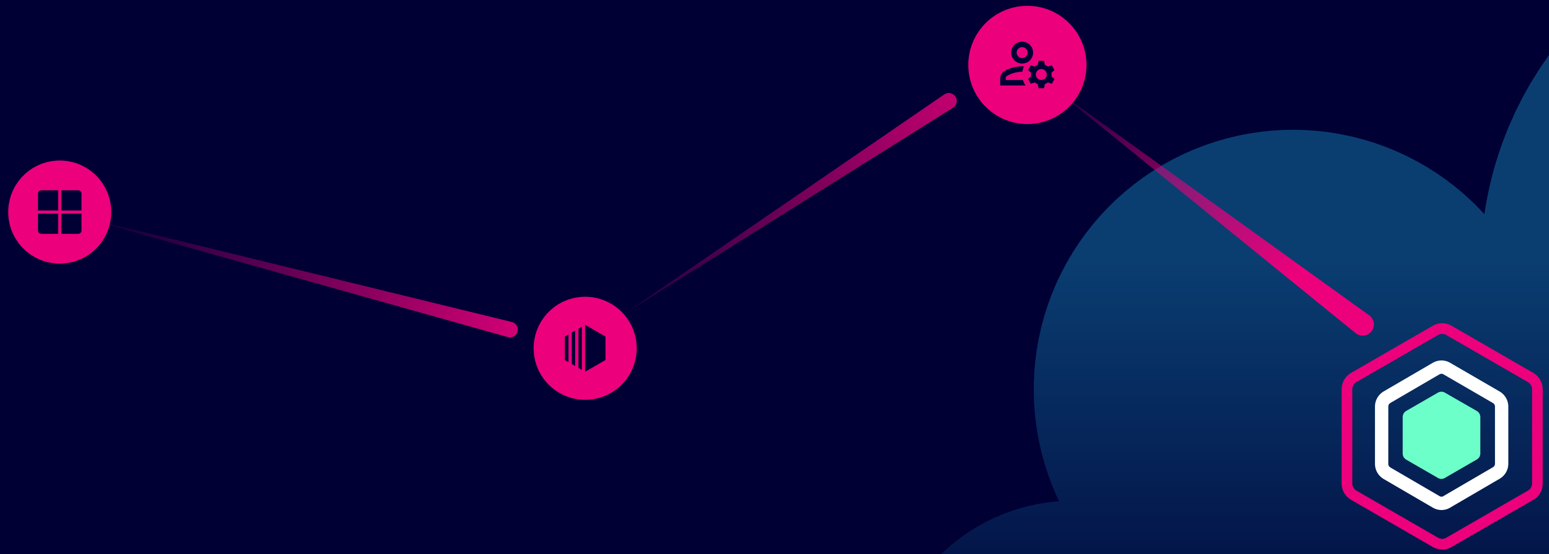
The Power of Attack Paths in the Cloud



XM Cyber

Introduction: Stuck Between a Rock and a Hard Place

In the ever-evolving landscape of cybersecurity, organizations have diligently implemented various tools and systems to identify and address security vulnerabilities. But despite these efforts, a significant challenge persists—the inability to visualize how these vulnerabilities interconnect and create critical security gaps. This disconnect arises from organizational silos, both on-premises and in the cloud, where different security aspects are managed independently.

Within your organization, you likely employ distinct tools to handle identity management, active directory, vulnerability scanning, misconfigurations, and security control configurations. While these tools serve their purposes, they often operate in isolation within different departments, hindering a comprehensive and cohesive understanding of your security posture.

What's missing is the ability to see your security landscape through the eyes of an attacker. An adversary possesses a unique advantage—they can discern how all the pieces of the puzzle fit together and skillfully leverage them to target your critical assets.

As more organizations make the transition from on-premises infrastructure to the cloud, this disconnect and its associated challenges are further magnified. Ensuring a secure cloud environment demands a fresh perspective—one that brings clarity to the relationships between various security components, identifying potential attack paths that may threaten valuable assets.

71%

of orgs have exposures in their on-prem networks that put their critical assets in the cloud at risk.

Once there,

92%

of critical assets become vulnerable.

