XM Cyber | Cyentia INSTITUTE

NAVIGATING THE PATHS OF RISK

The State of Exposure Management in 2024

Table of Contents

Executive Summary

What if you could identify all the ways in which your organization is exposed to cyber attacks, understand how adversaries will exploit those exposures, and prioritize remediation efforts to reduce risk most effectively? Well, that is exactly what this report is all about.

This report presents key insights drawn from hundreds of thousands of attack path assessments conducted through the XM Cyber Continuous Exposure Management (CEM) platform during 2023. These assessments uncovered over 40 million exposures affecting 11.5 million entities deemed critical to business operations. Data gathered from the XM Cyber platform were anonymized and provided to Cyentia Institute for independent analysis to generate the insights that fill the pages to follow.

Everyone's talking about exposure management

Exposure Management seems to be the hot topic on everyone's lips right now, but defining what this means and how best to implement a Continuous Threat Exposure Management (CTEM) framework is still causing some confusion.

Aiming to move away from the pain point of endless lists of vulnerabilities, organizations are embracing technologies that claim to provide greater coverage of exposure types, and additional context to aid the prioritization and risk analysis of these different exposure types. However, the context is still often limited to each individual asset or focused solely on the intrusion risk, as in which asset is the mostly likely breach point.

At XM Cyber, we've been providing holistic Exposure Management powered by our XM Attack Graph Analysis™ for over 8 years. We're proud to once again distill those findings into this third edition of our annual State of Exposure Management report. We hope these insights will bolster your security team's important mission over the next year.

We present some highlights of this year's analysis on the next page.

Key findings

Exposure Management is much more than just CVEs.

Organizations typically have about 15,000 exposures across their environments that attackers could exploit. Traditional CVE-based vulnerabilities account for less than 1% of those and just 11% of all exposures to critical assets.

Effective Exposure Management needs to integrate attack path modeling.

XM Attack Graph Analysis™ identifies that 2% of exposures reside on "choke points" of converging attack paths that adversaries can use to reach critical assets. There's a 20x difference in choke point ratio between organizations with the worst vs. best security posture.

Identity and credential issues represent a huge exposed attack surface.

Active Directory typically accounts for 80% of all security exposures identified in organizations as well as one-third of their issues that put critical assets at risk.

Poor cyber hygiene plagues the security of endpoints.

79% of organizations have problems with cached domain credentials or local credentials that are present on multiple machines across the network. While most organizations use EDR (91%), over a quarter of devices aren't typically covered.

Cloud environments are not exempted from the risk of exposure.

Over half (56%) of critical asset exposures are in cloud platforms. Furthermore, attackers can traverse on-premises to cloud environments in 70% of organizations and then compromise 93% of critical assets in the cloud in just two hops.

One size doesn't fit all for managing exposures.

On average, financial firms manage 5x more digital assets than the energy sector, but the proportion of exposures affecting critical assets is 21x higher in the latter.

Exposure Management can't be a one-time or annual project.

It's an ever-changing, continuous process to drive improvements. Organizations with poor posture scores have six times the number of security exposures (30k) compared to high scorers (5k). What's worse is that the gap between those groups widened over time.

Measuring Security Posture

Organizations still struggle to get a holistic view of risk posture

We'll soon dig into our detailed analysis of attack paths, but let's first set the stage with an overall assessment of organizational risk exposure. The XM Posture Score™ provides such a view.

XM Cyber evaluates the risk to critical assets for various attack scenarios, each of which receives a score from 0 to 100. This score is based on the number and complexity of paths leading to critical assets in that scenario. A lower score indicates higher risk due to numerous shorter, simpler attack paths. Higher scores signify the opposite; critical assets are less susceptible to compromise. Scores for all scenarios are averaged to derive the overall security score for the organization.

Cyber risk can't be a one-time or annual project. It's an ever-changing, continuous process to drive improvements.

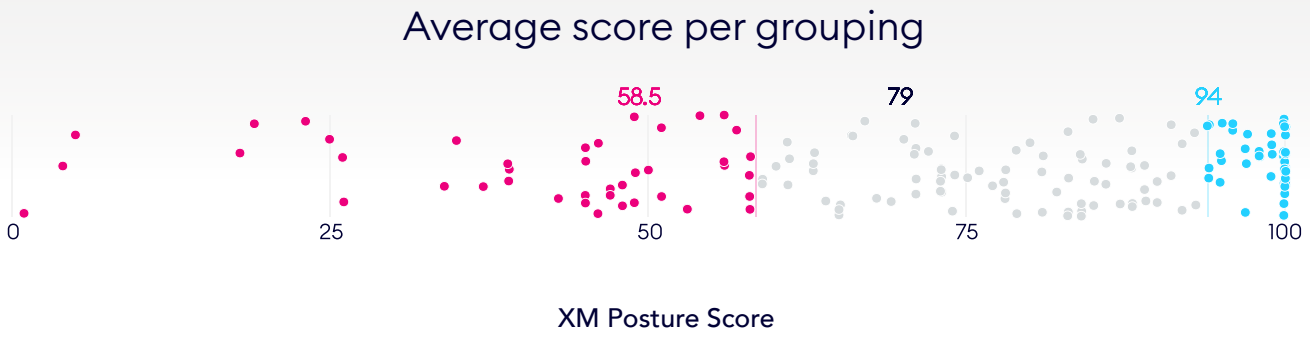


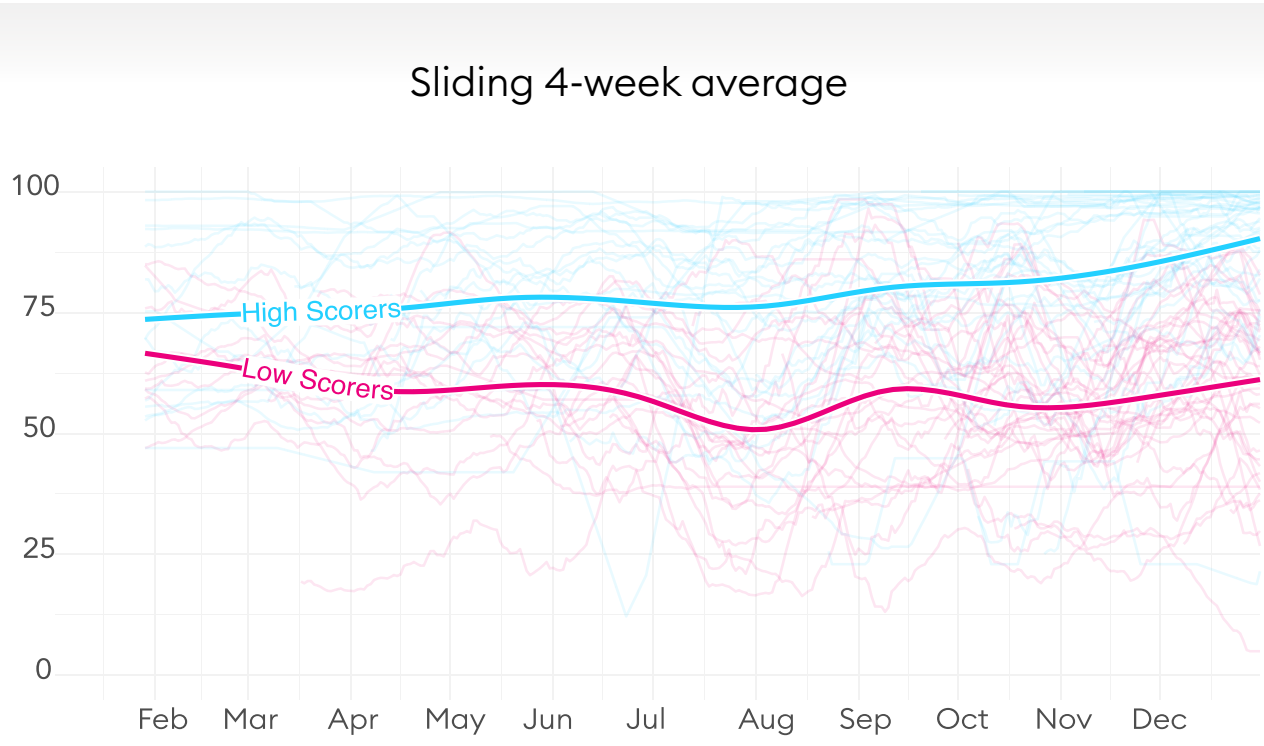
Figure 1: *Organizations with the highest (blue) and lowest security scores (red)*

Figure 1 shows the distribution of security posture scores for individual organizations as of their latest assessment in 2023. Those earning the highest 25% of scores are indicated in blue and can be considered top performers. Organizations in red ranked in the lower 25th percentile of scores. The middle half of organizations is faded out to draw more contrast between the top and bottom performers. The median score across all organizations is 79.

The "as of their latest assessment" caveat brings up an important point—security scores are not static over time. Per the faded lines in the background of Figure 2, they shift up and down as changes in the environment and evolving attack scenarios alter risk to critical assets. The moving average among both high- and low-scoring organizations is fairly steady but grows apart over time. The high scorers show steady improvement during the year, while low-scoring organizations trend down.

The final chart in the section serves as a very visual reminder that managing cyber risk can't be a one-time or annual project. It's an ever-changing, continuous process to drive improvements. In the next section we will dig into those attack path details we promised.

Figure 2:
Daily security scores with moving averages for high- and low-scoring organizations



XM Cyber Takeaways & Recommendations

From the results, it's clear that security is never done. However, when operationalized effectively, a Continuous Threat Exposure Management (CTEM) methodology can have a positive impact on the overall security posture. Throughout 2023 we have seen positive improvements to the XM Posture Score™, in our more mature and established customer base. As you read through the following sections of the report you will see some common trends in security improvements that go hand in hand with these posture improvements, such as a reduction in exposures, a 20x decrease in the number of choke points, resulting in the successful closing of attack paths to critical assets. All of these are key drivers and objectives for security professionals and CISOs across the globe, as outlined in our survey report: The State of Security Posture 2024.

A Primer on Attack Paths

Organizations face a constant threat of cyber-attacks that can jeopardize critical assets, exfiltrate data or disrupt business operations. Although these cyber attacks are ever-evolving, they typically follow a logical set of steps referred to as the Cyber Kill Chain, which provides an effective structure for an adversary or attacker to breach an organization's defenses. Whereas the Kill Chain represents the individual stages of an attack, the term Attack Path refers to the logical path across your network and around your different security defenses that the attack takes in order to execute their Kill Chain and reach the end goal of your business-critical assets and systems.

