Research Report

Analyzing Identity Risks (AIR) 2022

Illuminating identity risks that leave every organization vulnerable to attack

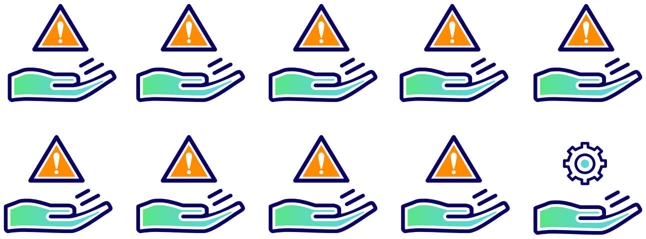
EXECUTIVE SUMMARY

From ransomware to APTs, identity is the top vector for attacks. The complexity of managing Active Directory has resulted in the presence of exploitable privileged identity risks in all organizations at a rate of 1 in 6 endpoints. These identity risks include unmanaged local admins with stale passwords, misconfigured users with unnecessary privileges, cached credentials left exposed on endpoints, and much more.

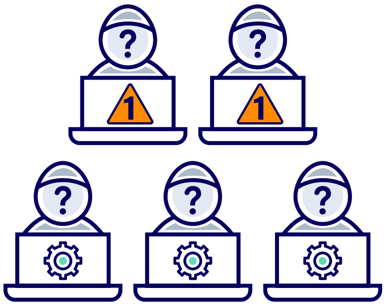
When an attacker compromises an endpoint with these privileged identity risks, it becomes trivial for them to install malicious software and steal data. Privileged identities represent the keys to the kingdom, which attackers exploit to steal the crown jewels. Unfortunately, most organizations are unaware of this risk – either until they are attacked or until Illusive helps illuminate these blind spots.

KEY FINDINGS

Every organization has exploitable identity risks at the rate of 1 in 6 endpoints



87% of local admins are not enrolled in a privileged account management solution



40% of shadow admin risks can be exploited in one step

Privileged account passwords are left exposed on 13% of endpoints

INTRODUCTION
Every Organization is Vulnerable to Identity Risks

Evidence of pervasive identity risks surrounds us. According to the 2021 Verizon Data Breach Incident Report, credentials are the most sought-after data type in a breach.[1] The Identity Defined Security Alliance reports that 79% of organizations have experienced an identity-related security breach.[2] The Identity Theft Resource Center reports that ransomware attacks doubled in 2021 and are on pace to pass phishing as the root cause of data compromises in 2022.[3]

However, what may come as a surprise is that all organizations lack visibility into these identity risks. Illusive has witnessed these blind spots firsthand while working with numerous security teams in the financial services, healthcare, and retail sectors (among others), which often have the most mature security programs. This work was completed during the past 12 months to analyze their identity risks, which we now present in our inaugural *Analyzing Identity Risks (AIR) 2022* report.

Privileged identities have unusual power in your organization. They can reset passwords, change policies, install software, and extract or encrypt data. When an attacker compromises an endpoint with one of these privileged identities, it is like playing a video game with cheat codes – they can do almost anything they want. Exploitable identity risks enable attackers to gain initial access, establish their persistence on a network, elevate their privileges, evade defenses, and accelerate their lateral movement until they have taken complete control.

Unfortunately, Illusive research reveals that all organizations are vulnerable and that 1 in 6 endpoints have at least one exploitable identity risk. This research examines these risks across three dimensions: unmanaged identity risks, misconfigured identity risks, and exposed identity risks. Many of these risks overlap with one another, and the reality is that Illusive discovers examples of unmanaged, misconfigured, and exposed identity risks in every organization.

Figure 1: **Every organization has exploitable identity risks at the rate of**

1 in 6 endpoints

UNMANAGED IDENTITY RISKS

Unmanaged identity risks can manifest in the form of outdated local admin passwords, the use of temp or test admin accounts, or local admins that have not been enrolled in an account management solution, among other things. For example, during the analysis of a financial services organization, Illusive discovered nearly 400 local admins that were enrolled in Microsoft's Local Administrator Password Solution (LAPS), but nearly 500 local admins that were not – a failing grade, but still far better than the average.

As a best practice, local admins should be enrolled in privileged account management solutions; however, constant changes and certain limitations with these solutions can result in the proliferation of unmanaged and forgotten local admins. One purpose of solutions like LAPS is to make sure that each local admin has a unique password. In the absence of these solutions, there is a greater likelihood of password reuse, enabling attackers to compromise hundreds of local admin accounts – as easily as one.

