XM Cyber | Cyentia Institute

NAVIGATING THE PATHS OF RISK

The State of Exposure Management in 2023

Table of Contents

Executive Summary

Ask anyone responsible for managing cyber defenses about their biggest pain points, and they'll likely mention being overwhelmed by fixing too many things and facing too many threats. As a result, the need to pinpoint and prioritize the most critical risks sits atop the wish list of many security leaders.

This is one reason why exposure management is receiving so much attention of late. In a nutshell, exposure management holistically evaluates all the ways attackers can compromise key information systems and spotlights the most likely paths to those assets. This allows your security team to focus on critical paths, effectively stopping attackers in their tracks.

Our second annual report[1] presents key insights drawn from tens of thousands of attack path assessments conducted through XM Cyber's exposure management platform during 2022. These assessments uncovered over 60 million exposures affecting 10 million entities deemed critical to business operations. Anonymized datasets were exported from the XM Cyber platform and provided to Cyentia Institute for analysis. We present highlights from that analysis below.

Key Findings

- **Only 2% of exposures lie on choke points leading to critical assets.** Focusing on these maximizes risk reduction while minimizing remediation workload.
- **Techniques targeting credentials and permissions affect 82% organizations** and constitute over 70% of all identified security exposures.
- Organizations typically have **11,000 security exposures attackers could exploit,** and some larger enterprises have over 20x that number!
- **Attackers can access 70% of critical assets in on-prem** networks in just 3 steps. It's even worse in the cloud, where 90% of critical assets are just one hop away from initial compromise.
- **7 in 10 firms are vulnerable** to prominent remote code execution vulnerabilities, but these vulnerabilities collectively exploit less than 3% of critical assets.
- On the positive side, **75% of exposed resources lead to dead ends** that can't reach critical assets. Deprioritize these and focus on the exposures that have attack paths to critical assets.
- **71% of firms have exposures that enable attackers** to pivot from their on-prem to cloud environment. Once there, 92% of critical assets lie just one hop away.
- Endpoint detection and response capabilities **cover fewer than half of all devices in 38% of firms.**

[1] Download the 2021 Attack Path Management Impact Report: https://info.xmcyber.com/attack-path-management-impact-report

A Primer on Attack Paths

Organizations face a constant threat of cyber attacks that can jeopardize their critical assets. Attack paths are the most common way that attackers use to penetrate enterprise defenses. Many organizations, however, rely on tools that are narrowly focused on certain types of exposures, such as unpatched vulnerabilities.

This approach is flawed because attackers do not see networks and systems as individual exposures. Instead, they leverage a combination of vulnerabilities, misconfigurations, overly permissive identities, and other security gaps to move across environments and reach target assets. This route is called an attack path, and attackers can remain hidden inside networks for weeks or months, causing significant and ongoing damage.

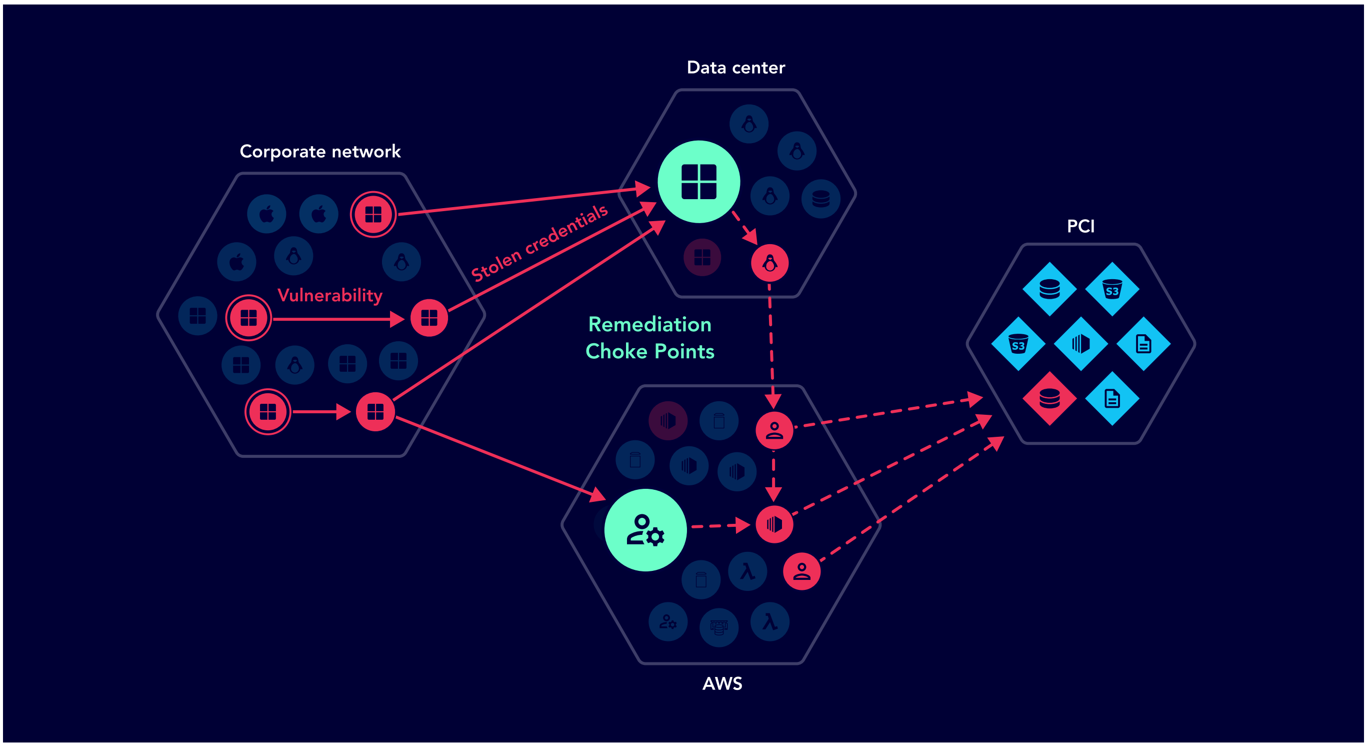


***Figure 1:** Example attack graph showing paths toward critical assets*

The attack graph depicted in Figure 1 shows possible attack paths toward enterprise assets, with the green circles representing choke points—key junctures where multiple attack paths converge toward critical assets. Focusing defenses on such choke points allows for efficient reduction of risk for the organization.

At XM Cyber, we believe that understanding the relationship and context of attack paths toward critical assets is essential to mitigating risk. By visualizing all possible attack paths on an attack graph, we can quickly and accurately remediate issues by focusing on the most critical exposures that converge on choke points, thereby making all exposures leading to choke points less critical as they can't lead an attacker to critical assets. This approach enables productive remediation that reduces risk in the most cost-efficient manner.

Lessons From a Year of Attack Path Assessments

A typical organization has **11,000** exploitable security exposures in a given month.