The attack path is formed of individual hops between many different entity types, across all parts of your enterprise infrastructure. They stretch from edge-of-network devices and perimeter defenses, spreading laterally through laptops, desktops and workstations in the campus. They can traverse vertical network layers from physical, to virtual and cloud entities, and can even traverse the vertical layers of data plane, to the control plane to the management plane and back again. Attack paths aren't just formed from different device types, but can leverage extended entity types, like software applications, kubernetes clusters, user credentials, API tokens, and other identity types.

Due to this expansive array of entity types and infrastructure layers, it's difficult to truly understand the risk varying attack paths present. Considering only one type of exposure, such as vulnerabilities (CVEs), or one infrastructure layer, such as cloud, severely limits your ability to see the full extent of the exploitability of your attack surface and the potential attack paths towards your critical assets.

To help address this challenge, Attack Path Modeling is a foundational methodology needed for Exposure Management. It helps cyber defenders and security stakeholders identify and map potential routes that threat actors could take to exploit vulnerabilities, misconfigurations and weak security posture in order to compromise critical assets.

But why limit this model to only a single Attack Path?
XM Cyber has pioneered the use of Attack Path Modeling for Exposure Management since its inception. However, to truly see all ways an attacker could breach your organization, you need to see all attack paths from a holistic viewpoint and in a comprehensive state.

Introducing XM Attack Graph Analysis™

XM Attack Graph Analysis™ gives you clear and concise exposure intelligence, built from context-based insights across all exposures from Cloud to Core, by pinpointing key intersections where attack paths converge and present the most critical risk to business operations. This helps Security and IT teams prioritize remediation efforts, and work collaboratively to have a positive impact on security posture and a reduction to cyber risk.

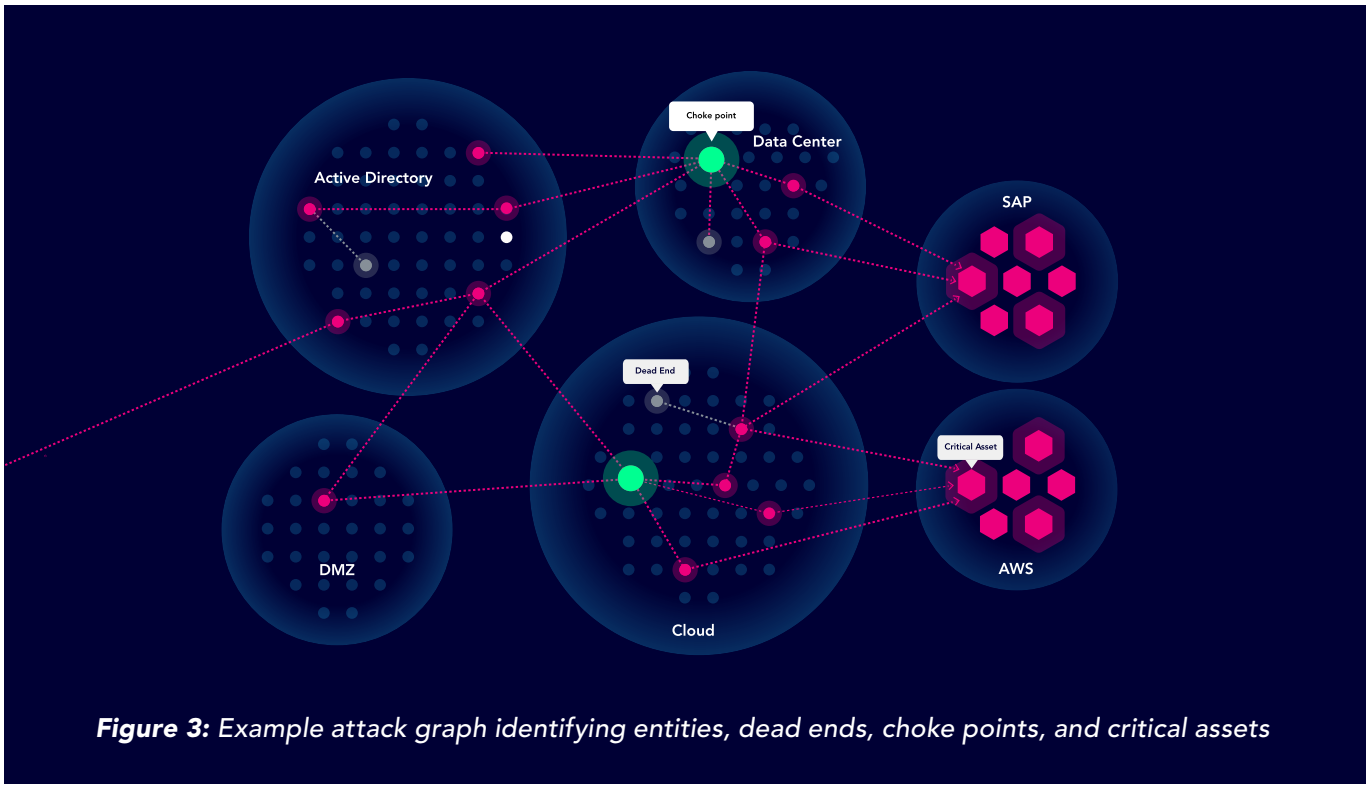


Figure 3: *Example attack graph identifying entities, dead ends, choke points, and critical assets*

Understanding the relationship and context of attack paths toward critical assets is essential to mitigating risk. By visualizing all possible attack paths through the XM Attack Graph Analysis™, the platform can correlate all validated attack paths, to uniquely identify the key intersections where attack paths converge and highlight them as **Choke Points** that present the most impactful risk to your critical assets.

By identifying entities with the weakest and most exploitable security posture, we can assess the intrusion risk and most likely breach points to your organization. Our attack scenarios continuously calculate all potential attack paths from the breach point through to the critical assets. This, in turn, allows for a more validated approach to risk prioritization that reports all attack tactics, techniques, and processes (TTPs) that the attacker could utilize, in order to exploit the specific exposures of each entity along the attack path.

The analysis and statistics shown in this report are all taken from the XM Attack Graph Analysis™, leveraging the key metric of critical assets at risk, presented by a particular exposure type, or attack TTP.

Our advanced approach to Attack Path Modeling gives you the context you need to make faster, more confident decisions about your exposure risk profile, and where to focus your remediation efforts. Continue reading this report for unique insights taken from the XM Attack Graph Analysis™.

Enumerating Exposures

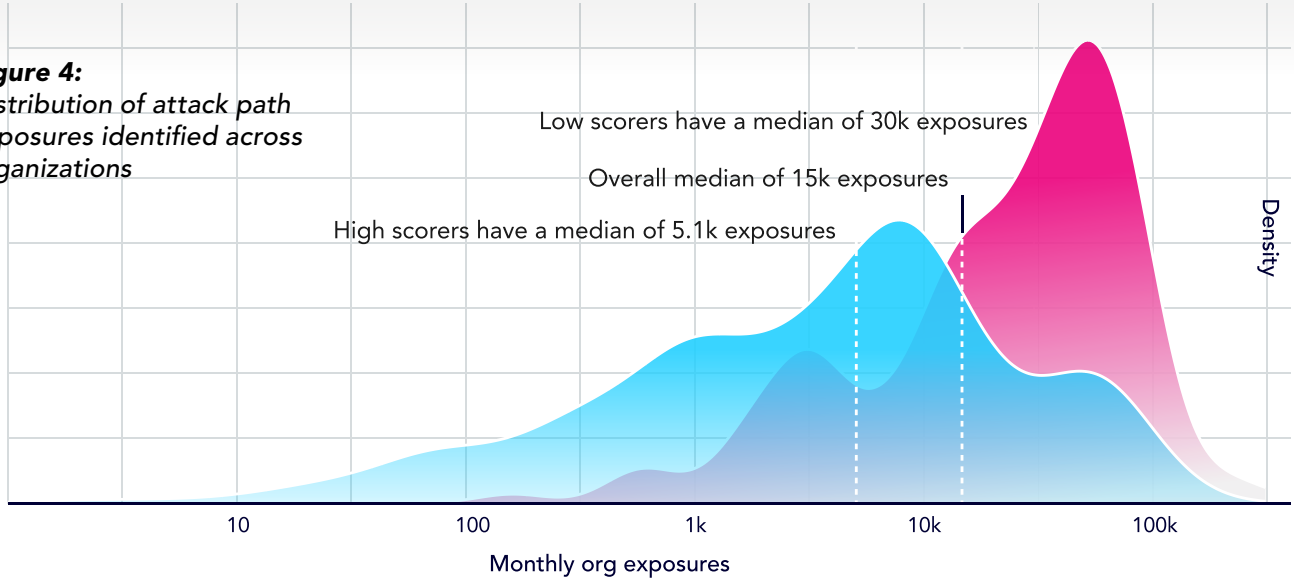
Lessons learned from another year of attack graph analysis

Data collected from XM Attack Graph Analysis™ continually points to a core cybersecurity challenge facing every organization: there are just too many issues for defenders to realistically fix and too many ways for attackers to exploit them. Even the best teams become overwhelmed.

"Overwhelmed" is rather vague, so let's put some numbers around that in Figure 4. We typically identify 15,000 security exposures that attackers could exploit in each organization on a monthly basis (that's the overall median). The median among organizations with high overall security posture scores is just 5,100, while low scorers contend with six times that amount!

We typically identify **15,000** exposures attackers could exploit in each organization. **Some have over 100,000!**

Figure 4: *Distribution of attack path exposures identified across organizations*



Entities: Any endpoint, workstation, server, identity, access tokens, cloud resources, etc. in an environment that an attacker can use to advance an attack path toward critical assets.

Exposures: Exposures are combinations of techniques and entities susceptible to those techniques. They essentially enumerate the many options attackers have at their disposal.

Points of convergence

Rather than treating all exposures equally, a far more manageable approach is to identify the subset of issues that represent the highest risk and prioritize those for remediation. The majority (74%) of security exposures afflicting organizations are on "dead ends" that limit attackers' lateral movement toward critical assets.

A small subset of exposures, however, affect critical assets and/or represent "choke points" of converging attack paths that adversaries can leverage to escalate and broaden their access through the target environment. Defenders can also target those same choke points to reduce risk more efficiently and effectively.

This concept is depicted in Figure 5, which represents the typical enterprise attack surface. Choke points and directly-exposed critical assets are highlighted in yellow and red, amid the sea of all exposures. We distinguish the red ones because about 1 in 5 choke points exposes 10% or more of the critical assets in the organization. Compromising those opens the door for attackers to cause severe impact. Addressing these should be at the absolute top of your security remediation to-do list.