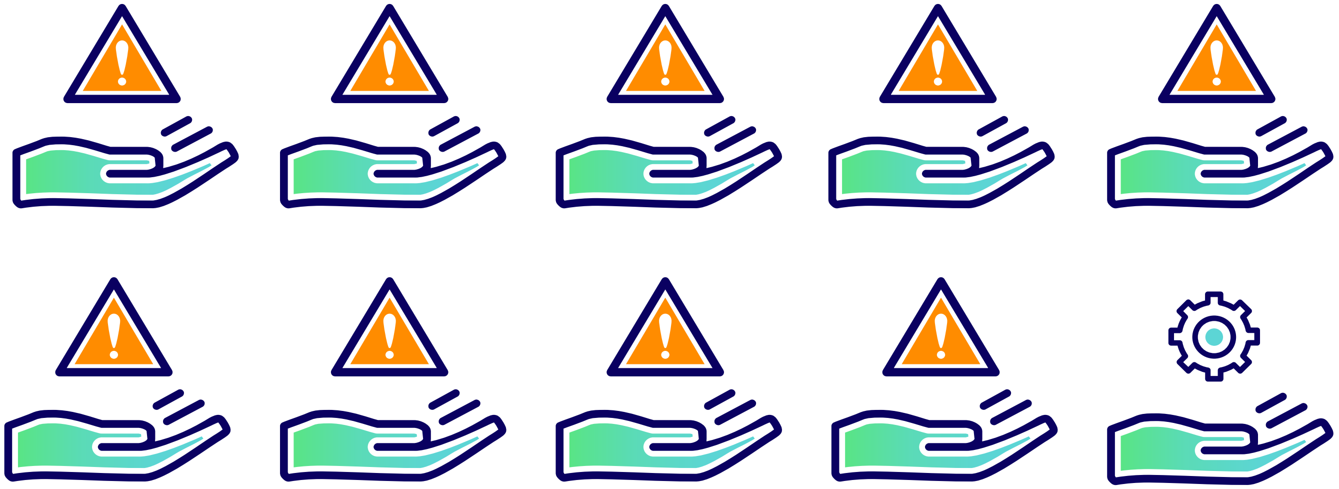


Figure 2: **87% of local admins are not enrolled in a privileged account management solution**

UNMANAGED IDENTITY RISKS

Figure 3: **21% of local admins use the default account name (i.e., Administrator)**

On the flip side, the use of default account names (i.e., Administrator) for local admins also lowers the barrier to entry for attackers. The use of default account names compounds the risk of unmanaged local admins. If these default admin accounts all use the same password, there is nothing to stop an attacker from taking control of them all.

Likewise, outdated passwords are another source of unmanaged identity risk. As a best practice, admin passwords should be changed every 30 to 90 days. The older a password becomes the more susceptible it is to a variety of brute force attacks; especially in the case of password reuse. Furthermore, the use of outdated passwords suggests an underlying risk that these local admins remain unmanaged.

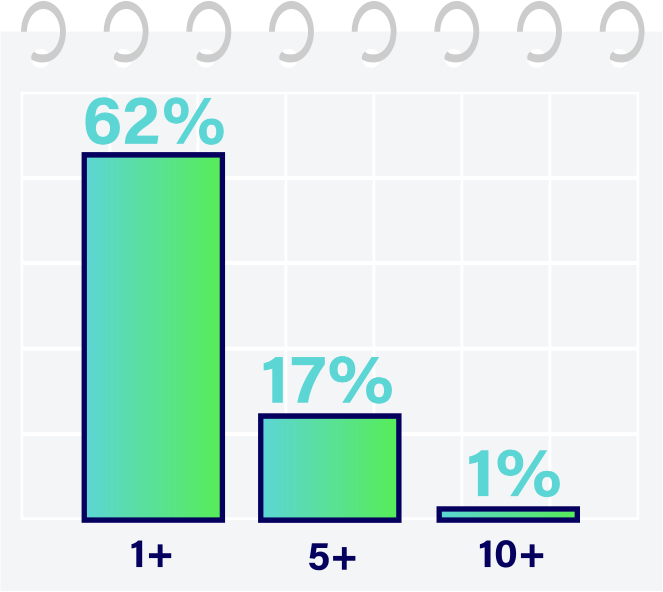


Figure 4: **A breakdown of local admin password age – 62% were unchanged for more than 1 year, 17% were unchanged for more than 5 years, and 1% of passwords were unchanged for more than 10 years**

UNMANAGED IDENTITY RISKS

Another risk related to passwords is when a local admin password has never been set. There are academic arguments in favor of never setting an admin password, but the reality is that it significantly increases the risk of insider attacks and may be catastrophic in the case of a lost or stolen device.