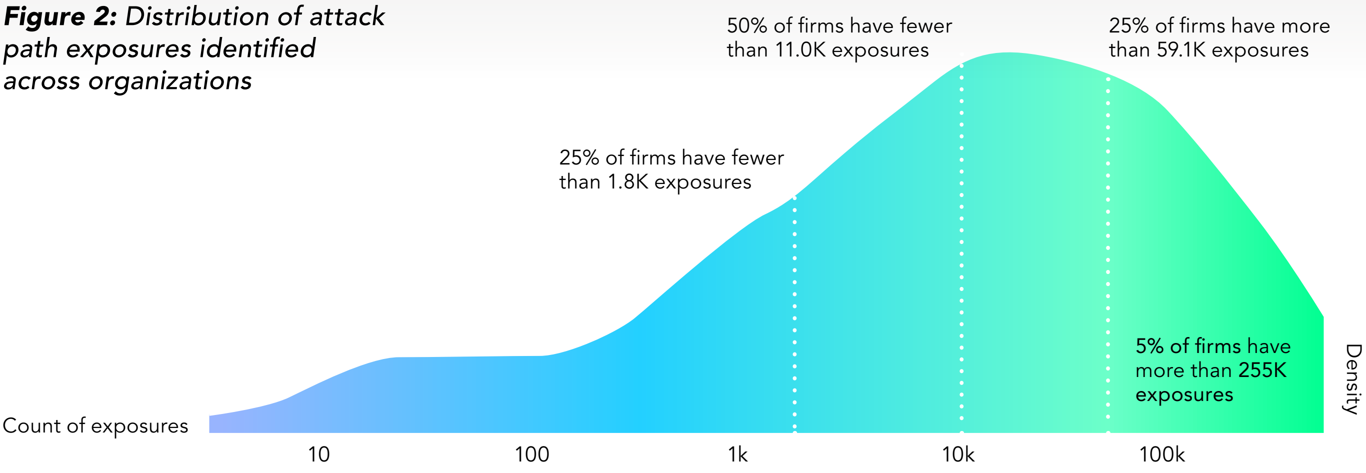
Organizations are overwhelmed by security exposures

For many organizations, cybersecurity devolves into a never-ending game of whack-a-mole. Security exposures pop up; security teams knock out as many as they can as quickly as possible, and all the while, new issues continue to emerge. And contrary to the talk track of many industry thought leaders, it's the volume rather than the vigor of cyber threats that overwhelm most security programs.

We're not in the business of making empty claims, so let's quantify that volume based on what XM Cyber has observed across its customers over the last year. The typical organization has 11,000 exposures that attackers could leverage to compromise assets. And the top 5% of firms—mainly larger enterprises—contend with over 20x that number! This includes unpatched vulnerabilities, system misconfigurations, mismanaged credentials, inadequately protected resources, and a host of other security issues.

Larger enterprises can have over **250,000** open exposures.

***Figure 2:** Distribution of attack path exposures identified across organizations*



Exposure: Any combination of a vulnerable resource and credible threat technique along an attack path. Identifying which exposures represent the most risk to critical assets is the core concept behind exposure management.

Research shows that the typical organization can only address about 10% of the vulnerabilities in their environments in any given month[2]. Since firms are better equipped to address vulnerabilities than the broader array of security exposures identified in attack path analysis, the true remediation ratio is almost certainly even lower. The good news is that organizations don't need to fix them all—at least not with the same priority. We explain why in the next section.

Research shows firms only fix **10%** of their vulnerabilities.

> *Many organizations have too many assets on their network to identify the key risk points, or even to map their assets. This makes it difficult to assess where and how much money should be spent. Without a way to clearly map risks to value-creating assets or processes, as well as a plan of action arising from this, it is hard to quantify and justify the resources that should be allocated to mitigating them."*
>
> *World Economic Forum Global Cybersecurity Outlook 2023*

XM Cyber Takeaways & Recommendations

From our results, it's clear that organizations need a way to better prioritize remediation efforts to reduce risk more efficiently. The problem is that too many get distracted by less important issues while completely overlooking those that matter most. For example, we often discover powerful administrators and Group Policy Objects that are vulnerable to exploitation as well as low-level admins that can do privilege escalations to gain full administrative rights. The priority of such exposures (and many others) won't become clear without seeing things through an adversary's eyes using attack path analysis.

[2] Cyentia Institute: https://www.cyentia.com/p2p-vol3-wade/

Most security exposures don't represent a critical risk

Many looking to assess cyber risk begin with the conceptual "equation" of Threat × Vulnerability × Impact. While too simplistic to actually quantify cyber risk[3], it does, at least, include some key factors to evaluate. It also points to the fact that risk is minimized as any of these factors approach zero.

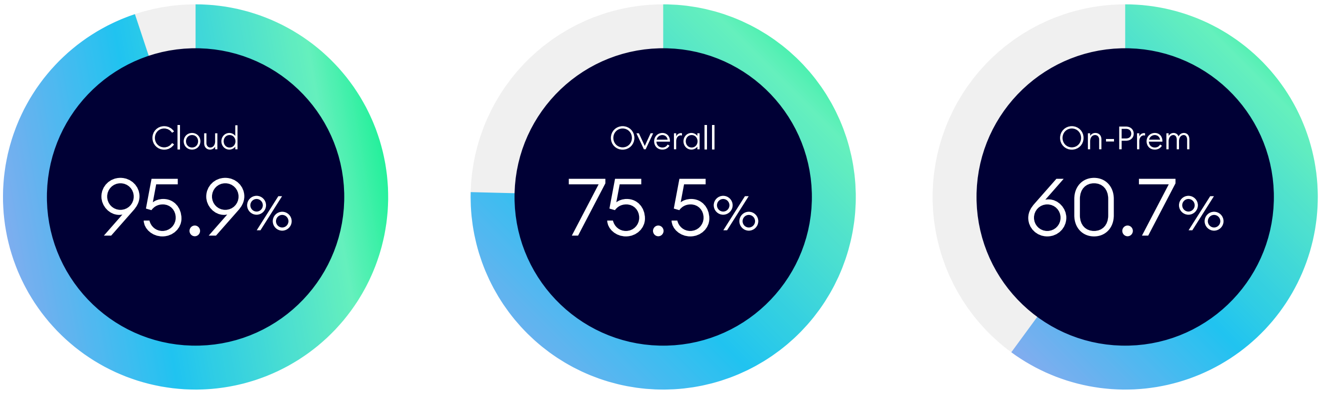
We've already shown that vulnerability is decidedly NOT zero. Organizations have a multitude of security exposures that make them vulnerable to attacks. But what about the other two factors, threat and impact? Our attack path analysis offers insight into these.

On the threat side of the equation, we confirmed an average of 39 unique techniques in each firm that attackers could leverage to compromise assets. That may not seem like much until one realizes those techniques multiply into complex attack paths through myriad vectors. Deterrence is a possible strategy, but there's not a lot the typical organization can do to stop attackers from attempting to use those techniques against them. Thus, zeroing out the threat component of risk is a dubious proposition.

Each organization is susceptible to an average of **39** different attack techniques.

75% of exposures lead to dead ends that can't reach critical assets.

Figure 3: *Proportion of attack paths that lead to dead ends*



[3] Factor Analysis of Information Risk (FAIR) is better suited to that purpose: https://www.fairinstitute.org/what-is-fair

That leaves impact. All organizations have critical information assets that, if compromised, would cause major operational and financial impacts. Those assets obviously can't be eliminated, but threats and vulnerabilities that don't jeopardize them can be effectively "zeroed out" (deprioritized) so that security teams can focus on the most damaging exposures. Our analysis finds that three out of four exposures along attack paths lead to "dead ends" that cannot impact critical assets and therefore represent minimal risk.

As seen in Figure 3, dead ends tend to be more prevalent in cloud than on-premises environments. This has much to do with a combination of two factors. First, many cloud identities tend to be powerful in the sense that they have broad access to resources within the account. Second, many of those resources are not critical assets, which creates more dead ends.

Threats and vulnerabilities that don't jeopardize critical asssets can be effectively **"zeroed out".**

Dead End: An isolated exposure that can't be used by attackers to compromise critical assets. Fixing dead ends will not lead to significant risk reduction and comes with high opportunity costs.

XM Cyber Takeaways & Recommendations

In the previous section, we saw that organizations cannot realistically remediate all exposures in their environment. That means they must prioritize those that represent the most risk and deprioritize those that do not. Unfortunately, the security industry tends to over-rate everything as "critical," while offering very little to help organizations determine whether a risk can be safely ignored, delayed, or otherwise deprioritized.

Part of that challenge is that it's difficult to rule out the possibility that threats and vulnerabilities can negatively impact the organization. This is where seeing the adversary's perspective through attack path analysis is so valuable. We're able to determine that the necessary preconditions for exploiting certain paths do not exist (and know if that changes in the future). It's a lot easier to find the needle when the haystack is much, much, smaller.