The Big Disconnect: A Siloed Reality

Identity Issues

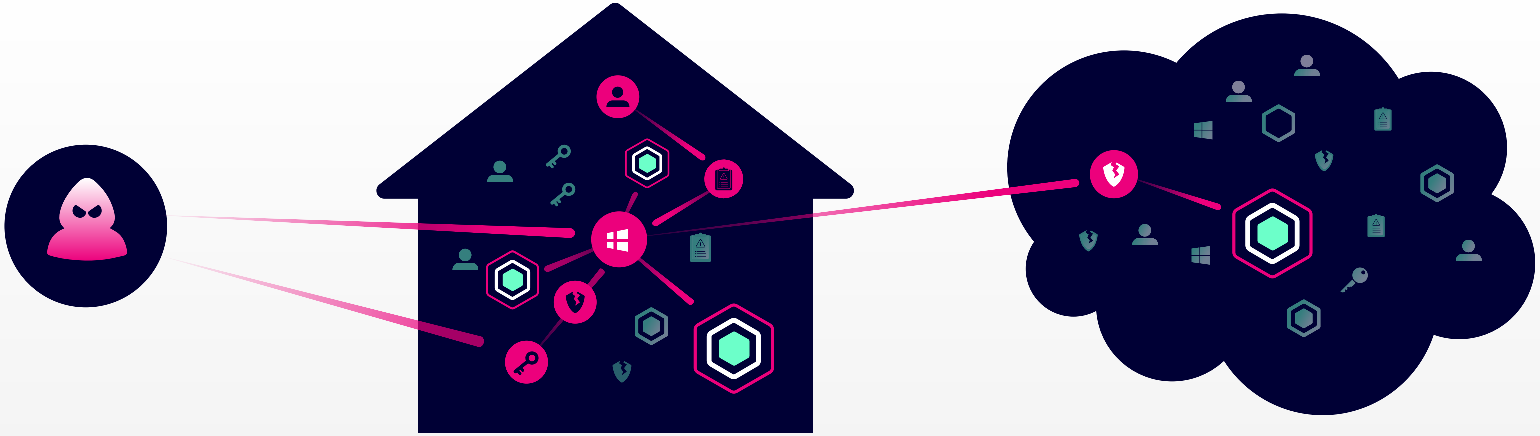
Alerts

Vulnerabilities

Security Controls Configurations

Active Directory

The Attacker's Perspective



On-prem
People, Processes & Technology

Cloud Environment
People, Processes & Technology

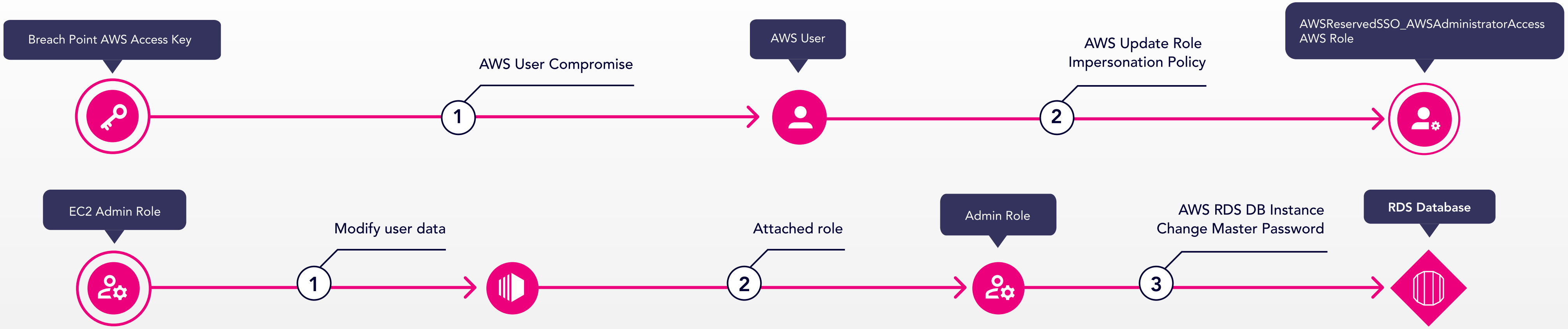
In this eBook, we delve into the intricacies of these critical attack paths in cloud environments that significantly impact organizations. Understanding these exposures and vulnerabilities is essential for developing robust cloud security strategies to safeguard valuable data and systems from potential threats.

Join us as we explore these real-world attack scenarios and equip your organization with the knowledge needed to bolster cloud security defenses effectively. By harnessing the power of attack graphs, you can proactively anticipate potential attack scenarios and strengthen your cloud defense strategies.

