IAM infrastructure.

In addition to detecting unauthorized changes, an effective way of improving detection controls for identity threats is to use the MITRE ATT&CK knowledge base of TTPs. Gartner's How to Use MITRE ATT&CK to Improve Threat Detection Capabilities describes how TTP-based threat detection focuses on adversarial behavior in the form of specific techniques used during attacks. Industry research has confirmed that it is an effective way of detecting malicious activity. [7]

A modified version of the Pyramid of Pain is shown in Figure 3. It shows the relationship between detection methods and the pain caused to the adversary.

Figure 3. Pyramid of Pain



Gartner

Beside the prioritization of TTPs, good detection controls in ITDR come with analysis derived from a combination of threat signals. SIEM tools and emerging XDR solutions (that include NDR and EDR capabilities) are one way to start building detection logic for TTPs. They have built-in detection logic for current TTPs. For a nonexhaustive list of TTPs specific to MFA attacks, see Note 1.

Additional controls to improve detection for ITDR include:

- **Security-conscious employees:** An approach to identity threat detection should focus on processes and procedures, and enhance employees' security awareness. Two examples highlight the need for this:
  - NOBELIUM (also known as Cozy Bear and APT29) — the actor behind the attack against SolarWinds, the SUNBURST backdoor, and TEARDROP malware and related components — was initially discovered by an alert administrator questioning enrollment of a new phone for MFA.
  - Lapsus$ attackers made extensive use of social engineering attacks, such as impersonation of IT help desk staff and MFA prompt bombing (see Note 3).
- **Monitoring of underground IABs:** [8] Digital risk protection services can help organizations identify leaked credentials (see Market Guide for Security Threat Intelligence Products and Services). Have I Been Pwned is an example of a website where huge numbers of stolen credentials have been aggregated.
- **User behavior analytics (UBA)**, as provided by:
  - Infrastructure security tools such as firewalls, SSE, EDR, NDR, SIEM and XDR tools.
  - Adaptive access controls in AM and authentication tools, and anomaly detection in CIEM tools, for example.
- **Deception techniques:** Attackers attempting to utilize any fake credentials created by deception tools can be detected with a low false-positive rate.
- **Account takeover (ATO) mitigation:** A range of capabilities, such as device identification, behavioral biometrics and location intelligence, can be used to detect anomalies at the point of login due to credential misuse by humans or automated actors.
- **Bot mitigation techniques:** These are typically provided by fraud detection tools to detect and mitigate automated attacks by bots that abuse business logic on web, mobile or API channels. Examples of such abuses include ATOs, password stuffing and password cracking, as well as other types of attack on identity systems, such as distributed denial of service.

Master the Response

Compared with other types of threat response approach, ITDR requires much more intensive interoperability with the IAM toolset during the response phase. The initial response after an investigation requires user identity, device and possibly network isolation to contain the threat. IAM controls to elevate trust (such as step-up authentication or session termination) are useful for ATO mitigation. Containment of compromised administrative credentials via risk-based adaptive access is the most common automated response action. ITDR responses may trigger manual or semiautomated processes (to disable identity synchronization jobs, for example), if the IAM infrastructure itself (or its data) is compromised.

The response to an identity threat must enable interoperability between IAM and security operations. This requires integration of procedures and security operation tools for facilitating investigation and automating response actions.

In addition to preparing for and detecting threats and attacks, SRM leaders should prepare a response plan and playbook for the most common identity threats, ideally based on a TTP use case (see Toolkit: Cybersecurity Incident Response Plan and Toolkit: Creating a Ransomware Playbook).

At minimum, this identity threat response playbook should include the following actions:

- **Contain and eradicate:**
  - Isolate the threat by disabling command and control (C2) traffic. [9]
  - Disable ID sync jobs between directories, on-premises targets and cloud user repository targets.
  - Freeze all automated provisioning.
  - Stop all account changes in IGA and PAM.
  - Use automated threat containment approaches, such as risk-based adaptive access (step-up authentication and session termination).
  - Quarantine users (by using Azure AD user risk and remediation, for example) who are performing suspicious activities.
  - Use SSE to provide a containment layer for SaaS apps, thus stopping access to apps in the event of an attack.