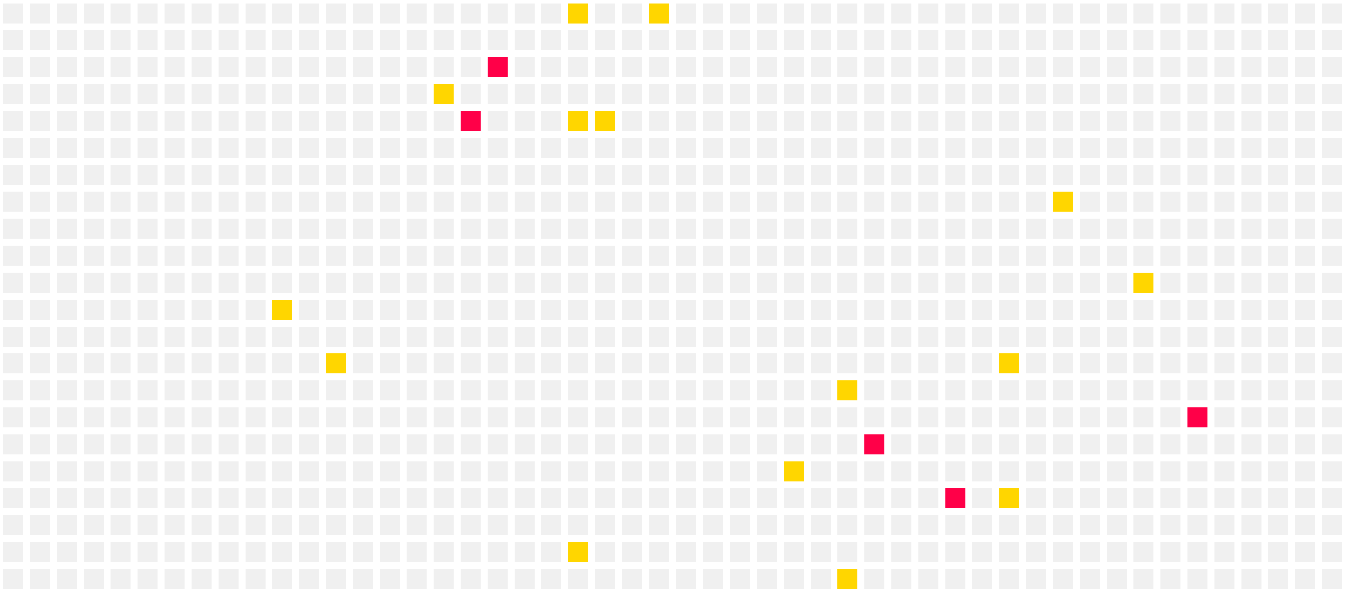
Attack path analysis enables ultra-efficient remediation

Earlier, we saw that the typical organization has 11,000 security exposures that attackers could exploit. These are denoted by the squares in Figure 4, each of which represents 10 exposures. The vast majority of exposures are dead ends or don't put critical assets at risk, which is why we've grayed them out.

About 2% (~200) of these exposures are located on choke points - entities through which multiple attack paths converge en route to critical assets. These "choke points" are colored yellow and red (we'll get to the distinction in a moment). If you're looking for quick wins to reduce substantial risk, these offer compelling focal points.

Organizations can practically **eliminate all attack paths to critical assets by remediating just 2% of exposures** that lie on choke points.

Figure 4: *A depiction of the ratio of exposures on choke points (yellow and red squares) among all exposures (gray squares) in the typical attack surface*



Choke Point: A key entity where multiple attack paths converge before reaching critical assets. Fixing choke points exposures cuts off multiple attack paths at once, resulting in significant risk reduction.

But wait—it gets even better! Our analysis reveals that about one in four choke points exposes 10% or more of the critical assets in the environment (red squares). In other words, these exposures put attackers on the fast track to causing major harm to the organization. Prioritizing these "game over" choke points represents a minimal effort, maximum effect approach that equates to a whopping 99.6% reduction in the scope of remediation!

But how do you identify the subset of truly critical points amid the throng of 11,000 ways threats may impact your organization? XM Cyber does exactly that with attack path analysis. You can continuously see your hybrid network through the eyes of an attacker and shore up the riskiest routes of an attack before they happen.

One in four choke points exposes **10%** or more of the critical assets.

XM Cyber Takeaways & Recommendations

Gartner® recommends[4] that organizations should "establish regular repeatable cycles as part of your continuous threat exposure management program, with each cycle adhering to a five steps process — scoping, discovery, prioritization, validation and mobilization — thus guaranteeing consistent threat exposure management outcomes." Together, dead ends and choke points identified through attack path analysis are the yin and yang of exposure management.

Identify and ignore dead ends to reduce workload. This will free up resources to focus on choke points for remediation. Start with the highest priority choke points that represent the largest potential impact to critical assets and work backwards from there. This, of course, is not a one-time act. In complex and ever-changing environments, organizations must have a continuous approach to exposure management.

[4] Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program, 21 July 2022, Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Attack paths are abundant – and short

The efficiency gains highlighted in the last point are amazing, but exposure management isn't just about reducing workload for defenders. It's also about making attackers work harder to accomplish their goals. As it stands, you might be surprised how easy it is for them to succeed.

Terms like "advanced" and "persistent" are often used to describe modern cyber threats. But do you want to know the cold, hard truth? Threat actors don't work any harder than they have to, and most find success using attacks more aptly described as "simple" and "short."

In support of this claim, we uncovered valid attack paths to critical assets in all organizations. Since our methods mimic those used by attackers, it's reasonable to assume attackers can find a route to exploit just about any target, provided they do their homework and are sufficiently motivated.

Hops: Steps taken by attackers from the point of initial foothold to compromising critical assets. Hops consist of various techniques used to exploit vulnerable resources, which become the staging ground for the next hop.

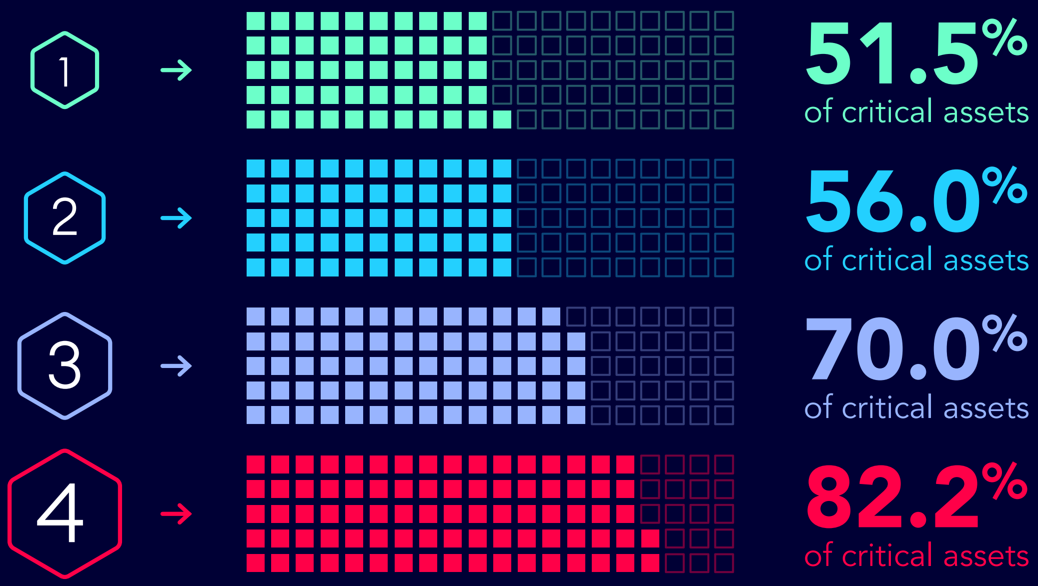


Figure 5: *Scope of critical assets at risk with each additional hop along on-prem attack paths*

But it's not merely that vulnerable paths exist—it's what they lead to that's most concerning. Just over half (52%) of critical assets are reachable with a single hop from the initial access point. A couple more hops put 70% in reach, and by four hops in, attackers can compromise 82% of critical assets in corporate on-prem networks.

This broadening of access as attackers progress deeper into the enterprise is depicted in Figure 5. The moral of the story is simple: more hops = more harm. Identifying the early-stage footholds in attack paths will dramatically lower the potential scope of compromise.