Critical Cloud Attack Paths Affecting Organizations

In the following 5 examples, we will delve into anonymized attack scenarios we came across within the customer environments. By deeply examining how exposures chain together to create attack paths, we can see what actions need to be taken to cut attackers off at key choke points.

#1. Privilege Escalation with Ease


Breach Point AWS Access Key
AWS User Compromise
1
AWS User
AWS Update Role Impersonation Policy
2
AWSReservedSSO_AWSAdministratorAccess AWS Role
EC2 Admin Role
Modify user data
1
Attached role
2
Admin Role
AWS RDS DB Instance Change Master Password
3
RDS Database

The Risk:

This role receives a custom managed policy that can be leveraged to allow users to escalate to admin privileges.

The Finding:

Many roles have permissions enabling several privilege escalation attack techniques; Managed policies are often used with potentially unintentional increases in risk exposure.

This example shows an easy way to escalate permissions within the AWS environment.

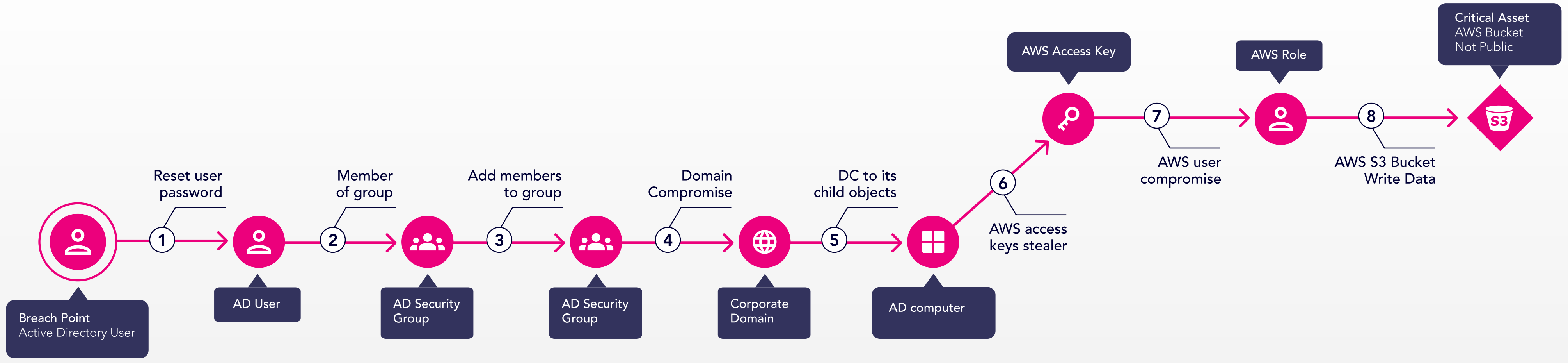
In the first vector, the focus lies on a compromised access key, which serves as a potential gateway for unauthorized pivoting within a cloud account. This compromised access key was related to an AWS user. The user could modify the role impersonation policy of an administrative role and compromise it, which means that the attacker could compromise the whole AWS account. The risks associated with such actions are evident.

In the second vector, the attacker was able to compromise an EC2 admin role, which means that, by design, they could manage (and obviously compromise) all EC2 instances. One of the instances had an administrative role attached to it, allowing the attacker to gain access to everything within the account – and one of the assets was an RDS database that contained sensitive information.

What's important to note is that these permissions were originally configured by the team to facilitate functionality and workflow within the cloud platform. However, from an attacker's perspective, these same permissions can be exploited for malicious purposes, allowing them to pivot freely within the cloud infrastructure.

It is crucial for organizations to be aware of these vulnerabilities and take proactive measures to prevent such incidents. Understanding the configuration and thoroughly examining permissions can go a long way in safeguarding the cloud environment from potential threats.

#2. Active Directory to AWS



The Risk:

An Active Directory user could compromise the entire organization.

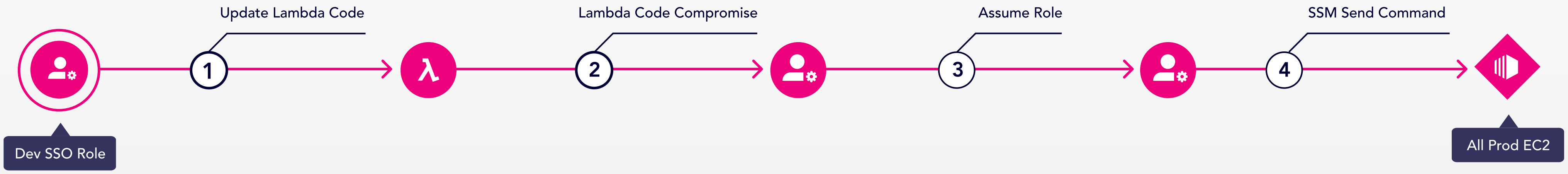
The Finding:

The attacker got a foothold inside the organization network, and tried to leverage it to reach to the cloud.

