XM Cyber

Attack Path Management Impact Report

2021 Year in Review

Insights from the XM Cyber Research Team

XM Cyber

Table of Contents

About XM Cyber Research

XM Cyber Research is a top tier research team that eats, sleeps and breathes attack path management. Analyzing the platform and constantly understanding today's threat landscape keeps the platform up to date with the latest attack techniques used in the wild as well as the research team's own personal findings.

Executive Summary

XM Cyber's first annual Impact report. This report shares insights from the XM Cyber Research team's analysis of the Attack Path Management platform from January 1st, 2021 – December 31st, 2021

The Impact report begins with a close look at the methodology of attack paths and then reveals the impact of attack techniques used to compromise critical assets across organizations, whether hybrid, on-prem or multi-cloud.

Close to 2 million entities were analyzed as part of the report. An entity represents an endpoint, file, folder, or cloud resource in the environment the attacker can use to advance in an attack path towards your critical assets.

Key insights from this year's report include:

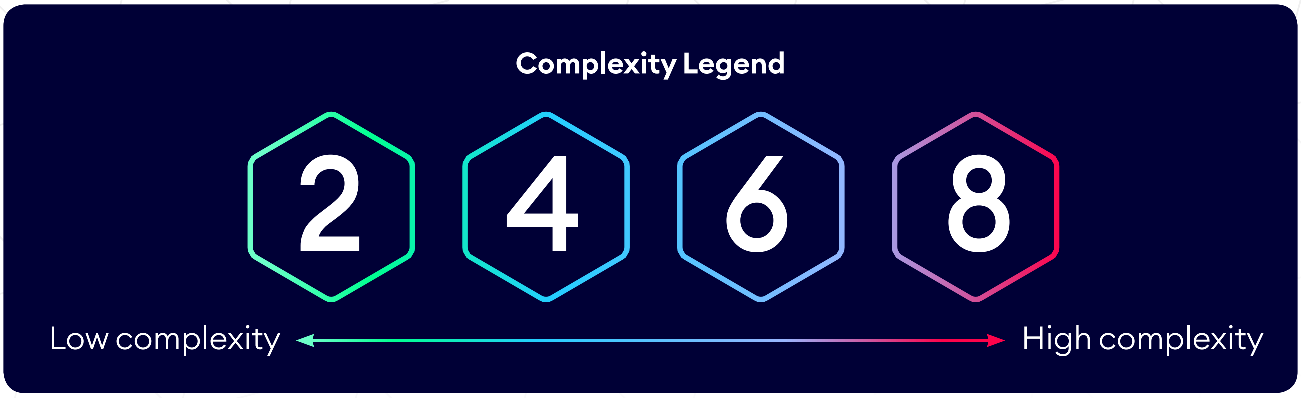
- In less than 4 hops, 94% of critical assets can be compromised from the initial breach point
- 75% of an organizations' critical assets could have been compromised in their then-current security state
- 73% of top attack techniques involve mismanaged or stolen credentials
- 95% of users in an organization have long term access keys attached to them which can be exposed creating risk to critical assets
- 78% of businesses can potentially be compromised whenever a new RCE (Remote Code Execution) technique is found
- 75% of organizations have an external facing EC2 machine posing risk to critical assets
- 80% less issues to remediate by knowing where to disrupt attack paths

Methodology of Attack Paths

XM Cyber's graph-based simulation technology continuously discovers the attack paths that lead to critical assets, enabling full visibility into organizational security posture. This allows users to understand how vulnerabilities, misconfigurations, user privileges etc. chain together to create a cyber-attack path that jeopardizes critical assets.

At XM Cyber, we determine the likelihood of compromise to a critical asset by two main factors, the complexity of the attack and how many hops it takes an attacker to get to your critical assets. By combining the complexity and the amount of hops it takes to put critical assets at risk is how we analyze attack paths and calculate the actual risk.

Complexity of an Attack



Complexity Legend

2 4 6 8

Low complexity ← → High complexity

The complexity of an attack path across entities is determined by many factors, including what prerequisites are required, how long it takes, what access is needed, and how many steps are needed for the attacker to get from the breach point to your critical asset. At each step in the path, the attacker uses a technique to compromise the entity, and uses that entity to step to the next entity in the path on his way to the target.

Based on the complexity of the attack path, we are able to determine what percentage of critical assets can be compromised across organizations in their then-current security state:

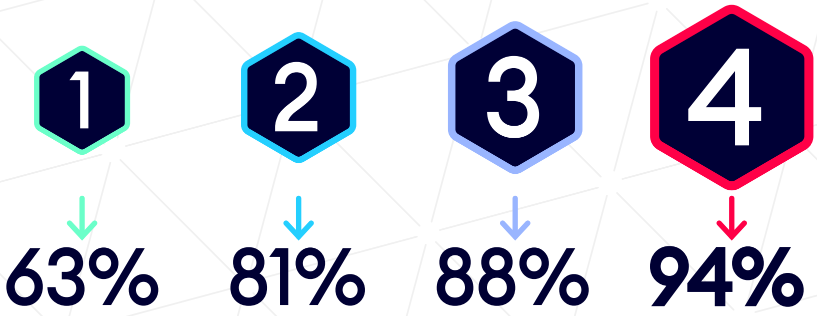
2 → **55%** 4 → **66%** 6 → **70%** 8 → **72%**

Any complexity → **75%**

Bottom line: *The majority of our assets can be compromised – without knowing where to look we are blind. Prior to the emergence of attack path management, there was not an efficient way to identify and then break the critical points in the attack chain. In order to do that, you need a clear view into the entirety of your environment from the eyes of an attacker. It is not enough that you are just monitoring the threats and alerts; it's about understanding the context of these vulnerabilities within your environment and the attack paths that these vulnerabilities offer to an attacker looking to breach your critical assets. This is achieved through a deep analysis of the environment and only then can we define the steps needed to eradicate, or at least mitigate, the risk to our organizations.*

How many hops to asset compromise

Definition of hops – the amount of steps an attacker takes from breach point to compromise of critical assets. Each hop uses a single attack technique.



1	2	3	4
63%	81%	88%	94%

In 4 hops or less

94%

of critical assets can be compromised from the initial foothold

Bottom line: *Majority of attacks that take place involve more than just 1 hop to reach an organizations' critical assets. It is during the network propagation stage that the attacker is trying to connect exploits together to breach critical assets that we can leverage attack path management to see all the ways they can connect techniques and cut them off at key junctures. In just 4 hops the attacker can almost compromise anything they want in the environment - if in just 4 hops they can compromise 94%, in just another hop or two it can be 100%. It is important to note traditional Breach & Attack Simulation (BAS) solutions can only check one of the hops in an attack path, siloed, while our attack path management platform models the entire attack path across the whole environment.*

Synopsis of an Attack Path

In order to effectively secure your assets you need to know where they are – these assets could be virtual servers, they could be data, they could be functions or any other category of technology asset that supports the enterprise. Our technology makes it simple to see precisely how a combination of exploits chain together to form attack paths from breach points to critical assets. The XM Cyber Research team will reveal insights into all the different types of attack techniques and multiple attack paths threat actors use to compromise organizations.

Attack Vectors

An attack vector is a method that cyber-attackers use to compromise a system. Although the terms are sometimes mixed, attack vectors are not to be confused with an attack surface, which is best defined as every possible point where an adversary can attempt to gain entry into your network or system.

An attack path is a visualization of the chain of events that occurs when attack vectors are exploited. In this sense, an attack vector acts as a doorway, while an attack path is a map that shows how an adversary entered the door and where that adversary went.

Malware, ransomware or phishing are all examples of common attack vectors. While cloud attack vectors can be used to target a security gap within your network or system, vectors can also be leveraged to exploit human error.

Adversaries will often take advantage of multiple vectors when conducting an attack. When you combine multiple attack techniques together you can create an attack vector and when you combine multiple attack vectors together you can create an attack path. It's also important to know that attack vectors may exist even when they appear to be mitigated. For example, creating an extremely strong password won't help much if you don't realize that password is available on the dark web, just waiting for an attacker to use it against you. The attack path management platform's uniqueness is that it can generate many combinations of different attack techniques to create a single attack flow, hence the real number of attack techniques is much larger.

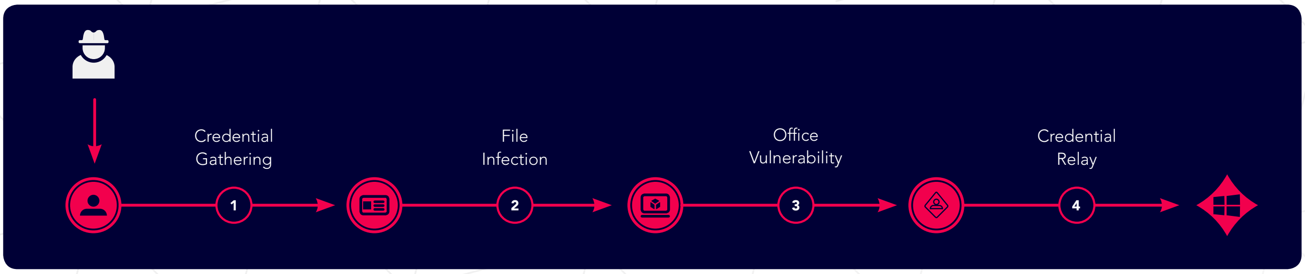
Here is an example of how an attacker can join techniques together to make an attack vector:

1. Uses one of the Credential Gathering techniques (of which there are many)

2. Uses a File Infection technique to infect an Office file

3. Uses an Office Vulnerability technique to grab NTLM SSP

4. Uses a relay technique, for example NTLM, to relay this credential and compromise the asset



Example Attack Vector

Each of the above steps could be replaced with other techniques. For example:

The attacker could replace the Office vulnerability with a Foxit Reader Vulnerability technique and compromise the node immediately.

With some red computers acting as the file share, the attacker could also replace the credential gathering techniques and file infection with the local File Infection technique.

The attacker could replace the Office exploit with the forced authentication technique and only then relay the credential.

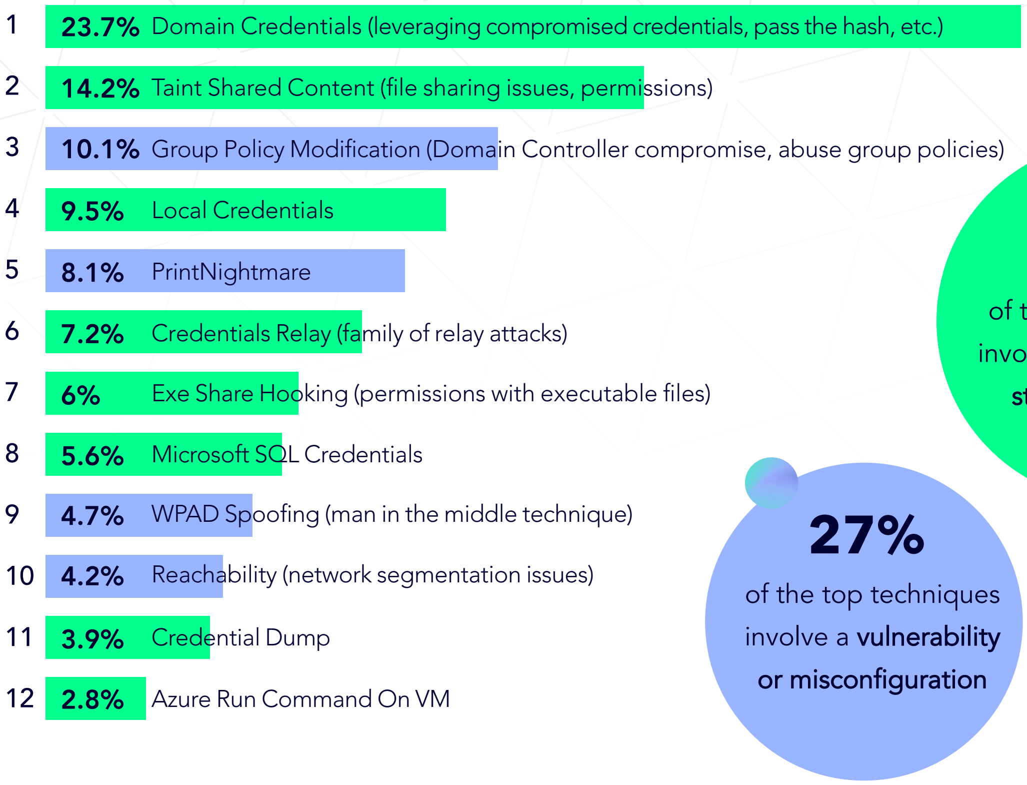
Many of the attack techniques have been mapped and aligned with MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework, while others are unique to XM Cyber, based on the XM Cyber Research team's vast cyber offensive expertise.

Credentials are the Achilles Heel of the Cloud:

2021 Top Attack Techniques used to Compromise Critical Assets

When it comes to securing the cloud, knowing is half the battle. Each cloud provider has differing, but usually complex, configurations to grant access and authorization to services and resources. Determining the exact roles and appropriate level of permissions for each user can be difficult and time consuming. Permissions within cloud providers are granular and complex, often inhibiting least privileges approaches when developers or operators may (unfortunately) seek shortcuts – or perhaps be subject to time constraints that make adopting such good practices difficult. For example, when creating a custom policy with permissions on an EC2 instance, it may be time consuming to allow permission for each user that potentially needs access, but much quicker to just allow permission for a whole group. Let's examine the key attack techniques that took place across environments and see what security teams need to focus on when applying their security measures across the hybrid cloud.

Top 12 attack techniques analyzed used a combination of the following vulnerabilities, misconfigurations and mismanaged or stolen credentials to compromise critical assets:



73%

of the top techniques involve **mismanaged or stolen credentials**

27%

of the top techniques involve a **vulnerability or misconfiguration**

__Bottom line:__ strong patch management will reduce attack vectors and prevent vulnerabilities from being exploited. In addition, by using security features from the operating system itself, like user authentication, we can prevent lots of attack vectors that abuse the different credential issues. Not only should we focus on vulnerabilities, it is a misconception to believe patching CVEs will fix everything and stop lateral movement. The research shows nearly 30% of an attacker's techniques abuse misconfigurations and credentials to compromise and breach the organization.

Top 6 AWS attack techniques used:

1	**24.5%**	User Exploit
2	**19.5%**	EC2 Exploit
3	**16%**	Update Role Trust Relationship
4	**16%**	EC2 Modify Instance User Data
5	**12%**	Abuse Assume Role Permissions
6	**12%**	Credentials Stealer

64%

of top AWS techniques involve **mismanaged or stolen credentials**

36%

of top AWS techniques involve **vulnerability or misconfiguration**

Top 6 Azure attack techniques used:

1	**35%**	Abuse Run Command On VM
2	**21%**	Abuse Microsoft Intune Execute Script
3	**15.5%**	Abuse Run Command On VM Using VM Extensions
4	**12.5%**	Application Owner Can Compromise Service Principle
5	**8.5%**	Read Blobs
6	**7.5%**	Upload Blobs

100%

of top Azure techniques involve **mismanaged or stolen credentials**

__Bottom line:__ credentials are here to stay, but in truth they are harder to resolve, while vulnerabilities come and go and are easy to patch. The main attack vectors in the cloud are misconfigurations and over permissive access that attackers can leverage to get to critical assets. Attack path management can help identify exposures that combined together grant attackers access to the cloud.

Eradicate Risk at Key Junctures

One way to prioritize security team activities is to identify where attack paths converge towards critical assets and focus remediation efforts there. The XM Cyber Attack Path Management platform continuously uncovers hidden attack paths to your critical assets across cloud and on-prem environments, so you can cut them off at key junctures and eradicate risk with a fraction of the effort. This overcomes the big disconnect that security teams experience when they're presented with endless alerts, yet can't see which exposures impact risk the most, how they come together to be exploited by an attacker, or how to efficiently eliminate them.

Of the almost 2 million entities across organizations - on average a mere **5 entities** are responsible for creating risk to almost **58% of critical assets.** That's more than half of the organization that can be compromised.

__Bottom line:__ by directing resources to fix issues at individual choke points, you can quickly reduce overall risk and the number of potential attack paths. Organizations using XM Cyber can see the smallest number of actions to be taken that have the biggest impact on risk.

New Attack Techniques Used in 2021

When we analyzed the new attack techniques that were used in 2021 alone, it revealed how wide the attack surface is and how Advanced Persistent Threats (APT) are being used. APT attacks are all about combining multiple techniques to compromise the target.

Of the new techniques in 2021 used against organizations we wanted to understand how many of them actually appear in environments. The XM Cyber Research team took all the attack techniques and categorized them into three groups: cloud techniques, Remote Code Execution (RCE), and techniques that combine the cloud and RCE attacks together to understand what the impact is towards an organization being compromised. The XM Cyber Research team analyzed the attack techniques that could be discovered in environments:

87%
of all new cloud techniques were found in environments

70%
of new RCE techniques were found in environments

82%
of new techniques that combine RCE/Cloud were found in environments

vs these attack techniques that could be simulated and potentially compromise organizations:

32%
of organizations could be compromised by new cloud techniques

78%
of organizations could be compromised by new RCE techniques

90%
of organizations could be compromised by new techniques that combine RCE/Cloud techniques

Bottom line: *these are techniques organizations need to focus on and actively work to eliminate them in their environment. Nearly 80% of organizations can be compromised when a new RCE technique arises and when strung together in an attack path with cloud techniques, 90% of organizations can be compromised with their current security state. Clearly the organizations' patch management is sub-par and not effective if so many vulnerabilities can easily be exploited.*

Your Cloud is not Isolated, Cross Platform Insights

As a leading hybrid cloud security company we wanted to see what insights we gather from cross platform attack techniques. Not just the cloud, but from on-prem to the cloud and back again.

On average

23%

of all critical assets had a compromising attack towards them involving a technique that was classified as cross platform. The attack originated on-prem and the asset was a cloud entity, or vice versa

On average

28%

of all organizations can experience a cross-platform attack

Bottom line: *You are not alone in the cloud. The XM Cyber Research team predicts this number will only grow due to the accelerated digital transformation across enterprises as we are already seeing this number increase looking into 2022.*

The Road Less Traveled

With the attack path management platform continuously and safely running simulated scenarios 24/7 against the newest threats, not all attack paths are successful. By saving analyst time and cutting off attack paths at key choke points, with a least cost, maximum impact approach we can reveal how organizations using XM Cyber in fact have 80% less issues to remediate by knowing where to disrupt attack paths.

80%

less issues to remediate by knowing where to disrupt attack paths

80% of entities were discovered with security issues however they did not put at risk or attack any critical asset, meaning, they were dead ends. Typically security teams would have worked to resolve these issues, defocusing their efforts on what really matters. As a result, there is no need to focus time and resources to fix these issues immediately as they don't pose a threat, regardless of the vulnerability severity or how many alerts there are. In a typical enterprise this would be thousands of vulnerabilities and alerts that security teams receive which they don't need to deal with as urgent.

Bottom line: *Understanding attack paths and attack vectors — and how the smart practice of attack path management can minimize risk — should be a key priority for defenders. We can't defend effectively against what we can't see, which means that visualization of attack paths, and the risk they present to business-critical assets, is one of the best tools we have to know where to focus our resources and how to protect our business.*

Key Findings across On-prem and Cloud

Attack paths can become very complex in hybrid network architectures. The research shows the security gaps and attack techniques that exist across our on-prem and cloud environments and how important it is to not just focus your security efforts on a specific environment but to view your critical assets holistically across all environments in the network.

Businesses do not always clearly define a strategy in their migration to the hybrid cloud world. Organizational decisions can be made to allow individual units to adopt their own migration strategies but sometimes business units make their own arbitrary decisions to source cloud resources without input from IT. Sometimes the lack of a single strategy is down to wider business events, like if an organization with one cloud vendor acquires or merges with another organization using a different cloud vendor. This unplanned large scale of cloud environment complexity and attack surface volume affects security across the entire enterprise IT resources, including: your assets, network security, security of your platform, and application security.

The XM Cyber Research team key finding: an Intune Administrator user was able to compromise Active Directory. In the finding below a compromised on-prem desktop offers a low complexity attack path to compromise Active Directory via Azure.

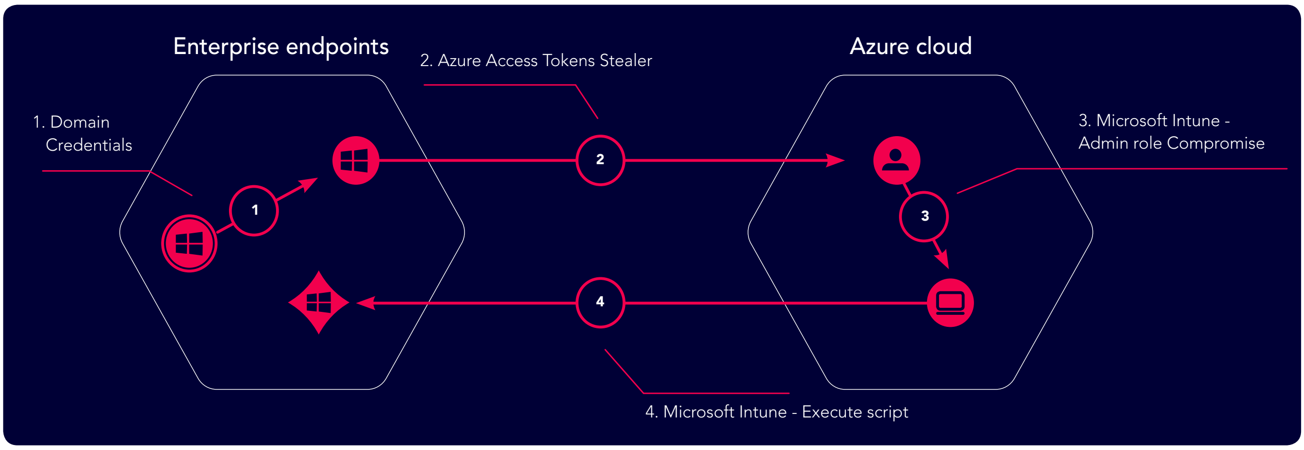
Here is an example of how an attacker can compromise Active Directory:

Hop 1: the initial breach point is via compromise of a Windows machine

Hop 2: the attacker steals domain credentials from the breach point

Hop 3: the hacker takes the access token from the compromised endpoint and uses it to authenticate to the Azure tenant

Hop 4: the compromised access token has Intune privileges and allows attacker to execute commands back on the on- prem critical asset machine(s)


Enterprise endpoints
2. Azure Access Tokens Stealer
Azure cloud
1. Domain Credentials
3. Microsoft Intune - Admin role Compromise
1
2
3
4
4. Microsoft Intune - Execute script

Attack Vector: On-prem to the Cloud and back again | 4 Hops to compromise critical asset

The XM Cyber Research team took an extended look into the attack techniques used specifically in Hybrid Cloud, AWS and Azure environments:

Hybrid Cloud

41%

of hybrid cloud organizations (more than one cloud vendor) had On-prem to Cloud techniques used in their environments

38%

of Azure organizations had Cloud to On-prem techniques used in their environments

95%

of users have long term access keys attached to them which can be exposed creating risk to critical assets

Bottom line: *Even by design, identities can be leveraged in order to perform lateral movement to the cloud and from the cloud, there is a large probability that even if it is built by design it can still lead to compromise. Our research reveals organizations have a disconnect between the cloud and on-prem networks - in many cases you have devops teams that manage X, while the enterprise team that manages Y, but no context to connect between them - these attacks reveal the hidden connection between them as they really are a sight unseen. Only by seeing attack paths across hybrid networks can teams collaborate and understand how to close gaps efficiently.*

XM Cyber

AWS

75%

of organizations have an external facing EC2 machines posing risk to critical assets

37%

of organizations contain Users or Roles with cross account permissions between accounts

69%

of organizations have AWS Users or Roles which can perform IAM privilege escalations

Azure

23%

of organizations have an external facing Azure VM that pose risk to critical assets

23%

of organizations that had critical assets impacted by Azure users

54%

of organizations that had users that can escalate privileges

38%

of organizations that had critical assets impacted by third party applications

Bottom line: *Regardless of how your access management is handled, organizations are unaware of the power users they have in their network. You might have 100 accounts in your environment, or more, you may have a user that has access to all those accounts; these permissions and roles need to be monitored and mapped strictly. These types of users provide "keys to the city" and exploiting them can be costly. It is hard to monitor everything and know what the consequences are when you add more resources or deploy more accounts. Without a system that automatically correlates credentials and how they can compromise a critical asset, enterprises put their security posture at severe risk.*

Conclusion

Recommendations

The XM Cyber Research team recommends that organizations focus their security efforts by looking across environments to understand how attackers can move from on-prem to the cloud or vice versa. When we look at on-prem it is important to notice - it is not just vulnerabilities, there are so many other issues that we need to take care of and direct resources towards the bigger picture. As we saw, in less than 4 hops, 94% of critical assets can be compromised from the initial breach point. This is a big disconnect between the existence of cyber security tools and the level of protection they provide, we are paying for these controls and not the actual performance associated with mitigating the risk, across the entire network. Siloed security tools will continue to look only at one specific security effort - but it is the combination of multiple attack techniques that pose the greatest risks to our organizations'. Security teams need to hone in on hybrid cloud attacks and misconfigurations and identity issues that are living in their environments.

In the cloud, there are many small issues that seem like legitimate permissions, but when tying them together you can see there is a big risk, an unintended consequence. When you put this all together, on-prem and cloud and the relations between them are key areas we need to address. Be aware that is a big problem - ask yourself, do I know my own security status compared to the stats presented in the report? If I do, can I map it and understand all the risks that can compromise our business across on-prem and cloud environments?

To understand whether an organization's most critical assets are safe, it's imperative to have visibility into how things change over time, and how those changes affect risk. Modeling attack paths to predict the likelihood of a breach is one way to do this. This approach provides a consistent predictive model that cuts through the noise of what can be bypassed, and what cannot, and contextualizes this information within the framework of critical assets.

Set out a plan to ask yourself key questions and steps to best answer them:

What can be compromised today?

What is the likelihood of that happening?

What is the aggregate impact?

What is the level of operational risk?

Are my critical assets protected?

About XM Cyber

XM Cyber is a leading hybrid cloud security company that's changing the way innovative organizations approach cyber risk. Its attack path management platform continuously uncovers hidden attack paths to businesses' critical assets across cloud and on-prem environments, enabling security teams to cut them off at key junctures and eradicate risk with a fraction of the effort. Many of the world's largest, most complex organizations choose XM Cyber to help eradicate risk. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, and Israel.

Learn more at xmcyber.com

Appendix

Example of attack techniques included in AWS:

AWS Update Role Impersonation Policy

MITRE ATT&CK TTP ID	MITRE ATT&CK Tactic	Platform
T1078, T1078.004	Defense Evasion, Persistence, Privilege Escalation, Initial Access	AWS

Using iam:UpdateAssumeRolePolicy permission, attacker could allow the role to be impersonated by anyone.

AWS IAM Add User Policy Privilege Escalation

MITRE ATT&CK TTP ID	MITRE ATT&CK Tactic	Platform
T1550, T1550.001, T1078, T1078.004	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement	AWS

An attacker with a stolen AWS Identity that possesses the required permissions, including
• iam:AttachUserPolicy • iam:PutUserPolicy
can alter and add malicious permissions for other AWS users under attacker control.

AWS Create Access Key

MITRE ATT&CK TTP ID	MITRE ATT&CK Tactic	Platform
T1136, T1136.003	Persistence	AWS

Using iam:CreateAccessKey permission, an attacker could add access keys to other users and compromise them.

AWS Modify Group Policy

MITRE ATT&CK TTP ID	MITRE ATT&CK Tactic	Platform
T1078, T1078.004	Defense Evasion, Persistence, Privilege Escalation, Initial Access	AWS

The AWS IAM permission, "iam:AttachGroupPolicy", attaches a managed policy to the specified IAM group. This permission can be dangerous: an attacker could use it to add a permissive managed policy (such as AdministrativeAccess) to a group and use a compromised user account that is a member of that group to obtain the permission(s).

AWS Over-Privileged EC2 Instance Creation

MITRE ATT&CK TTP ID	MITRE ATT&CK Tactic	Platform
T1078, T1078.004	Defense Evasion, Persistence, Privilege Escalation, Initial Access	AWS

The IAM permissions, 'ec2:RunInstances' and 'iam:PassRole', allow the identity possessing them to create a new EC2 instance to which those identities have access via SSH.
With such access, they can pass a role to the instance with permissions that the instance user does not currently possess. This permission can be dangerous: an attacker could use it to escalate current permissions by passing an over-privileged role to the new EC2 instance.

AWS Over-Privileged Lambda Function Creation Creation

MITRE ATT&CK TTP ID	MITRE ATT&CK Tactic	Platform
T1078, T1078.004	Defense Evasion, Persistence, Privilege Escalation, Initial Access	AWS

The IAM permissions 'lambda:CreateFunction', 'lambda:InvokeFunction' and 'iam:PassRole' allow the identity possessing them to create new Lambda functions and to pass an over-privileged role to those function.
With such access, the identity can pass a role to the Lambda function with permissions that the function does not currently possess. These permissions can be dangerous: an attacker could use them to escalate current permissions by passing an over-privileged role to the Lambda function.

Example of attack techniques included in Azure:

Azure Reset Application Credentials

MITRE ATT&CK TTP ID	MITRE ATT&CK Tactic	Platform
T1078, T1078.004	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Azure

Having compromised an Azure Service Principal or User with the following roles: Global Administrator, Application Administrator, Cloud Application Administrator, Hybrid Identity Administrator, Partner Tier1 Support and Partner Tier2 Support

Azure Reset User Password of Azure MySQL

MITRE ATT&CK TTP ID	MITRE ATT&CK Tactic	Platform
T1078, T1078.004	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Azure

An attacker with a stolen access key can reset the MySQL administrator password when they have the following permissions:
• "Microsoft.DBforMySQL/servers/read" • "Microsoft.DBforMySQL/servers/write"

Azure Reset User Password of Azure PostgreSQL

MITRE ATT&CK TTP ID	MITRE ATT&CK Tactic	Platform
T1078, T1078.004	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Azure

An attacker with a stolen access key can reset the PostgreSQL administrator password when they have the following permissions:

- "Microsoft.DBforPostgreSQL/servers/read"
- "Microsoft.DBforPostgreSQL/servers/write"

Azure Reset User Password of Azure SQL

MITRE ATT&CK TTP ID	MITRE ATT&CK Tactic	Platform
T1078, T1078.004	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Azure

An attacker with a stolen access key can reset the SQL administrator password when they have the following permissions:

- "Microsoft.sql/servers/read"
- "Microsoft.sql/servers/write"

Azure Application Can Add Password to Applications

MITRE ATT&CK TTP ID	MITRE ATT&CK Tactic	Platform
T1078, T1078.004	-	Azure

Having compromised an Azure application with the API permission "Application.ReadWrite.All", an attacker can add passwords to other applications in the tenant, and subsequently compromise the service principals of those applications in all tenants.

Azure Application Owner Can Compromise Application Service Principals

MITRE ATT&CK TTP ID	MITRE ATT&CK Tactic	Platform
T1078, T1078.004	-	Azure

An attacker with a stolen Azure identity that is an application owner in the tenant can compromise all service principals associated with this application in all tenants, for example by resetting the application password.