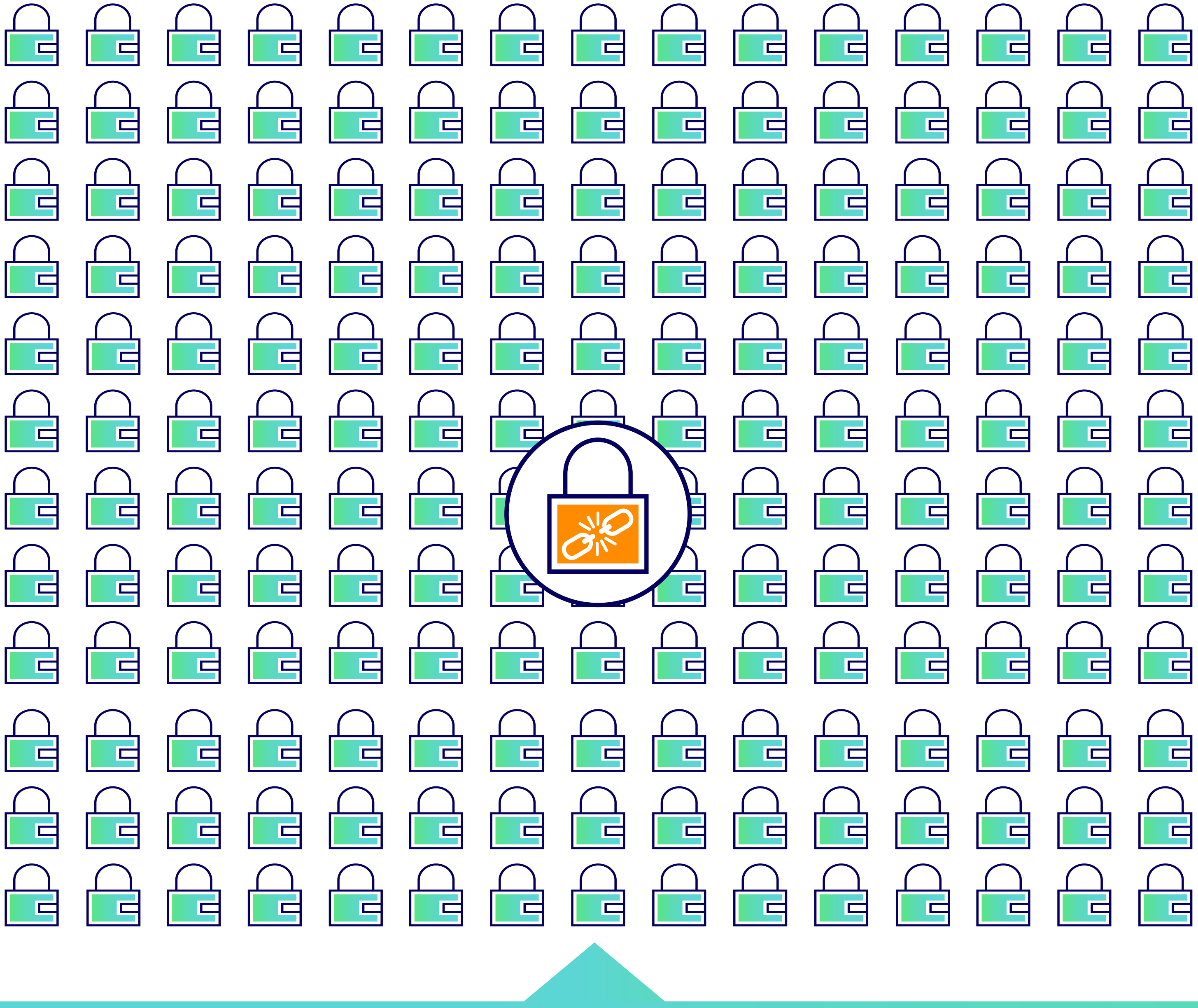


Figure 5: **1 in 180 local admin passwords have never been set**

UNMANAGED IDENTITY RISKS

One final unmanaged risk is the presence of completely unknown local admins. These admins tend to be named "temp" or "test." You may be wondering how we can quantify this risk as unknown – it is because every single time we present our findings to these organizations they admit they have no idea who those admins are. As these accounts are highly privileged, yet unknown, security teams should prioritize the remediation of such a risk.