In the typical organization, credible attack vectors exist for **90%** of critical assets.

Attackers can access **70%** of critical assets in on-prem networks within just 3 steps.

How do attack paths in cloud environments compare to those in on-prem environments?

Glad you asked—we're headed there next!

XM Cyber Takeaways & Recommendations

The low number of hops required to compromise high percentages of systems is alarming. But there are some root issues that heavily contribute to this state of affairs and make it increasingly easy for attackers to succeed. You can get a view of the top techniques used by attackers to compromise on-prem networks in Appendix A, and we'll discuss these in more detail in an upcoming section.

By analyzing these common techniques and how they combine to form attack paths, defenders can make it more challenging for adversaries to infiltrate systems. As discussed in prior sections, removing choke points that put adversaries on the fast track to critical assets is a key strategy for practically accomplishing this.

You can't protect the cloud without protecting on-prem

Most organizations use cloud-based infrastructure or services to some degree these days. This trend gives us ample opportunity to analyze attack paths to and within major cloud platforms. First off, it's clear that attackers able to successfully compromise corporate networks likely won't find it difficult to expand their access to other environments. We detected exploitable attack paths from on-prem to cloud platforms in 71% of organizations.

Comparatively, Amazon Web Services (AWS) offers the fewest opportunities for attackers to migrate to the cloud (47% of firms), Microsoft Azure is slightly more susceptible (80% of firms), and Google Cloud Platform (GCP) falls square in the middle of that range. There are many plausible explanations for this difference, but a big driver is how these platforms tend to be used. Azure has a larger user population in most enterprises due to extensive SaaS offerings (e.g., Microsoft 365), whereas AWS is generally more restricted to DevOps staff. There's also more connectivity between on-prem and Azure environments in most enterprises because of Active Directory (AD) integration. This results in more opportunities for actors to move from on-prem to cloud.

71%

of firms have exposures that enable pivoting from on-prem to cloud.

After accessing cloud environments, **92%** of critical assets lie just one hop away.

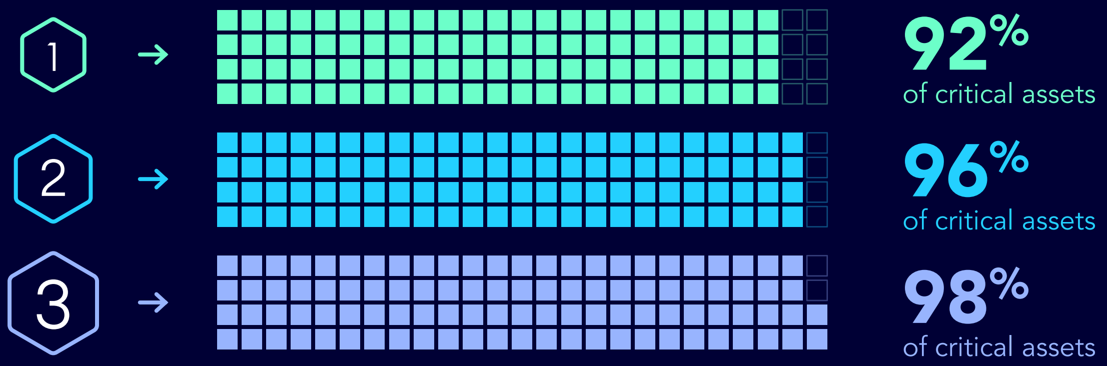


Figure 6: *Scope of critical assets at risk with each additional hop along cloud attack paths*

Pivoting from on-prem networks isn't the only way attackers infiltrate cloud platforms. On average, almost half of firms (48%) have public-facing virtual machines that expose critical assets. This makes the process of gaining an initial foothold in the cloud even easier.

Regardless of the initial access vector, attack paths in the cloud tend to be much shorter than on-prem. We found that an average of 92% of assets hosted by firms in the cloud can be compromised in a single hop! And for this statistic, there's no significant difference across the big three cloud platforms.

48%

of organizations have public-facing virtual machines that expose critical assets.

XM Cyber Takeaways & Recommendations

Organizations face tough challenges in managing their diverse on-prem and cloud environments. Part of that struggle stems from failing to consider the big picture and only focusing on each piece in isolation. This creates gaps in security, which are exemplified by the statistics in this section. Half of organizations expose assets through public-facing VMs and the majority of them have holes attackers can use to pivot between on-prem and cloud environments.

Once attackers infiltrate cloud environments, it's very easy for them to compromise assets. Part of the challenge is that cloud security is not yet mature and many security teams don't fully understand what security issues to look out for. Challenges also arise from how cloud identities and permissions are (mis)managed. We need to rethink our approach to security to ensure that we are protecting all of our identities, systems, and interdepencies among them holistically.

Wondering how attackers hop around cloud environments so quickly?
That's definitely top of mind for us as well, and we dig into the top techniques in the next section.

Top attack techniques in 2022 reveal common themes

Understanding potential attack techniques is essential to exposure management because they are the building blocks of attack paths. Multiple techniques strung together create an attack vector, and multiple vectors comprise an attack path. The XM Cyber platform generates and tests many combinations of techniques to identify valid paths to critical assets.

Techniques targeting credentials and permissions **affect 82%** of organizations and **constitute 72%** of all identified security exposures.

How are techniques used in attack paths?

The example attack path below started from a random workstation machine in the on-prem environment. After exploiting some credentials issues in the enterprise environment, we were able to pivot into the cloud (Azure environment) by harvesting valid Azure access tokens (claimed with MFA). Once the Azure recon phase was complete, we were able to escalate our privileges and finally compromise an Intune (Azure MDM solution for managing devices) Administrator User. By abusing the permissions of that user, we could execute code back on the enterprise machines that he managed. Continued lateral movement would have led to the compromise of the entire enterprise environment.

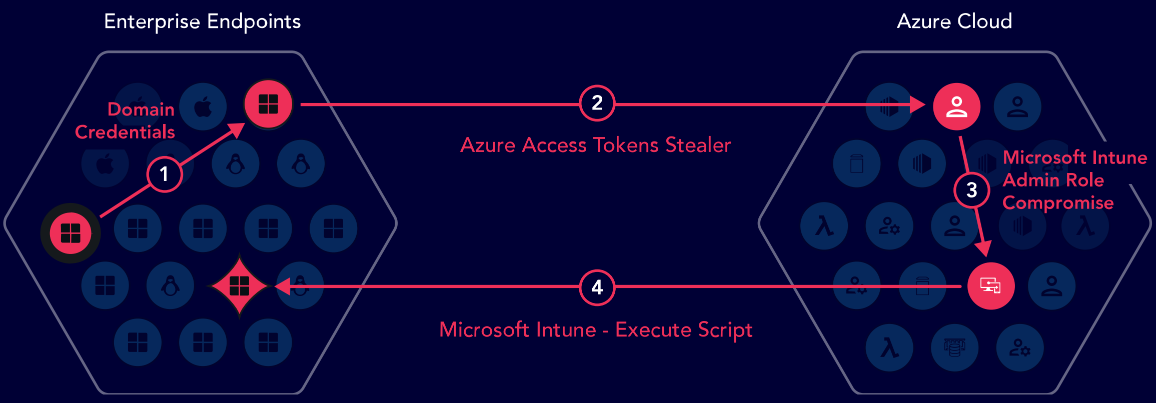

Enterprise Endpoints
Azure Cloud
Domain Credentials
1
2
Azure Access Tokens Stealer
3
Microsoft Intune Admin Role Compromise
4
Microsoft Intune - Execute Script

Figure 7: *Example attack vector consisting of multiple techniques*

It's important to know two things about attack techniques we discuss in the following sections. First, adversaries can use the same techniques multiple times across many attack vectors, greatly amplifying their total number of options available to them. Second, our analysis verifies that all conditions exist for attackers to successfully exploit these techniques in the target environment.

With that said, let's examine the top techniques observed by XM Cyber during attack path analyses conducted in 2022. We focus here on key themes or categories of techniques, but you'll find detailed listings of techniques for on-prem, Azure, AWS, and GCP in Appendix A.