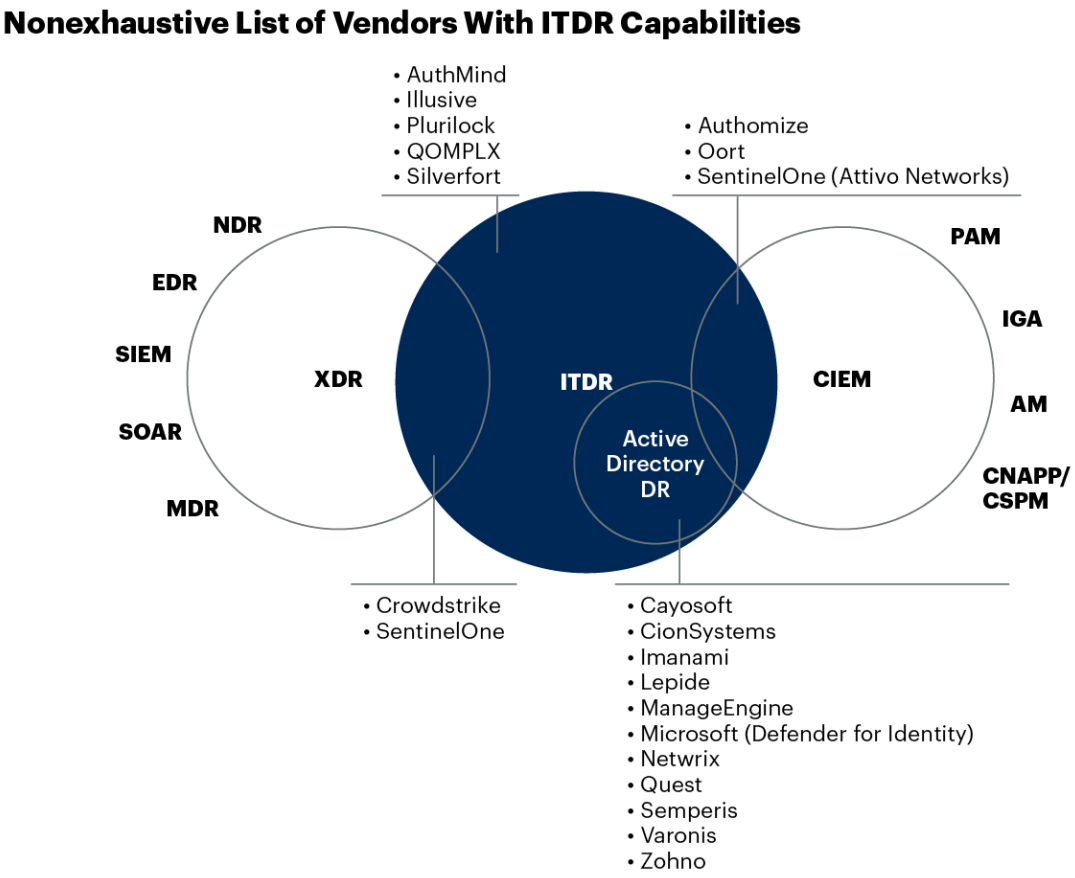
- **Recover:**
  - Restore from backups.
  - Collect evidence for investigation and preservation, including PAM, IGA and AM logs. Quick Answer: How Can We Reduce the Risks of SaaS-Based Identity and Access Management? describes other strategies for resilience that can be helpful during a SaaS IAM provider's recovery stage.
- **Report:**
  - Notify people early, including executives, legal staff and response teams. It is better to assume a posture of transparency and accountability by "overcommunicating," and then have to retract if the incident is less severe than originally thought, than to do the opposite.
  - Adhere to applicable regulations.
  - Send events to endpoint tools for incident response processing and for enhancement by adding details to them.
- **Remediate:**
  - Reset affected credentials.
  - Remove rogue and excessive accounts.
  - Patch systems.
  - Rotate security keys.
  - Update playbook and TTP knowledge base.
  - Update prevention and detection controls.

SRM leaders should also consider using XDR capabilities, such as playbook management integration, given their ability to address all necessary data sources and log data in one console. Additionally, SRM leaders in mature organizations should assess whether to orchestrate responses with a SOAR tool, as described in Market Guide for Extended Detection and Response.

Fill Gaps in ITDR by Evaluating Vendors' Emerging ITDR Capabilities

SRM leaders should continue to invest in best practices for preventive IAM infrastructure hygiene security. At the same time, they should evaluate the specialist ITDR tools available from vendors in several markets (see Figure 4). These can enhance their preparedness for, and responsiveness to, an attack, if their IAM infrastructure is compromised.