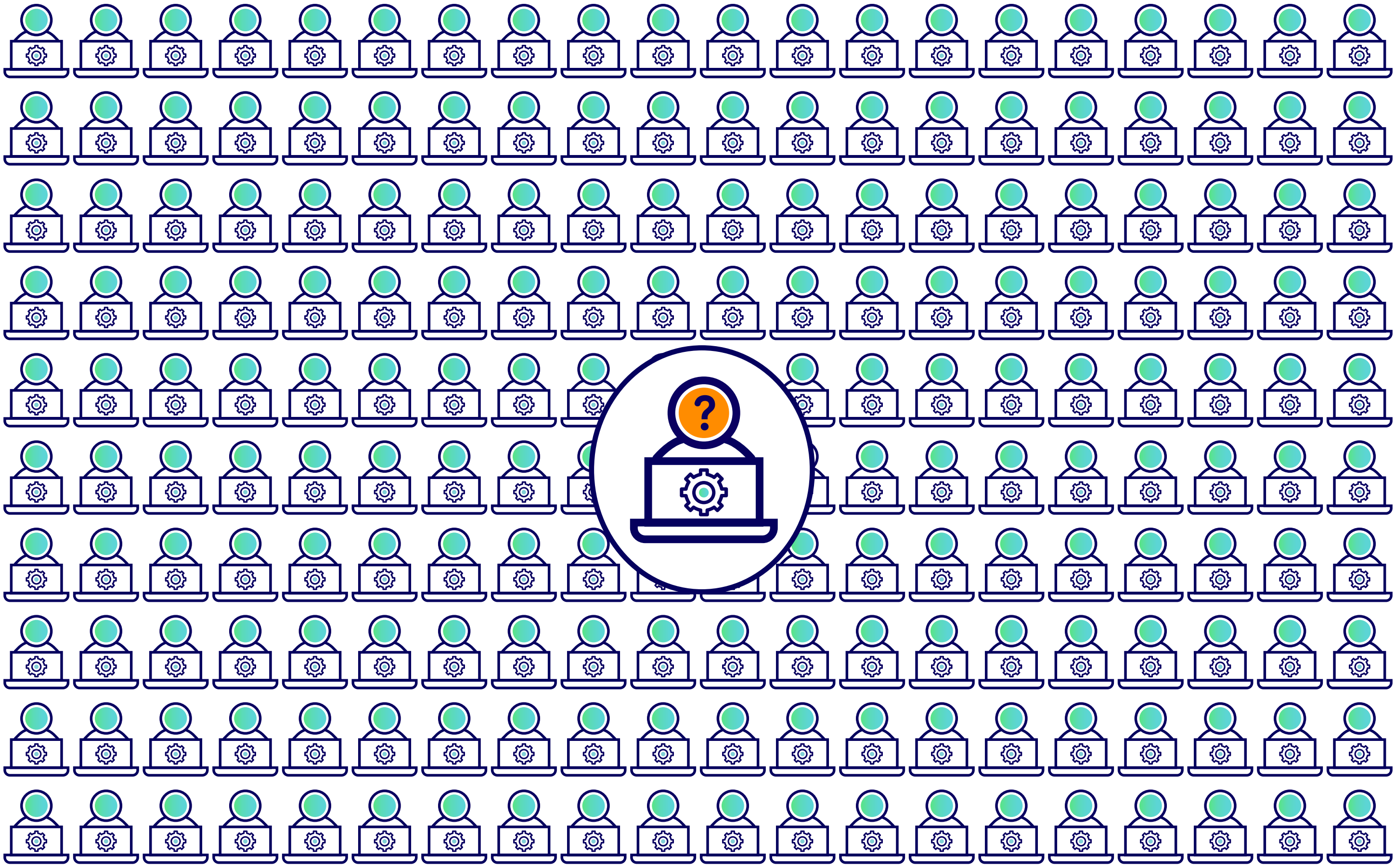


Figure 6: **1 in 200 local admins were completely unknown by the organization**

MISCONFIGURED IDENTITY RISKS

Misconfigured identity risks broadly embody what we refer to as "shadow admins." Just as shadow IT is defined by the deployment of IT systems beyond the visibility of IT admins, shadow admins are defined by users with permissions beyond the visibility of IT admins – permissions that could be used to escalate privileges. In our analysis of identity risks, Illusive discovered examples of misconfigured shadow admins in all organizations.