As measured from the proportion of organizations affected, attack path techniques targeting network and IT services are the most common themes overall. Frequently observed techniques in these categories include proxy spoofing, DHCPv6 DNS poisoning, exploits against Windows Server Update Services, dumping and using private SSH keys, and hijacking SSH sessions. It's noteworthy that these technique categories are decidedly less dominant when you measure the percentage of detected exposures they potentially exploit. In other words, they offer attackers broad but relatively shallow use.

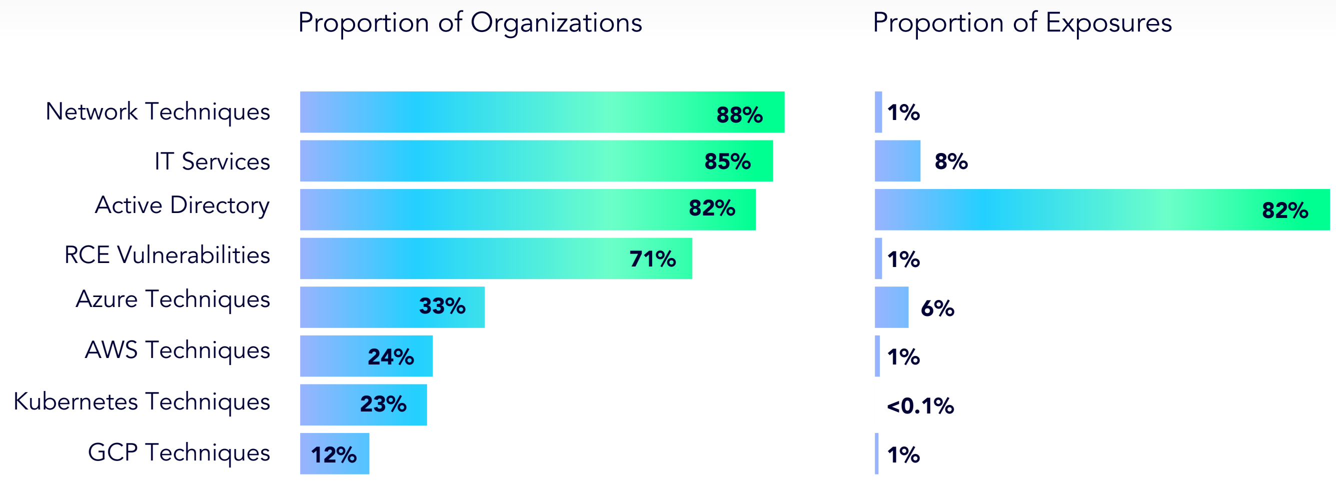


***Figure 8:** Categories of techniques targeting exposures identified by attack path analysis*

Techniques that target AD and misappropriate user credentials are also very common (82% of organizations). What's more, these techniques are able to exploit 72% of all identified security exposures! That's important enough to warrant additional analysis, so we'll leave it be for now and pick up this AD thread in a dedicated section to follow.

Exploits of prominent remote code execution (RCE) vulnerabilities in the CVE List were observed in 71% of firms but associated with just 0.7% of exposures. That points to a common misconception about exposure management—that it's all about patching vulnerabilities. While patching is absolutely a core component of security operations, there's a lot of risk exposure that falls outside that scope. We explore this further and provide more details about those CVEs in the next section.

And that brings us to the top techniques targeting each of the three major cloud platforms and Kubernetes. Their prevalence across organizations is, of course, largely dependent on which are more widely used. In terms of total exposures, Azure offers the largest attack surface for the same reasons we mentioned earlier (larger user population and deeper AD integration).

XM Cyber Takeaways & Recommendations

We find that many security teams overlook attack paths that leverage credentials and permissions. It's also a common misconception that implementing a zero trust architecture is sufficient to protect against all techniques that exploit forms of trust. These results, however, make it clear that attackers prey upon trusted administrative services and identities.

Attack paths exploiting AD are of particular concern because they represent a huge attack surface. The relationships within AD can be highly complex and difficult to understand. It's crucial that organizations pay close attention to AD exposures and not solely rely on zero trust security measures.

Exposure management goes far beyond vulnerabilities

In the prior section, we saw that the majority of organizations (but a small minority of exposures within them) have active attack paths that exploit known vulnerabilities (CVEs). This is particularly interesting because XM Cyber is not a traditional vulnerability scanner that seeks to identify all unpatched vulnerabilities across the enterprise. In general, our attack path analysis looks for vulnerabilities that involve remote code execution and are widely exploited by attackers. Research puts the percentage of published CVEs exploited in the wild at about 6%.[5]

The top vulnerabilities identified through XM Cyber's attack path analysis are shown in the chart below. The infamous "PrintNightmare" exploit (CVE-2021-34527) reigns supreme across all four measures, affecting 54% of organizations, 0.5% of total exposures, and about 3% of all critical assets and choke points. A patch for this CVE has existed for some time, but there are some registry key configurations that make the patch irrelevant. Text4Shell and Log4j exploits also rank high on the list in terms of vulnerable organizations and assets.

71%
of firms are vulnerable to prominent remote code execution vulnerabilities.

These vulnerabilities collectively exploit less than
3%
of critical assets.

Figure 9: *Top vulnerabilities identified by attack path analysis.*

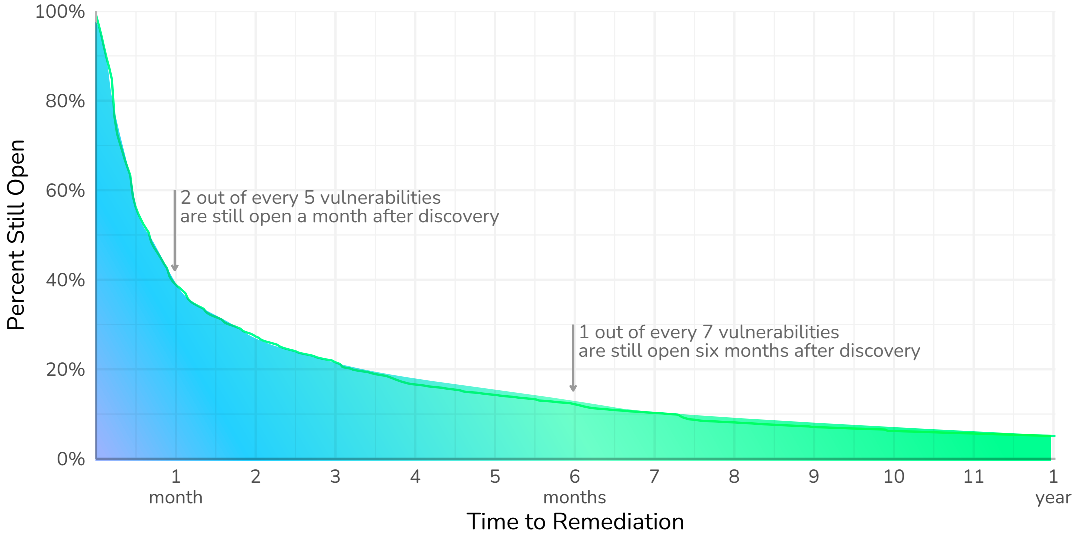
	Organizations	Exposures	Critical Assets	Choke Points
PrintNightmare - Windows Print Spooler (CVE-2021-34527)	54.2%	0.5%	2.8%	3.3%
Text4Shell Vulnerability	42.7%	0.0%	2.6%	0.1%
UltraVNC Vulnerabilities (CVE-2019-8277)	18.8%	0.1%	0.2%	0.6%
Log4j Vulnerabilities	33.3%	0.0%	2.6%	0.1%
DejaBlue	28.1%	0.0%	0.5%	0.0%
EternalBlue (CVE-2017-0144)	18.8%	0.0%	0.2%	0.0%
Follina - Microsoft office (CVE-2022-30190)	25.0%	0.0%	0.0%	0.1%
SMBGhost (CVE-2020-0796)	16.7%	0.0%	0.5%	0.0%
aPAColypse (CVE-2017-11907)	18.8%	0.0%	0.0%	0.0%
Spring4Shell - CVE-2022-22965	20.8%	0.0%	0.7%	0.0%
BlueKeep (CVE-2019-0708)	17.7%	0.0%	0.1%	0.0%
LNK Exploits	21.9%	0.0%	0.0%	0.0%
ProxyNotShell RCE (CVE-2022-41040 and CVE-2022-41082)	13.5%	0.0%	0.4%	0.0%
NoPac (CVE-2021-42278, CVE-2021-42287)	8.3%	0.0%	0.3%	0.0%

Scanning over the rest of the top vulnerabilities, one may wonder why CVEs published back in 2017 (e.g., UltraVNC, aPAColypse) still enable valid attack paths 5+ years later. The simple answer is that it can take a surprisingly long time to remediate vulnerabilities in enterprise environments.

[5] Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights.

The chart below applies a technique called survival analysis to project how quickly organizations remediate these vulnerabilities based on data provided by Kenna Security[6]. About 40% of vulnerabilities remain open a month after discovery and 5% persist for longer than a year without being remediated. And keep in mind that these are critical vulnerabilities that have known exploits and should receive priority attention!

Figure 10: *Survival analysis of vulnerabilities identified by attack path analysis*



Obviously, improving the speed at which these (and other) vulnerabilities are remediated would reduce exposure. But let's not lose sight of a critical point made in the previous section: exploiting CVE-based vulnerabilities is only one category of techniques attackers employ to infiltrate target organizations and compromise critical assets. Exposure management must address all attack vectors, particularly those on an attack path toward critical assets. We'll examine the most common issues (identities, credentials, and permissions) in the next two sections.

XM Cyber Takeaways & Recommendations

In terms of overall risk to critical assets, exposures associated with CVE-based vulnerabilities are dwarfed by those involving compromised identities and credentials. That doesn't mean vulnerabilities shouldn't be patched…but it absolutely does mean that protecting critical assets requires a much more holistic approach to exposure management. This includes misconfigurations, mismanaged credentials, excessive permissions, user behaviors, etc. These things, along with vulnerabilities, comprise your exposed attack surface.

[6] See survival analysis applied to a broader array of CVEs and specific platforms in Prioritization to Prediction Vol. 5

Active Directory is the Achilles' heel of exposure management

The preponderance of AD and other identity and access management issues is hard to ignore (72% of all exposures!). As are the findings of a five-year study[7] of extreme cyber events that pointed to credential-related attacks as the most common and costly technique used by attackers.

Active Directory is a prime target in such attacks because it offers a veritable treasure trove of credentials for privilege escalation and lateral movement. This is why credential dumping and domain credentials rank high on the list of top Active Directory attack techniques in the chart below. Tools like Mimikatz make this all-too-easy to execute and are extremely popular (as the "Groups" and "References" sections on the MITRE page attest).

80%
of organizations are vulnerable to credential dumping techniques.

Figure 11: *Top Active Directory techniques identified by attack path analysis*

	Organizations	Exposures	Critical Assets	Choke Points
Credential Dump	80.2%	2.7%	7.3%	4.3%
Reset User Password	76.0%	18.8%	3.2%	3.5%
Domain Credentials	75.0%	2.7%	7.0%	15.7%
Resource-Based Constrained Delegation	76.0%	8.5%	3.6%	7.9%
Add Logon Script	76.0%	18.7%	2.8%	3.8%
Add Members to Group	77.1%	14.8%	2.1%	0.5%
Credentials Relay	58.3%	0.4%	3.1%	4.2%
Member Of Group	72.9%	6.7%	2.9%	0.4%
Add ACE to OU	66.7%	0.9%	2.9%	0.0%
Change the GPO Path	58.3%	0.3%	0.5%	0.1%

[7] The Cyentia Institute

It's never a good thing when credentials are abused through techniques like those listed in Figure 11. But it's so much worse when those credentials gift attackers far more access than necessary for legitimate use. The concept of "least privilege" is one of the oldest in the infosec field, prescribing that users and computers shouldn't have more permissions than necessary for their functions. That's easier said than done, which is why some say "least practiced" would be a more fitting term. Our data suggests they might be right.

About one in five (22%) of organizations grant elevated privileges to at least half of their user population. Even more concerning, greater than half of the computing devices in over a third (36%) of the organizations have sufficient privileges to access critical assets if compromised. You don't have to be a mathlete to know those numbers don't equate to least privilege, or, the more current en vogue term, Zero Trust principles.

36%
of firms grant permissions enabling at least half of their devices to access critical assets.

XM Cyber Takeaways & Recommendations

AD is a critical, yet highly complex, component in almost every organization. As a result, the attack surface associated with AD can be extensive and pose a substantial risk to critical assets (as evidenced by these findings).

Unfortunately, AD issues can be challenging for organizations to understand and solve. This leads to their being overlooked or under-prioritized, while attackers take advantage of them on a daily basis. It's therefore crucial to protect credentials and prioritize efforts to shore up AD security. These lessons[8] shared by Microsoft's Detection and Response Team should help get you started.

[8] Total Identity Compromise: DART lessons on securing Active Directory

Organizations are too lax with local credentials

Dumping credentials and exploiting excessive permissions are standard techniques in attackers' repertoires, and most security teams at least have them on their radar. Something that often flies under the radar, however, is the propensity for credentials to be cached and/or stored locally. Granted, doing this is sometimes necessary for administrative purposes. But, in our experience, administrative credentials have a tendency to scatter well beyond their intended scope.

We'll start with some observations around cached credentials. We identified highly privileged users whose credentials were cached on multiple machines in 76% of organizations. On average, 12% of Active Directory users have cached credentials on more than one machine. Of those, about 10% have admin-level permissions on 100 or more devices. Perhaps a few specialized organizations need that level of broad access, but most simply aren't aware of the issue at all.

Let's focus on local credentials, which are generally a far riskier issue—yet relatively easy to solve. We identified local credential issues in two-thirds of organizations. A quarter of organizations (26%) have what we suspect are "golden image" issues, whereby local credentials may be unwittingly replicated to devices or virtual machines when new instances are deployed from the image.

In **76%** of organizations, we identified highly privileged users whose credentials were cached on multiple machines.

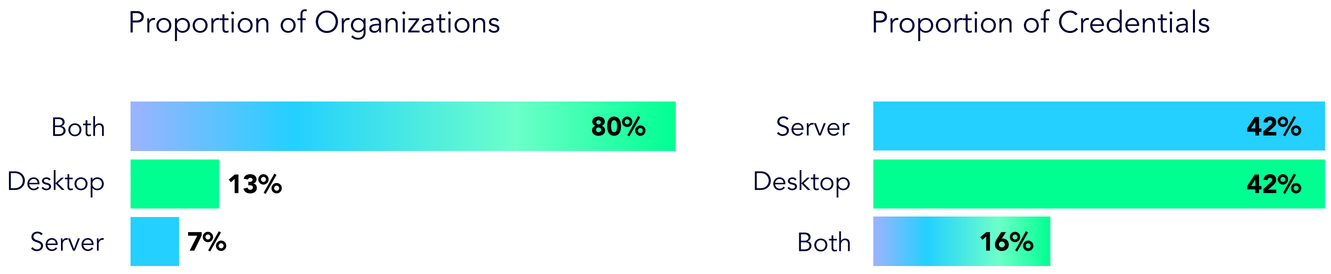


Figure 12: *Prevalence of local credentials across desktops and servers*

While there might be a tendency to think of this as more of a desktop problem, the reality is that 80% of organizations with local credential issues have golden image–sourced credentials on both desktops and servers within their environment. With respect to the credentials themselves, they're scattered evenly between desktops and servers (~42% each). The remaining 16% are duplicated to both.

67%
of organizations have issues with local credentials.

XM Cyber Takeaways & Recommendations

In general, credential issues pose a big risk within organizations. Credentials are used many times by attackers to move laterally within the organization, supporting the fact that organizations need to have an easy way of finding and reducing this attack vector and a dedicated remediation process that regularly reviews and monitors their privileged user access and credential management practices. This includes auditing cached credentials and ensuring that administrative privileges are only granted on a need-to-know basis.

Additionally, organizations should prioritize the elimination of local credential issues by implementing security measures such as secure password management, reducing the use of golden images, and implementing least privilege access controls. By taking these steps, organizations can reduce their risk of credential theft and minimize the potential impact of a security breach.

EDR is not the silver bullet many think it is

As cyber threats proliferated, it became apparent that traditional security tools like antivirus and network intrusion detection systems couldn't adequately protect user devices. A new generation of solutions evolved under the moniker of endpoint detection and response (EDR). Many security teams view EDR as a fail-safe last line of defense when adversaries circumvent all other controls to make their way to endpoints.

But increasing EDR adoption hasn't seemed to slow the regular drumbeat of headlines announcing new security breaches. This begs the question of why.

First, it's worth confirming that our data does indeed point to the widespread adoption of EDR. Only about one in five organizations don't have it deployed in at least some part of their environment. Those deployments cover 73% of the endpoints identified by our analyses. Among those, Linux and MacOSX endpoints are the least likely to have EDR.

38%
of firms have endpoint protection running on fewer than half of their endpoints.

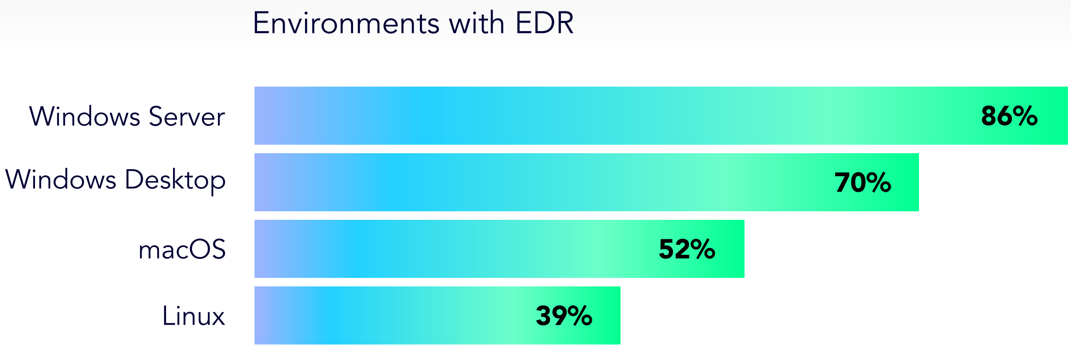


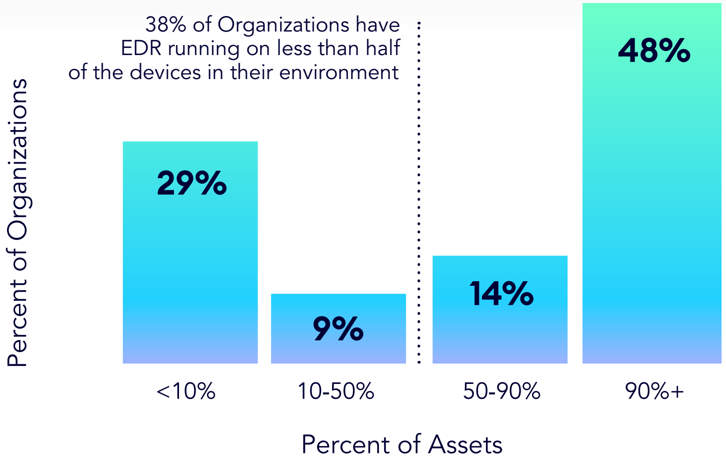
Figure 13: *DR coverage by category of endpoint*

Some may view these high EDR adoption rates as contradictory to earlier sections that detailed how large proportions of critical assets can be compromised in just a few steps. Perhaps you're asking, "Is that only the case in environments without EDR?" The answer is no. We see little difference in those statistics between organizations with pervasive and shallow EDR deployments.

How do we resolve this apparent contradiction? Well, first, we see wide disparity when it comes to the breadth and depth of EDR deployment. Over a third of organizations (38%) have EDR running on less than half of the devices in their network. Only about one in ten have EDR fully functional on at least 90% of their endpoints. That might tick the "has EDR" box, but it won't stop savvy adversaries from forging a path to unprotected assets.

The truth is that EDR solutions aren't a silver bullet. Partial deployments, improper configuration, and management challenges are the norm. Unfortunately, these issues allow attackers to bypass this presumed last line of defense without much resistance. Curious about how daunting your EDR solution looks from an attacker's point of view? We're happy to help with that—but be forewarned—you might not like what you see.

Figure 14: *Percentage of endpoints running EDR among organizations*



XM Cyber Takeaways & Recommendations

We see two major erroneous assumptions when it comes to EDR. First, organizations assume their solution is running on all applicable endpoints (our results show it rarely is). Second, they assume that "EDR has our back" and offers a rock-solid last line of defense. The reality is that we find just as many attack vectors to critical assets among heavy EDR deployments as we do among lite EDR environments.

It's essential to ensure that your security measures are configured properly and deployed consistently across all environments. This is important because you cannot always rely on your endpoint detection and response (EDR) solutions to detect and mitigate all threats. Therefore, it's crucial to have a comprehensive and proactive security strategy that includes multiple layers of defense, such as network security, identity and access management, and endpoint security. By implementing a well-configured and integrated security solution, you can enhance your overall security posture and reduce the risk of successful attacks.

Concluding Thoughts

As we analyzed data and reflected on the findings for this report, my mind kept coming back to one concept: the cost of attack. I've long been preoccupied with the concept of making it more costly for attackers to successfully compromise our organizations than the value they get from doing so. In fact, I wrote this in the very first edition of Verizon's Data Breach Investigations Report in 2008:

"Though some movie plots would have us believe otherwise, cyber attacks in the real world rarely involve Mission Impossible-like scenarios. Quite the opposite, in fact… Given enough time, resources and inclination, criminals can breach virtually any single organization they choose. They cannot breach all organizations…Unless the value of the information to the criminal is inordinately high, it is not optimal for him to expend his limited resources on a hardened target while a softer one is available. The goal, then, is to implement security measures such that it costs the criminal more to compromise your organization than other available targets."

2008 was a long time ago, and I'd like to think we would have reached that goal by now. But as best I can tell, we haven't—at least not for the majority of organizations. And that's why I'm fascinated with what we learned in this analysis based on what XM Cyber are doing through attack path analysis.

We can see what the attacker sees and identify their least costly (quickest, easiest) routes to whatever it is they value. The concept of choke points shows where we can disrupt those routes most efficiently so attackers cannot achieve their objective. If we can operationalize that knowledge, I have hope that we actually can shift the cost of attack in our favor. And that would make me very happy, indeed!

Wade Baker, Ph.D.,
Co-Founder, Cyentia Institute

To operationalize this data, XM Cyber recommends that organizations should:

- Conduct a comprehensive exposure assessment of their systems and infrastructure to identify all exploitable security exposures.
- Prioritize the remediation of exposures that lie on choke points, as they provide attackers with a fast track to causing major harm to the organization.
- Deprioritize vulnerabilities and exposures that do not jeopardize critical assets and focus on live attack paths.
- Focus on techniques targeting credentials and permissions as they affect a large percentage of organizations and exploit a significant portion of all identified security exposures.
- Grant elevated privileges only to those users who need them and ensure that they have access only to the critical assets that they require to perform their jobs.
- Deploy EDR on all endpoints to protect against savvy adversaries who may attempt to forge a path to unprotected assets.
- Monitor and track progress regularly to ensure that exposures are being remediated in a timely manner.
- Implement Zero Trust principles and limit local credentials to reduce the risk of unauthorized access to critical assets.

Appendix A: Top Attack Path Techniques

Let's examine the top techniques observed by XM Cyber during attack path analyses conducted in 2022. As we do, it's important to recognize that there are several valid ways of measuring "top" techniques, each of which offers a different, useful perspective. The figures that follow present all four measures for easy consideration and comparison.