This path was initiated when a user received a phishing email and clicked a malicious link. This particular user had elevated password privileges and now the attacker was able to reset user passwords which meant he could elevate privileges and jump to the next user. Then he had permission to add members to that strong group and inherit all the permissions there. He added himself to the helpdesk group, which is a very strong group which allowed the attacker to elevate more permissions, and therefore to add domain admin permissions. He could then compromise all the domain's admins and get access to the entire domain.

Then from the Domain Controller, the attacker could get to the child objects – in this case, the computers – to make their way onto Steve's computer. On this computer, he found an AWS access key and with that access key, he could compromise users in IAM, create new EC2s, add more resources and get to the S3 buckets to write data.

#3. Account Takeover Compromise at a Fortune 500 Bank



The Risk:

Attacker compromising SSO credentials with access to AWS.

The Finding:

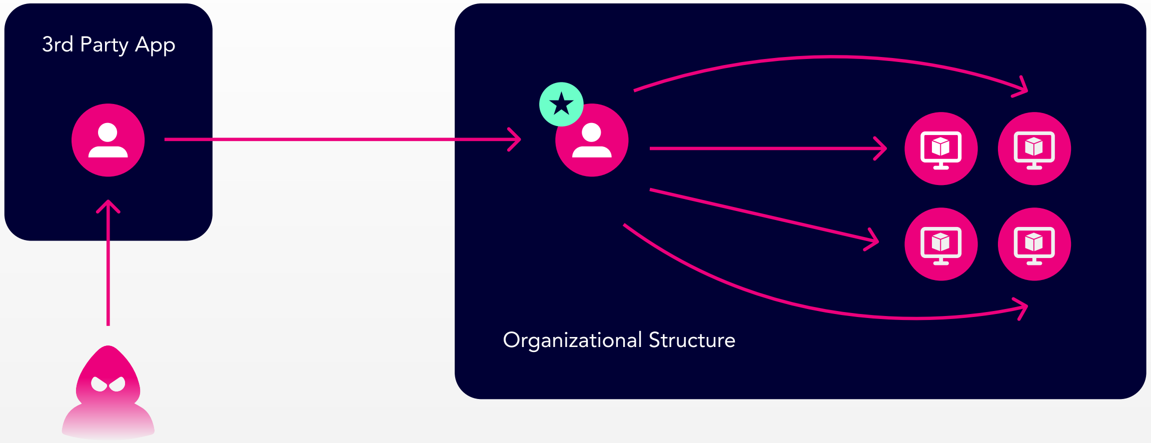
The bank was able to identify that an attacker with access to this low-level role could escalate privileges in 4 steps to compromise ALL production EC2s in the AWS account.

In this example, we explore a scenario where an account was compromised through two different roles initially associated with DevOps tasks. The situation arose when a developer was granted excessive permissions, and was able to update lambda code, leading to the compromise of their system role. As many are aware, the system role holds significant privileges within the AWS console, enabling control over all the institutions and systems in production.

Historically, this issue occurred due to an oversight. The developer's role was mistakenly left with elevated privileges, granting access to critical resources. Initially, this role was intended for use during the migration and setup of various accounts and objects in the cloud. Unfortunately, there was no system in place to monitor and detect such lingering high-privileged roles, posing a risk to the organization.

Upon discovering the issue, immediate action was taken to mitigate the risk. The developer's excessive permissions were promptly removed from the policy, and necessary remedial measures were implemented to address the vulnerability. By rectifying this oversight and enhancing role management protocols, the organization was able to improve its security posture and minimize potential threats to the cloud infrastructure.

#4.
3rd Party Risk to Azure Environment



The Risk:

An attacker compromises an external user of the Azure tenant and can compromise all virtual machines.