Figure 4. Nonexhaustive List of Vendors With ITDR Capabilities



Source: Gartner
Note: CNAPP = cloud-native application protection platform; CSPM = cloud security posture management
765882_C

Gartner

Gartner

Evidence

[1] 2022 Data Breach Investigations Report, Verizon.

[2] Compromised US Academic Credentials Identified Across Various Public and Dark Web Forums, FBI, 26 May 2022.

[3] D. Goodin, Lapsus$ and SolarWinds Hackers Both Use the Same Old Trick to Bypass MFA, Ars Technica, 29 March 2022.

[4] R. Nafisi, FoggyWeb: Targeted NOBELIUM Malware Leads to Persistent Backdoor, Microsoft Security Blog, 27 September 2021.

[5] Gartner's 2021 The Future of Active Directory survey found 33% adoption of threat detection and response for Active Directory. This survey was conducted online from 13 April through 18 April 2021 with 119 participants. Fifty-seven were members of Gartner's IT and Business Leaders Research Circle — a Gartner-managed panel — and 62 were from an external sample. Respondents were qualified based on their knowledge of current and planned usage, strategy or roadmap for IAM and Active Directory, other enterprise directories, or cloud-based identity services.

[6] M. Jaffe, The Identity Security Paradox: How Do You Protect Identities with IAM and PAM?, Illusive blog, 19 May 2022 (about the theft of credentials from system memory).

[7] Detecting Abuse of Authentication Mechanisms, U.S. National Security Agency, December 2020.

R. Daszczyszak and others, TTP-Based Hunting, MITRE, March 2019.

Enterprise Techniques, MITRE (MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.)

[8] C. Pernet, Initial Access Brokers: How Are IABs Related to the Rise in Ransomware Attacks?, TechRepublic, 15 December 2021.

[9] Customer Guidance on Recent Nation-State Cyber Attacks, Microsoft Security Response Center, 13 December 2020.

Note 1: Attacks Against Multifactor Authentication

MITRE ATT&CK M1032 lists attack techniques used against MFA, and recommended mitigations.

MFA is no "silver bullet." Many modern attacks have demonstrated that MFA can be defeated.

MFA is typically implemented by taking login with a legacy (e.g., AD) password as a first step and adding another authentication factor, such as a one-time password (OTP) token or a mobile push app — as a second step. Most common "MFA" tools are therefore only "+1FA" tools. Each factor may be defeated by different attacks.

Passwords are vulnerable to a variety of attacks: phishing, malware, credential stuffing, password spray attacks and so on. Adding an additional factor might compensate for these vulnerabilities in principle, but this does not mean that good password policy can be ignored.

Reducing password security will increase risk:

- Where conditional access rules can skip the additional factor.
- In any use cases where the password persists as a single-factor authentication method, such as with legacy protocols like IMAP, POP, SMTP and Messaging API (MAPI) that do not support MFA.

Some modern tools, especially passwordless "mobile MFA" tools, provide "true" MFA, where both factors are combined in a single step — for example, the user is prompted to use a PIN or local biometric method within a mobile push app. Passwordless methods avoid one class of attack, but might still be vulnerable to a single attack in another class.

Below is a nonexhaustive list of TTPs that are used alone or in combination to attack MFA. (For brevity, the wide variety of attacks against passwords is not enumerated.)

Preparatory:

- **Initial access broker (IAB):** An organization that buys and sells stolen username and password combinations or authenticated-session cookies on the dark web. Cookies can be used in pass-the-cookie (PTC) attacks.
- **Info stealer:** A type of malware (such as a Trojan horse) used to steal authenticated-session cookies from compromised systems. These cookies are then sold through IABs or used directly in PTC attacks.

Attacks against second factors (+1FA) include:

- **PTC attacks:** Authenticated-session cookies are created when a legitimate user has already used MFA to let them skip the second step (second factor) on subsequent logins within a set interval. A PTC attack enables an attacker to use a stolen cookie on their own machine to bypass that second step and successfully authenticate with just a stolen username and password.
- **SIM swaps:** A popular attack on out of band (OOB) authentication using SMS and voice modes, where the attacker impersonates a target through social engineering and convinces a mobile network operator's employee to swap the target's phone number to the attacker's new SIM card. All future OOB authentication prompts are then redirected to the attacker's device. As OOB SMS is often used to authorize password resets, this attack can ultimately defeat both authentication factors.

Attacks against second factors (+1FA) or passwordless MFA include:

- **Social engineering:** An attacker may, for instance, call the target directly, impersonating a trusted party (such as a bank employee or the target's employer), and ask the target to provide, for example, an OTP from their token or authenticator app over the phone.
- **Man-in-the-middle (MITM) attacks:** MITM attacks against OTP methods have been in use for many years. Recent examples are the "phishing as a service" toolkit dubbed EvilProxy (which also uses cookie injection), Evilginx and Modlishka.
- **Prompt bombing:** A prompt-bombing attack tries to wear down a user by deluging them with (typically) mobile push authentication prompts as the attacker repeatedly attempts to log in with a username and password that they have already obtained in some way. After multiple notifications, the targeted user may give in and tap the "accept" button, completing the log in for the attacker (see Note 3).
- **Denial of service (DoS) attacks:** Fail-open configurations that enable users to get access in the event of an authentication service outage allow attackers to bypass authentication steps if they can use a DoS attack to bring down the authentication service. Note: Fail-open configurations should not be configured for high-risk privileged users; PAM tools can provide contingent access if an authentication service is unavailable (a "break glass" scenario; see Critical Capabilities for Privileged Access Management).
- **Attacks exploiting software vulnerabilities:** Attackers may be able to exploit flaws in the authentication service to bypass authentication steps — for example, a WS-Trust MFA bypass, through spoofing of the HTTP header.

- **Attacks exploiting misconfiguration errors:** Attackers may be able to exploit improperly configured authentication tools. If, for example, a policy permits concurrent sessions for the same user, an attack may be able to open a new session that inherits the authenticated state of the target's existing session. In the worst case, a policy might not enforce MFA at all, when it should. Although not strictly a misconfiguration, continued use of legacy email protocols, such as IMAP, which are often "on" by default, also means that MFA cannot be supported.

Note 2: How to Address the Risk of a Single Point of Failure in Detection and Response Architecture

As described in Innovation Insight for Extended Detection and Response, an XDR strategy requires a high level of dependence on a single vendor. This may present the risk of a single point of failure, among other risks. ITDR may present the same risks when converged with traditional IAM technologies, such as AM and MFA.

The security market is ripe for consolidation. However, when dealing with ITDR — an emerging discipline — it is advisable to evaluate both ITDR capabilities provided by specialist tools and the converged capabilities of IAM and infrastructure security tools. A layered approach involving ITDR is the best way to enhance preparedness for cyberattacks, until ITDR technology matures.

Keep the focus on the identity infrastructure; otherwise, you may be spreading controls too thinly.

Note 3: How to Mitigate the Risk of MFA Prompt-Bombing Attacks

The most robust response to the threat of a prompt-bombing attack is to eliminate the risk by migrating to a "phishing resistant" authentication method such as FIDO2 (see the U.S. Office of Management and Budget's memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles). Gartner's Innovation Insight for Many Flavors of Authentication Token advises caution about new investments in legacy methods (including mobile push) and recommends migrating to FIDO2 within two or three years.

However, if you need to mitigate the risk, you can do so by:

- Choking login attempts (for example, by temporarily locking an account after two consecutive rejected attempts).

- Providing additional context with prompt messages, so that an attacker-initiated prompt is obviously bogus.
- Binding the authentication to the session (for example, by asking the user to match a code displayed on the login screen).
- Requiring that phone and endpoint device are in the same location (within the normal range of error bars of location services).

As passwordless mobile MFA methods involve a "higher friction" action (a PIN or biometric method), users might not be quite as susceptible to this kind of attack, but it might still succeed.

Lastly, ITDR can help detect consecutive prompts or abnormal MFA prompting activity.

None of these compensating controls are foolproof, but a combination can reduce the risk of MFA prompt bombing, so that it is within an organization's risk tolerance level.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Top Trends in Cybersecurity 2022

Market Guide for Security Threat Intelligence Products and Services

How to Use MITRE ATT&CK to Improve Threat Detection Capabilities

Quick Answer: How Can We Reduce the Risks of SaaS-Based Identity and Access Management?

Maverick* Research: You Will Be Hacked, So Embrace the Breach