EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Sponsored by:

Attivo NETWORKS

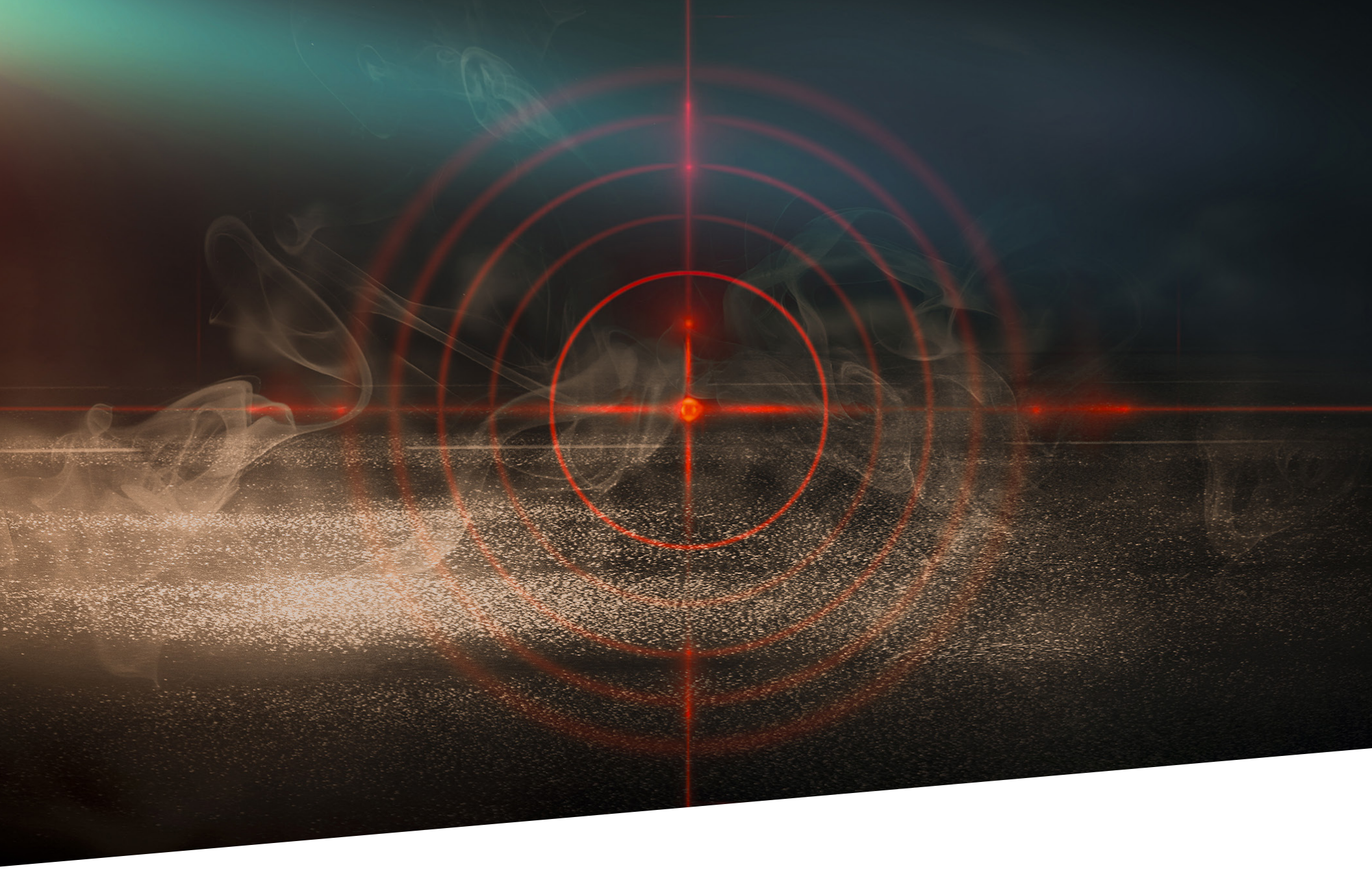
tenable

The Rise of Active Directory Exploits: Is it Time to Sound the Alarm?

September 2021 EMA Research Report

By Paula Musich
Research Director, Security and Risk Management

Table of Contents



Introduction

For years, Active Directory has been a prime target for attackers looking to get a leg up into high-value enterprise resources, but it has not been front and center in most enterprise security teams' list of priorities. While gaining access to Active Directory elements, such as access control lists and privileged accounts, is not the end attackers are seeking, it most often delivers the means to get to those valuable assets, whether those include customer information, intellectual property, or operating data that can be held for ransom.

The complexity of the directory-based identity services platform used by 90% of enterprises around the world, coupled with the need for at least two different teams to collaborate to properly secure it and the constantly changing nature of its configuration, make it a difficult attack surface to protect. Active Directory's complexity makes it impossible for administrators and security teams to understand what end users actually have access to and what they actually control. Instead, it shows those teams a subset of everything under the control of individual users. Active Directory configurations are a moving target, with new users and groups being added or changed, new applications coming online, new cloud workloads spinning up and down, and merger and acquisition activity contributing to the constant state of flux.

Smart attackers who understand the intricacies of Active Directory can turn thousands of individual vulnerabilities or exposures into an exponentially larger number of attack paths they can traverse to get to their goal. In the SolarWinds Sunspot breach, attackers executed what's known as a Golden SAML (Security Assertion Markup Language) attack in which they created fake user credentials, mimicked real users, and bypassed two-factor authentication. They then moved laterally within victims' networks under the cover of those stolen, elevated permission levels to access and exfiltrate sensitive data. Those attackers were also able to move between victim networks and their cloud environments thanks to the Active Directory Federated Services protocols.

Given the severity of this threat, Enterprise Management Associates sought to understand how organizations are adapting to the growing risk, how their priorities around securing Active Directory are changing, and what obstacles they face in protecting the identity management, user authentication, and access control platform. EMA polled 250 IT professionals and executives from organizations with at least 1,000 employees representing at least 10 different vertical industries.

Key Findings

Priorities & Spending	Challenges & Threats	Assessments	Remediation
56% increased their priority for securing AD somewhat or significantly in 2021	**50%** experienced attacks on AD in the last 1 to 2 years	**38%** still rely mostly on audits to improve AD security	**26%** take between 1 to 4 hours to remediate AD exposures once detected
51% plan to slightly increase their spending on AD security	**42%** of those attacks were successful	**34%** perform assessments weekly	**71%** accept AD exposures because of operational concerns
35% plan to significantly increase their spending on AD security	**25%** say the biggest AD security challenge is detecting live attacks	**44%** discover 11 to 50 exposures in each assessment	**35%** take 1 to 4 hours to remediate actual AD attacks

Priorities and Spending for Active Directory Security

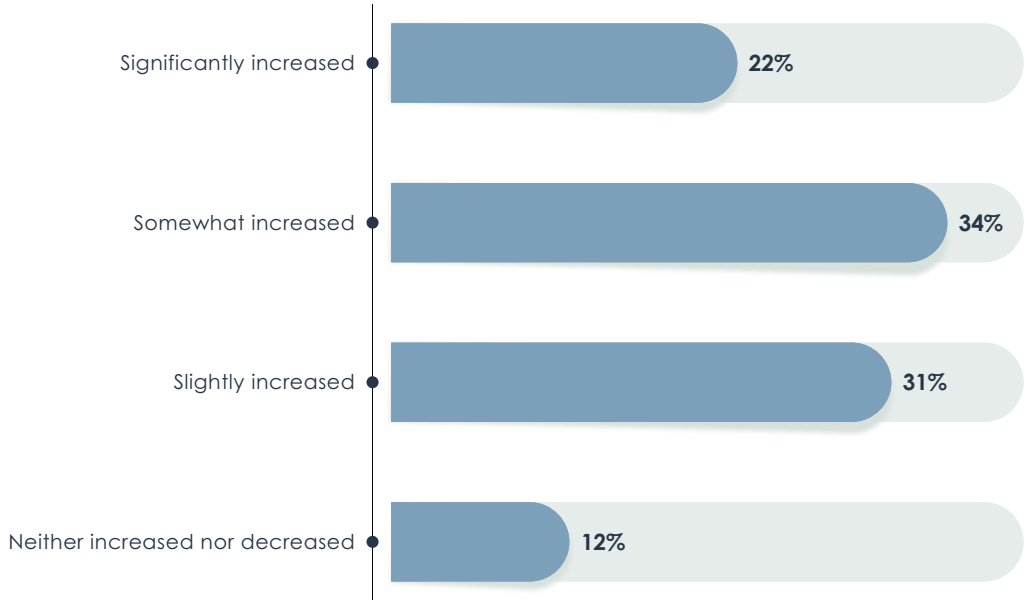
Analysis

Given the growing number of headlines around Active Directory exploits—think SolarWinds, LockBit ransomware—it should be no surprise that organizations in 2021 are placing the security of AD higher on their list of priorities. These organizations are coming to grips with the knowledge that Active Directory has become a much larger target for bad actors as they seek to carry out their attacks, whether those are ransomware attacks or the theft of sensitive data. Just over one-third of respondents indicated that the priority for securing AD has somewhat increased, while just under one-quarter of respondents said it significantly increased.

Commentary

The ubiquitous use of Active Directory across enterprises of all sizes, coupled with the complexity of securing the rather convoluted system used for access control and user authentication, makes it a prime target for a range of different attackers. New automation in LockBit 2.0 makes it possible to automate the distribution of ransomware throughout a Windows domain without having to write scripts. The fifth step in the cyber kill chain—domain privilege escalation—is all too common in insider and advanced attacks where perpetrators find and leverage unauthorized access in AD access control list objects. As more IT organizations come to realize the stakes involved in adequately securing Active Directory, the more often they will seek to shore up its defenses.

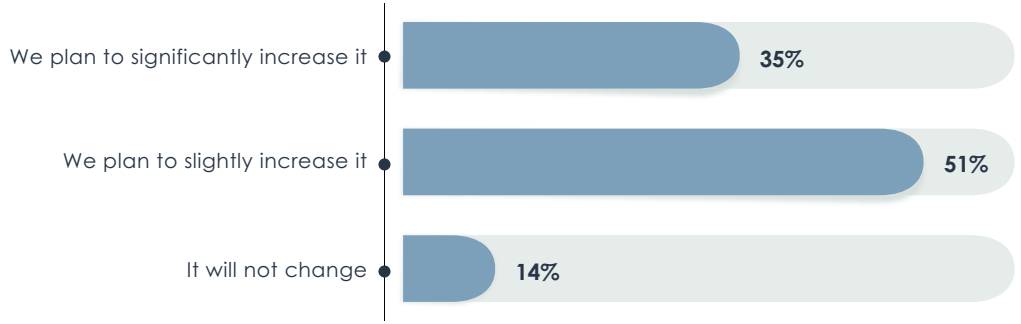
How has your organization's priority for securing Active Directory changed in 2021, if at all?



Analysis

Given the increased priority in securing Active Directory, it's not surprising that a large majority of respondents indicated their organizations plan to increase their spending on its security. Eighty-five percent said their organizations planned to either slightly or significantly increase their spending on Active Directory security. Only 14% said their spending level on its security would not change.

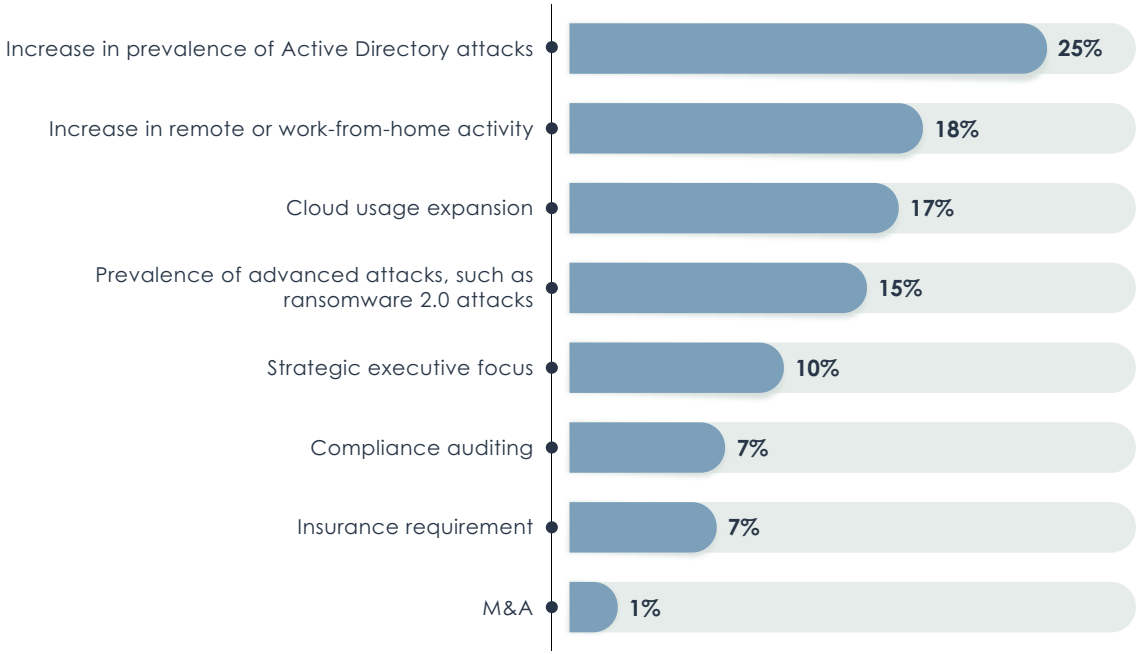
Which of the following statements best describes your organization's future spending plans for Active Directory security?



Commentary

The increase in the prevalence of Active Directory attacks drove the largest percentage of organizations to plan an increase in spending on its security, but there are other issues spurring such decisions. The global pandemic caused two major, interrelated changes in IT activity: it created the need to support largescale remote or work-from-home activities, and it accelerated cloud migration plans for a large number of enterprises. Both of those changes caused organizations to increase AD security spending by 18% and 17%, respectively. It is worth noting that the percentage of those who plan to increase AD security spending because of ransomware 2.0 concerns is likely to increase given new developments in the LockBit 2.0 ransomware as a service exploit, which can now automatically distribute itself across a domain when executed on a domain controller.

What is the primary reason that your organization plans to increase its Active Directory security spending?