The Finding:

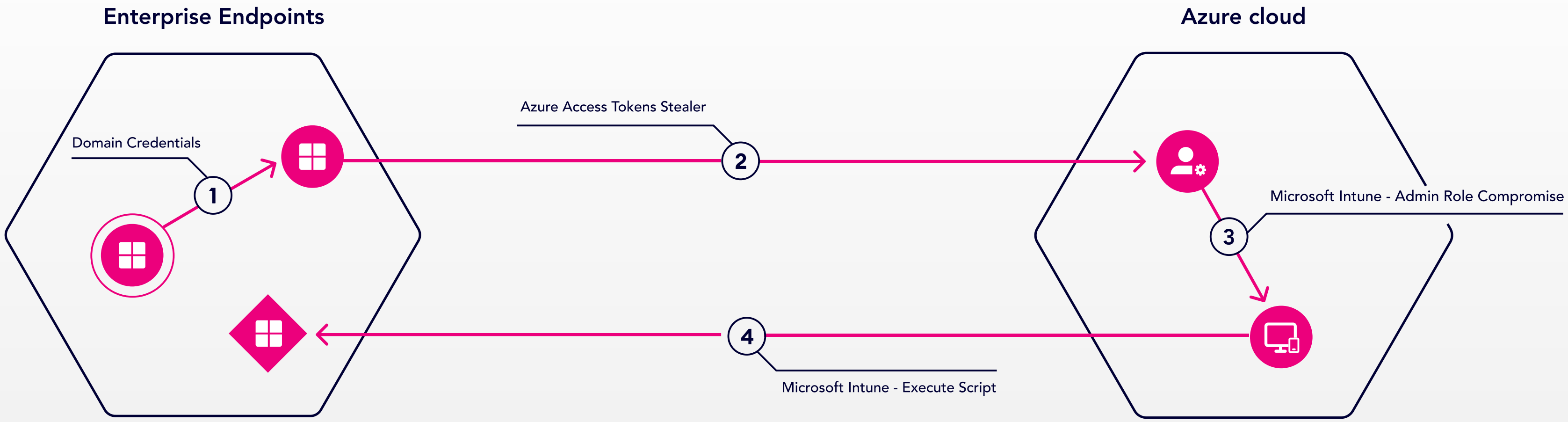
The customer forgot to remove an unused external user (3rd party vendor) of an Azure tenant. This user had elevated privileges and was able to take over the whole tenant.

This is an example of a scenario that has been a recurring issue in real-world attacks, particularly within Azure environments. As organizations use Azure Active Directory, they often create external user accounts to accommodate contractors, third-party vendors, or support personnel engaged in migration projects, managed by external service providers. However, understanding the associated risks is imperative.

These external users typically receive limited permissions, primarily for email or accessing specific Office 365 applications. The concern arises when certain permissions are mistakenly or intentionally granted for additional commands, only to be forgotten over time. In such cases, while these privileges may have been legitimately assigned for a valid project or action, they might be left unused or unnoticed for an extended period.

Consequently, if a compromise occurs, and the external user's account is breached, the consequences can be severe. The attacker could potentially exploit these permissions to gain control over and compromise all the virtual machines (VMs) within the affected customer's account.

#5. From On-Prem to Cloud and Back


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

The Risk:

A compromised on-prem desktop offered a low-sophistication attack path to compromise AD via Azure.

The Finding:

An Intune Admin was able to compromise AD.

In this example, we examine a hybrid attack path that extends from an on-prem environment to Azure and then back to on-prem. This scenario can happen when companies employ Microsoft Intune, a comprehensive solution for managing laptops and endpoints.

The attack starts by compromising user credentials, typically through the discovery of login details that grant access to Azure services and the cloud environment. Once a user with administrative permissions in Intune is identified, the attacker gains an important advantage. With these privileges, they can assert control over all devices managed by Intune by executing a script remotely on the targeted devices.