Organizations:
Percent of organizations in which the techniques were observed.
This indicates which techniques are most common overall.

Exposures:
Percent of detected exposures associated with the techniques. This indicates the scope of potential exploitation across the environment.

Critical Assets:
Percent of critical assets that can be compromised by the techniques. This indicates the potential impact or risk.

Choke Points:
Percent of choke points associated with the techniques. This indicates how often the technique leads to critical junctures that then lead to critical assets and therefore enable efficient mitigation of risk.

The figures that follow include techniques making the top 10 by any of these measures.

Top techniques in on-prem environments

	Organizations	Exposures	Critical Assets	Choke Points
Network Reachability	81.2%	7.9%	7.4%	17.8%
Reset User Password	76.0%	18.8%	3.2%	3.5%
Credential Dump	80.2%	2.7%	7.3%	4.3%
Domain Credentials	75.0%	2.7%	7.0%	15.7%
Resource-Based Constrained Delegation	76.0%	8.5%	3.6%	7.9%
Add Logon Script	76.0%	18.7%	2.8%	3.8%
Add Members to Group	77.1%	14.8%	2.1%	0.5%
Local Credentials	75.0%	0.6%	2.8%	4.7%
Member Of Group	72.9%	6.7%	2.9%	0.4%
Taint Shared Content	76.0%	5.6%	2.5%	1.8%
Credentials Relay	58.3%	0.4%	3.1%	4.2%
Proxy Spoofing	81.2%	0.3%	0.1%	2.1%
RDP Credential Usage	60.4%	0.9%	1.6%	7.5%
Microsoft SQL Credentials Usage	70.8%	0.1%	4.4%	0.7%
PrintNightmare - Windows Print Spooler (CVE-2021-34527)	55.2%	0.5%	2.8%	3.3%
Add ACE to OU	66.7%	0.9%	2.9%	0.0%

***Figure A1:** Top techniques identified by attack path analysis in on-prem environments*

Top techniques in AWS environments

	Organizations	Exposures	Critical Assets	Choke Points
AWS IAM Add Policy Privilege Escalation	19.8%	0.2%	2.5%	3.1%
AWS Update Role Impersonation Policy	19.8%	0.1%	2.5%	2.5%
AWS EC2 (AttachVolume, DetachVolume) Take Over	19.8%	0.1%	2.1%	1.1%
AWS Modify EC2 Instance User Data	18.8%	0.1%	2.1%	1.1%
AWS Create User Access Key	18.8%	0.0%	2.0%	0.6%
AWS Update Lambda Code	18.8%	0.0%	1.4%	0.6%
AWS Update Login Profile	17.7%	0.0%	1.9%	0.6%
AWS Over-privileged AWS EC2 Instance Creation	19.8%	0.0%	2.0%	0.3%
AWS S3 Bucket Read Data	19.8%	0.1%	0.6%	0.0%
AWS S3 Bucket Write Data	18.8%	0.1%	0.6%	0.0%
AWS Over-privileged AWS Lambda Function Creation	17.7%	0.0%	1.7%	0.4%
AWS EC2 Role Compromise	20.8%	0.0%	1.4%	0.2%
AWS EBS Share Volume Snapshot	17.7%	0.1%	0.1%	0.0%
AWS Lambda Change Function Role	17.7%	0.0%	1.2%	0.4%
AWS EC2 Change Machine Role	17.7%	0.0%	1.5%	0.3%
AWS Add User To Group	16.7%	0.0%	1.5%	0.4%
AWS EC2 SSM SendCommand takeover	12.5%	0.0%	1.5%	0.4%

Figure A2: *Top techniques identified by attack path analysis in AWS*

Top techniques in Azure environments

	Organizations	Exposures	Critical Assets	Choke Points
Azure Member Of Group	30.2%	1.0%	23.0%	0.2%
Azure Run Command On VM	28.1%	0.3%	20.6%	0.1%
Azure Run Command On VM Using VM Extensions	28.1%	0.3%	16.6%	0.1%
Azure Application Owner Can Compromise the Application Service Principals	31.2%	0.2%	2.6%	0.2%
Azure Add Role Assignment	30.2%	0.0%	38.4%	0.3%
Azure Tables Compromise	24.0%	1.2%	9.9%	0.0%
Azure Graph Role Compromise	29.2%	0.0%	35.4%	0.0%
Azure Read Blobs	17.7%	0.9%	9.1%	0.0%
Azure Group Member of Group	22.9%	0.1%	1.5%	0.0%
Azure Queues Compromise	16.7%	0.3%	3.0%	0.0%
Azure Reset Application Credentials	1.0%	0.1%	0.0%	0.2%
Azure Resource Attached Identity Compromise	22.9%	0.0%	18.9%	0.0%
Azure Applications Can Add Passwords to Other Applications	14.6%	0.1%	0.3%	0.1%
Microsoft Intune - Execute Script	9.4%	0.0%	0.8%	0.1%
Azure Upload Blobs	16.7%	0.3%	1.8%	0.0%
Read OneDrive Files using Azure Applications	26.0%	0.0%	0.0%	0.0%
Azure Application Can Read E-Mails	24.0%	0.0%	0.0%	0.0%
Azure Automation Account Compromise	19.8%	0.0%	3.8%	0.0%
Azure Key Vaults Compromise	24.0%	0.1%	0.4%	0.0%
Azure List Functions publish XML keys in Azure Site	21.9%	0.1%	1.0%	0.0%
Azure Automation Account Application Compromise	8.3%	0.0%	3.8%	0.0%

Figure A3: *Top techniques identified by attack path analysis in Azure*

Top techniques in GCP environments

	Exposures	Critical Assets	Choke Points
GCP Create Service Account Key	0.0%	1.2%	0.3%
GCP Service Account From Resource	0.0%	1.2%	0.1%
GCP Compromise Linux VM	0.1%	0.8%	0.2%
GCP Allows Signing of Arbitrary Payloads	0.0%	1.1%	0.0%
GCP Create VM with Specified Service Account	0.0%	1.0%	0.2%
GCP Create Function with Specified Service Account	0.0%	0.9%	0.2%
GCP Set a Project IAM Policy	0.0%	1.7%	0.1%
GCP Read BigQuery	0.1%	0.9%	0.0%
GCP Set Storage IAM Policy	0.0%	0.4%	0.3%
GCP Read Data From Bucket	0.1%	0.5%	0.0%
GCP Member Of Group	0.0%	1.2%	0.0%
GCP Request Service Account Token	0.0%	1.1%	0.0%
GCP Access Token Stealer	0.0%	0.1%	0.0%
GCP Set a Folder IAM Policy	0.0%	1.5%	0.0%
GCP Write Data To Bucket	0.1%	0.4%	0.0%
GCP Compromise Function	0.0%	0.1%	0.0%
GCP Write BigQuery	0.1%	0.9%	0.0%
GCP Set an Organization IAM Policy	0.0%	1.2%	0.0%
GCP Set Service Account IAM Policy	0.0%	0.9%	0.2%
GCP Request Service Account Token By Implicit Delegation	0.0%	1.1%	0.0%
GCP Signing Well-Formed JWT	0.0%	1.1%	0.0%

Figure A4: *Top techniques identified by attack path analysis in GCP*

XM Cyber

XM Cyber is a leading hybrid cloud security company that's changing the way organizations approach cyber risk. XM Cyber transforms exposure management by demonstrating how attackers leverage and combine misconfigurations, vulnerabilities, identity exposures, and more, across AWS, Azure, GCP and on-prem environments to compromise critical assets. With XM Cyber, you can see all the ways attackers might go, and all the best ways to stop them, pinpointing where to remediate exposures with a fraction of the effort.

Visit www.xmcyber.com to learn more.

119 Cyentia INSTITUTE

Analysis for this report was provided by the Cyentia Institute. Cyentia is a research and data science firm working to advance cybersecurity knowledge and practice. We do this by partnering with security vendors and other organizations to publish a range of high-quality, data-driven content like this study.

Find out more at www.cyentia.com

NAVIGATING THE PATHS OF RISK

The State of Exposure Management in 2023