Active Directory Security Challenges and Threats

Analysis

The top challenge in securing AD, according to one-quarter of all respondents, is the difficulty in detecting live attacks on AD. That was followed by how hard it is to coordinate AD security across multiple groups within IT. Twenty-one percent of respondents ranked that as the top challenge. Third was a lack of historical data to understand the consequences of changes made to AD, at 15% of respondents. Still, there is not universal agreement in ranking the severity of different AD security challenges. Not far behind the lack of historical data is the difficulty that security teams have in trying to keep up with a constantly changing Active Directory environment and a lack of adequate visibility in trying to identify exposures.

Commentary

Most organizations only discover they've been hit by ransomware after attackers have already successfully executed their attacks. Unless ransom is their aim, threat actors typically fly under the radar of IT security teams in looking to exploit exposures and misconfigurations in Active Directory. AD provides those actors with the lay of the land, helping them to learn what resources are attached to the network, learn where valuable targets reside, and escalate privileges to access those targets. They employ a variety of tactics to hide their tracks as they go. Contributing to the difficulty in hardening Active Directory against attackers is the organizational challenge in bringing together different groups, each with different goals, to resolve exposures and remediate threats.

The Most Difficult Challenges in Securing Active Directory

Challenge	Percentage ranking it most difficult
Hard to detect live attacks on AD	25%
Too hard to coordinate security across multiple groups	21%
Can't keep up with constant changes in AD	15%

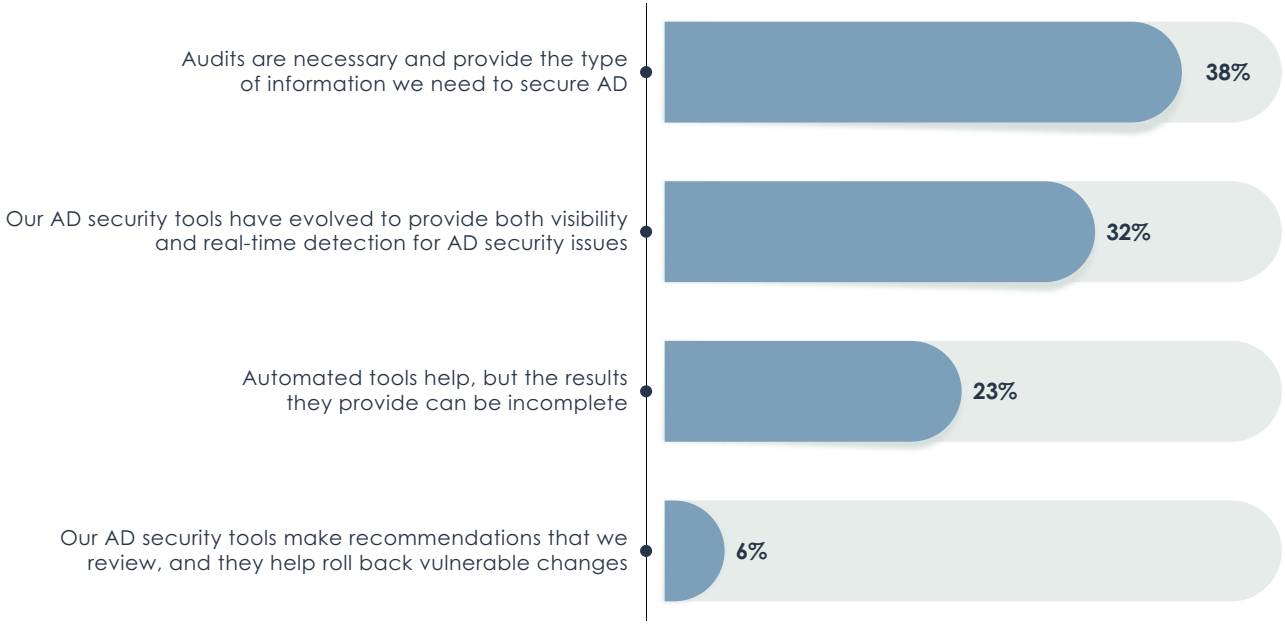
Analysis

No IT professional involved in securing Active Directory would argue that it's a simple task. Audits have historically been the go-to method of looking for exposures that could lead to a breach of the directory system. Given that tradition, it's no surprise that the most frequently cited approach to managing the complexity involved in securing AD is to conduct audits of it. Thirty-eight percent of respondents indicated that audits are necessary and provide the type of information needed to secure AD. However, as attacks against AD ramp up, more organizations are evolving their AD security tools to provide both better visibility and real-time detection of AD security issues. Thirty-two percent of respondents indicated as much.

Commentary

Traditional approaches to securing Active Directory have centered on conducting periodic audits of the identity system or performing log analysis correlated with SIEM data. The former only provides a snapshot in time, which quickly goes out of date with frequent changes to Active Directory configurations being constant in most enterprises—especially larger ones. The latter is time-consuming and costly. Both can lead to undetected malicious activity directed at AD. As the battle with attackers escalates, more organizations are turning to tools that provide detection of questionable activity in real time.

Which of the following best describes your organization's approach to dealing with the complexity of securing Active Directory?



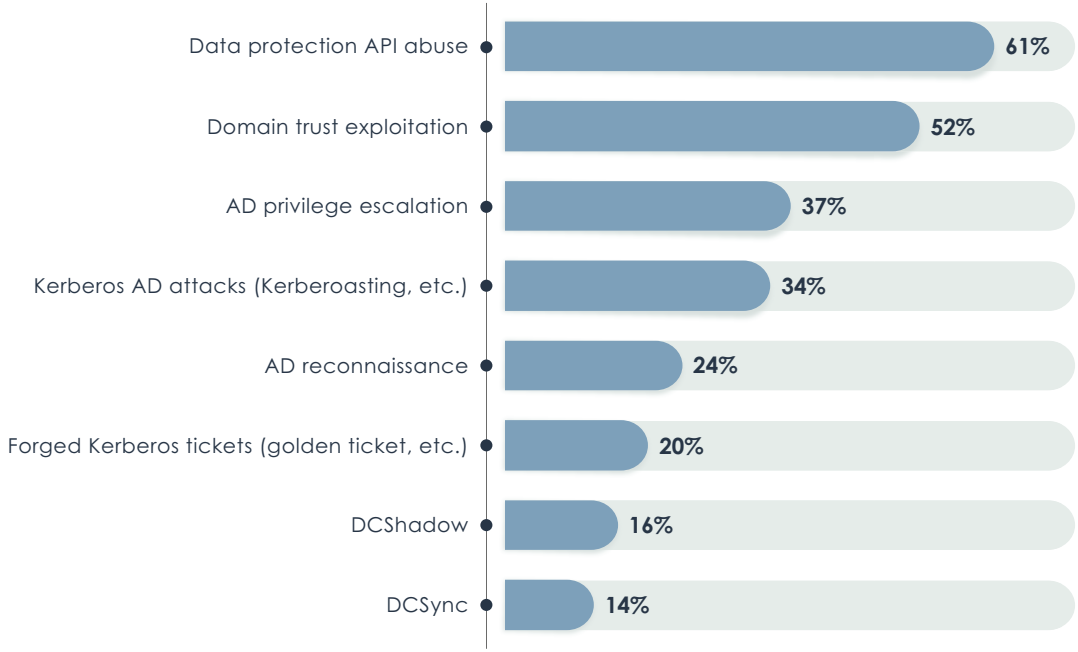
Analysis

Given that attackers have had years to hone their Active Directory exploitation skills, and given the huge attack surface it represents, a range of different tactics or attack types are now being directed at Active Directory implementations. Those range from the Golden SAML attack that was used as a part of the SolarWinds Sunspot breach to Active Directory privilege escalation. The three types of Active Directory attacks that enterprises fear most include data protection API abuse, which 61% of respondents selected out of a possible eight types of attacks. That was followed by domain trust exploitation reported by 52% of respondents and AD privilege escalation, chosen by 37% of respondents.

Commentary

More attack types are being discovered by security researchers and attackers on a regular basis, but not all attacks are viewed as equally threatening. Some more easily and thoroughly give away the keys to the cyber kingdom, and thus require greater vigilance.

Of the following types of Active Directory attacks, please indicate the three that are the greatest concern for your organization.



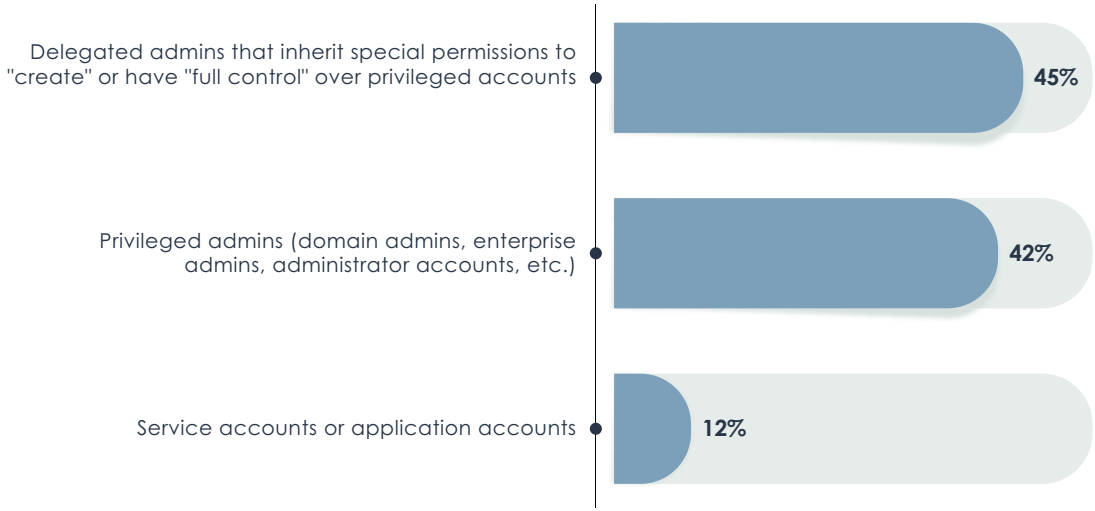
Analysis

There are two primary Active Directory threat vectors that organizations view as the most risky—with good reason. The first, with 45% of respondents, is delegated administrators that inherit special permissions to have or create full control over privileged accounts. The second, with 42% of respondents, is privileged administrators in general, whether those are domain administrators, enterprise administrators, or administrator accounts. Both have far greater access to resources across the enterprise and are easily misconfigured if not thoroughly thought out.

Commentary

Best practices for Active Directory administration dictate the creation of custom groups that are delegated specific access. However, if it's not done right, there is danger that the delegation can allow greater resource access than intended. Domain administrators have complete administrative access privileges to all endpoints, whether end-user devices or servers, as well as domain controllers, group policy, and all of Active Directory, essentially giving those administrators the keys to the enterprise's kingdom.

Which of the following Active Directory threat vectors does your organization view as riskiest?



Analysis

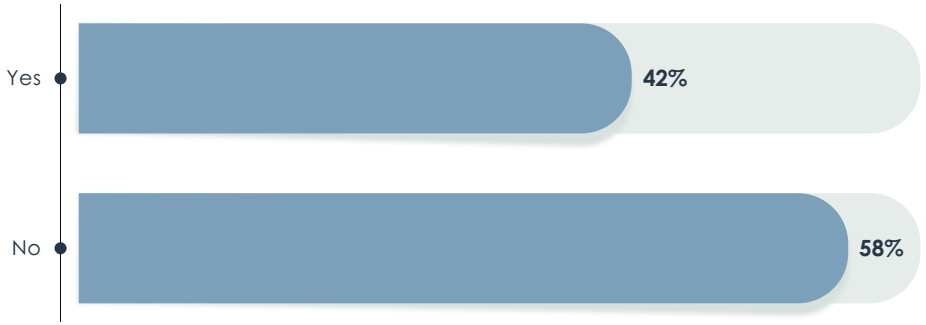
Among all respondents in the EMA survey, half reported that their organization's Active Directory implementation had been attacked by bad actors over the last 12 to 24 months, and half said they had not experienced an attack. Of those that were attacked, 42% said the attacks successfully breached their Active Directory implementation.

Commentary

Because of the combination of a high rate of attacks against Active Directory and the lack of visibility into live attacks, it's quite possible that a significant portion of those who said their AD implementation had not been attacked could have missed stealthy attackers who successfully covered their tracks. Seasoned Mandiant threat hunters estimate that 90% of the incident response engagements Mandiant conducts with clients involve Active Directory in some manner. For those who discovered such attacks, the high success rate of attacks against Active Directory deployments is alarming and should focus a spotlight on shoring up its defenses.

In the last 12 to 24 months, has your organization experienced an attack by malicious actors against your Active Directory implementation?

Did those attackers successfully breach your organization's Active Directory implementation?



Assessing the Security Posture of Active Directory

Analysis

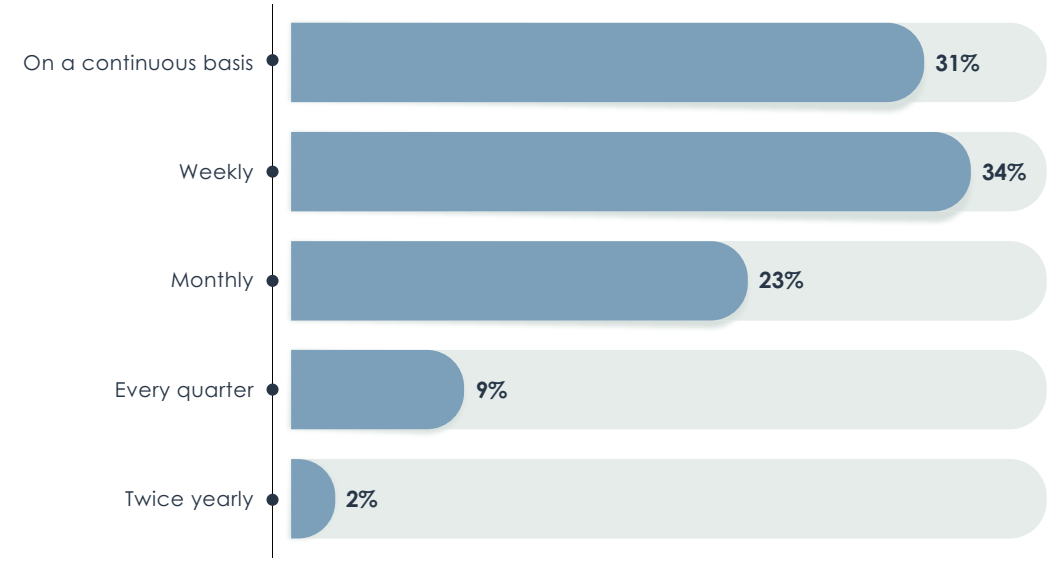
For companies that rely heavily on audits or assessments to shore up their Active Directory security posture, such assessments are most often conducted on weekly basis, with 34% indicating that frequency. Only a slightly smaller percentage take a more aggressive approach to Active Directory security assessments, with 31% indicating that such assessments are conducted on a continuous basis. On the other end of the time spectrum, less than 1% of respondents indicated their organizations conducted such assessments annually, and less than 1% said they were conducted on an ad hoc basis.