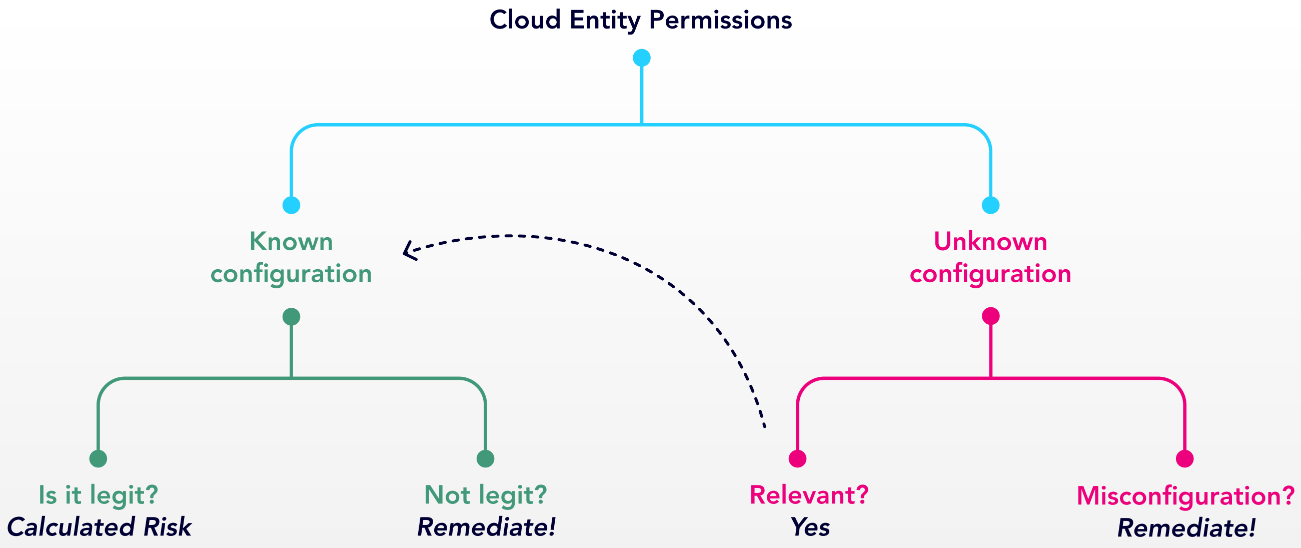
The consequences of this compromise are particularly concerning when we consider that the affected part of the network is the sensitive Active Directory. This critical component can become vulnerable due to the chain of misconfigurations and exploits, leading to an unforeseen and often unknown risk.

Such hybrid attacks, traversing from on-prem to the cloud and then back again, are frequently executed in a round-robin fashion, making detection even more challenging. Unfortunately, many organizations remain unaware of the existence of such attack paths, exposing them to potential security breaches.

How to Identify Cloud Risks & Best Practices to Increase Cloud Security Posture

Cloud Risk Approach

The following flow will assist with addressing the potential risk and determining the next steps in such cases.



Let's explore an effective approach to managing cloud risk and mitigating potential vulnerabilities. By following this methodical flow, organizations can address risks and determine the necessary steps to enhance their cloud security posture.

When analyzing cloud entity permissions, it is essential to examine the configuration of each object. Whether presented in reports or other analytical tools, the first step is to ascertain the familiarity of the object's role and associated security policies. If the configuration is known and considered legitimate, the risk can be calculated accordingly.

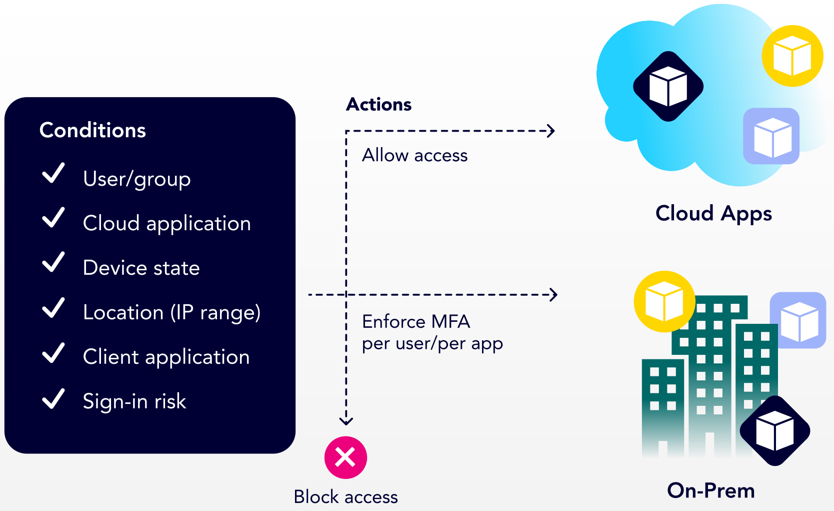
However, if the configuration is not legitimate, indicating unexpected or undesired permissions or roles, immediate remediation is imperative. By adjusting the object's configuration, organizations can ensure that it adheres to the intended security policies.