The majority

74%

of exposures lead to dead ends.

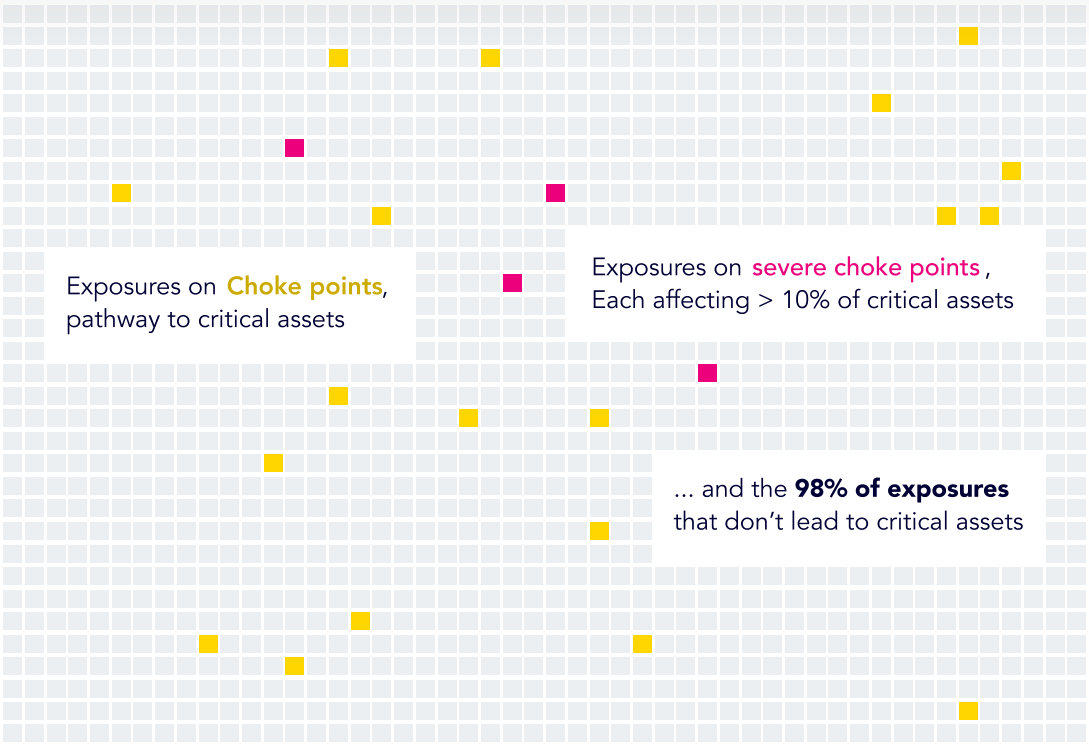


Figure 5: *A depiction of the typical attack surface, showing the ratio of "choke points" (yellow and red squares) among all identified exposures (gray squares).*

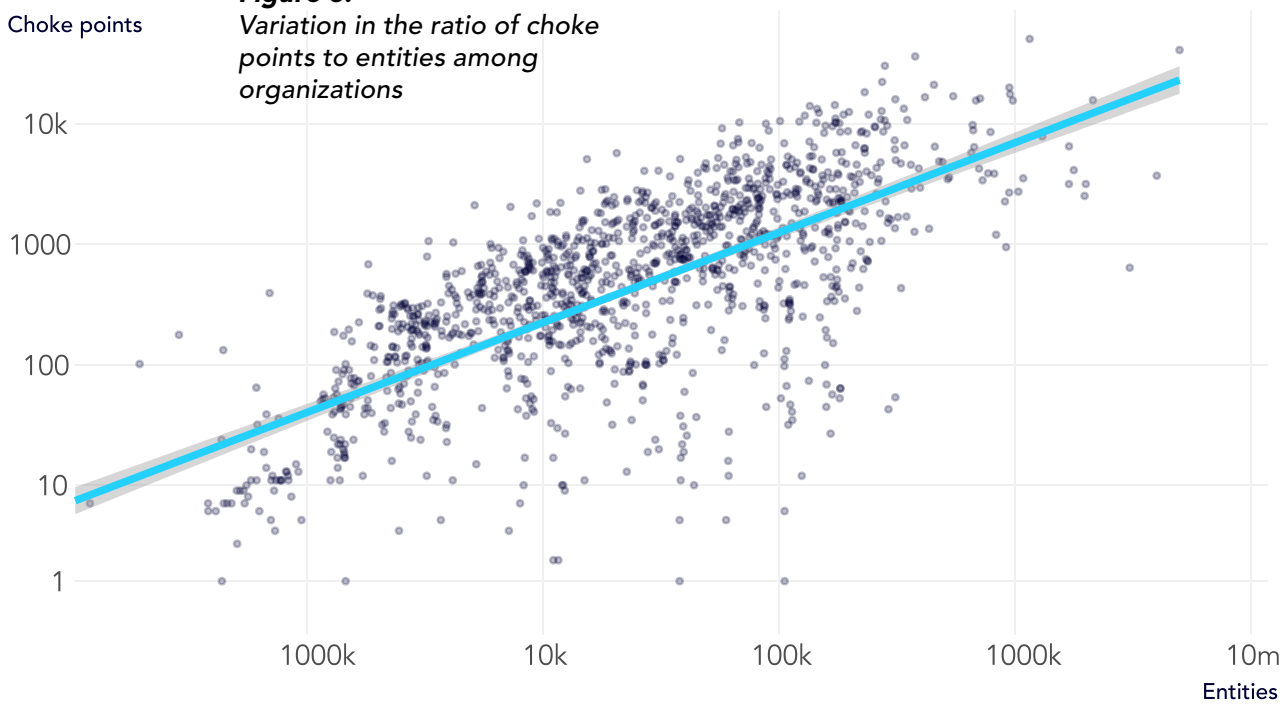
Our last report placed the typical ratio of choke points to exposures within organizations at about 2%. In the interim year, we conducted tens of thousands of additional assessments of a significantly larger population of organizations, which reestablished a similar ratio (1.5%).

We feel obligated to stress that this doesn't mean the remaining supermajority of exposures don't matter or shouldn't be fixed. They are security issues and they do enable attackers to persist in the environment. That said, remediation has to start somewhere. And we suggest focusing first on the exposures that matter most—and that's clearly the choke points towards critical assets. This is the power of the XM Cyber approach to exposure management—98% reduction in effort for maximum risk reduction efficacy!

2%

of exposures affect critical assets and/or represent choke points of converging attack paths that adversaries can leverage to escalate and broaden their access.

Figure 6:
Variation in the ratio of choke points to entities among organizations



In addition to updating the choke point stat based on the latest and greatest data, we thought it would be instructive to explore how much variation exists among firms. Each dot in Figure 6 plots an organization's entities (x-axis) and choke points (y-axis) in a given month. The overall trend remains fairly steady regardless of how many entities are present, but the choke point ratio does vary substantially among organizations.

Practically speaking, that means some organizations will find it significantly harder (or easier) to efficiently stop attack propagation than others. This should not be surprising, since all environments contain a different mix of assets, data, configurations, controls, etc. It reinforces the importance of knowing your environment and understanding its strengths and weaknesses relative to attackers' ability to cause harm.

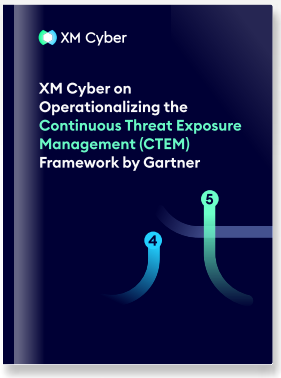
This is the power of the XM Cyber approach to exposure management–

98%+

reduction in effort for the same level of risk reduction!

To learn more about how the 5-stage CTEM framework can help your organization monitor, evaluate, and reduce your risk of exploitability through the validation of exposures, check out our comprehensive guide.

check out our comprehensive guide.



XM Cyber Takeaways & Recommendations

It's clear that organizations are still overwhelmed by the sheer volume of security exposure reported across their diverse attack surface. Organizations have an average of over 15,000 security exposure identified on a monthly basis, that if left unchecked can grow exponentially to well over 100,000. To tackle this it's clear that effective Exposure Management needs to integrate Attack Path Modeling, to identify choke points and offer clear remediation guidance as to how to address the exposure that presents the highest impact-risk to business critical assets and systems. For guidance on how to achieve this for your own organization, check out our Operationalizing CTEM guide. It's still advisable to aspire to fixing all your exposures through automation and a CTEM-like operation cadence, but to drive the most positive improvements, your teams should focus on what matters most, by first validating the exploitability of exposures and the business risk they pose.

Organizational Comparisons

When it comes to security, one size never fits all!

Figure 7 demonstrates the effect that your environment has on attack paths. It compares key exposure statistics between organizations with the highest and lowest security posture scores. Low scorers typically have 6X more exposures and a 23X higher ratio of choke points. That doesn't mean their risk fate is sealed, but it does suggest the starting point and the effective mobilization of Exposure Management matters quite a bit

Critical Exposures: Exposures that have been validated to be exploitable and present an onward attack path towards critical assets using the XM Attack Graph Analysis™

	Exposures	Critical Exposures	Choke point ratio
High Scores	5.1K	0.46%	0.33%
Low Scores	30K	0.47%	7.7%

Figure 7: *Comparison of exposure statistics for organizations with high vs. low security scores*

We offer a similar comparison among industries in Figure 8. Let's start with the number of digital entities detected in the first column. From this, we see that the Healthcare & Pharmaceuticals, Financial Services, Manufacturing & Technology, and Retail sectors tend to manage environments that are larger and more complex than many other types of organizations. These industries traditionally have many digital assets to track and protect.

In general, industries that have a lot of entities also have a lot of exposures. This makes sense because entities vulnerable to attack are, by definition, exposures. The fact that the median number of exposures affecting healthcare providers is 5X that of the Energy and Utilities sector points to the inherent challenges of minimizing risk in those environments.

	Entities	Exposures	Critical Exposures	Choke point ratio
Healthcare & Pharmaceuticals	72k	55k	0.04%	1%
Financial Services	59k	46k	0.5%	7%
Retail	41k	38k	0.07%	0.3%
Business Services & Consulting	29k	30k	0.1%	0.7%
Manufacturing & Technology	48k	26k	0.1%	1%
Agriculture & Food	19k	25k	0.2%	3%
Education & Government	18k	15k	0.6%	0.4%
Transportation & Automotive	14k	12k	7%	21%
Energy & Utilities	11k	11k	11%	33%
Telecommunication & Media	16k	9.2k	0.2%	0.2%

Figure 8: *Comparison of exposure statistics by sector*

Speaking of minimizing risk, the third column offers a more risk-centric perspective. It shows the proportion of all exposures that put critical assets at risk. The tables are turned here, and we see unusually high ratios of critical exposures for the transportation and energy sectors. A similar pattern applies to the choke point ratio. The lower exposure count in the denominator contributes to that calculation, but the basic fact remains. Managing high concentrations of critical assets and choke points requires a different approach than risk-sparse environments.

XM Cyber Takeaways & Recommendations

Every environment is unique and presents their own level of exposure risk, with individual nuances and challenges. And as such, security tools and the approach to security strategy needs to be flexible and adapt to dynamic changes in the attack surface. As an example, from the charts above, you will see that although on average financial firms manage 5X more digital assets than the energy sector, the proportion of exposures affecting critical assets is 21X higher in the latter. Why is this? Well it's likely down to two factors, the first being the tendency to use relatively flat networks, combined with the number of critical assets across the network for an energy or utility company. It may also be down to the use of legacy operating systems and hardware. Understanding the threats that exist and the risk they present to your unique attack surface is an essential first step to success with the cybersecurity strategy. Hopefully this report, combined with our Most Potent Attack Paths, series is starting to frame the picture for where you need to focus.

Finding & Categorizing Exposures

The challenge with identification and classification of critical asset

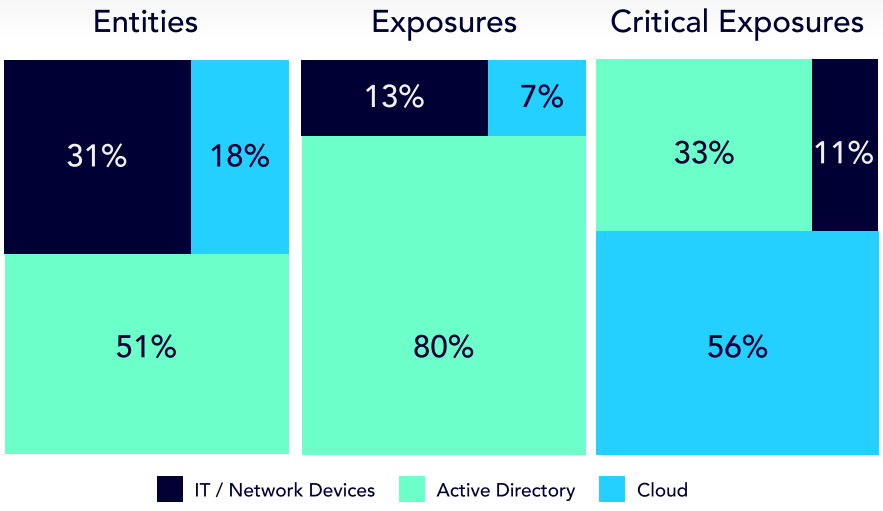
We've explored challenges associated with the high volume of security exposures across enterprise environments, but important questions remain. Where do all these exposures exist? How do attackers exploit them? What attack techniques can cause the most harm? In this section, we'll seek those answers and more.

To a certain extent, answers to these questions are a matter of perspective. Many view their attack surface as consisting of everything in their environment. And there's truth to that; organizations should protect all their assets. But to do that effectively, they need to know where those assets are located and how they're exposed to attack.

The left-most chart in Figure 9 represents the attack surface based on broad categories of digital entities discovered during XM Cyber's attack path assessments. Active Directory constitutes just over half of entities identified across all environments. On-premises IT and network devices account for another 31% of entities and cloud environments house the remaining 17%.

Where/What are our biggest exposures? Well, the answer depends on how you define "biggest..."

Exposure Management must encompass all environments and account for where critical assets are most at risk.



Not all entities, however, are exposed via attack paths. If we change the scope of the attack surface to include only vetted exposures (entities susceptible to attack techniques), things look different. The middle chart captures this perspective and Active Directory exposures dominate the attack surface.

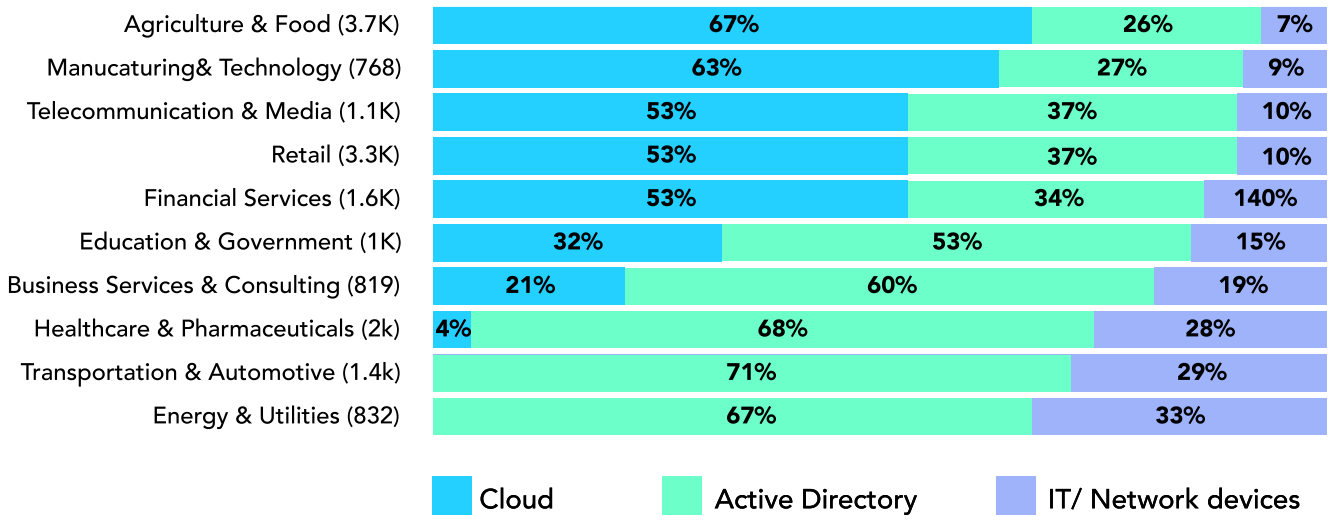
Figure 9: *Categorical breakdown of entities, exposures, and critical exposures*

But not all of those exposures affect critical assets. To be truly effective, Exposure Management must encompass all environments and account for where critical assets are most at risk. If we once again rescope the attack surface to focus on exposures to critical assets, a very different picture emerges, which is captured in the rightmost chart of Figure 9. Cloud environments now encompass over half of all critical asset exposures, followed by AD at 33% and IT/Network devices at 11%.

Given that defenders often specialize along lines which are not too different from these high level categories, an organization could find itself adequately staffed and skilled to manage entities based on their overall counts, but coming up short when managing the outsized impact presented by riskier—albeit less numerous—ones. With too many entities and too little time, weeding out benign exposures is crucial to matching effort to risk.

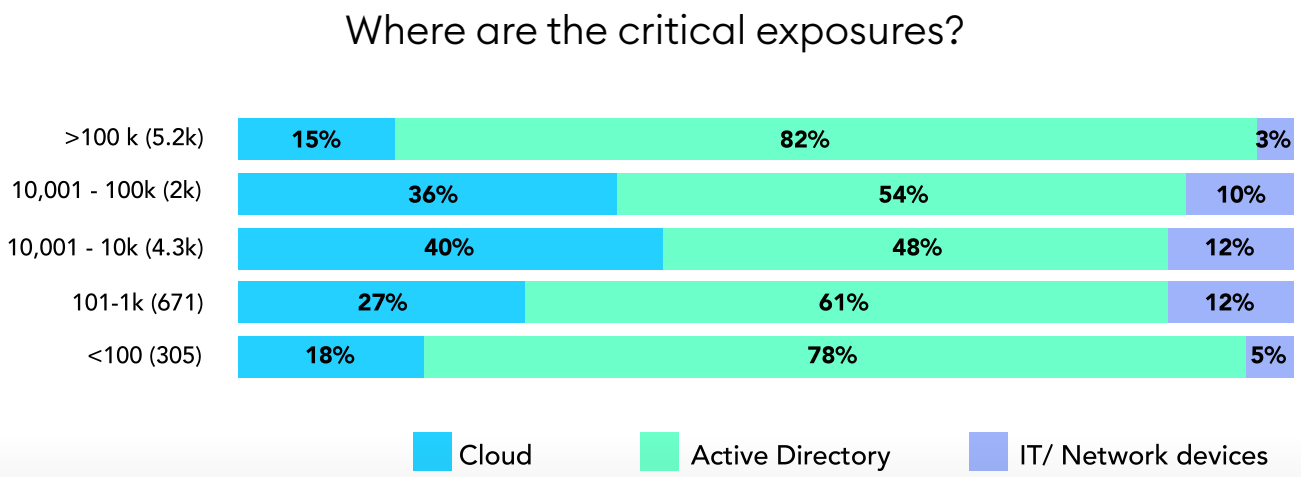
Active Directory is the largest attack surface, but the largest share of exposures to critical assets is in the cloud.

Where are the critical exposures?



We compare the relative distribution of exposures to critical assets across industries in Figure 10. About half follow the overall pattern of Cloud > Active Directory > IT/Network devices. But there's quite a bit of variation and some sectors buck that trend entirely. For example, very few of the critical asset exposures affecting the Energy, Transportation, and Healthcare sectors are in the cloud. On the other hand, the share of critical exposures in cloud environments is much higher than average in the Agriculture and Manufacturing industries.

Figure 10:
Categorical breakdown of entities, exposures, and critical exposures by sector



The distribution of critical exposures for organizations of different sizes is revealed in Figure 11. Cloud infrastructure represents the largest share for all groups but the extent of that majority varies among them. Interestingly, the highest concentration of exposed critical assets in the cloud are seen in the smallest and largest organizations.

Figure 11: *Categorical breakdown of entities, exposures, and critical exposures by organization size*

At this point, you may be wondering how attackers can exploit these exposures in on-prem infrastructure, cloud, and Active Directory. Since each of those environments often involve different teams and skillsets to manage them, we'll explore each individually in the sections that follow.

XM Cyber Takeaways & Recommendations

Business Critical Assets and Services are everywhere. With the diversity and increasing sprawl of the attack surface, needed to support business initiatives and drive digital services, it's often very difficult to understand exactly what you have where, how important it is, and how well protected it is. Identifying what critical assets you have and classifying them into logical groups of importance can be very challenging. Leveraging Clouds and new forms of Identify types is all part of the journey and further complicates the picture. Shown in the findings, we report that attack surfaces and the number of exposures they present vary by industry and organizational size, but one thing stays consistent - the number of security exposure is still overwhelming.

To help address this XM Cyber continues to add new capabilities to better detect and protect critical assets, adding attack technique detection for both Kubernetes and SAP this year, and expanding our intrusion-risk and breach point detection capabilities through the launch of our External Attack Surface and Exposed Credential Threat Intelligence services.

Exposures in IT/Network Devices

Vulnerabilities and CVEs are abundant, but are they really what you should be focusing on?

The IT/Network devices category wasn't the largest in any of the breakdowns we showed in the previous section for entities, exposures, and critical exposures. But we've chosen to start here anyway because many organizations in our sample operate predominantly on-premises infrastructure. Plus, even among those with extensive cloud environments, enterprise networks are often the starting point for exposure management.

Hops to compromise on-prem assets

Enterprise networks can be complex labyrinths, but that doesn't mean attackers can't navigate quickly through them. Our attack path assessments mimic how attackers do this to better understand the difficulty involved. Generally speaking, organizations want to make attack paths as difficult and convoluted as possible to hinder lateral movement and compromise of critical assets. Unfortunately, that's not typically what we find.

Over 60% of critical assets can be compromised in just a single hop from the initial point of intrusion into on-prem networks. Successive hops bump that to 65% (2) and 73% (3), and after four hops in, 80% of all critical assets are reachable. This escalating scope of compromise is captured in Figure 12.

We suspect these numbers will seem high to many readers. But this is largely the result of choke points; they enable attackers to move quickly through the environment. That's why remediating those choke points is so effective in restricting access and reducing risk.

62%

of critical assets can be compromised in just a single hop from the initial point of intrusion into on-prem networks.

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.

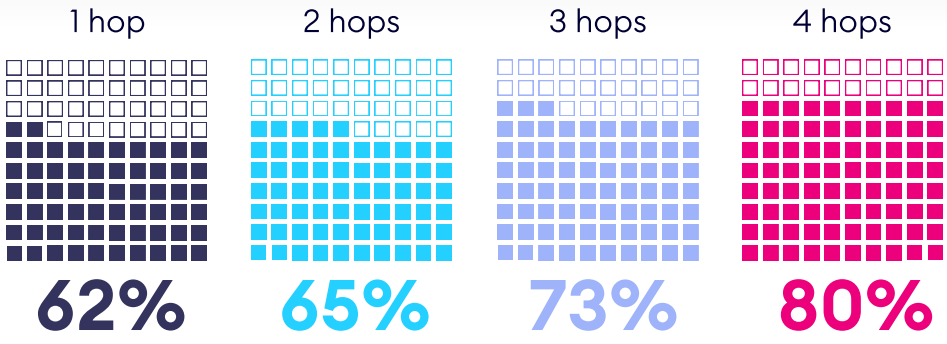


Figure 12: *Scope of critical assets at risk with each additional hop along on-prem attack paths*

Top on-prem attack techniques

Some may assume attackers primarily exploit traditional CVE-based vulnerabilities to execute hops and move about the environment. CVEs definitely contribute to this but they're not the biggest factor identified during our attack path assessments.

Although XM Cyber is able to identify all CVEs on endpoint devices, they do not all factor into the XM Attack Graph Analysis™. Each attack scenario focuses extensively on remote code executable vulnerabilities that can be used by attackers to spread either laterally or vertically to other entities along the attack path. The attack techniques that are deemed to be successful in propagating the attack are then reported on a per-technique or per-entity basis to simplify remediation efforts. We found exploitable vulnerabilities in most organizations (86%) but they accounted for less than 1% of all exposures and 11% of critical exposures.

That begs the question of what techniques account for the bulk of exposures and Figure 14 supplies the answer. There are two biggies from a critical assets perspective: Taint Shared Content and Local Credentials.

remote code executable CVEs accounted for less than

1%

of all exposures

and Less than

11%

of critical exposures.

The most common CVE among attack paths was CVE-2021-34527 (aka "PrintNightmare"). A cluster of CVEs associated with file loaders targeting Microsoft Office Documents used in multiple campaigns exposed the largest percentage of critical assets (e.g., CVE-2021-40444). Such vulnerabilities definitely contribute to the ability of attackers to compromise critical assets and should be remediated. But Exposure Management obviously must be much broader than CVEs to adequately manage risk.

Figure 13: *Prevalence of exposures associated with exploitable vulnerabilities (CVEs)*

The first technique involves attackers "tainting" files in shared folders with malicious code. When users access those shared files, the code executes, allowing adversaries to compromise remote systems and move through the network. This is widely considered to be bad practice and difficult to solve at scale, which is why it remains a top issue. There is a MITRE ATT&CK technique under the same name with more details and examples. The DFIR report also provides examples of this technique.

Attack techniques associated with local credentials are a big problem, identified in 86% of organizations and behind 24% of critical exposures. This issue generally entails common or shared accounts created locally on multiple devices, which introduces a high risk of compromise.

Attack techniques associated with local credentials affect

86%

of organizations **and 24% of critical exposures.**

	Organizations	Exposures	Critical Exposures
Taint Shared Content	89.5%	61.0%	28.0%
Local Credentials	85.8%	7.03%	24.0%
DHCPv6 DNS Poisoning	75.3%	6.63%	0%
Proxy Spoofing	72.8%	2.99%	1.77%
SSH Private Key Dump	71.6%	0.813%	1.67%
Microsoft SQL Credentials Usage	69.8%	0.527%	8.81%
Identical Password	63.6%	0.344%	3.44%
RDP Credential Usage	48.8%	2.70%	3.37%
Network Reachability	45.7%	15.7%	5.89%
File Infector for Microsoft Office Documents	45.1%	0.116%	0.903%
Linux Remote Session	43.8%	0.993%	4.49%
IIS Web Shell	39.5%	0.0516%	4.44%
Insecure JMX	29.0%	0.166%	1.99%
SSH Private Key Usage	25.3%	0.362%	3.35%

Even worse, 24% of organizations have what we suspect are "golden image" issues wherein local credentials are present on more than 10% of devices. This often occurs unintentionally as the credential-laden golden image is replicated across many desktops and servers, exposing them to compromise.

Figure 14: *Top IT/Network techniques identified by attack path analysis*

EDR coverage and efficacy

Endpoint Detection and Response (EDR) solutions aren't limited to on-prem IT infrastructure but that's the traditional use case. Most (91%) of the organizations we assess have EDR deployed and the average coverage across in-scope devices is 72%. That, of course, means over a quarter of endpoints aren't typically covered by EDR.

Does EDR make attack paths more difficult? There's some evidence for that, yes. But it's probably not as strong as you may expect because EDR, at least among the organizations we analyze, is table stakes (see Figure 15). Plus, attacks that bypass EDR are becoming more common and effective.

Most organizations we assess have EDR deployed and the average coverage across in-scope devices is

72%

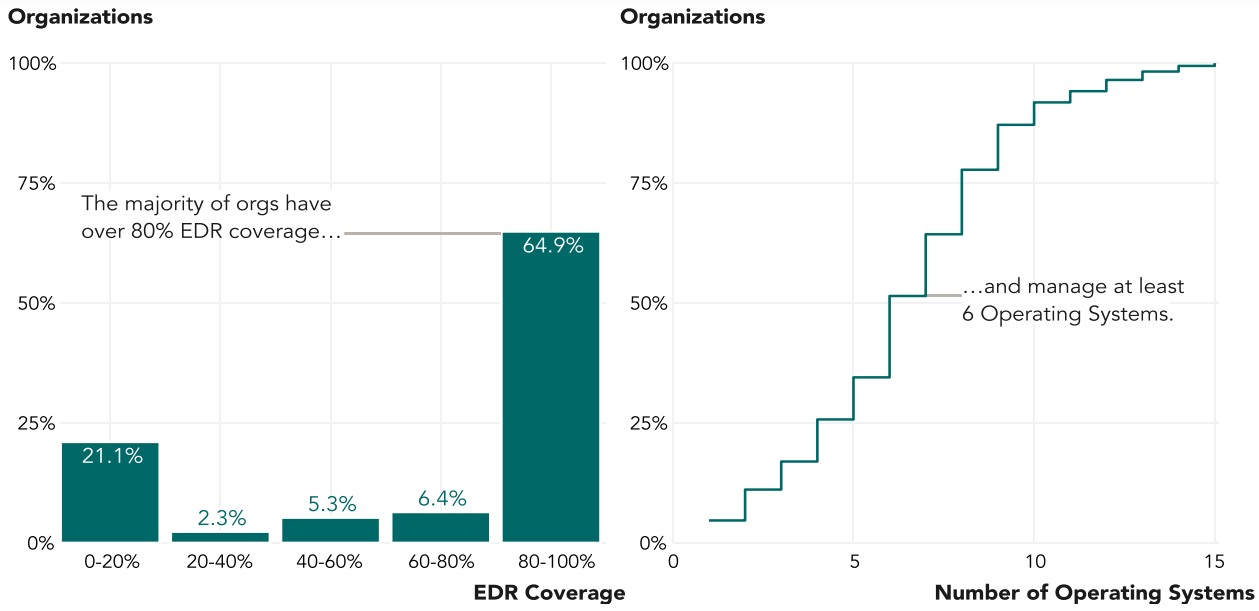


Figure 15: *Scope of devices and number of operating systems covered by EDR*

Per Figure 16, EDR coverage tends to be slightly more comprehensive for workstations than servers. The workstation statistic would be even higher if not for the traditional lower coverage rates for non-Windows devices. We find the fact that one-third of servers fall outside the protection of EDR particularly concerning since servers are generally considered higher-risk assets than workstations.

The variety of operating systems covered by EDR in the organizations we analyzed is quite high. Half of organizations run at least six different OS and 16% manage more than 10. This is a good reminder of the coverage challenges with OS-specific EDR tools.

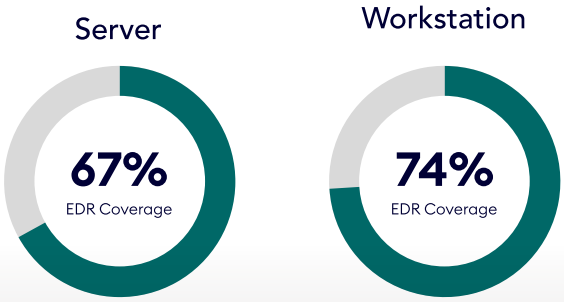


Figure 16:
Comparison of average EDR coverage for servers vs. workstations

Organizations with the highest overall security posture scores have somewhat higher EDR coverage (average 76% of devices), but the lowest scorers have extensive deployments, too (average 67%). EDR is not the fail-safe line of defense that many think it is. 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.

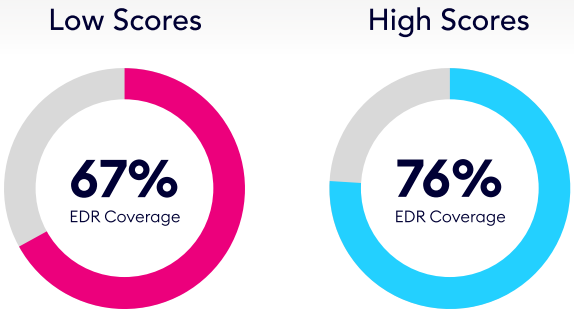


Figure 17:
Comparison of average EDR coverage for organizations with high vs. low security scores

XM Cyber Takeaways & Recommendations

We can draw three key conclusions from the findings in this section of the report. The first being that Vulnerabilities and CVEs are still the heaviest contributors to the alert fatigue noise that overwhelms security defenders and limits the effectiveness of proactive security. They equate to over 85% of the exposure reported, but when interrogated by XM Attack Graph Analysis™, they result in one 1% of the exposure that allow onward and lateral movement to propagate attack paths. The next key takeaway is that the most successful (or damaging) attack paths are typically accomplished across multiple hops, with more often than not only a single hop being accredited to a CVE. The more hops the attack can take, the further away from your perimeter defense they get, and the more place they have to potentially hide. Each hop opens up more options for the next hop, so attackers can be selective in their approach, and opt to exploit the next-weakest link aiming to further evade detection and increase their dwell time.

This leads to the third takeaway, regarding the somewhat alarming statistics around EDR coverage. It's a well know fact, that keeping security agents up to date across your endpoints is challenging to say the least, and EDR is just one of those agents you need to keep on top of along with local Firewalls, DLP & VPN to mention just a few. Establishing a good base of cyber hygiene is essential for security and should not be overlooked. For some suggestion on how to foster a good standard of cyber hygiene, check out our recent Enterprise IT Cyber Hygiene blog.

Exposures in Cloud Environments

Where there are clouds, there is rain, and it's raining attack paths!

Before analyzing attack paths IN the cloud, let's first recognize that many of those paths originate on-prem. For example, the attack path in Figure 18 starts from an enterprise workstation. After exploiting domain credentials, the attacker pivots into the cloud environment by harvesting valid Azure access tokens (claimed with MFA). The attacker is then able to escalate privileges and compromise an Intune (Azure MDM solution for managing devices) Administrator User. Abusing the permissions of that user enables code execution back on the enterprise machines and further lateral movement.

We found exposures in **70%** of organizations that allow attackers to pivot between enterprise networks and cloud environments.

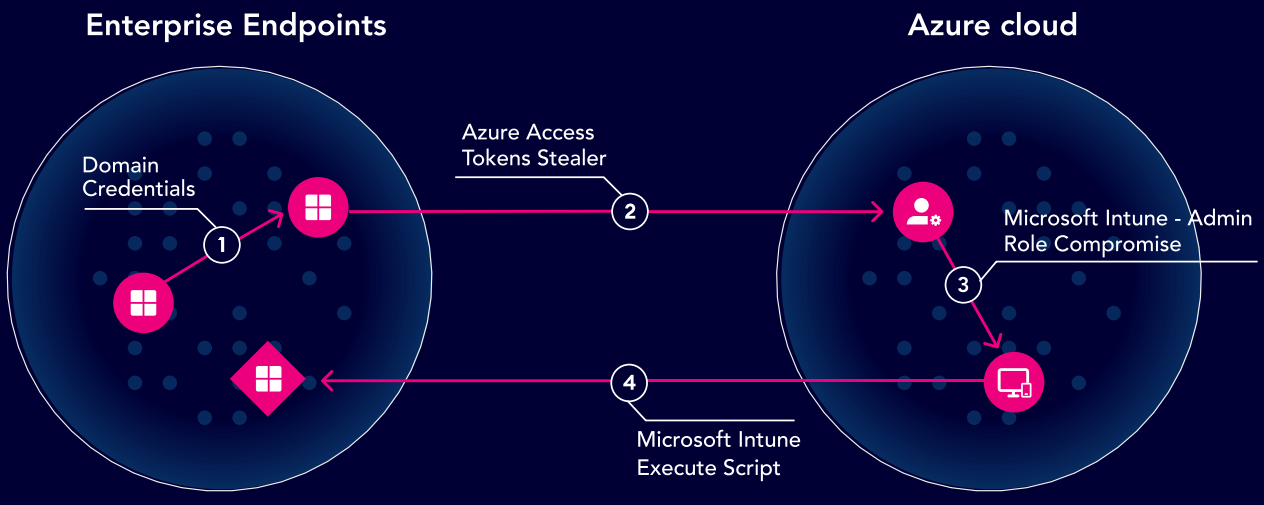
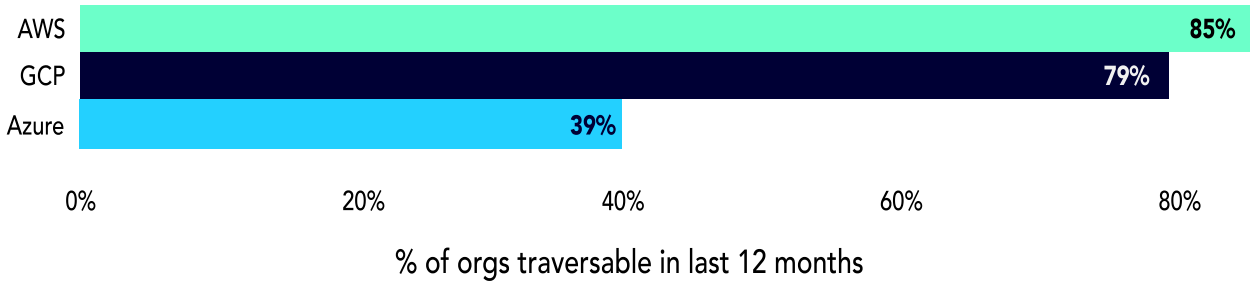


Figure 18: *Example attack path for traversing enterprise and cloud environments*

During attack path assessments over the last year, we found exposures in 70% of organizations that allow attackers to pivot between enterprise networks and cloud environments. That rate varies among the "Big 3" providers, Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), as shown in Figure 19.



Of course, pivoting from on-prem networks isn't the only way attackers infiltrate cloud platforms. For example, over a quarter of firms (26%) have public-facing virtual machines that expose critical assets. Such exposures circumvent the need to compromise enterprise networks first.

After gaining access to a cloud environment, attackers can compromise

88%

of critical assets in a single hop.

Hopping on clouds

Per Figure 20, attack paths in the cloud are much shorter than on-prem. After gaining initial access to a cloud environment, attackers can compromise 88% of critical assets in a single hop. 96% after just 3 hops.

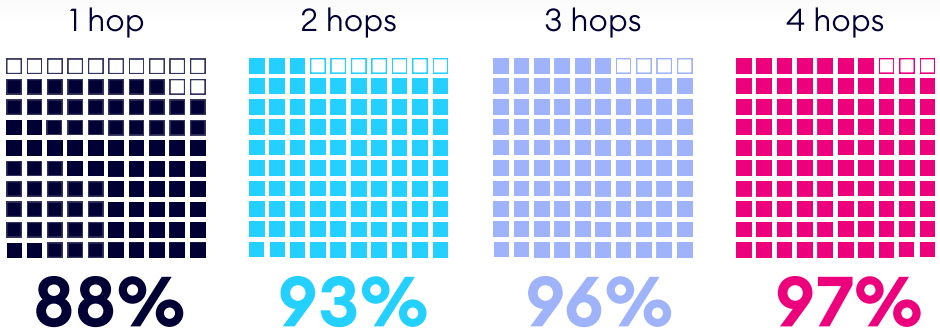


Figure 20: *Scope of critical assets at risk with each additional hop along cloud attack paths*

Why do cloud attack paths offer a fast-track to critical assets?
Part of the reason is that cloud security practices are still relatively immature in many organizations. Managing identities and permissions in cloud environments can be very different from their equivalents for enterprise infrastructure. Mistakes are common and many teams aren't trained on how to spot them.

Top cloud attack techniques

Appendix B lists the top techniques identified for attack paths in each cloud platform based on prevalence across organizations, total number of exposures, and critical assets at risk. Since that makes for a rather lengthy list, we highlight the three that grant the highest exposure of critical assets in Figure 21. A few observations stand out to us.

First, we note that attack techniques differ for each cloud platform. This is not a result of simply naming things differently. Each platform supports different configurations and comes with their own set of best practices. Each requires dedicated knowledge and skills to properly defend against attacks. The expanded list of platform-specific techniques in Appendix B reinforces this.

Want to know more about attack paths in the Cloud? Review our Continuous Exposure Management for the Cloud Use Case pages, to find out how you can gain holistic visibility and analysis for end-to-end exposure management. Or download our new eBook The Power of Attack Paths in Cloud.

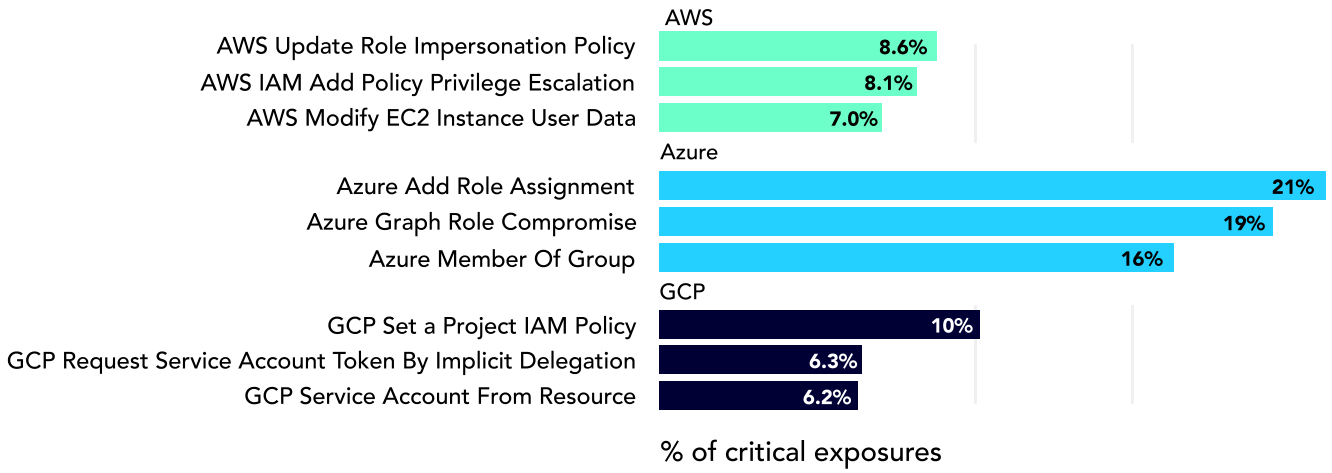


Figure 21: *Top techniques identified by attack path analysis for AWS, Azure, and GCP*

That said, we do find some common themes here. Most of these cloud attack techniques target credentials and privileges. Though each cloud has its own constructs and object types around identity, credentials, and access rights, they all suffer from misconfiguration issues. The complexity with identity management in cloud specifically is opening a new technology market for Cloud Infrastructure Entitlement Management (CIEM) as an extension to Exposure Management for the Cloud.

Our third and final observation related to Figure 21 derives from the first two. If attack techniques and configuration requirements differ among cloud platforms, then exposure management becomes even more difficult (and important!) in multi-cloud environments.

XM Cyber Takeaways & Recommendations

Cloud security isn't easy, and needs to be integrated in to your continuous exposure management security cadence. Here are some recommendations to help you achieve this, and to better protect your cloud infrastructure and the critical systems they host.

Establish your Cloud Risk Profile:

Know which clouds you are using, how many you have, what exactly are they doing, and who across your teams are responsible for managing and securing them. It's key to understand exactly what systems and services you are hosting, whether they are for internal use or customer facing. How critical are they to the business, what data are they storing, and should they really be there? Make sure to to check for all Cloud types and hosting locations, and not just the Big 3 public cloud providers.

Once you know the risk, now switch your focus to their Security Posture:

After establishing who the owner is for each cloud, it's good to know which team or individual actually configures their security. Do they have the knowledge, guidance and resources needed to properly manage and protect the systems that reside in the cloud? Do they have the tools they need and the policies they should adhere to? Make sure to regularly, if not continuously, assess the security posture and exposure risk, from both the inside and outside. As in, using cloud native or API-based security tools at the management and control plane level, along with internal sensors, that understand and assess assets at the individual entity level.

Cloud to on-prem interdependencies and attack path pivoting:

As mentioned in this report, due to the interdependencies between Cloud environments and your on-prem infrastructure, it's clear that in the majority of customers we analyzed, attackers can easily pivot from on-prem to Cloud, and from Cloud back to on-prem - siloed tools, or separate security policies that only cater for one of these locations, will lead to security gaps and plenty of places for attackers to hide.

Establishing consistent standards for cyber hygiene and security posture across all environments should be a primary focus of any Continuous Threat Exposure Management framework.

For more information on Cloud-specific attack paths, download our eBook, The Power of Attack Paths in Cloud.

Exposures in Active Directory

Organizations are still neglecting their largest attack surface!

Active Directory is the key to your network, responsible for connecting users with network resources—but it's also a prime target for attackers. An attacker who has compromised an Active Directory account could use it to elevate privileges, conceal malicious activity in the network, execute malicious code, and even gain access to the cloud environment.

	Organizations	Exposures	Critical Exposures
Member of Group	95.1%	13.9%	18.5%
Add Members to Group	94.4%	18.1%	10.7%
Reset User Password	92.6%	17.7%	8.68%
Add Logon Script	92.0%	17.4%	8.08%
Credential Harvesting	91.4%	1.81%	5.48%
Domain Credentials	90.1%	5.60%	13.9%
Resource-Based Constrained Delegation	89.5%	13.1%	11.9%
Add ACE to OU	83.3	2.12%	1.03%
Credential Dump	81.5%	3.81%	10.3%
Add ACE to Container	76.5%	0.0157%	0.188%
Credentials Relay	66.0%	0.277%	2.73%
Active Directory Modify Key Credential Link	54.3%	5.02%	2.72%

Figure 22: *Top techniques identified by attack path analysis for AWS, Azure, and GCP*

As we saw in an earlier section, Active Directory accounts for a huge proportion (80%) of security exposures across the typical enterprise network. Top attack techniques associated with those exposures are listed in Figure 22. Scanning the list reveals two broad categories of issues: misconfigurations and credential attacks.

Many of these exposures stem from the inherent nature of dynamic configuration issues in Active Directory as well as the challenge of keeping it updated. This creates a blind spot that appears secure on the surface but hides a nest of problems that many security tools can't see. For example, issues related to managing members and resetting passwords in Figure 22 present a challenge for nearly every organization.

Numerous high-profile attacks exploit credentials, which means adversaries go to great lengths to compromise them.

That's why techniques like credential harvesting, dumping, relay, and domain credentials feature prominently in Figure 22. Tools like Mimikatz make these techniques even easier to execute and are extremely popular.

Poor practices also make credential-related attack paths easier and more harmful. For example, we identified highly privileged Active Directory credentials cached on multiple machines in 79% of organizations. About 5% of Active Directory users have cached credentials and one in five of those have admin-level permissions on 100 or more devices.

Download this handy checklist to make sure you're following best practices and keeping your organization's Active Directory safe from threats

Download the Checklist

XM Cyber Takeaways & Recommendations

Active Directory is crucial to the functioning of your network, facilitating the connection between users and network resources. This is why it is also a top priority for cyber attackers, and when compromised, can put the entire business at risk, often with devastating consequences. As AD itself has been around for such a long time, and is pretty much the defacto Identity provider for any enterprise business, it's often taken for granted that the technology, people and processes around its security are well defined and optimized. However our research continues to show that this isn't the case.

AD continues to represent the largest attack surface of exposure and misconfigurations that an attacker can seek to take advantage of. It simply has a wider variety of attack techniques to escalate privileges, change group membership and extract key sources of identity information from.

This underscores the importance of safeguarding user credentials, systems, sensitive information, software, and applications to prevent unauthorized access.

Even in a world of Zero Trust, the basic hygiene of Active Directory is still being overlooked.

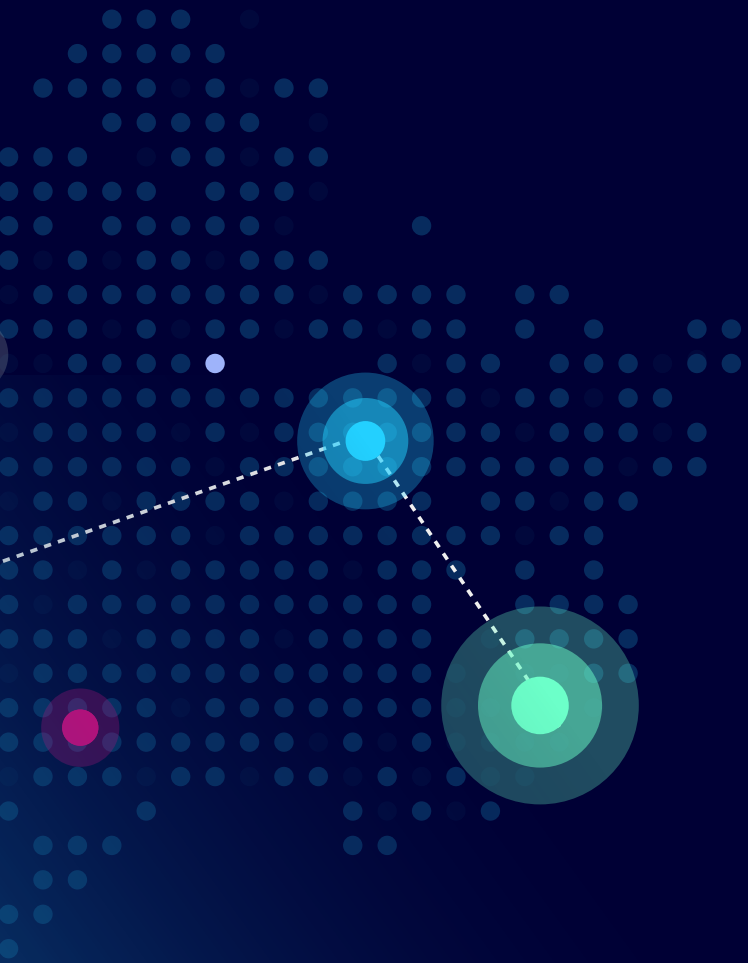
As such, we have recently published a new Active Directory Security Checklist as a quick handy guide to some of the best practices you can implement. We also recommend reading these lessons learned shared by the Microsoft Detection and Response Team.

Conclusion

In conclusion, the report highlights the importance of Exposure Management as a multifaceted task that involves more than just addressing vulnerabilities and CVEs. Organizations must transition to a holistic and continuous Exposure Management methodology, integrating attack path modeling to identify and remedy choke points in their infrastructure. The significance of addressing identity issues, Active Directory exposures, and poor cyber hygiene in cloud environments is emphasized, along with the need for customized solutions based on industry type and size. Effective utilization of tools like XM Cyber is crucial for successful Exposure Management, as evidenced by the correlation between security score and the number of exposures.

Despite the overwhelming number of security exposures identified across diverse attack surfaces, operationalizing effective Exposure Management through XM Cyber Attack Graph Analysis™, which focuses remediation efforts on choke points, validated and prioritized based on the risk they pose to business-critical assets, organizations can greatly enhance their security posture and reduce exposure risk.

The findings also stress the importance of adopting a Continuous Threat Exposure Management (CTEM) approach to improve overall security posture and mitigate risks across diverse attack surfaces. Common trends in security enhancements, such as reducing exposures and closing attack paths to critical assets, are identified, along with the significance of addressing critical security exposures, maintaining cyber hygiene, and securing Active Directory. Integrating cloud security and establishing consistent cyber hygiene standards are key steps to safeguarding infrastructure and critical systems. Overall, the report underscores the ongoing nature of security and the necessity of proactive measures to mitigate exposure risks in a dynamic threat environment.



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 2024

Appendix A: Security Posture Scores by Sector

Comparing overall security scores across industries in Figure A1 reveals some notable differences among them. We'll highlight three sectors that piqued our interest and leave readers to mull over scores for industries most relevant to them.