For example, in one instance with a healthcare organization, Illusive discovered a level 1 help desk employee responsible for resetting passwords who also had the level 3 permission to add domain admins. If this level 1 admin account was compromised, then an attacker could add their account as a domain admin to escalate their privileges. And frankly, we see these risks in many organizations.

Most significantly, 40% of shadow admin risks can be exploited in one step – if an attacker compromised one of these misconfigured identities, they would only need one entitlement, such as resetting the password of a domain admin, to elevate their privileges to a Domain Admin. This is low hanging fruit for attackers – it is easy to find and easy to exploit.

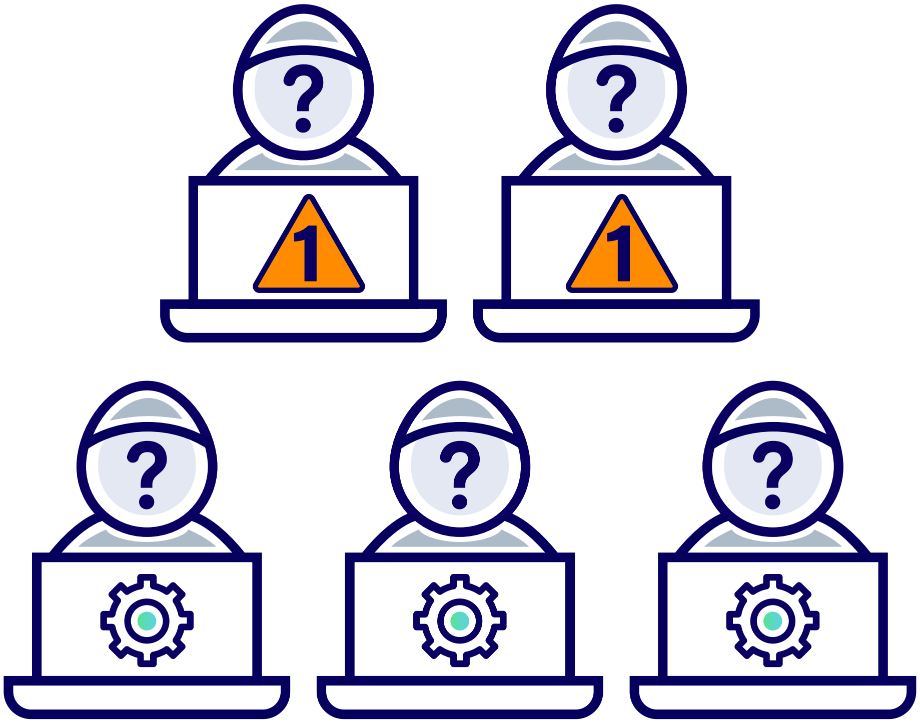


Figure 7: **40% of shadow admin risks can be exploited in one step**

MISCONFIGURED IDENTITY RISKS

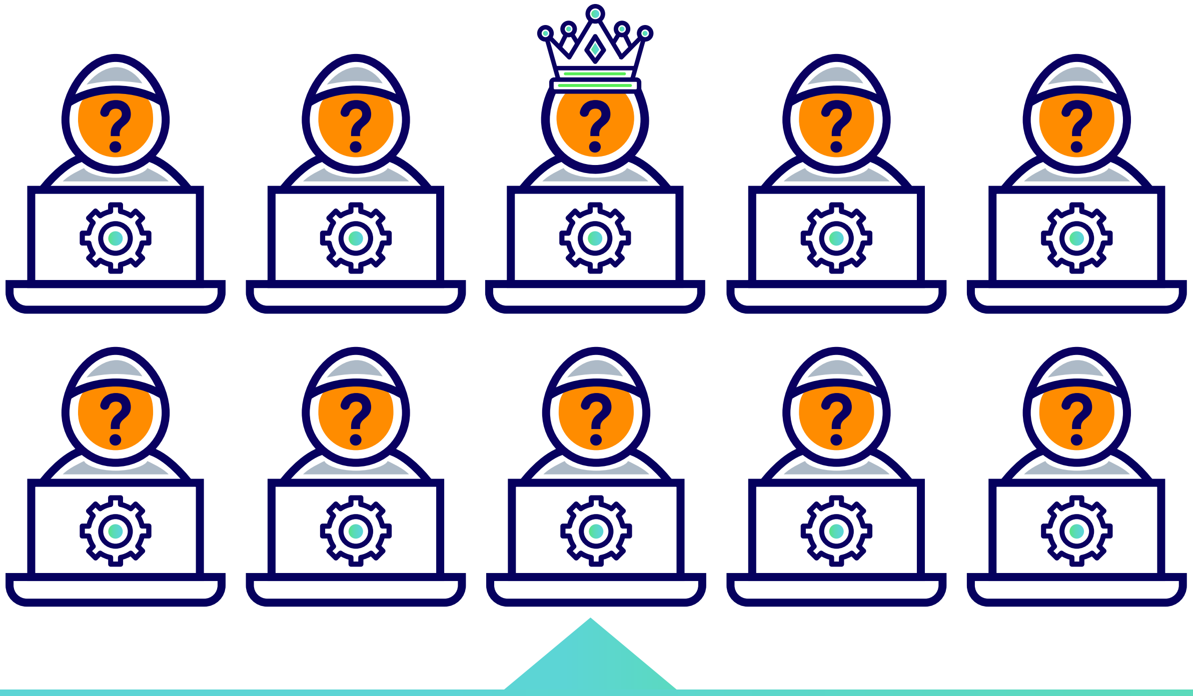


Figure 8: **13% of shadow admins have Domain Admin privileges**

A more concerning risk, although observed less frequently, are shadow admins with the ability to take over the entire domain – if privileged identities are the keys to the kingdom, then these are the kings of the kingdom. If an attacker compromises one of these shadow admins, there is very little that they cannot do.

The biggest risk, yet observed even less frequently, are shadow admins with Microsoft Active Directory DCSync permissions (1.7% of shadow admins have DCSync permissions). DCSync permissions are essentially the crown jewels of an organization – they provide the ability to copy the domain controller to create a new one or to sync between two controllers. It is the highest level of permission.