For objects with unknown configurations, caution is warranted. A "yellow card" scenario emerges, signifying the need for further evaluation. Organizations must determine whether the permissions are necessary for the object's function. If the required permissions align with a known and acceptable configuration, no action is needed.

In contrast, if the unknown configuration represents a misconfiguration, indicating unauthorized or unintended permissions, swift action is required. Organizations should directly rectify the situation by correcting the misconfiguration and ensuring it aligns with the intended security policies.

Best Practices to Increase Cloud Security Posture

1. Logs/Logging
2. Least Privilege Concept
3. Privileged Identity Management (PIM)
4. Conditional Access



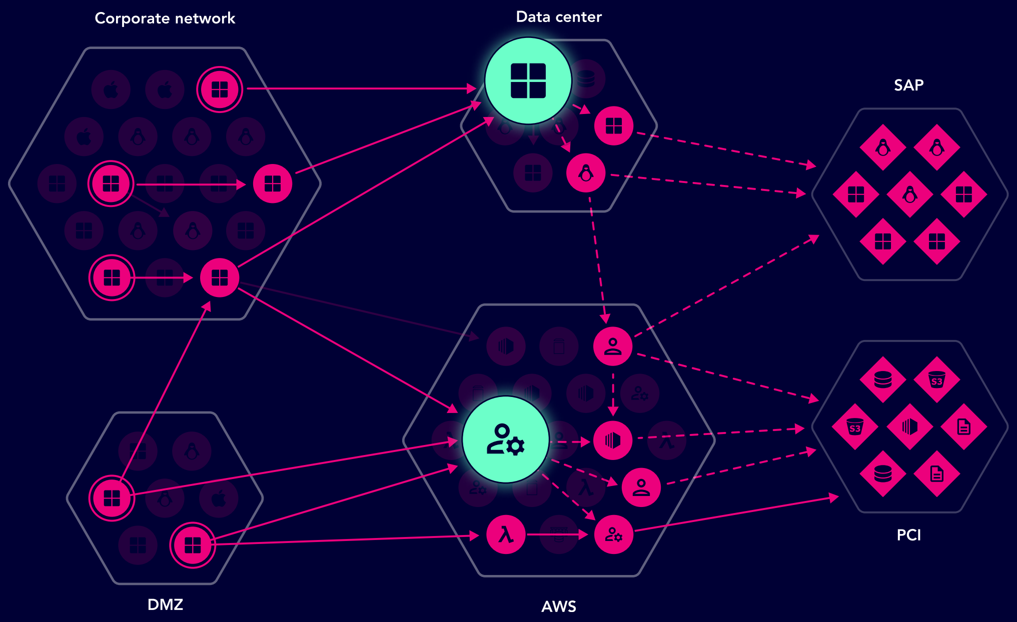
First and foremost, logging plays a critical role in cloud security. Despite the associated storage costs, enabling comprehensive logs provides invaluable visibility into the cloud environment. By focusing logging efforts on the most sensitive parts of the infrastructure, organizations gain essential insights to build robust security processes.

The least privilege concept is fundamental in preventing potential attacks. By carefully assessing existing permissions and policies, organizations can identify sensitive network areas and potential risks.

Custom roles offer a preferred approach, allowing precise control over permissions and avoiding overly permissive built-in roles. Adopting a whitelist approach further enhances security, ensuring a clear understanding of allowed actions and minimizing potential role chaining.

Incorporating Privileged Identity Management (PIM) is crucial, particularly in cloud environments like Azure. By applying PIM on sensitive roles and users, organizations enhance visibility and gain significant control over permissions, preventing unauthorized access to resources.

Finally, the significance of conditional access cannot be overstated. Conditional access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. This well-established concept remains essential for controlling access to sensitive actions and resources. By setting conditions for access, organizations can ensure that only authorized personnel can reach critical resources, mitigating potential risks.



Conclusion

By mapping exposures against the automated discovery of attack paths in the environment, the amount of risk created by exposures becomes clear. This illuminates the handful of exposures that actually pose risk among the many thousands that don't.

XM Cyber addresses the challenges of mounting security issues and complex hybrid cloud environments. By incorporating the internal context of exploitability along attack paths to critical assets, XM Cyber transforms *perceived* risk into *actual* risk. This approach enables organizations to establish a common language for discussing risk, facilitates team alignment and collaboration, and delivers measurable risk reductions. Moreover, it alleviates security and IT frustrations and enables executive reporting on risk reduction.

XM Cyber

Learn More

Book a Demo