For each assessment, the most common number of issues or exposures uncovered range between 11 and 50, with 44% indicating that range. Another 32% of respondents reported discovering between 1 and 10 exposures per assessment.

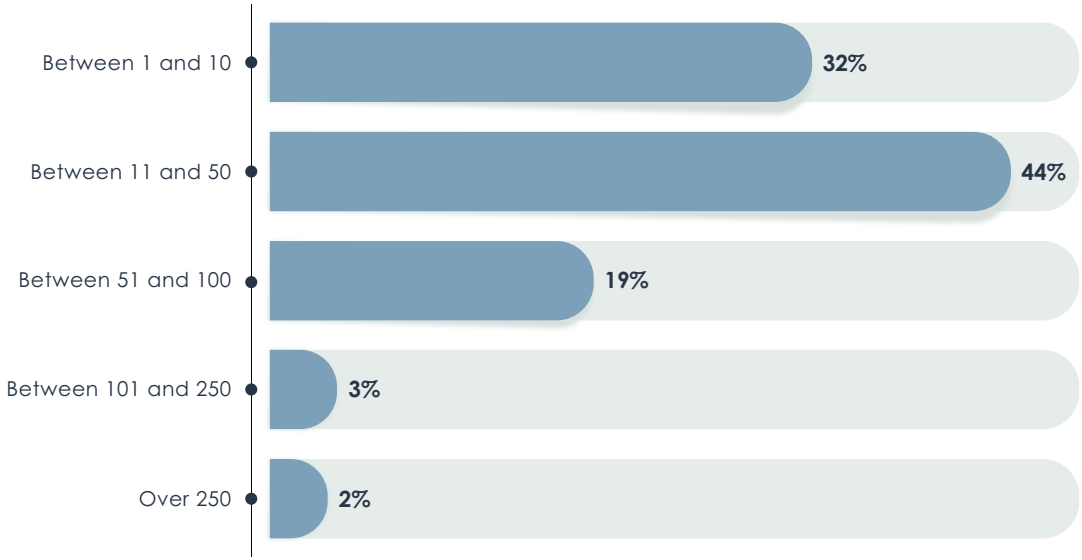
Commentary

Given the large number of attacks that involve Active Directory, the frequency with which Active Directory configurations are changed, and a heavy reliance on assessments, conducting audits on a continual or near-continual basis is crucial in maintaining good security hygiene for Active Directory. At the same time, traditional monitoring tools for Active Directory have not provided adequate insights into how configuration changes create exposures that can be exploited by bad actors.

Please indicate the frequency of your organization's Active Directory assessments.



On average, how many issues or exposures are discovered per assessment?



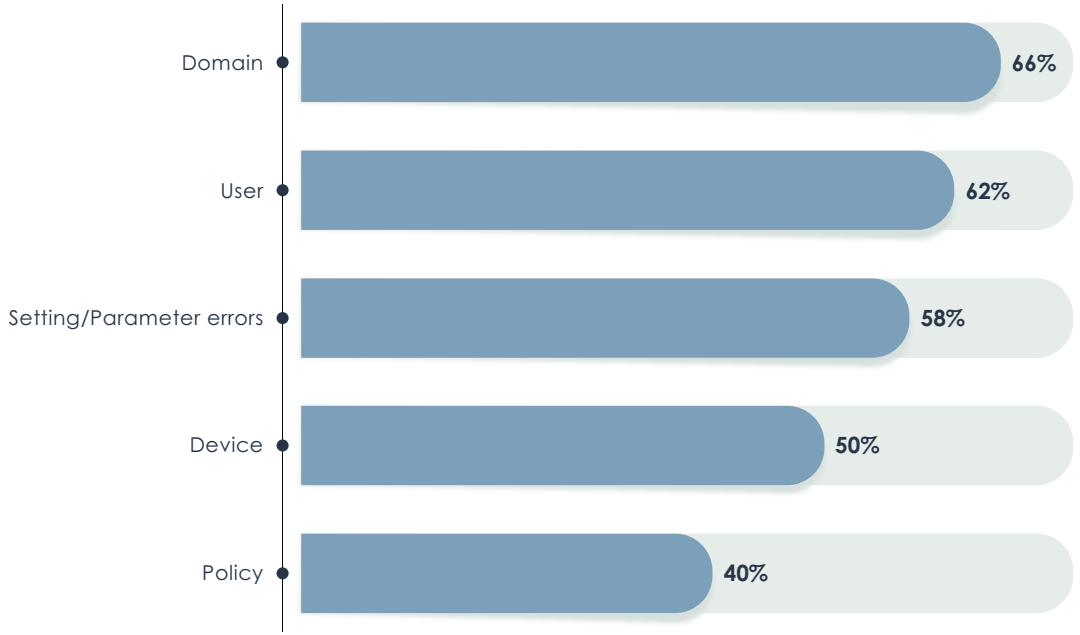
Analysis

The most common classes of exposures and misconfigurations uncovered in these assessments center around domains and users, with over 65% and 61% of respondents indicating those classes. Parameter errors and device exposures are also very common.

Commentary

Active Directory exposures can exist at multiple levels, including the domain, user, and device levels. At the same time, settings can be changed in a way that creates exposures that attackers can exploit, and policies (if not carefully crafted) can inadvertently allow attackers in. All of this speaks to the complexity of the world's most widely used registry and authentication system.

Which classes of exposures and misconfigurations has your organization uncovered in Active Directory assessments?



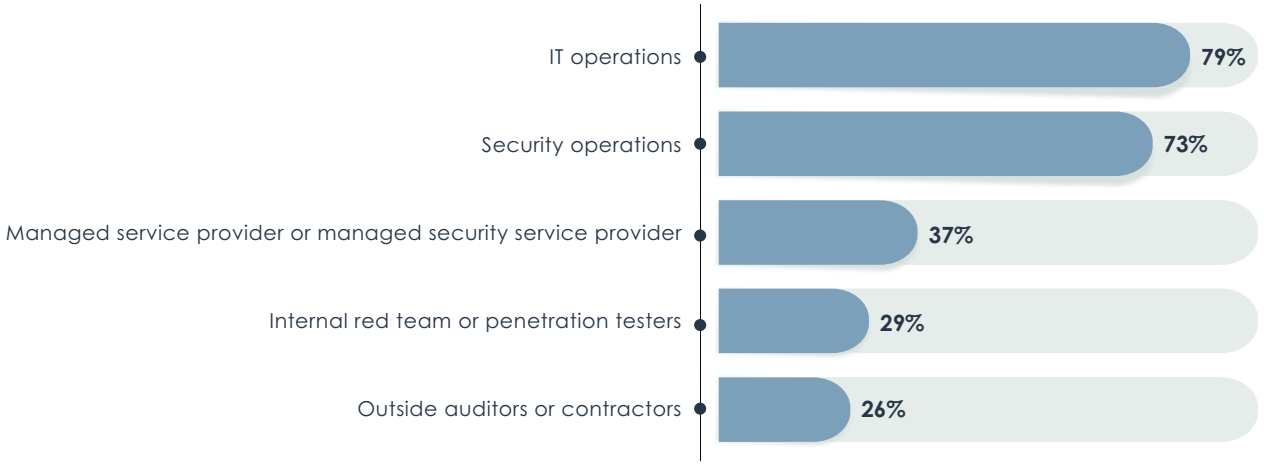
Analysis

Given the heavy reliance on assessments to maintain good Active Directory security posture, it's not surprising that organizations will rely on more than one group to conduct those assessments. Although IT operations and security operations teams are the primary groups tasked with conducting assessments, they are also periodically supplemented with assessments conducted through internal red team or pen testing activities or conducted with the help of outside auditors that bring specific expertise to the exercise. For smaller organizations that don't have the needed expertise, external managed security services providers can sometimes fill in that gap.

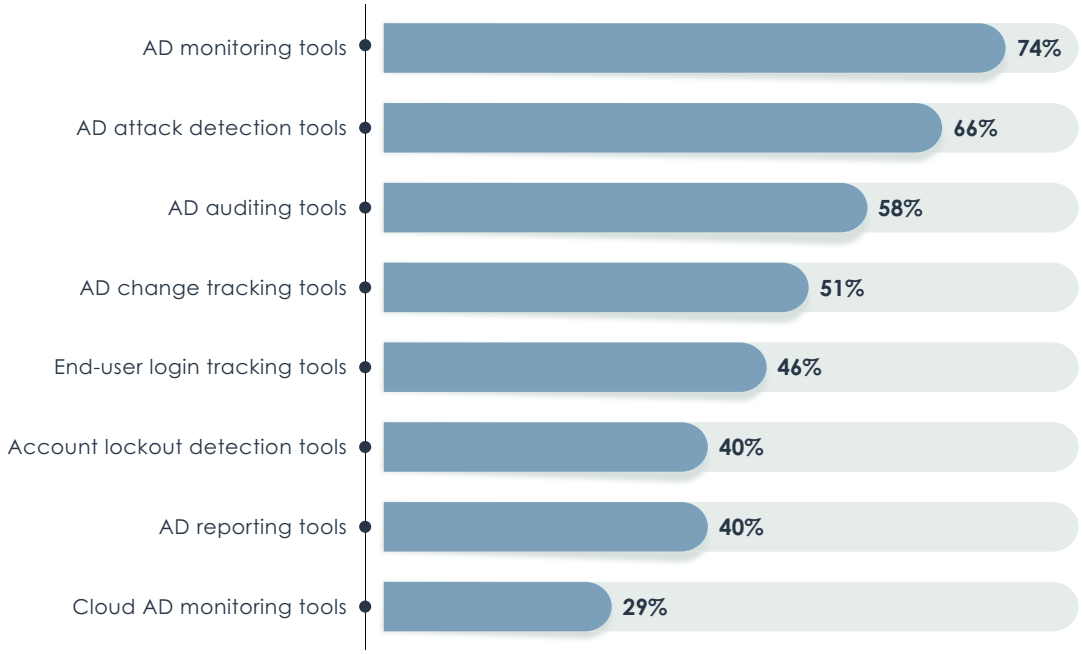
Commentary

The reliance on more than a single group to conduct Active Directory security audits speaks to the importance of maintaining a good security posture in the complex structure of Active Directory. At the same time, the expertise required to maintain that posture resides in both the security team and the Active Directory domain administrators. The obvious requirement to use more than one type of tool to conduct these assessments shows that there is no one-size-fits-all type of tool for doing them.

Which group(s) perform(s) Active Directory assessments for your organization?



In conducting Active Directory assessments, which tools does your organization use?



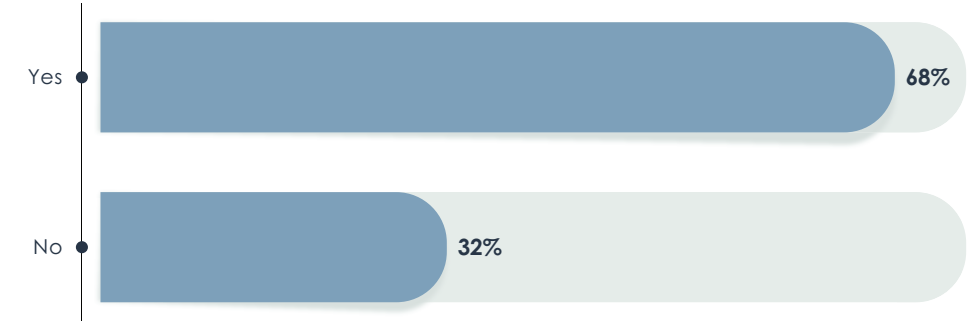
Analysis

For the 20% of respondent organizations that conduct internal red team exercises or penetration testing against Active Directory, attempting to exploit Active Directory exposures as a part of those exercises is relatively common. For those that do so, the success rate is startlingly high.

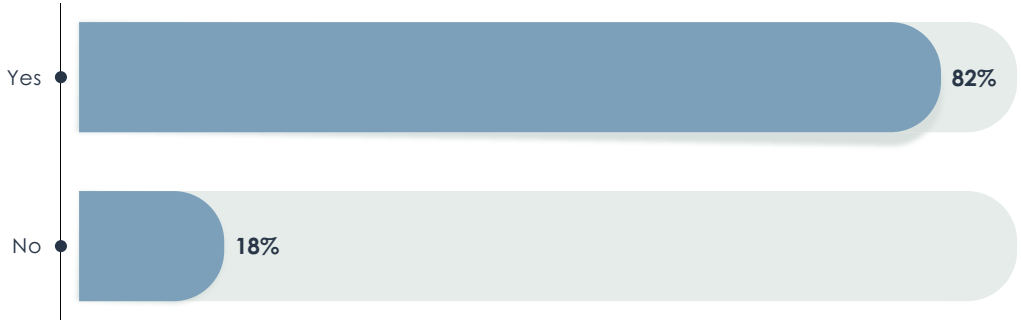
Commentary

Few organizations have the wherewithal to conduct such tests internally, given the deep level of expertise required to not only find vulnerabilities, but to understand the complex nature of Active Directory and the types of errors that can lead to exposures. Automated penetration testing tools or breach and attack simulation tools only take security teams part of the way there.

In the last 12 to 18 months, have your internal red teams or penetration testers attempted to exploit any exposures in your organization's Active Directory implementation?



In those penetration testing exercises, were they successful in exploiting Active Directory exposures?