One other risk to note is that 1 in 50 shadow admins are regular users. This is a risk because they are even further removed from IT management (other shadow admins may at least be enrolled in privileged account management solutions). These could be users that began their career working in the IT department and were promoted into a new position, users that were inadvertently added to privileged groups, users that were temporarily granted permissions and forgotten, or users that were created from entirely unexpected means.

For example, in one instance with an online retailer, Illusive discovered a shadow admin named "Steve Rogers." If this name seems familiar it is because it is the alter-ego of Captain America. When we investigated this discovery further, we found that all of the Avengers (e.g., Tony Stark, Bruce Banner, etc.) were present as shadow admins. It turns out that these shadow admins had been created by a red team during a penetration test, but were never removed once the test was over. They existed in Active Directory for more than two years until discovered by Illusive.

EXPOSED IDENTITY RISKS

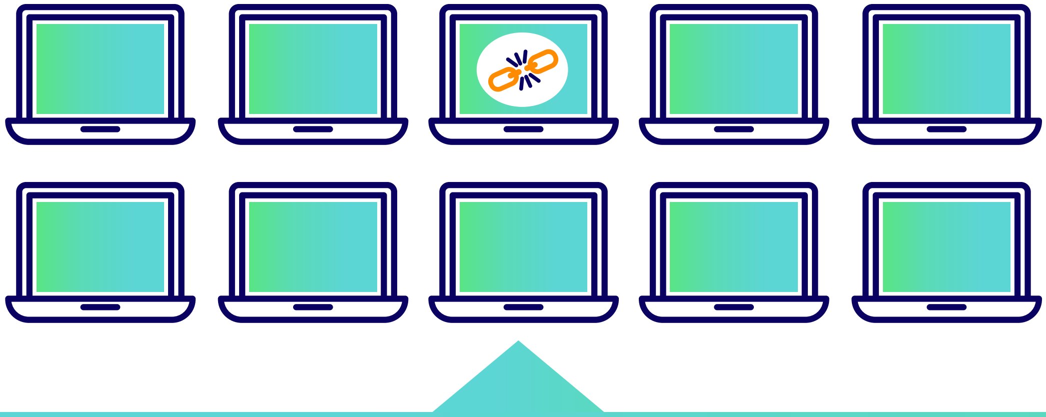


Figure 9: **Privileged account passwords are left exposed on 13% of endpoints**

Exposed risks include privileged identity information left accessible in cached credentials, in-app password stores, OS password stores and disconnected or "hanging" remote desktop protocol (RDP) sessions. These are the digital equivalent of leaving your username and password written on a sticky note, and there are a variety of tools that attackers utilize to dump these privileged credentials so that they can be exploited.

Unfortunately, more than 1 in 10 endpoints contain privileged account passwords that have been left exposed – it is one of the most prevalent identity risks. However, it is also one of the easiest identity risks to remediate; the exposed passwords just need to be removed from the endpoint.

