EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

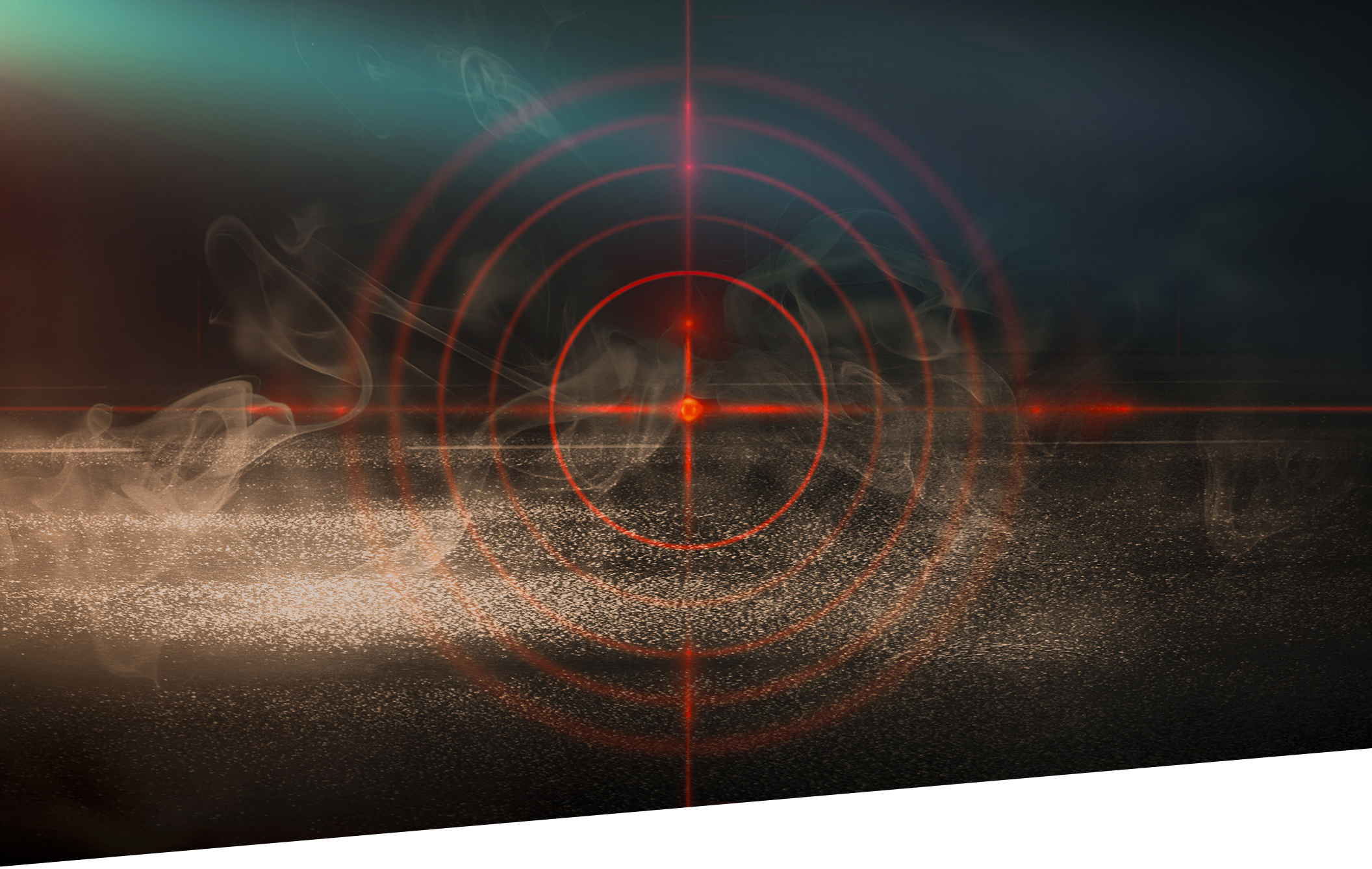
Sponsored by: semperis

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

September 2021 EMA Research Report Summary

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.