The Financial Services sector, which often ranks high for strong security posture, actually sits in the middle of the pack as measured here. While it's true that many financial firms have ample resources, they also tend to have high concentrations of critical assets that attract motivated attackers.

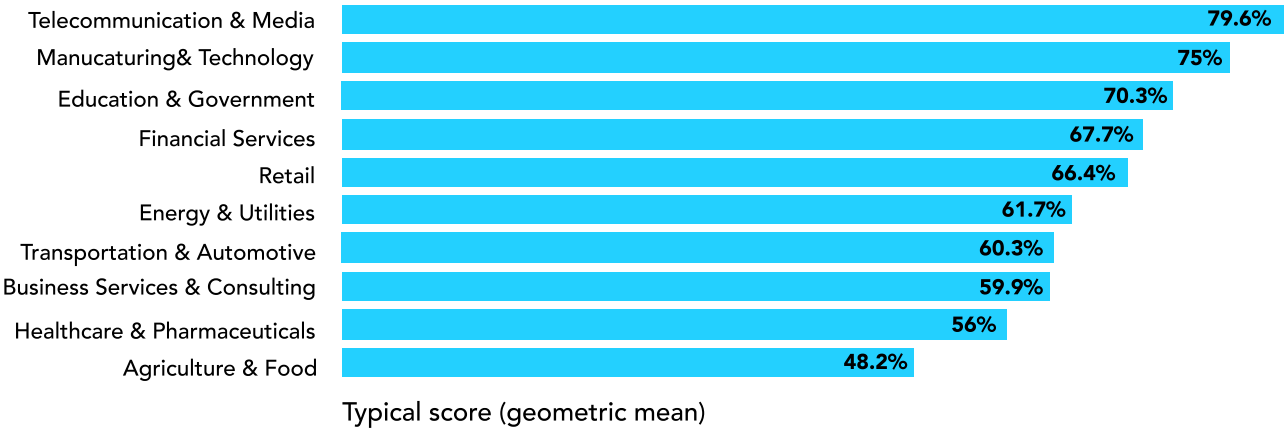


Figure A1: *Comparison of overall security scores by sector*

Healthcare institutions face numerous challenges when it comes to cybersecurity, and that fact is reflected in the relatively low security score for that sector. Those curious about the anatomy of attack paths in Healthcare can review two short case studies in this blog post from XM Cyber.

Finally, the Business Services industry warrants mention. Since such firms' primary mission is serving other organizations, their lower-tier score reinforces the importance of third-party risk management. Most service provider risk assessments are based on questionnaires or external assessments. This hints that probing deeper to understand the attack paths and asset exposures of the consultancies you work with could yield valuable risk insights.

We can also compare overall security scores based on organization size. One theory is that larger organizations with more resources and mature processes would maintain a stronger security posture (higher scores). An alternate theory is also plausible; large enterprises have large, complex environments that are MORE difficult to manage despite their greater resources.

Which theory is best supported by the evidence? Well, neither. As seen in Figure A2, overall security scores don't show an increasing or decreasing trend across the size tiers. The cluster of large enterprises with over 100,000 employees exhibits virtually the same score as the smallest companies with staff sizes under 100.

Figure A2: *Comparison of overall security scores by organization size*

Our takeaway from this is that cybersecurity challenges scale with the organization. Things won't get inherently easier or harder as your firm grows. Measuring risk to critical assets wherever you're at now and managing that reality to minimize exposure is imperative for organizations of all sizes.

Appendix B: Top Cloud Techniques

The figures that follow list the top techniques observed by XM Cyber during attack path analyses conducted in 2023. We use the same measures used throughout this report:

- **Organizations:** Percent of organizations susceptible to each technique
- **Exposures:** Percent of all platform-specific exposures identified by XM Cyber
- **Critical Exposures:** Percent of all platform-specific exposures to critical assets

	Organizations	Exposures	Critical Exposures
AWS Access Keys Stealer	30.2%	2.06%	1.37%
AWS IAM Add Policy Privilege Escalation	14.2%	10.7%	8.12%
AWS Update Role Impersonation Policy	13.6%	10.5%	8.63%
AWS Create User Access Key	13.6%	1.48%	6.54%
AWS Update Login Profile	13.6%	1.40%	6.38%
AWS S3 Bucket Read Data	13.0%	2.92%	1.80%
AWS S3 Bucket Write Data	13.0%	2.87%	1.72%
AWS EBS Share Volume Snapshot	12.3%	13.9%	0.0989%
AWS Modify EC2 Instance User Data	12.3%	12.3%	7.02%
AWS EC2 (AttachVolume, DetachVolume) Take Over	12.3%	12.1%	6.89%
AWS Over-privileged AWS EC2 Instance Creation	12.3%	1.36%	4.91%
AWS Add User To Group	12.3%	1.01%	3.43%
AWS AssumeRole Compromise	12.3%	0.312%	3.59%
AWS Update Lambda Code	11.1%	2.52%	4.42%
AWS Over-privileged AWS Lambda Function Creation	11.1%	1.37%	5.15%
AWS EC2 SSM SendCommand takeover	10.5%	3.21%	4.23%
AWS EC2 SSM StartSession Takeover	9.88%	2.92%	2.99%
AWS AssumeRole Compromise (Cross Account)	9.26%	0.153%	4.76%

Figure B1: *Top techniques in AWS environments*

	Organizations	Exposures	Critical Exposures
Azure Application Owner Can Compromise the Application Service Principals	31%	14%	4.4%
Azure Graph Role Compromise	31%	0.20%	19%
Azure Add Role Assignment	30%	0.66%	21%
Azure Access Token Stealer	28%	0.059%	0%
Azure Run Command On VM Using VM Extensions	27%	13%	4.7%
Azure Run Command On VM	27%	13%	4.5%
Azure Key Vaults Compromise	25%	0.56%	0.17%
Read OneDrive Files using Azure Applications	25%	0.026%	0.00014%
Modify OneDrive Files using Azure Applications	25%	0.025%	0.000058%
Azure Member Of Group	24%	0.71%	16%
Azure Tables Compromise	23%	20%	7.0%
Azure Read Blobs	21%	9.7%	3.1%
Azure Upload Blobs	20%	8.1%	2.6%
Azure Applications Can Add Passwords to Other Applications	19%	3.2%	2.8%
Azure Queues Compromise	17%	1.1%	0.42%
Microsoft Intune - Execute Script	15%	2.2%	1.3%
Azure Group Member of Group	9.9%	0.14%	3.4%
Azure Certificate Stealer from Disk	9.3%	3.7%	0.00029%

Figure B2: *Top techniques in Azure environments*

	Organizations	Exposures	Critical Exposures
GCP Access Token Stealer	14.8%	1.53%	4.10%
GCP Compromise Linux VM	6.79%	15.3%	4.79%
GCP Create Service Account Key	6.79%	12.1%	6.15%
GCP Write Data To Bucket	6.79%	5.93%	1.26%
GCP Read Data From Bucket	6.79%	5.59%	1.27%
GCP Read Secret	6.79%	5.46%	1.65%
GCP Set Storage IAM Policy	6.79%	3.02%	1.04%
GCP Create VM with Specified Service Account	6.79%	2.59%	5.47%
GCP Create Function with Specified Service Account	6.79%	2.49%	5.21%
GCP Service Account From Resource	6.79%	1.71%	6.19%
GCP Compromised Service Account Key	6.79%	0.165%	0.202%
GCP Read Firestore	6.79%	0.126%	0.0302%
GCP Request Service Account Token	6.17%	3.07%	6.13%
GCP Allows Signing of Arbitrary Payloads	6.17%	2.67%	6.00%
GCP Request Service Account Token By Implicit Delegation	6.17%	2.43%	6.29%
GCP Signing Well-Formed JWT	6.17%	2.42%	6.04%
GCP Set a Project IAM Policy	6.17%	1.78%	10.1%
GCP Set Service Account IAM Policy	6.17%	1.58%	5.57%
GCP Read BigQuery	5.56%	10.8%	2.55%
GCP Write BigQuery	4.94%	10.1%	2.49%
GCP Set a Folder IAM Policy	4.32%	0.104%	5.97%
GCP Member Of Group	3.09%	5.71%	6.01%

Figure B3: *Top techniques in GCP environments*

Appendix C: Top Attack Techniques

MITRE ATT&CK is a popular knowledge base of adversary tactics, techniques, and procedures (TTPs) used across the cybersecurity industry. Because of this popularity, we maintain a mapping between our attack path techniques and ATT&CK. Based on that mapping, Figure C1 lists the top ATT&CK techniques identified by XM Cyber in 2023.

***Figure C1:** Top ATT&CK techniques identified by XM Cyber attack path analysis during 2023*

	Organizations	Exposures	Critical Exposures
Valid Accounts (T1078)	99.4%	15.5%	37.2%
Use Alternate Authentication Material (T1550)	95.7%	10.3%	10.1%
Account Manipulation (T1098)	95.1%	36.3%	14.4%
Permission Groups Discovery (T1069)	94.4%	9.31%	2.72%
Remote Services (T1021)	93.8%	3.56%	6.58%
OS Credential Dumping (T1003)	93.2%	0.934%	1.53%
Boot or Logon Initialization Scripts (T1037)	92.0%	8.96%	2.06%
Scheduled Task/Job (T1053)	90.1%	2.88%	3.53%
Windows Management Instrumentation (T1047)	90.1%	2.88%	3.53%
Taint Shared Content (T1080)	89.5%	5.25%	2.88%
Adversary-in-the-Middle (T1557)	87.7%	0.951%	0.896%
Exploitation of Remote Services (T1210)	84.0%	0.355%	4.74%
Exploitation for Privilege Escalation (T1068)	83.3%	0.420%	2.60%

Figure C2 compares techniques that expose critical assets in on-prem networks, cloud platforms, and Active Directory. Overall, there's surprisingly little overlap between the columns. That suggests prioritization of TTPs and defenses should be done specific to the environment in view. It also reiterates the importance of context in threat and risk assessment.

***Figure C2:** Comparison of critical ATT&CK techniques identified by XM Cyber in different scenarios*

	Active Directory	Cloud	IT/Network devices
Account Manipulation (T1098)	33.5%		
Remote Services (T1021)	8.23%		31.5%
Scheduled Task/Job (T1053)	8.23%		
Taint Shared Content (T1080)			23.2%
Use Alternate Authentication Material (T1550)	15.3%	2.50%	26.3%
Valid Accounts (T1078)	6.77%	86.8%	
Windows Management Instrumentation (T1047)	8.23%		