Web browsers are one of the greatest sources of exposed identity risks. Cloud migration and remote work trends have resulted in the widespread adoption of software as a service (SaaS), but when privileged credentials become exposed in web browsers they often go unnoticed. Most privileged access management (PAM) solutions tend to overlook these risks. Yet threat actors have automated the collection and exploitation of these credentials, which spread across the domain at the speed of information. Within minutes, attacks could infect large portions of an organization.

Figure 10: **55% of exposed privileged identities are stored in browsers**

EXPOSED IDENTITY RISKS

One-third of exposed identity information is stored as "in-app" credentials, which also go unmanaged by PAM solutions. These credentials tend to be hard-coded in legacy applications, which exist outside of Active Directory. That means that any tool designed to audit Windows domains, such as Bloodhound, will miss one-third of exposed credentials. The remaining two-thirds of exposed credentials are from privileged Windows domain accounts.

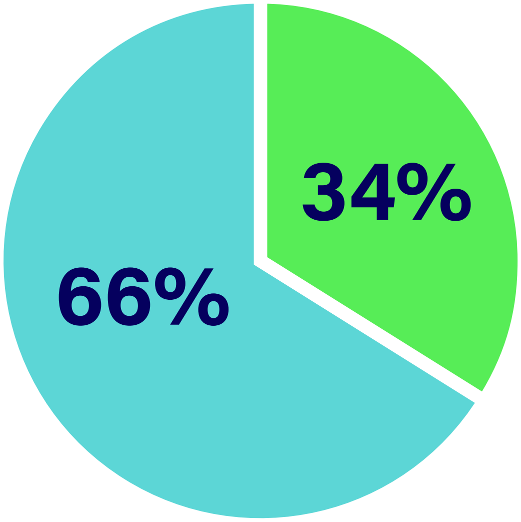


Figure 11: **34% of exposed identities are stored as "in-app" credentials; 66% of exposed credentials are from privileged domain accounts**

More than one-quarter of the exposed credentials from privileged Windows domain accounts are Domain Admins – again, these are the kings of the kingdom. If an attacker compromises an endpoint with an exposed Domain Admin account, then there is very little that they cannot do.

For example, in one instance with another financial services organization, Illusive discovered a Domain Admin service account with a password that had not been changed in more than 10 years. Even worse, this admin account credential was used by a software deployment agent, which left disconnected sessions exposed across the enterprise – every endpoint had the most privileged of accounts exposed.

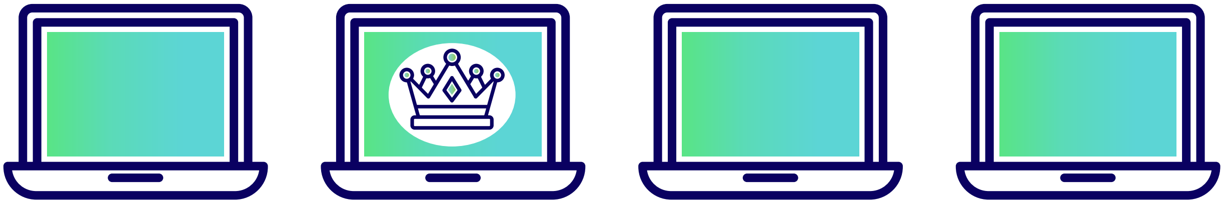


Figure 12: **26% of exposed privileged domain accounts are Domain Admins**

EXPOSED IDENTITY RISKS

Figure 13: **41% of exposed privileged domain accounts are shadow admins**

Furthermore, 41% of the exposed credentials from privileged Windows domain accounts are shadow admins. This is even more of a risk because shadow admins are generally unknown, which means other security controls won't be tuned to them, enabling attacks against them to remain undetected for longer.

This not only illustrates how these identity risks can overlap, but also how organizations struggle to obtain visibility into them. It is bad enough that shadow admins escape detection from existing identity management solutions, but finding them exposed means that they are actively in use. Organizations truly "don't know what they don't know" when it comes to these risks.

Finally, many of the exposed credentials from privileged Windows domain accounts had very stale passwords, which further illustrates how these identity risks can overlap. In fact, the age of the passwords for these exposed credentials is even older than the age of the local admin passwords we discussed at the top of this research, and the risk is just as significant.