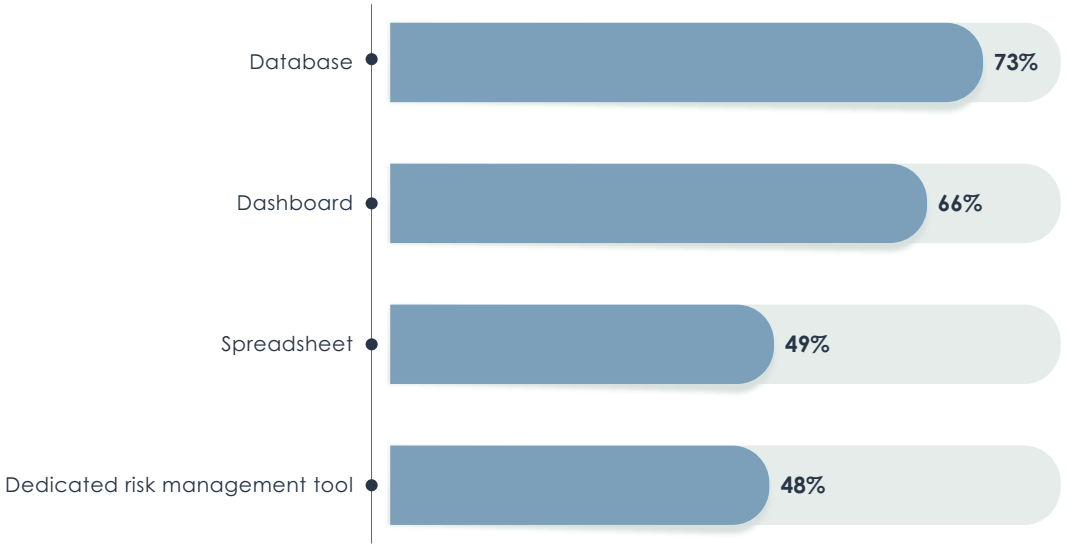
Analysis

In looking at these periodic assessments over time and tracking the progress of overall Active Directory security posture improvement, organizations have at their disposal a handful of tools to conduct that analysis. In most cases, organizations use more than one tool to analyze and report on that progress. Most often, organizations turn to databases and dashboards to report on and visualize progress toward improved AD security posture.

Commentary

Historically, there have been few tools dedicated to providing information that security teams can take to Active Directory domain administrators to demonstrate in concrete terms how to remediate exposures that have been uncovered. Even fewer tools exist to demonstrate for both IT operations and business executives what kind of progress is being made toward improving Active Directory's security posture. This lack of centralized tracking and reporting makes the job more complex for overtaxed security teams.

How does your organization analyze and trend Active Directory assessments?



Remediating Exposures and Attacks

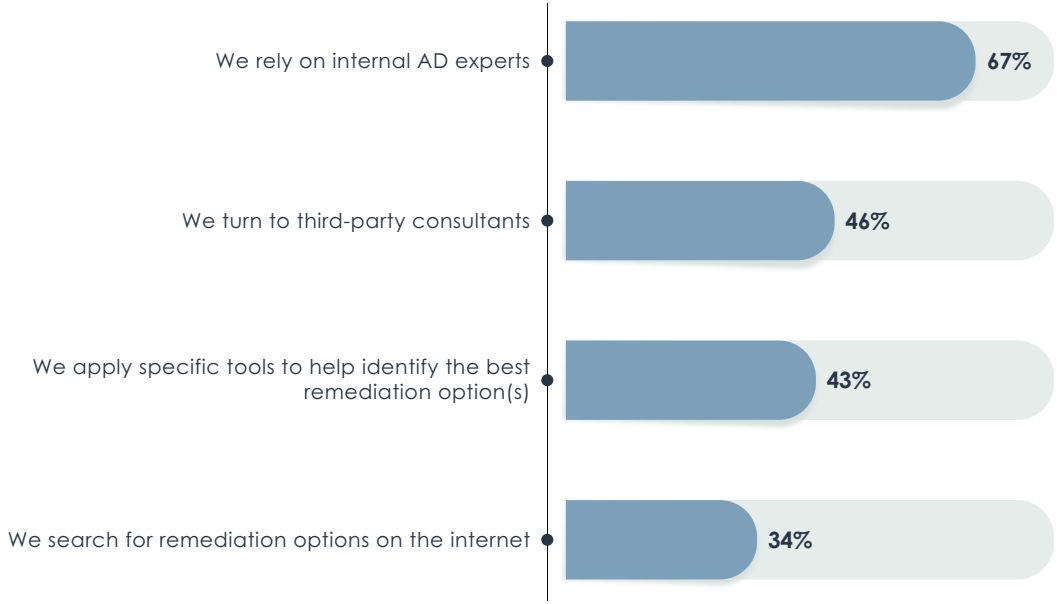
Analysis

Once exposures or misconfigurations are identified, quick remediation is crucial to shut down opportunities for attackers to gain a foothold. Given Active Directory's complexity, remediation requires a certain level of expertise. For the largest percentage of respondents, internal Active Directory experts provide the knowledge required to remediate such exposures without disrupting legitimate users' access to the applications and functions they need to do their jobs. Sixty-seven percent of organizations rely on those internal experts. For organizations that don't have the in-house expertise, outside consultants bring that expertise to bear on the exercise. Forty-six percent of organizations rely on consultants.

Commentary

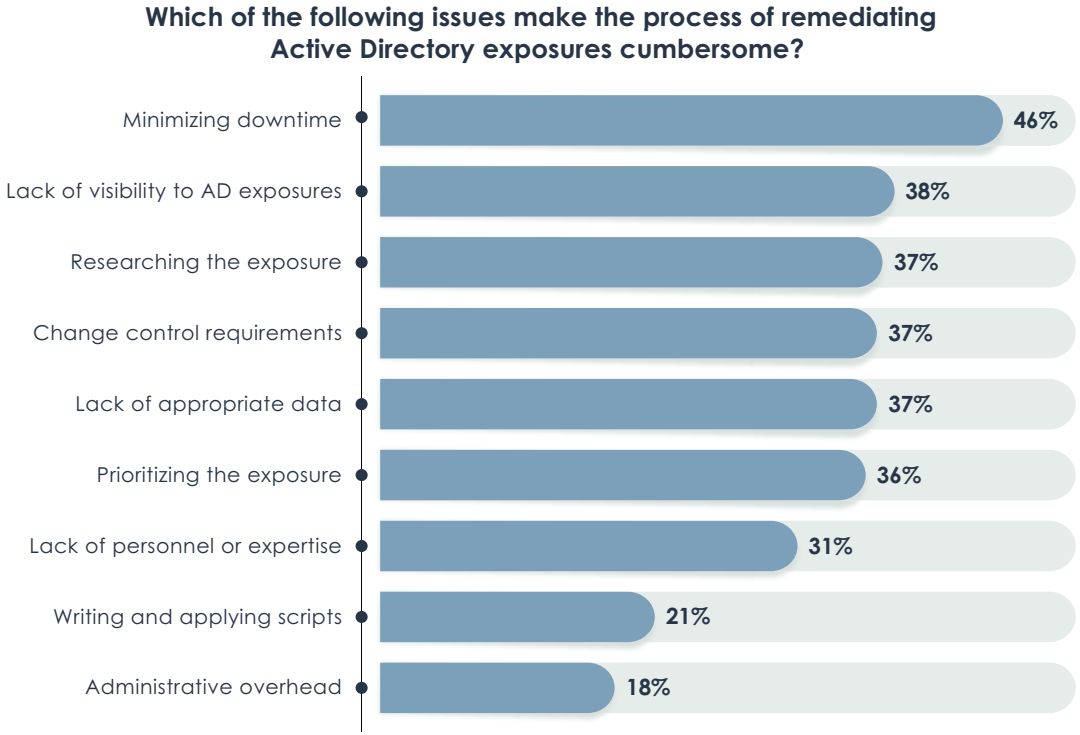
Relying on expertise, whether internal or outside consultants, is just one part of the remediation equation. Tools designed to identify the best remediation option can also be applied to the task, according to 43% of respondents. Whether that involves correcting user attributes or group misconfigurations, securing AD trusts, or a whole host of other configuration errors, the industry, including Microsoft itself, is stepping up to simplify that task.

Once an Active Directory exposure or misconfiguration has been identified, how does your organization determine the best remediation option?



Analysis

What drives the requirement for specific expertise and tools to help those experts remediate exposures and misconfigurations are different factors that make the process rather cumbersome. For the largest percentage of respondents, the single biggest factor is the effort required to minimize downtime while remediation takes place. Over 45% of respondents indicated that culprit. Other top problems that make remediation unwieldy include a lack of visibility into what those exposures are (38%), and owing to Active Directory's complexity, the requirement to research the exposure (37%). Still, those aren't the only issues that contribute to the burden for a healthy percentage of respondents. Thirty-six percent of respondents also said that figuring out how to prioritize the exposure for remediation, gathering the information necessary to remediate it, and change control requirements also contribute to the ponderous process.



Commentary

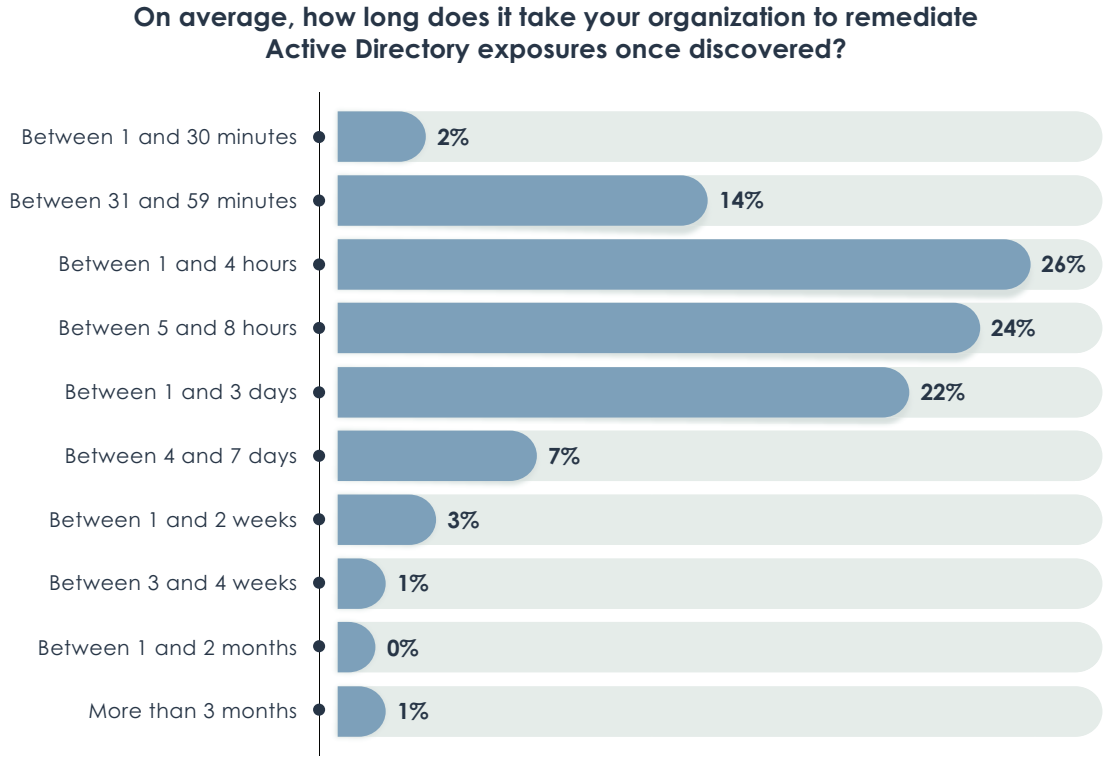
Active Directory is very powerful and very complex. The tools that come with managing its configuration don't make it easy to understand the potential impact of seemingly small changes. That makes it easy to misconfigure access, and these misconfigurations can build up over time to create exposures that attackers can chain together to gain access to valuable data.

Analysis

Given those issues, it's no surprise that remediating exposures once detected is not a slam dunk. On average, it can take hours, or in some cases even days, to remediate an exposure. For the largest percentage of organizations in the survey, that time span can range from one hour to as long as three days. Still, 67% were able to remediate these exposures in eight hours or less, which is very fast.

Commentary

Remediating Active Directory exposures requires a delicate balancing act, where speed is offset by the need to minimize downtime in the remediation process. It also requires good coordination between security teams and AD administrators or experts who must follow strict change control requirements. Ultimately, the biggest and most time-consuming activity is in finding the exposures, and manual assessments are only a snapshot in time.



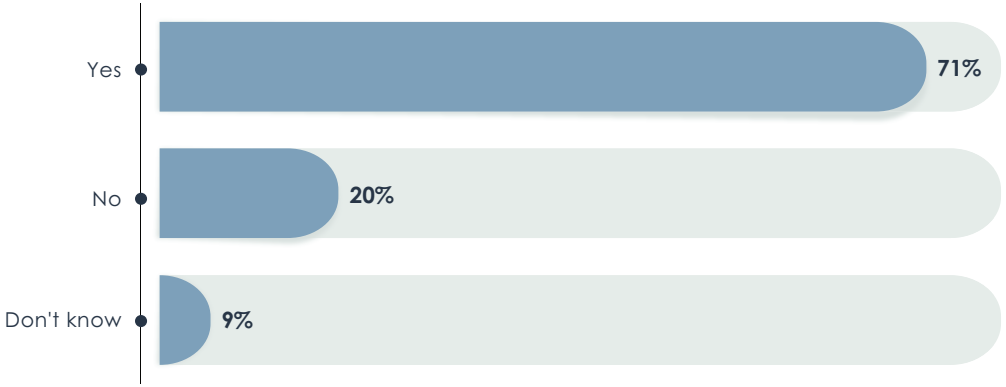
Analysis

In many cases, after painstaking research into exposures, security teams find that operational requirements trump the remediation options that are available. This turned out to be true for 71% of respondent organizations, while only 20% said it was not. Fewer than 10% of respondents were not sure.

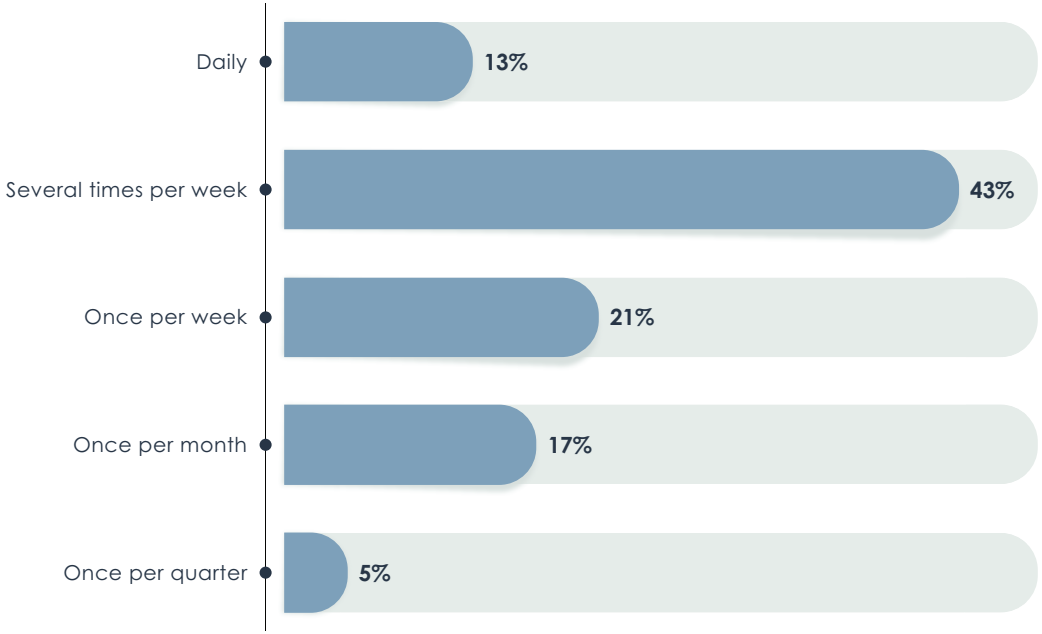
Commentary

For organizations that find they have to allow exposures to stand to meet operational requirements, the frequency of that finding can be several times per week, according to 43% of respondents. A smaller 21% find they have to accept these exposures on a weekly basis. Given that over 75% of organizations accept these exposures at least once per week, the frequency of accepting such risks is quite high. This puts additional pressure on security teams to constantly monitor for signs of attackers trying to exploit those exposures and try to gain as much visibility as possible into the AD attack surface.

Does your organization accept an Active Directory exposure for operational reasons?



How frequently does your organization accept Active Directory exposures for operational reasons?



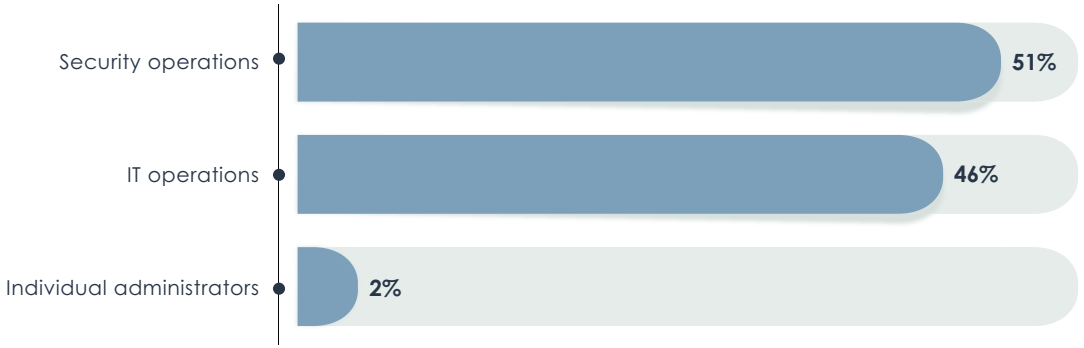
Analysis

When remediation moves beyond exposures to actual attacks, the responsibility to shut down such attacks and clean up after them falls fairly equal to both. For 51% of respondents, that responsibility belongs to IT security teams, but 46% report that task belonging to IT operations teams. A very small percentage rely on individual administrators, primarily among smaller organizations.

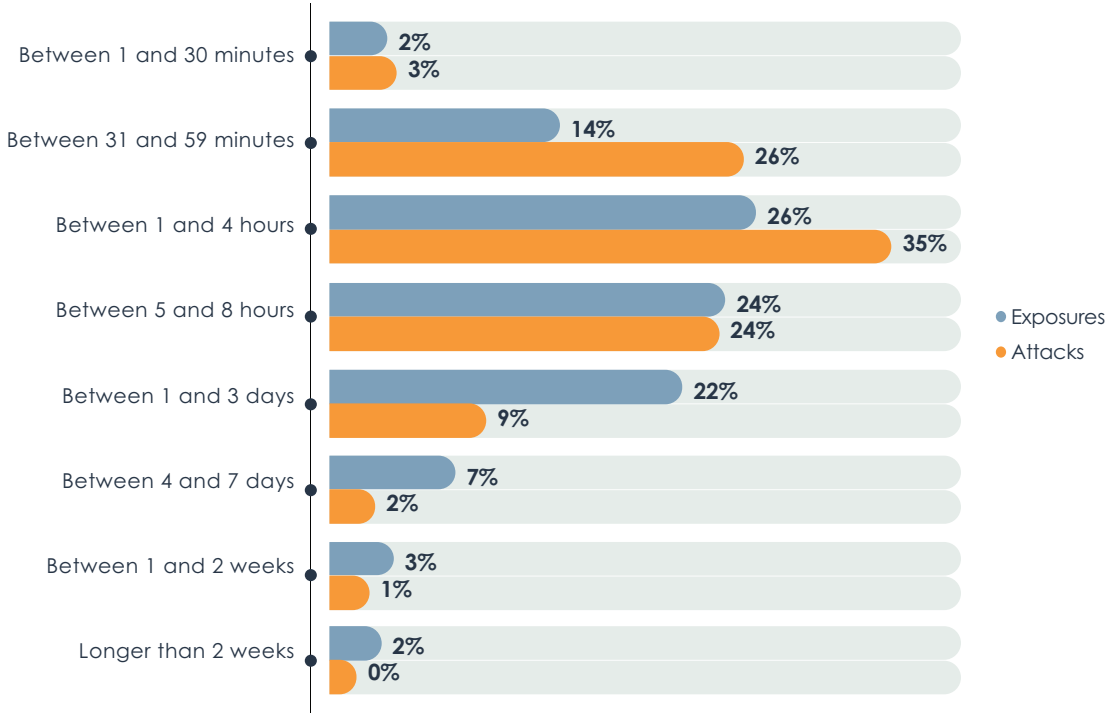
Commentary

No matter who is doing the remediation, it's clear that security and operations teams understand the urgency of stopping attackers as fast as possible. Comparing the time it takes to make attack remediation actionable and the time it takes to remediate discovered exposures not under attack, it's clear that these teams move much faster to shut down attackers. For example, while 14% of respondent organizations shut down exposures within 31 and 59 minutes, 26% of those teams shut down attacks within that same timeframe. While 26% shut down exposures in one to four hours, 35% remediate attacks in that time range.

Which individual or group within your organization is ultimately responsible for remediating Active Directory attacks?



Average time to remediate Active Directory exposures versus attacks



Risk Identification and Tracking

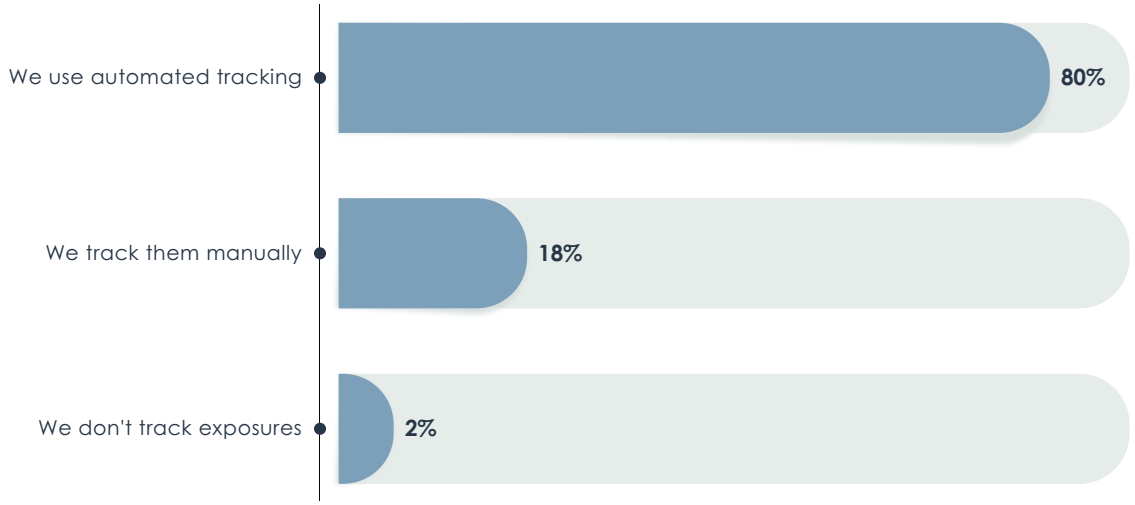
Analysis

Given the importance of tracking Active Directory risks to ensure they are addressed before attackers can exploit them, it's no surprise that most respondent organizations use automated tracking tools to keep an eye on exposures that have been uncovered. This is especially critical for larger IT shops that rely on separate IT operations and IT security teams to coordinate the discovery and remediation of exposures. Eighty percent of organizations use automation, rather than manually tracking exposures.

Commentary

With all of Active Directory's moving parts, it's easy to miss risks created by Active Directory objects, such as shared credentials, stale credentials, and service accounts. The number of exposures uncovered during periodic Active Directory assessments can be quite high. The time it takes to remediate such exposures can stretch out from hours to days. Given the constantly changing nature of Active Directory configuration, manual tracking of exposures is not an option for most medium and large enterprises.

How does your organization track Active Directory exposures?

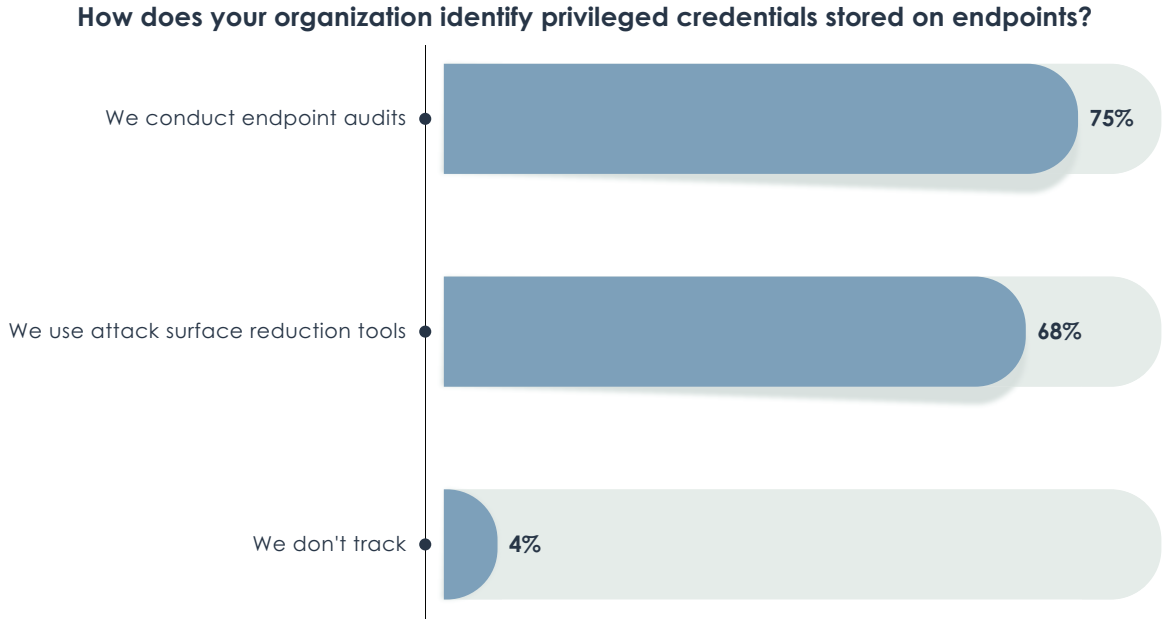


Analysis

Privileged administrator credentials are frequently stored on endpoints, although that is not a best practice for securing valuable assets. To identify such risks, most organizations use a combination of endpoint audits and attack surface reduction tools. Seventy-five percent of respondents indicated they conducted endpoint audits, and an overlapping 68% said they used attack surface reduction tools to complete that task.

Commentary

The practice of storing local administrator credentials on endpoints is so common that in recent years, attackers have developed credential-stealing malware to harvest those valuable privileges and move laterally within target networks.



Analysis

How well security teams coordinate with Active Directory domain administrators to keep track of potentially risky events can make the difference between a successful exploitation of exposures and the ability to prevent such events from occurring. It's reassuring that the vast majority of respondents said that when such risky events occur, those responsible for securing Active Directory are notified.

Commentary

While that seems encouraging on paper, there is no assurance that all such risky events are actually detected, let alone reported to the party responsible for keeping Active Directory secure. Given the complexity of Active Directory, without in-depth expertise to understand the implications of all configuration changes, many such events can go undetected. At the same time, investigation into risky events requires coordination and expertise, which can give attackers time to carry out their campaigns.

Protecting Active Directory

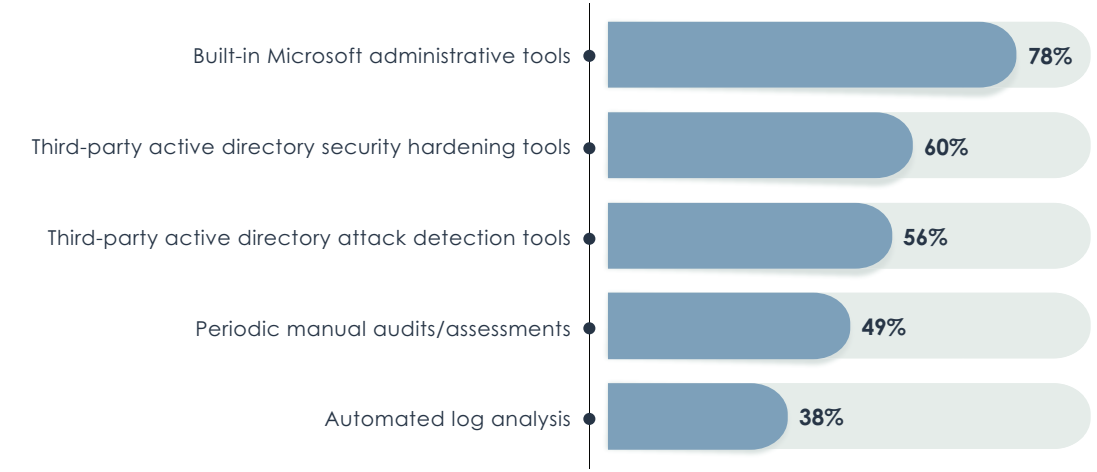
Analysis

Beyond patching Active Directory for known vulnerabilities, there are different protections that enterprises can apply to harden it against attackers. Respondent organizations apply a range of different protections to their AD environment, although the largest percentage still relies primarily on built-in Microsoft administrative tools, with 78% reporting using such tools. Another 60% turn to third-party hardening tools, and 56% rely on third-party tools designed specifically to detect AD attacks.

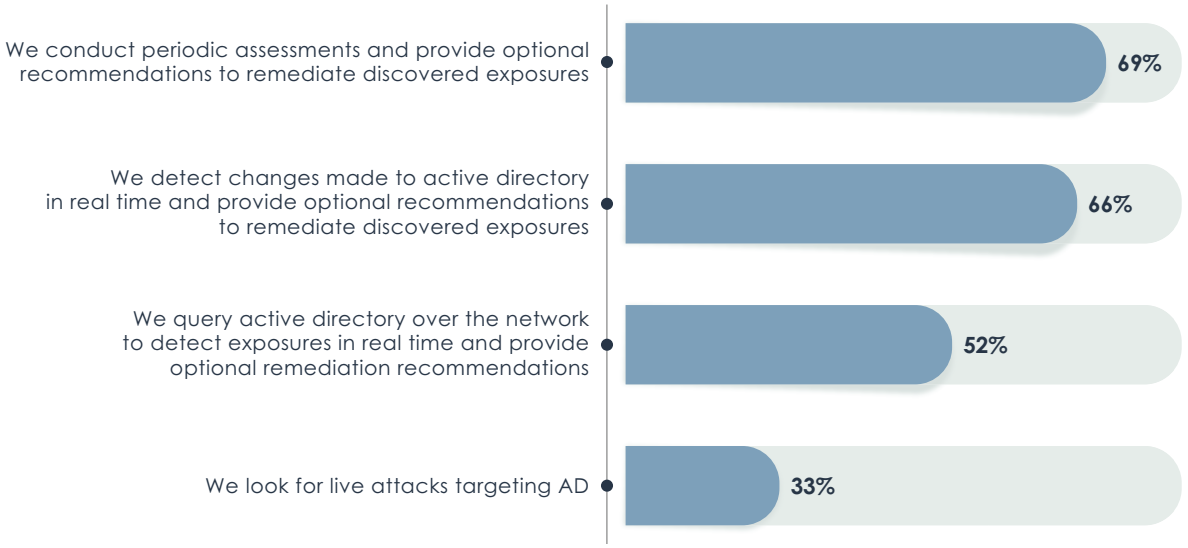
Commentary

Clearly, more help is needed beyond the tools that Microsoft provides to administer and secure Active Directory. How organizations go about putting their tools of choice to work varies. A fairly evenly split percentage of organizations either use them to periodically conduct audits or they automatically detect changes made to Active Directory in real time. In both cases, they then make optional recommendations to remediate detected exposures. Just over half of respondents query Active Directory over the network in real time to detect exposures, then make their recommendations. At this point in the market's evolution, a much smaller percentage hunt for live attacks against AD, but that's likely to change as more sophisticated tools become available and as more damaging Active Directory attacks are made public.

Besides patching, what protections for Active Directory does your organization employ?



Which of the following methods of securing Active Directory does your organization employ?



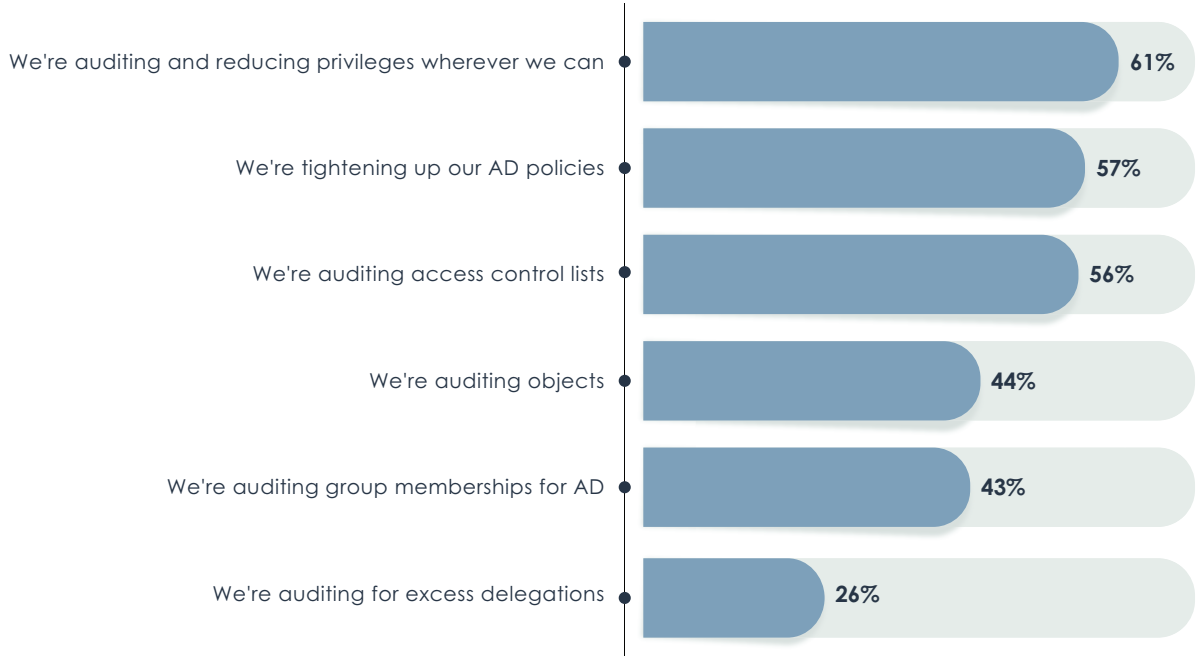
Analysis

In working to shrink the overly broad Active Directory attack surface, organizations are applying a range of techniques to close the window of opportunity on attackers. The most popular tactics to do that for most respondent organizations include auditing and reducing privileges wherever possible. Just over half (56%) also audit access control lists and tighten up Active Directory policies to reduce the number of exposures in their IT estate. Other auditing exercises include assessing objects, group memberships, and excess delegations.

Commentary

Given the frequent changes made in Active Directory as personnel come and go, change roles, hire contract workers, and execute on mergers or acquisitions, trying to keep the Active Directory attack surface to a minimum is a constant game of whack-a-mole. IT operations and security teams need multiple hammers and arms in order keep pace with exposures that open up.

What is your organization doing to reduce your Active Directory attack surface?



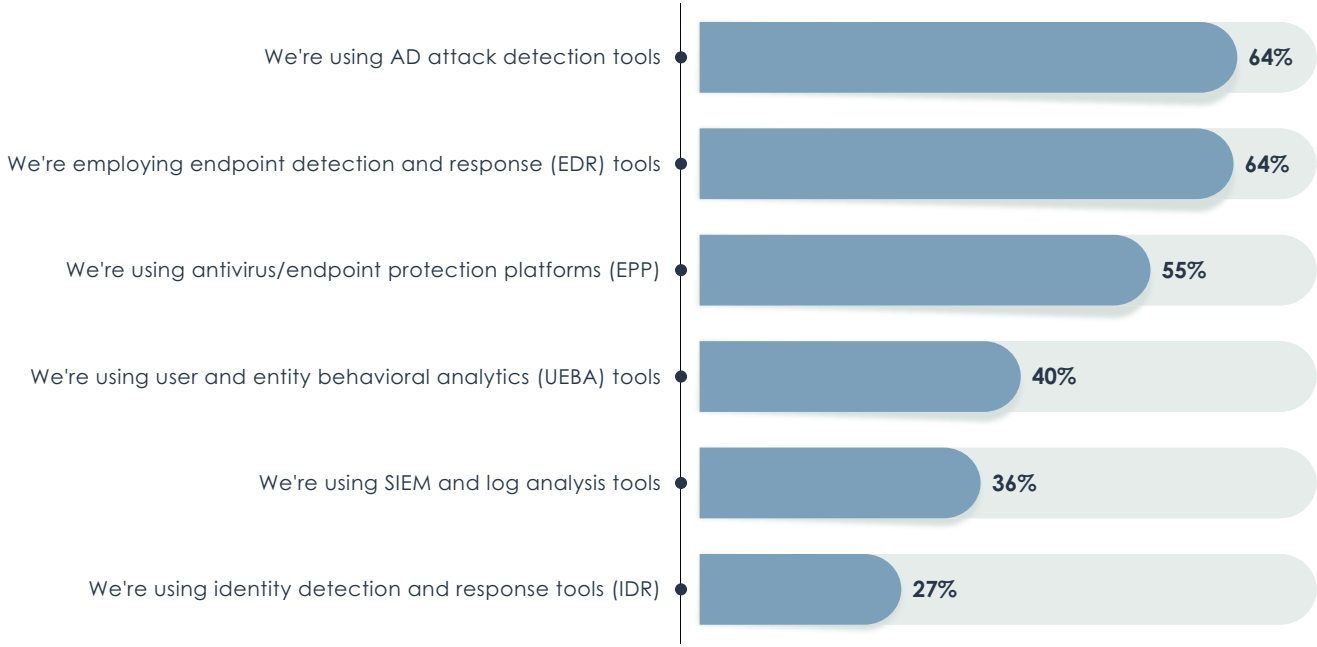
Analysis

When it comes to protecting against newer ransomware 2.0 attacks that specifically target Active Directory, a somewhat different array of tools is employed. Among the survey respondents, the two most popular tools in use include Active Directory attack detection tools and endpoint detection and response (EDR) tools, with 64% of respondents indicating each of those. Just over half are relying on the anti-ransomware protections added into their endpoint antimalware tools.

Commentary

An especially disturbing bit of news came out in late July 2021 about the LockBit 2.0 ransomware as a service. Researchers discovered that it can now automate the encryption of a Windows domain by using Active Directory group policies. Once executed on the domain controller, the ransomware automatically distributes itself across the domain, disabling existing Microsoft protections along the way.

What is your organization doing to protect against advanced attacks, such as ransomware 2.0, targeting Active Directory?



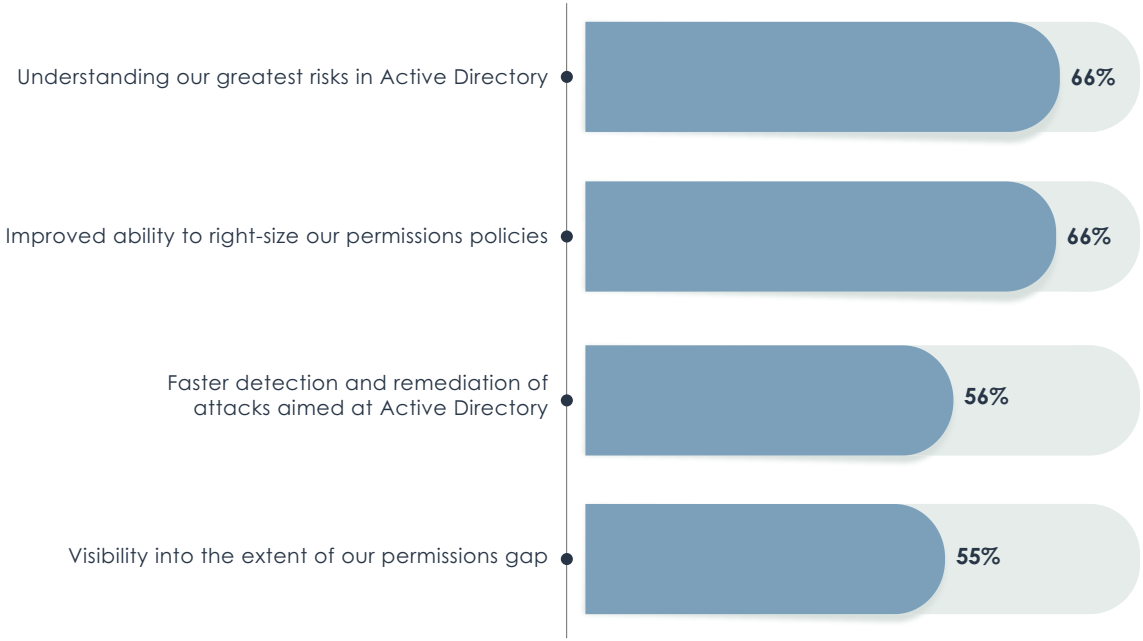
Analysis

The range of different tools IT operations and security teams use to protect Active Directory bring with them a handful of unique benefits to organizations. Chief among those is an understanding of which risks pose the greatest threat to the organization, and the opportunity to better right-size permissions policies, according to 66% of respondents.

Commentary

Given the constant firefighting mode that most IT security teams operate in, anything that helps them prioritize addressing the greatest risks to their organizations is a much-appreciated win. At the same time, adhering to the concept of least privilege is easier said than done.

Which of the following unique values or benefits does your organization believe Active Directory protection provides?



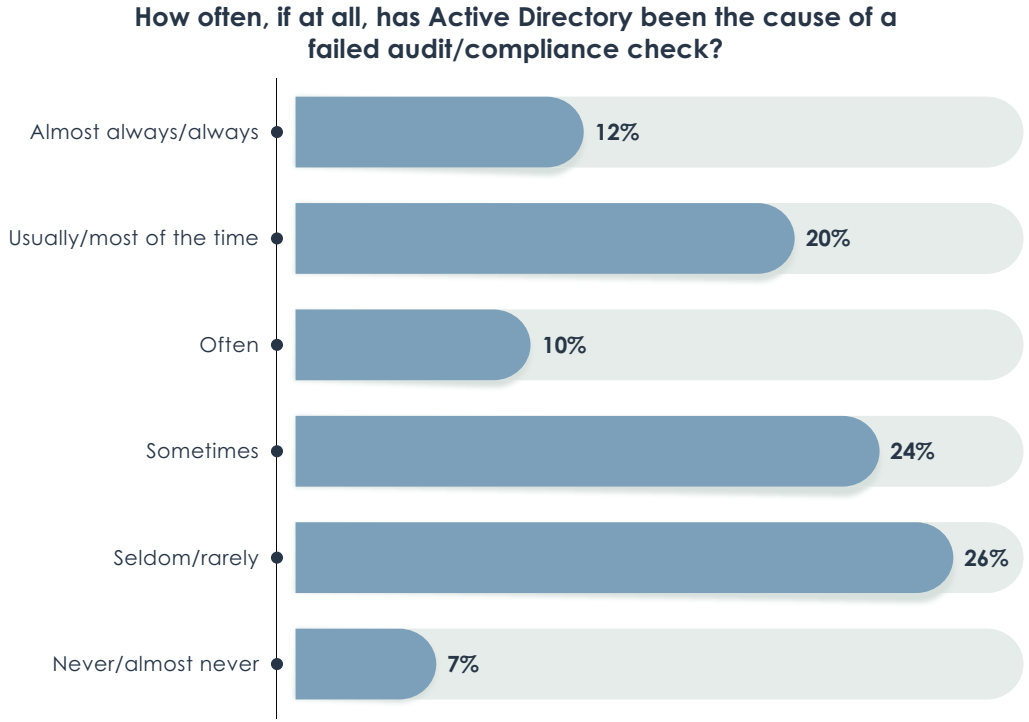
Active Directory and Compliance

Analysis

The research sought to understand how much of a role Active Directory played in causing regulatory compliance checks to fail, and that turned up a mixed bag of results. The largest percentage of respondents said that such failures due to Active Directory shortcomings seldom occur at 26%, but the third-largest percentage of respondents (20%) said it was the cause of a failed audit most of the time.

Commentary

For organizations governed by regulatory mandates, such as Sarbanes Oxley Act (SOX) or the European Union's General Data Protection Regulation, Active Directory can play a critical role in periodic audits. It can help provide the information necessary for these compliance checks, but that information can work for or against the organization. The research found a good news/bad news scenario for respondent organizations. Given the large range of Active Directory data types that need to be controlled and the individual nature of auditors' varying interpretation of these mandates, it's not surprising that it can frequently serve as the basis for failed audits.

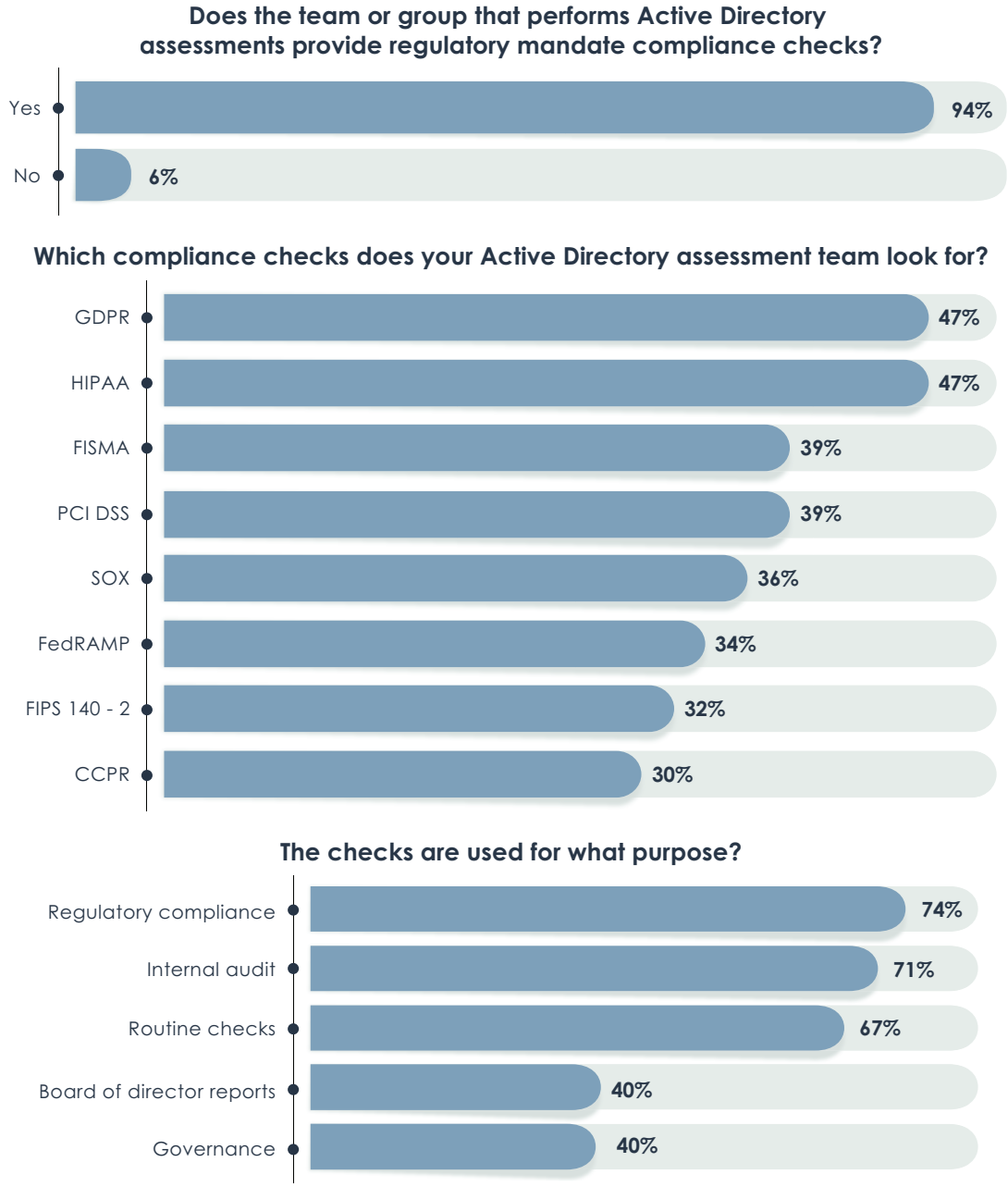


Analysis

Given the increasing size of fines for noncompliance and the disruptions caused by failed audits, it's a no-brainer that the teams that conduct AD assessments incorporate regulatory compliance checks in those assessments. The regulations covered in such checks range from PCI DSS to FedRAMP, although the largest percentage are focused on GDPR and HIPAA at 47% each.

Commentary

Beyond trying to keep auditors happy and fines to a minimum, it's worth noting that these regulatory compliance checks serve multiple purposes. They can be used as part of the organization's internal auditing exercise to support governance initiatives and to inform the organization's board of directors.



EMA Perspective

Given the level of access attackers can achieve by exploiting Active Directory exposures and vulnerabilities, it's no wonder that attackers target 95 million AD accounts on a daily basis, according to Microsoft.[1] More than half of all new malware includes code designed to actively target Active Directory. Attackers continue to up their game, as demonstrated not only by last December's SolarWinds Sunspot attack, but also this past summer in the new LockBit 2.0 ransomware as a service, which can automate the distribution of malware via group policies, allow attackers to disarm Microsoft Defender, and encrypt data with a single command. Periodic (and frequent) audits of Active Directory, whether through outside pen testers or internal red team/blue team exercises, are necessary to maintain a decent semblance of security hygiene for the authentication and access control platform used by the vast majority of enterprises. Those remain a primary method to identify and secure exposures by a majority of respondent organizations, but audits aren't the only method or tool security teams use to secure AD. Given the snapshot nature of audits, they are not sufficient to ensure that the majority of attack paths remain closed to attackers.

One other note worth mentioning is the way that Active Directory is integrated into Office365 and Azure. Its federation with AD on-premises means that once attackers have compromised Active Directory on-premises, they have equal access to the victim organization's resources in the cloud. Given the wholesale movement to cloud-based services, this greatly extends the attack surface. In fact, 86% of organizations are using Active Directory in the cloud today. The largest percentage are doing so by hosting AD controllers in their public cloud instances, but others are using Microsoft's Azure AD or doing both.

That federation also makes remediation of attacks not unlike the SolarWinds breach, which leveraged the golden SAML technique, very tricky to accomplish. Unless the attackers' presence is shut down in both the cloud and on-premises instances of Active Directory, they can use continued control in one domain to reestablish presence in the other.

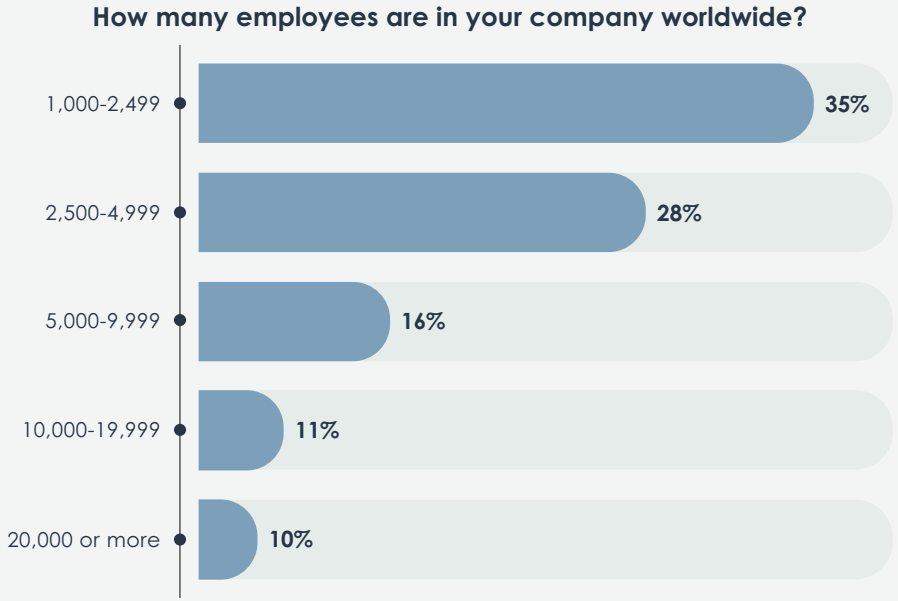
To be fair, Microsoft continues to improve the security of Active Directory, and it offers AD protection tools of its own in Microsoft Defender for Identity, formerly Azure Advanced Threat Protection. Still, that has not prevented the growth of a market niche for tools better designed to find exposures and vulnerabilities, and identify as well as remediate potential attack paths. Still others are designing tools that can spot signs or patterns of malicious activity in real time as attackers seek to gain access to privileged accounts and back doors.

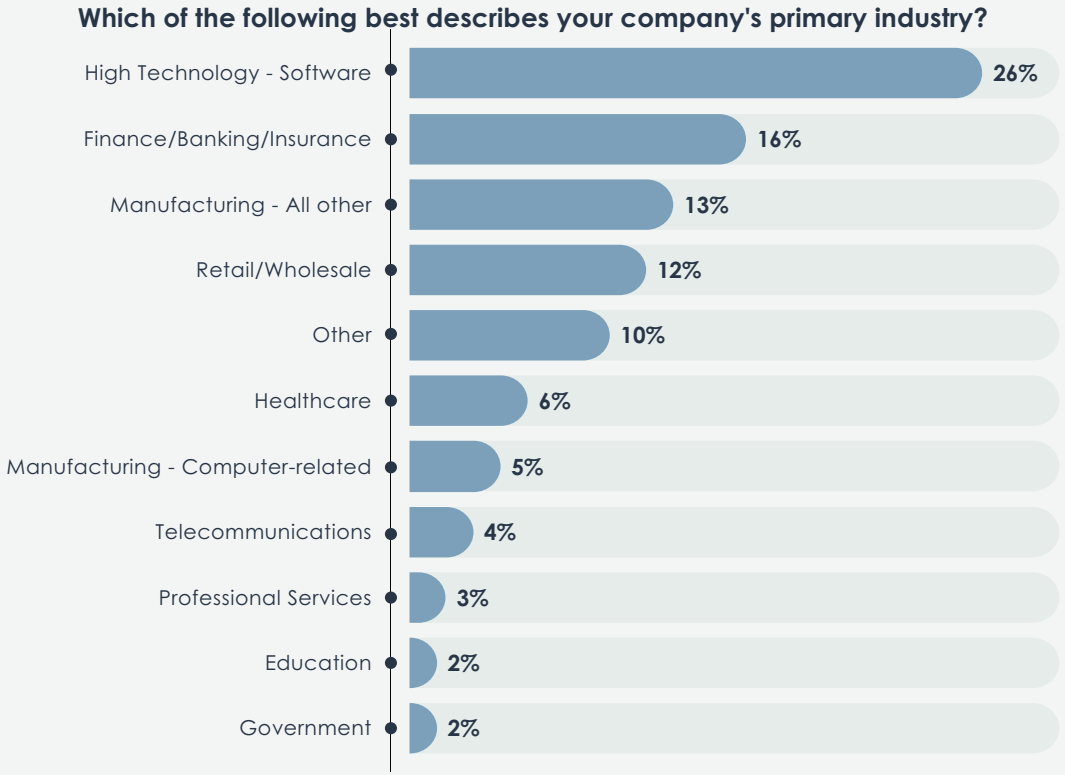
There are several unique benefits that these tools provide. Sixty-six percent of respondent organizations say such tools help their security teams understand the greatest Active Directory risks, and they enhance their ability to right-size their permissions policies. Over half also say that such tools provide faster detection and remediation of Active Directory attacks, and they provide visibility into the extent of their organization's permissions gap.

What's clear is that attackers over the last few years have up-leveled their Active Directory attack skills—no doubt with the help of open-source pen testing tools, such as Mimikatz and Metasploit. To keep pace, security teams need to adopt more best practices in defending Active Directory. Key is the ability to look at the Active Directory attack surface from the attacker's perspective, using tactics and tools that can help improve visibility into the true attack surface and quickly respond when live attacks are detected.

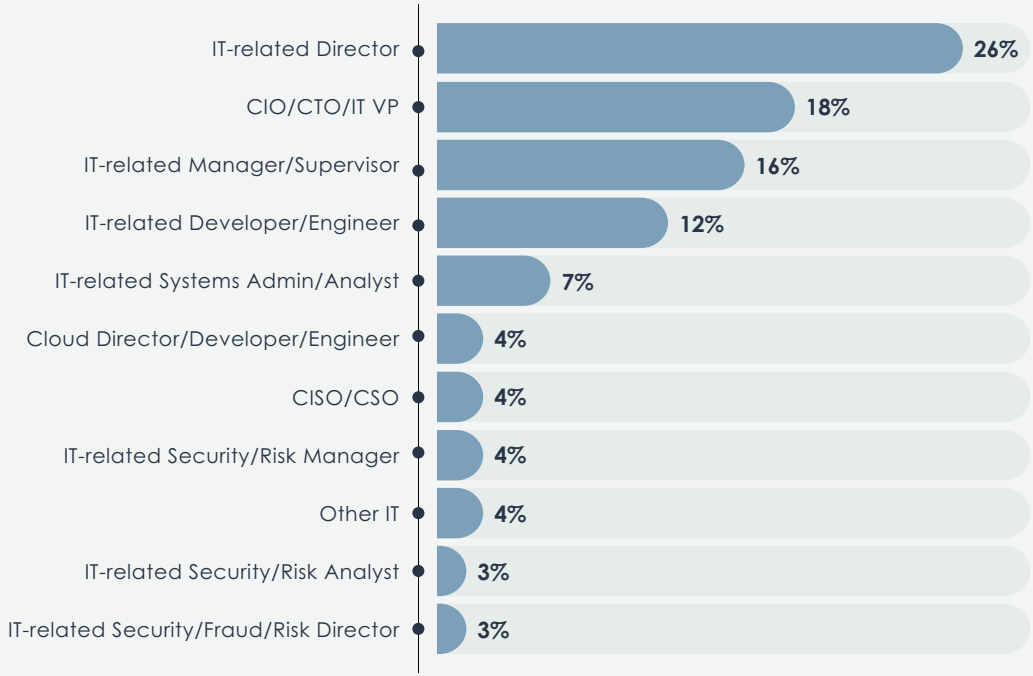
[1] https://www.zdnet.com/article/active-directory-czar-rallies-industry-for-better-security-identity/

Research Methodology and Demographics

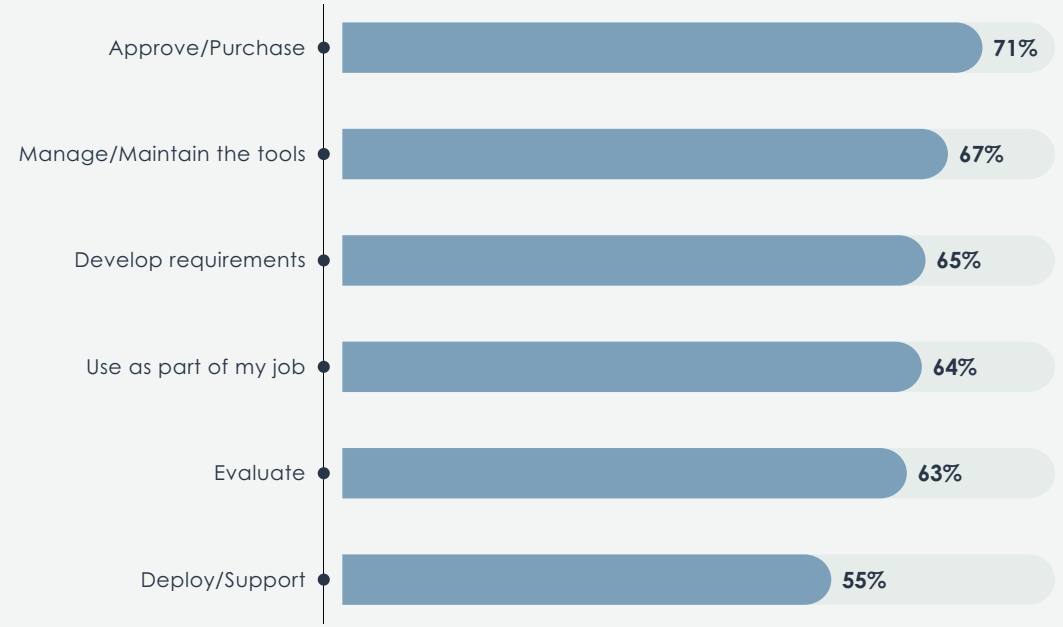

How many employees are in your company worldwide?
1,000-2,499
35%
2,500-4,999
28%
5,000-9,999
16%
10,000-19,999
11%
20,000 or more
10%


Which of the following best describes your company's primary industry?
High Technology - Software
26%
Finance/Banking/Insurance
16%
Manufacturing - All other
13%
Retail/Wholesale
12%
Other
10%
Healthcare
6%
Manufacturing - Computer-related
5%
Telecommunications
4%
Professional Services
3%
Education
2%
Government
2%

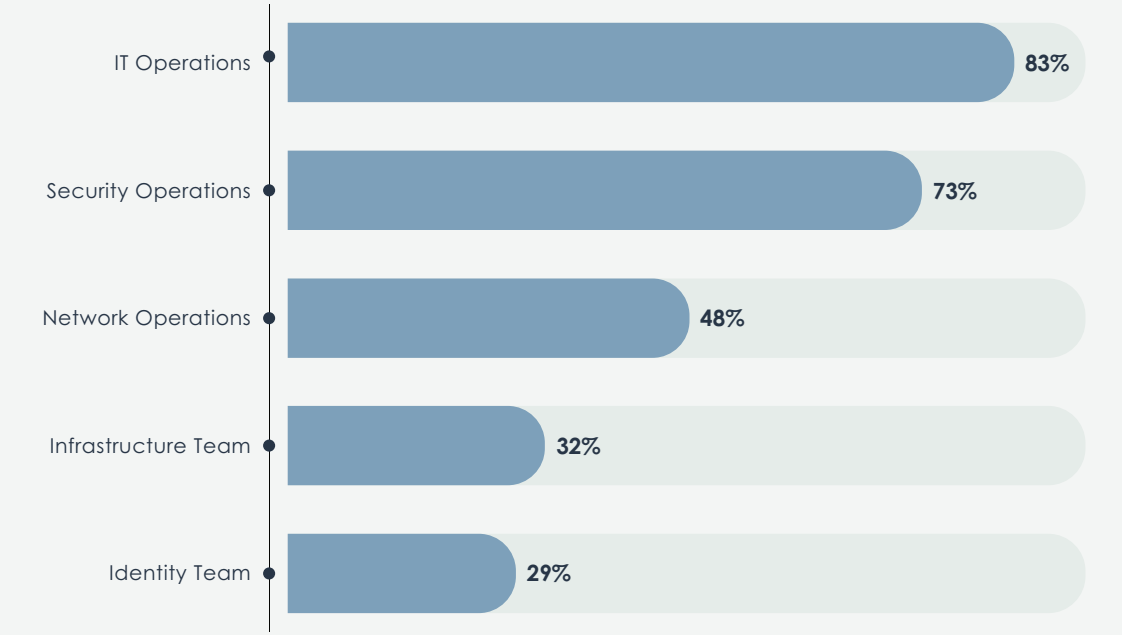
Which of the following best describes your role in the organization?

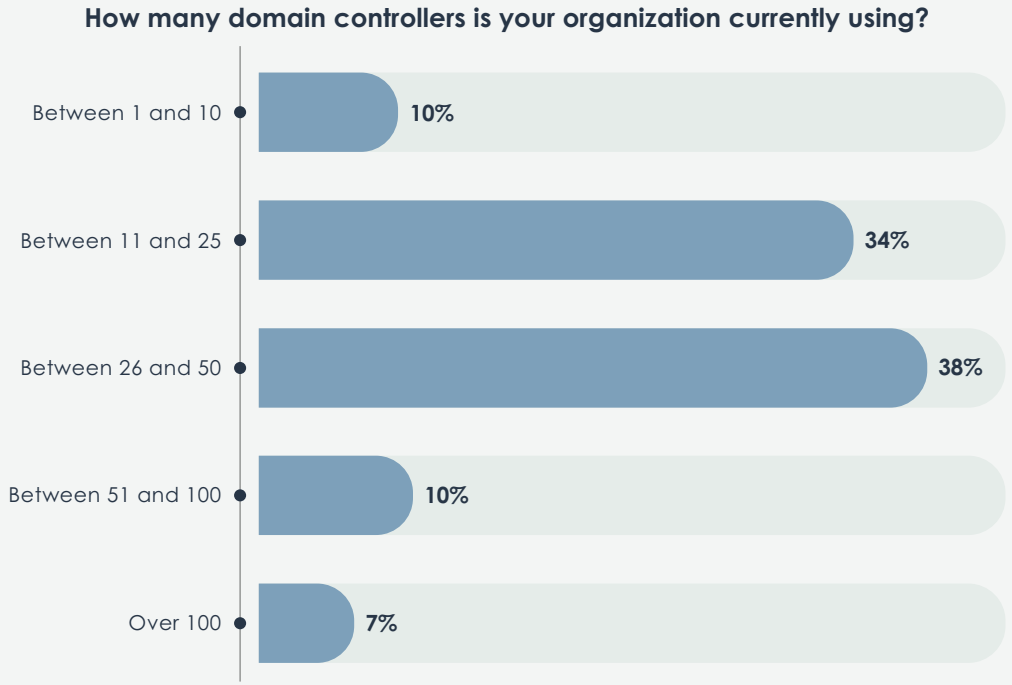


How are you involved with security management solutions within your organization?

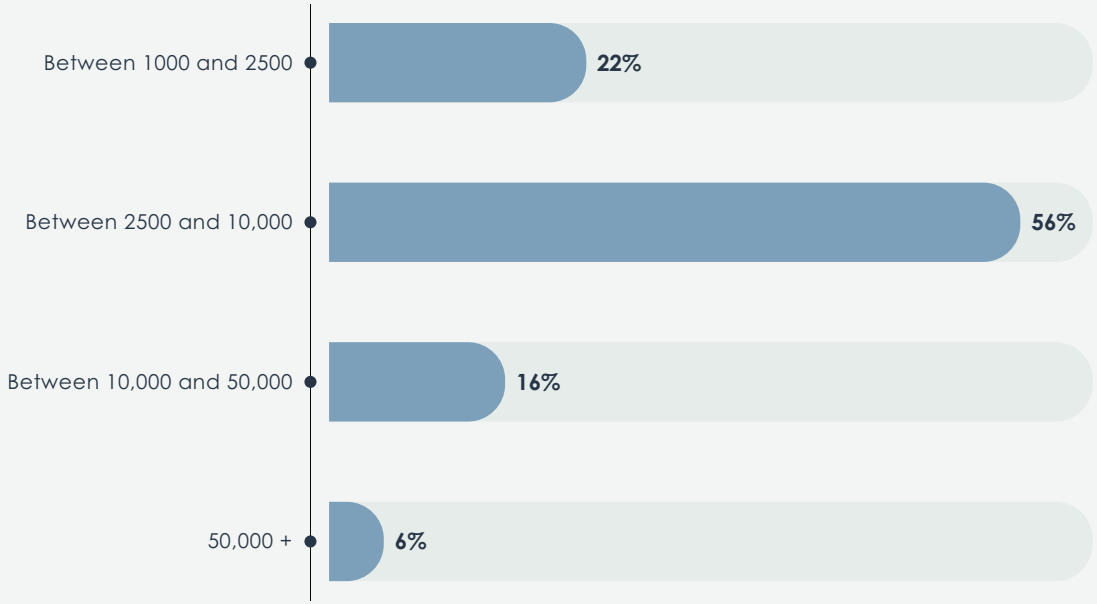


Which group(s) within your organization is/are responsible for securing active directory?

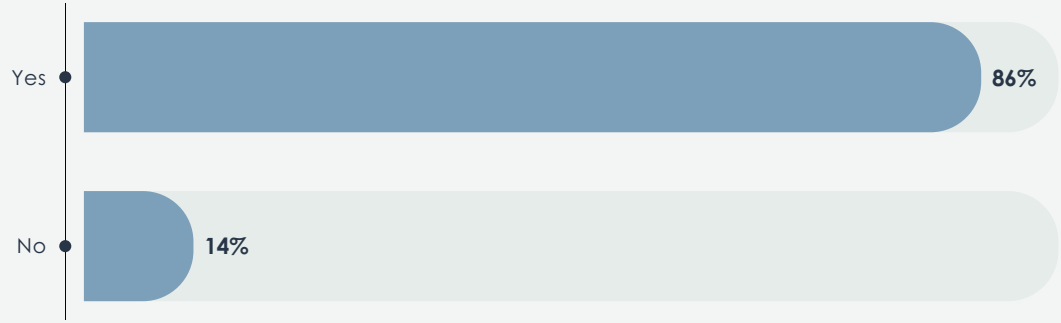



How many domain controllers is your organization currently using?
Between 1 and 10
10%
Between 11 and 25
34%
Between 26 and 50
38%
Between 51 and 100
10%
Over 100
7%

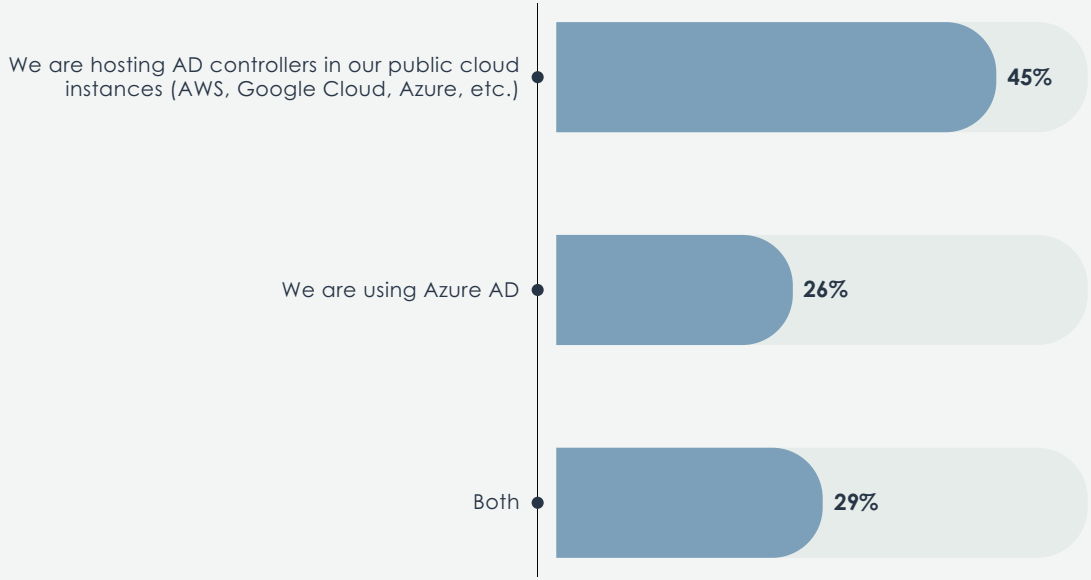
How many Active Directory accounts is your organization currently using?



Is your organization using Active Directory in the cloud?



You indicated that your organization is using Active Directory in the cloud. How is it deployed?



About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com**. You can also follow EMA on **Twitter** or **LinkedIn**.

This report, in whole or in part, may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2021 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common law trademarks of Enterprise Management Associates, Inc.

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 **www.enterprisemanagement.com**

4118.092121