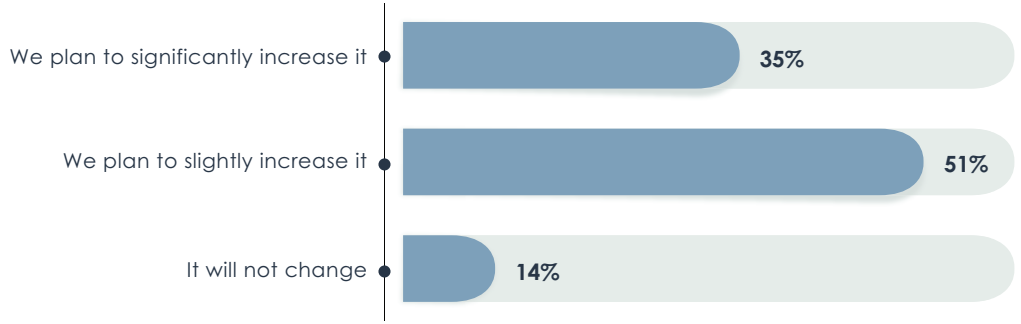
Given the severity of this threat, Enterprise Management Associates sought to understand how organizations are adapting to the growing risk, how their priorities around securing Active Directory are changing, and what obstacles they face in protecting the identity management, user authentication, and 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.

Priorities and Spending for Active Directory Security

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.

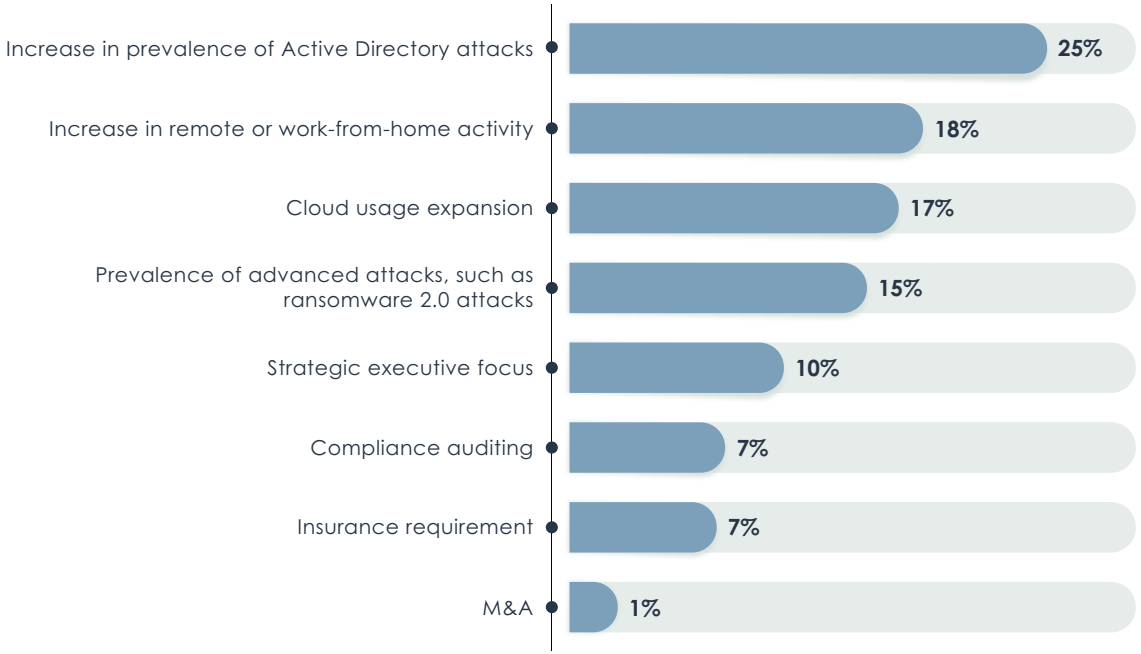
Which of the following statements best describes your organization's future spending plans for Active Directory security?



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%

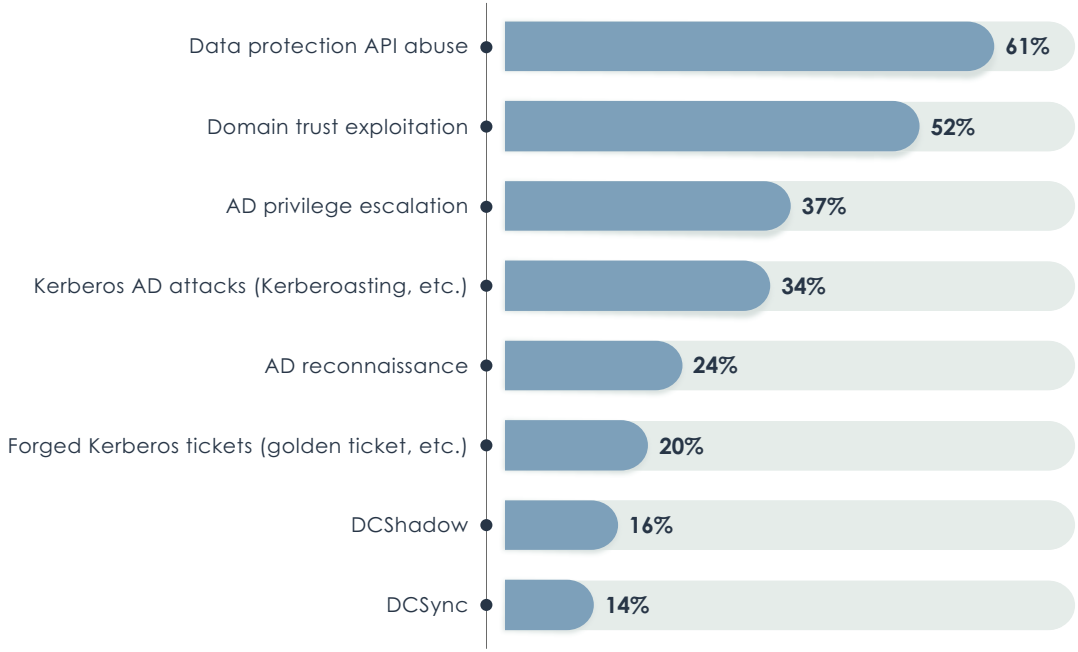
Analysis

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.



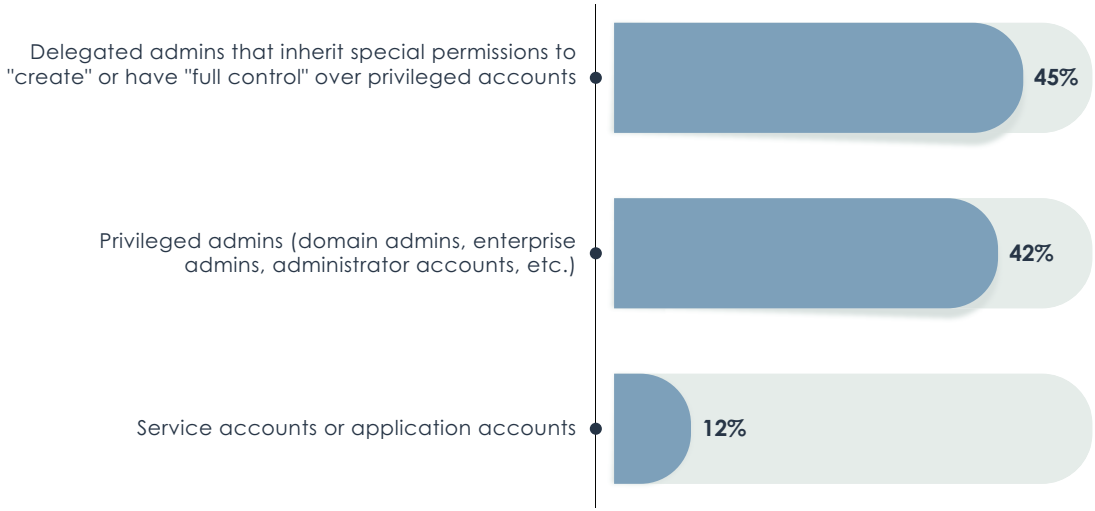
Analysis

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?



Assessing the Security Posture of Active Directory

Analysis

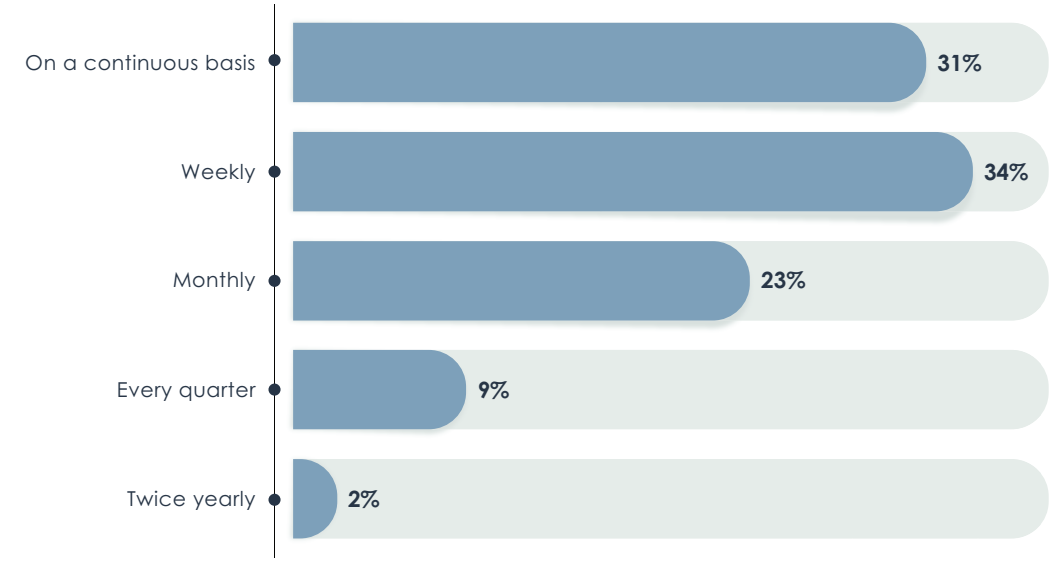
For companies that rely heavily on audits or assessments to shore up their Active Directory security posture, such assessments are most often conducted on weekly basis, with 34% indicating that frequency. Only a slightly smaller percentage take a more aggressive approach to Active Directory security 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.

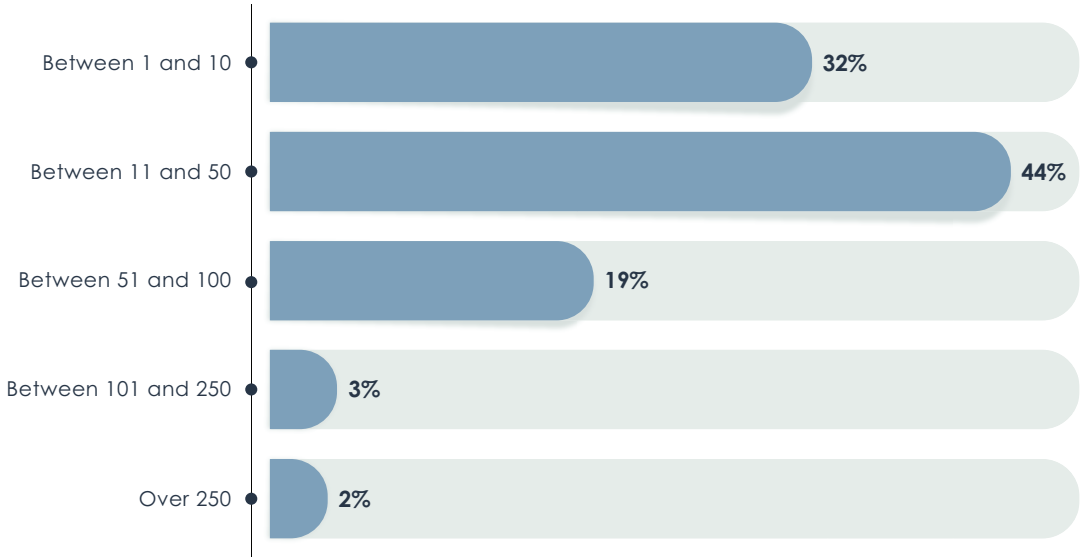
Commentary

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?



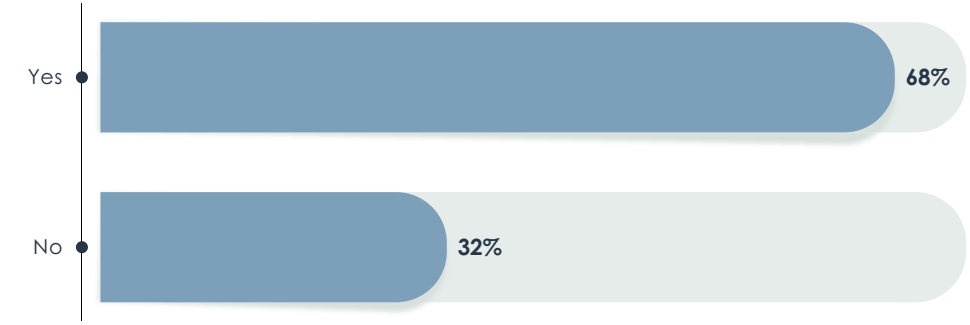
Analysis

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.

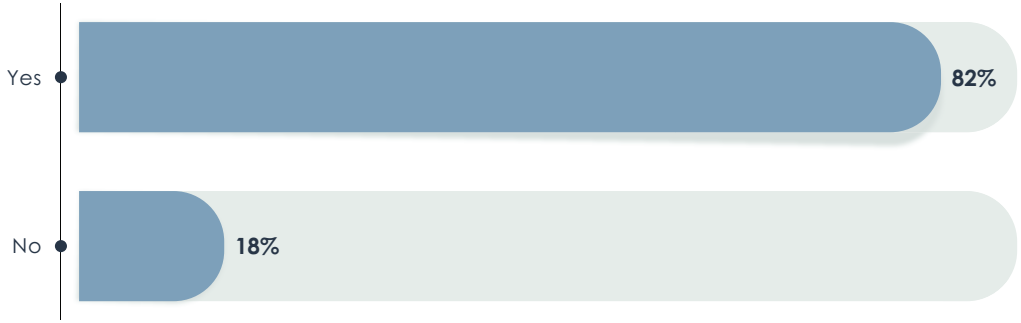
Commentary

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?



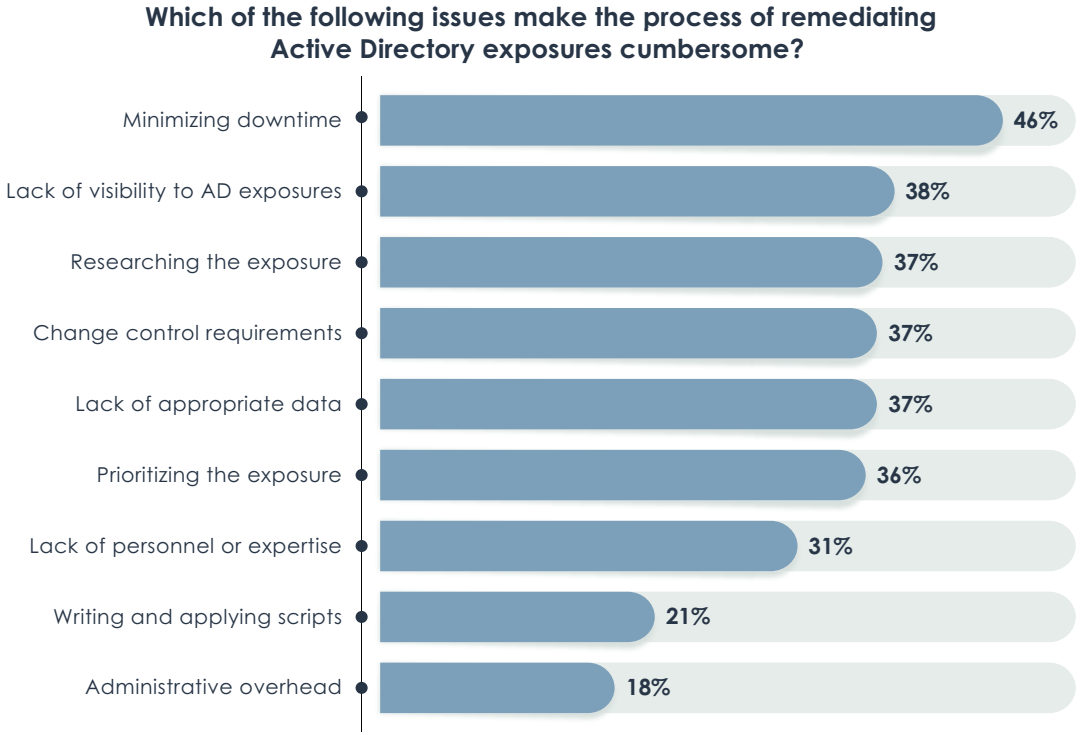
In those penetration testing exercises, were they successful in exploiting Active Directory exposures?



Remediating Exposures and Attacks

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.

Protecting Active Directory

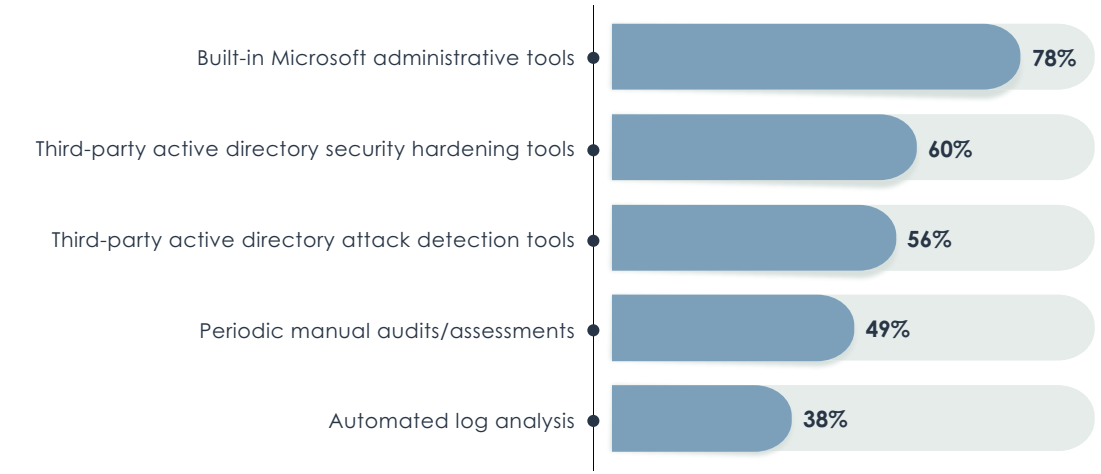
Analysis

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.

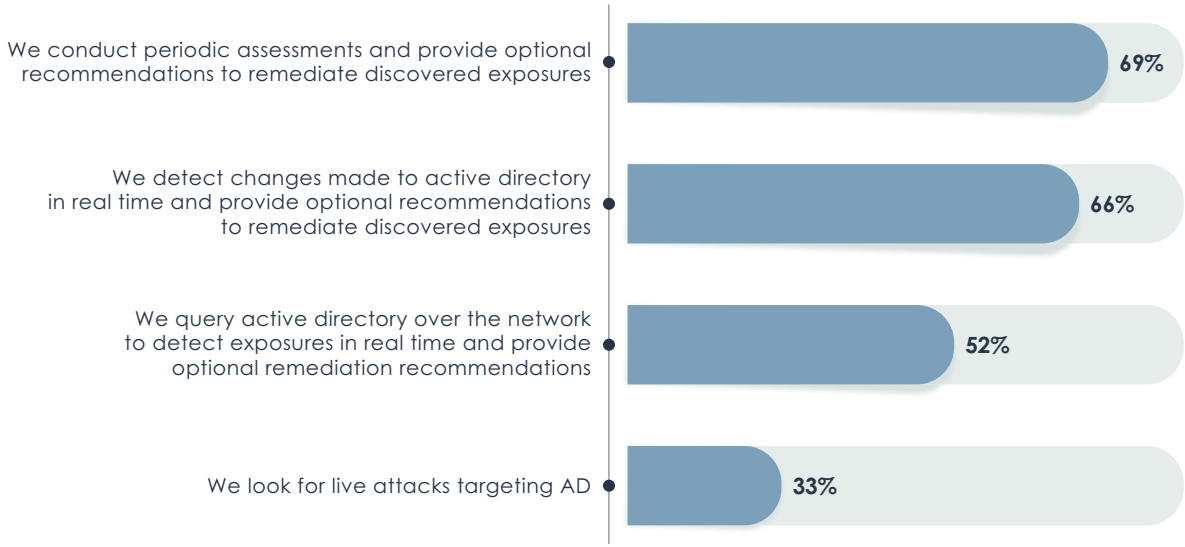
Commentary

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?



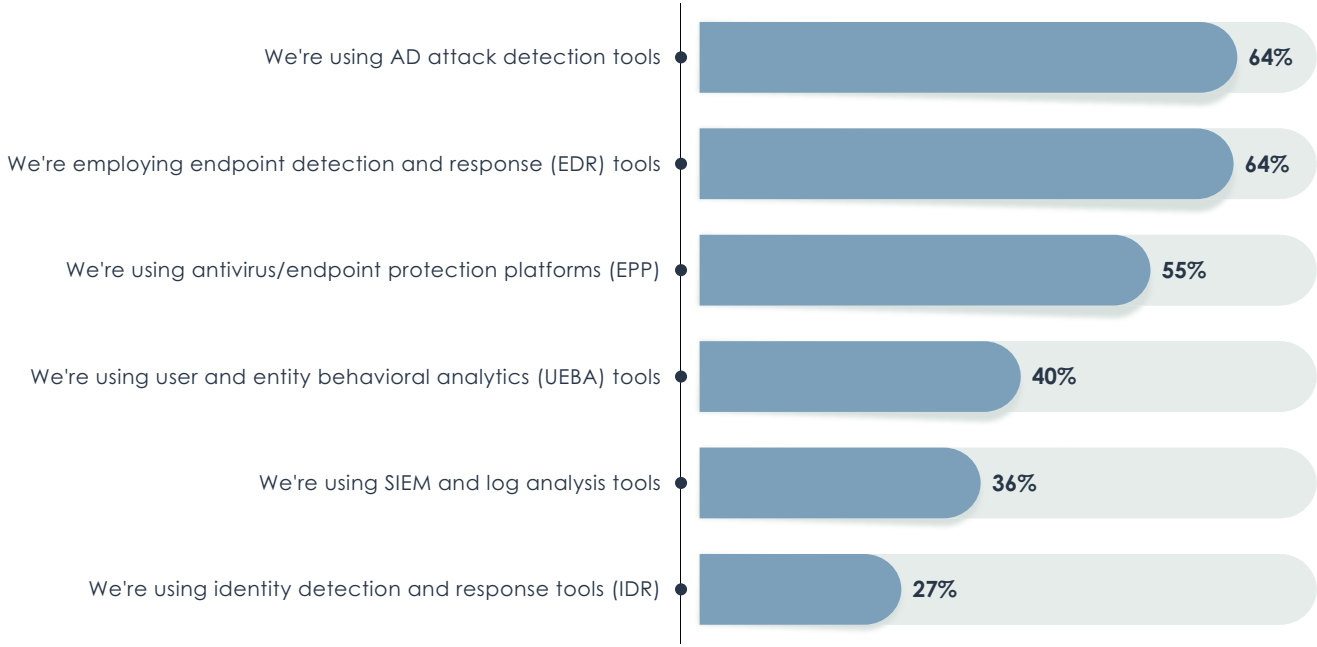
Analysis

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?



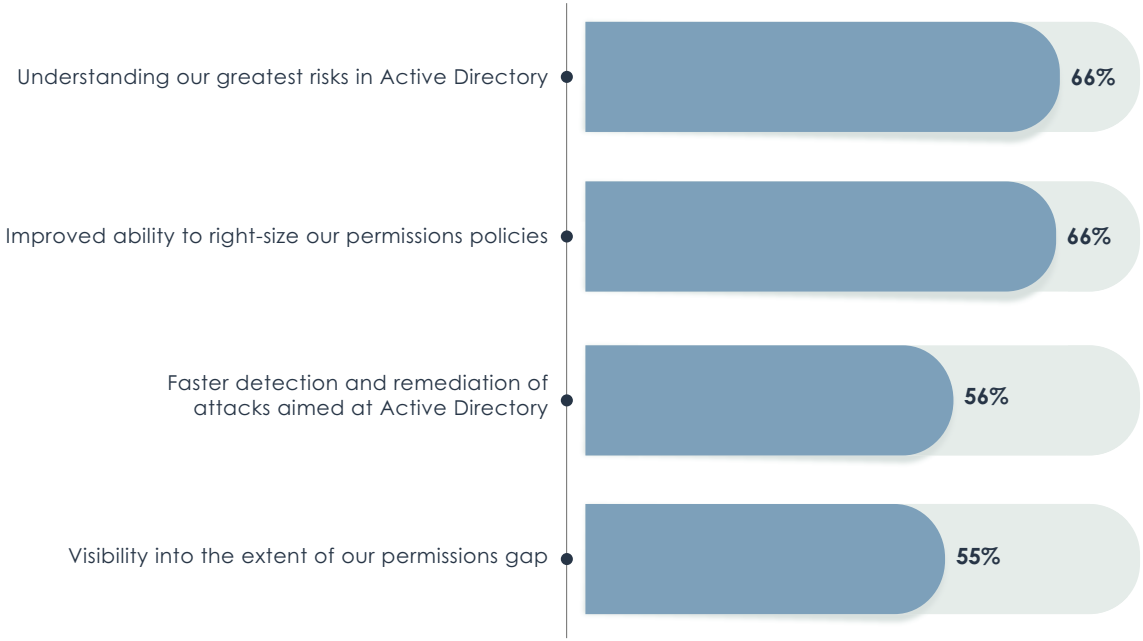
Analysis

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?



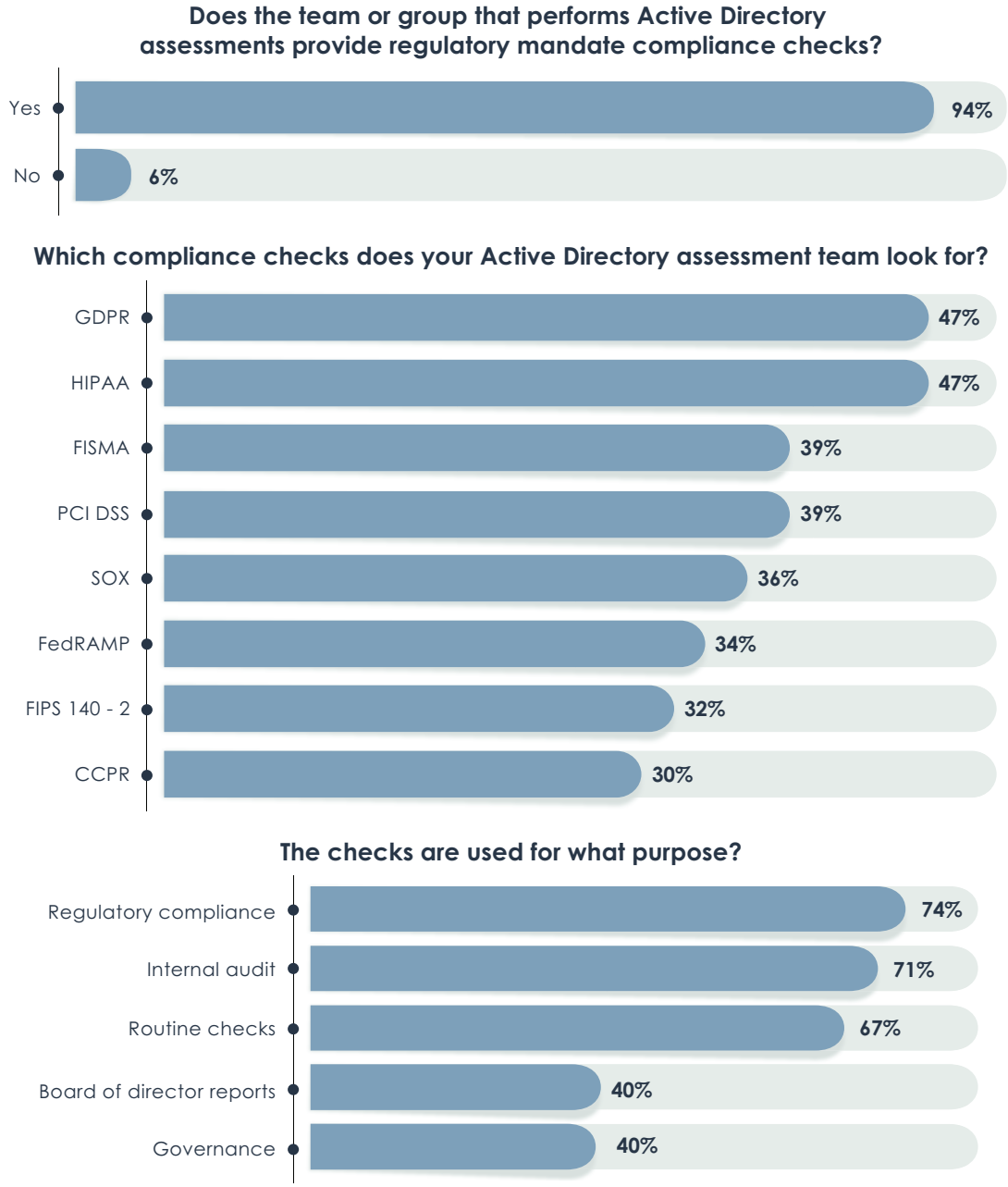
Active Directory and Compliance

Analysis

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.



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**.

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

4118.102521