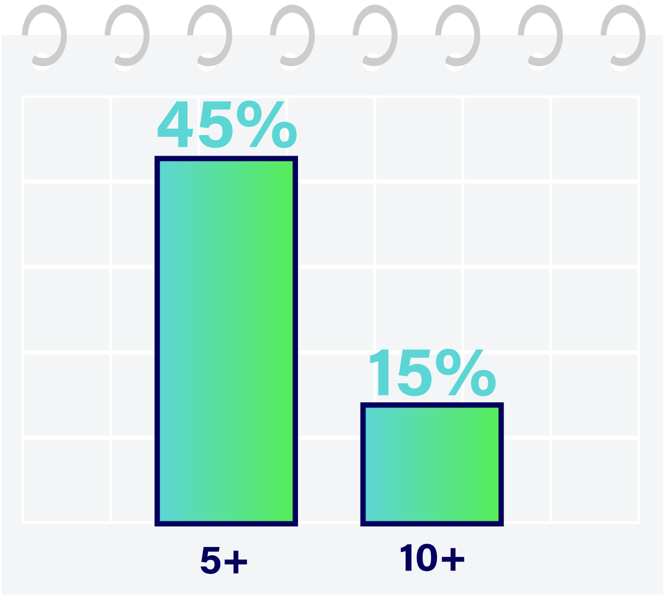


Figure 14: **A breakdown exposed privileged domain account password ages – 45% were unchanged for more than 5 years; 15% were unchanged for more than 10 years**

CONCLUSION - A Micro View of a Macro Problem

Every organization is vulnerable to unmanaged, misconfigured, and exposed identity risks. The number of identities which organizations have had to manage has dramatically increased, as businesses rely on growing numbers of systems and applications. Additionally, the constant change of identities and authentications to support the business, have led to massive complexities in both managing and securing identities. In an age where attackers have leveraged identity as their top vector of attack, even short exposures of privileged identities carry significant risk.

Most organizations seem to understand this risk since they have spent substantial time and effort managing identities and invested in the deployment of PAM and MFA solutions to protect their most privileged accounts. Despite this, they are unaware of the scale of identity risks that remain within their organization. While most organizations regularly scan for vulnerable code and applications, they do not scan for vulnerable identities.

The findings of this report help to explain the growing use of identity-based attack tactics by attackers in modern ransomware and other cyberattacks. The large number of gaps in security posture around identities, even at organizations with highly mature security practices, have simply made it easier for attackers to perform their crimes. Fundamentally, it is an issue related to visibility.

Even the most well-intentioned security teams can't mitigate identity risks unless they're aware of them. While some organizations have attempted to manage this risk by getting visibility through red team exercises, annual audits, scripts and spreadsheets, these have been vastly incomplete and therefore ineffective. Similar to how security teams manage vulnerabilities through the use of regular vulnerability scanners, these same teams need the ability to automatically and continuously scan for vulnerabilities in the identities used to run their business.

Ransomware attacks grab major headlines, but it can be much more difficult for organizations to gain visibility into their risk of an attack. Illusive is in a unique position to illuminate the identity risks that leave every organization vulnerable to attack when it conducts an Identity Risk Assessment.

This easy-to-execute remote assessment identifies critical vulnerabilities, including cached credentials, unmanaged local administrators, and shadow admins. These insights are invaluable in helping security teams make informed decisions around their risk to the top vector of attack – exploitable identities. Best of all, there is no cost and no obligation.

Contact Illusive today for a complimentary
Identity Risk Assessment

METHODOLOGY

From January 1, 2021 through December 31, 2021, Illusive analyzed a sampling of endpoints from the millions of endpoints on which Illusive is deployed. The sampling is from more than 25 organizations around the world, including some of the world's largest financial services, healthcare, and retail companies, with each sample ranging from approximately 1,500 to 75,000 endpoints each.

The Illusive AIR Team:
Lead Researcher – Tim Nursall
Lead Author – Clinton Karr

[1] https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

[2] https://www.idsalliance.org/wp-content/uploads/2020/05/Identity-Security-A-Work-in-Progress.pdf

[3] https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/

ABOUT ILLUSIVE

Illusive takes away the one thing attackers need to be successful – access to privileged identities.

Founded by nation-state attackers, Illusive protects customers against the attack vector exploited in all recent ransomware and targeted cyberattacks by discovering and automatically mitigating privileged identity risk. Illusive provides security teams with the visibility they need to prioritize risk mitigation efforts, enable zero trust initiatives, and avoid red-team embarrassments and audit findings.

Designed to beat attackers at their own game, Illusive's technology is trusted by the largest global financials and pharmaceuticals. Illusive has participated in over 140+ red team exercises and has never lost one!

Illusive Inc
1250 Broadway | Suite 2601
New York, NY 10001

Visit us: www.illusive.com
Email us: info@illusive.com
Find us: