Microsoft Security

2024 State of Multicloud Security Report

Trends and insights to drive an integrated multicloud security strategy

Executive Foreword

The advent of cloud computing ushered in a new era of innovation, empowering organizations to rapidly scale and embrace new opportunities. Today, multicloud environments have become the de facto way of doing business.

However, with all that innovation and flexibility came new risks. Many customers currently operate with a complex patchwork of interconnected technologies across different devices, applications, platforms, and clouds. Since most organizations connect these data sources so that data can seamlessly flow across boundaries, they need to know that their protection policies won't miss any blind spots between disparate technologies and in turn put their data at risk.

Today, organizations can deploy dozens of disparate security tools—each with its own security alerts to mitigate. Combined with the ongoing cyber workforce shortage and gaps in institutional knowledge, security teams are overwhelmed and unable to prioritize exposures with the greatest potential impact. In addition, because each cloud has a unique security infrastructure, decisioning logic, and concepts, organizations are left managing complexity that increases the potential for mistakes and heightens their risk of a breach.

At Microsoft, we have long embraced our commitment to protecting customers' environments, regardless of how many clouds they run on or which providers they use.

In February 2022, we became the first cloud provider to offer integrated cloud-native application platform protection (CNAPP) from development to runtime for Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP).[1] And we've continued to evolve our multicloud security offerings ever since through advancements like the Secure Future Initiative (SFI), which aims to transform software development, implement new identity protections, and drive faster vulnerability response.[2] Today, Microsoft delivers an unparalleled level of threat intelligence informed by more than 78 trillion daily security signals.

It doesn't stop there. Cybersecurity is an ongoing challenge. To keep pace with the rapidly changing tactics of adversaries, we must work together as a collective defense community to share insights, collaborate on best practices, and better secure our multicloud future.

In that vein, we invite you to read and share the following report to more deeply understand the state of multicloud security risk in 2024, and to evolve your security strategy to strengthen your digital enterprise moving forward.

Andrew Conway

Vice President of Security Marketing, Microsoft

[1] "Microsoft Announces New Security Capabilities for the Multicloud World," Microsoft Stories Asia.

[2] "Announcing Microsoft Secure Future Initiative to advance security engineering," Microsoft Security.

Introduction

Deploying applications and infrastructure across multiple clouds is the new normal in today's business climate. Approximately 86% of organizations have already adopted a multicloud approach thanks to its benefits including increased agility, flexibility, and choice.[3] However, as organizations deploy multicloud environments, they face many challenges, including managing security and compliance across multiple cloud service providers (CSPs), ensuring data portability, and optimizing costs.

Informed by usage patterns across Microsoft Defender for Cloud, Microsoft Security Exposure Management, Microsoft Entra Permissions Management, and Microsoft Purview, we have identified the top multicloud security risks across Microsoft Azure, AWS, GCP, and beyond:

[3] "SANS 2023 Multicloud Survey: Navigating the Complexities of Multiple Clouds," SANS Institute.

Key findings

1

Many organizations struggle to properly secure cloud-native applications and infrastructure throughout the full lifecycle.

At the development level, 65% of code repositories contained source code vulnerabilities in 2023, which remained in the code for 58 days on average.

During runtime, security teams are often overwhelmed and unable to prioritize the sheer number of potential risks and exposed assets they must remediate.

The average organization has 351 exploitable attack paths that threat actors can leverage to reach high-value assets. Among all organizations, over 6.3M exposed critical assets were discovered.

2

Securing human and workload identity access across multiple clouds is also a significant challenge due to the rapid growth in identities and bloated permissions.

Microsoft Entra Permissions Management discovered 209M identities across its customers' clouds in 2023.

Of the 51,000 permissions granted to those identities (a 22% increase from 2022), only 2% were used and 50% were considered high-risk.

3

This increased number of potential risks, exploitable attack paths, identities, and permissions impacts organizations' data security posture.

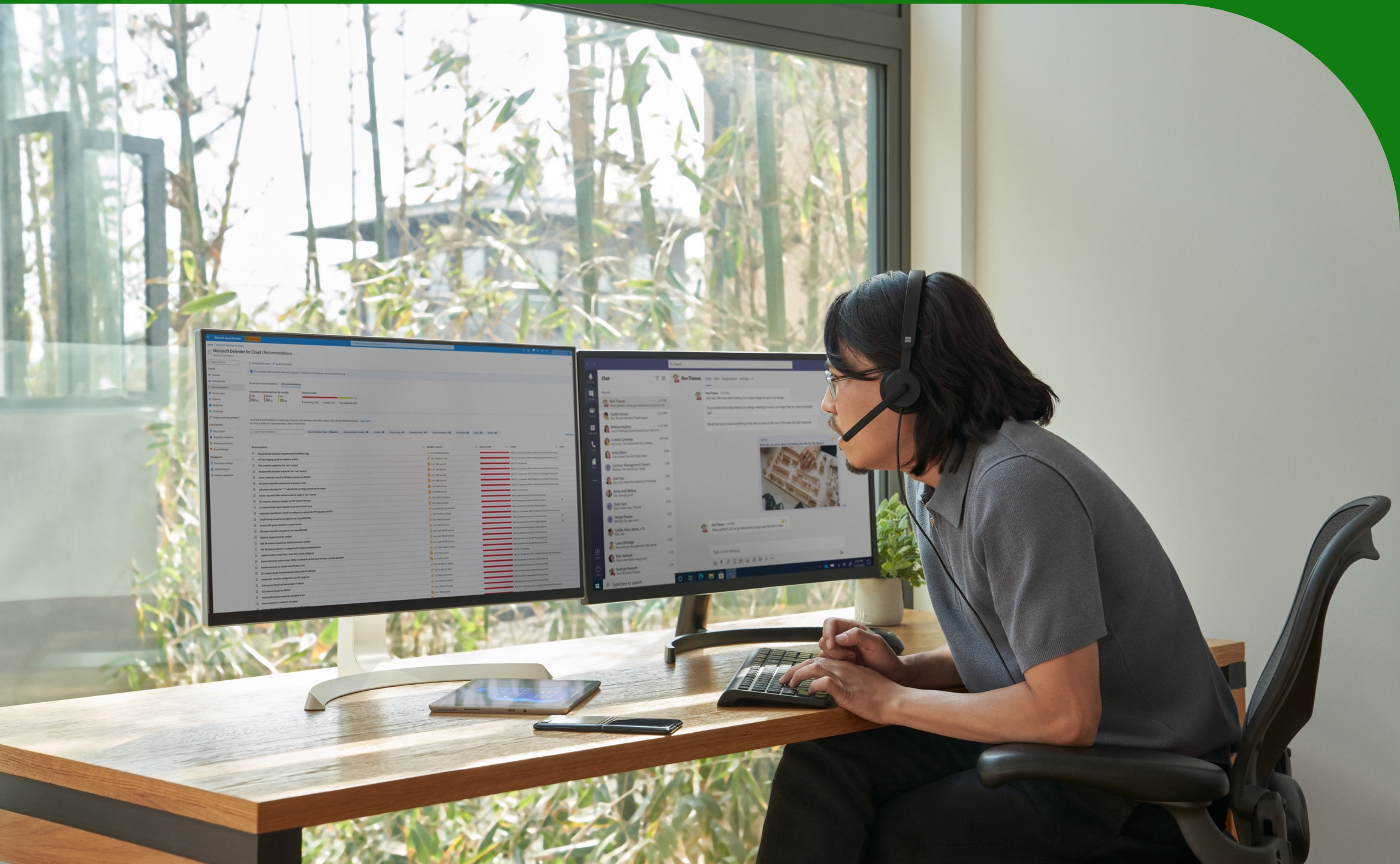
As multicloud environments grow in scale, so too does the data they house and produce. With more exposed data comes more risk.

Organizations face 59 data security incidents each year on average, and 74% of organizations experienced at least one data security incident in which business data was exposed.

Secure cloud-native applications and infrastructure

To ensure the security of your cloud-native applications and infrastructure, security must be embedded throughout the full lifecycle. Security teams need a holistic view of the entire development and deployment process to ensure comprehensive visibility across source code repositories all the way to cloud runtime environments.

To understand exactly why a secure development and deployment process is so critical, we looked at several key data points for 2023.



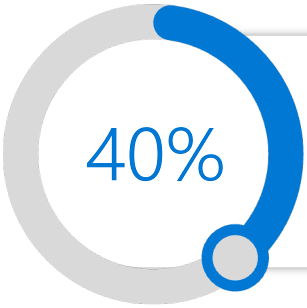
Shift left and embrace DevOps security

Attackers are shifting left, targeting vulnerabilities earlier on in the development lifecycle. In response, security needs to shift left too, moving into the very beginning of the development process as soon as you begin to create your code.

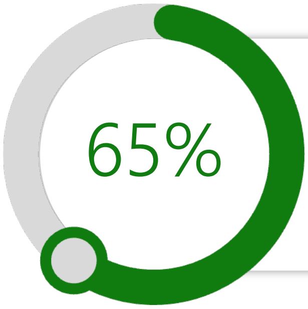
When examining multicloud environments, we discovered that many organizations lack strong DevSecOps hygiene, exposing them to greater risk. There are widespread vulnerabilities living within source code and code repositories. For example, nearly one-quarter (23%) of code repositories contained exposed secrets such as passwords and API keys in 2023. Adversaries can use this information to gain unauthorized access to your multicloud environment and trigger larger attacks that could result in data breaches, identity theft, and more.

In total, more than 1.4M vulnerabilities were discovered in connected DevOps repositories, each posing a serious risk to the security of an organization's infrastructure.

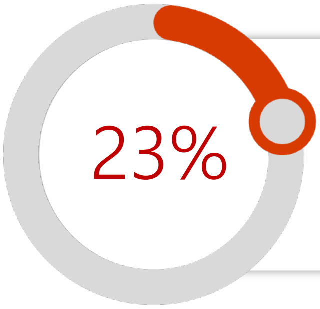
Of the code repositories we analyzed in 2023,



40% contained supply chain vulnerabilities



65% contained source code vulnerabilities



23% exposed company secrets, including passwords and API keys

Identifying and eliminating the number of common vulnerabilities and exposures (CVEs) in code is also essential, considering that CVEs can create serious issues during development and deployment. We found that CVEs remained in code for 58 days on average and could take anywhere from 57 to 64 days to resolve. This leaves a large window of time for attackers to capitalize on a vulnerability, given that 25% of high-risk CVEs are exploited within 24 hours of being published.[4]

58 days CVEs stay in code

57 days to fix high-severity CVEs

58 days to fix medium-severity CVEs

64 days to fix low-severity CVEs

25% of high-risk vulnerabilities are exploited on the same day they're published

Preventing these CVEs from being introduced into the code in the first place is key. A cloud-native application protection platform (CNAPP) can help by acting as a shared platform for security admins and developers alike. This allows security teams to unify, strengthen, and manage multipipeline DevOps security while shifting security left to enable full-lifecycle protections from a centralized dashboard.

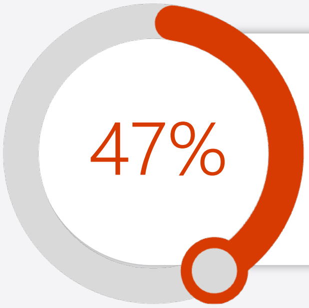
CNAPP

A unified platform that simplifies cloud-native application and infrastructure security by integrating multiple solutions to embed security from initial code development to provisioning and runtime to help mitigate risks across hybrid and multicloud environments.

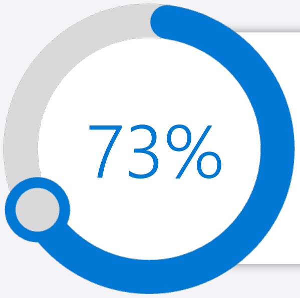
DevOps environments can also contain misconfigurations that put an organization's infrastructure at risk. For example, we discovered multiple instances of code repositories that lacked protection rules on the default branch. This indicates a broader trend of inadequate security measures in DevOps environments. Often, essential safeguards, such as protection rules for code repositories, are overlooked or not rigorously enforced. This can expose organizations to risks like unauthorized access, poisoned pipeline execution attacks, and code tampering.

[4] "1 in 4 high-risk CVEs are exploited within 24 hours of going public," SC Media.

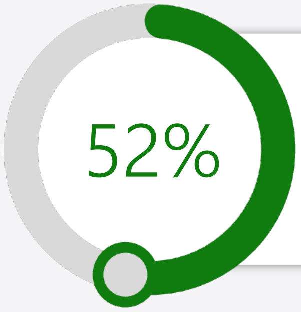
To address these weaknesses, it's essential to implement comprehensive security protocols across all stages of the development lifecycle.


47%

of service connections in Azure DevOps gave access to all pipelines


73%

of GitHub repositories lacked protection rules on the default branch


52%

of GitHub repositories that connected to Azure lacked protection rules on the default branch

These misconfigurations must be addressed if organizations are to lower their risk of sensitive data exposure, system compromise, user harm, and more.

Focus on a preventative, risk-based approach with attack path analysis

Another key tool for proactively securing cloud-native applications and infrastructure is attack path analysis, often delivered through a cloud security posture management (CSPM) solution. Understanding attack path analysis allows organizations to identify and remediate critical risks in their environment—such as misconfigurations, vulnerabilities, permissions, and sensitive data—before attackers can exploit them. Think of these risks as a string of vulnerabilities and misconfigurations that might seem innocuous when viewed in isolation. However, when they are surfaced by a CSPM tool and consolidated into an attack path, organizations can view the full impact of each risk and remediate them proactively.

Take the example of source code vulnerabilities. Attack path analysis can flag a vulnerability and show how attackers could use it to breach your environment and move laterally to reach critical assets. Even more crucially, attack path analysis can prioritize which attack path security teams should address first based on the potential impact to your environment and suggest remediation next steps.

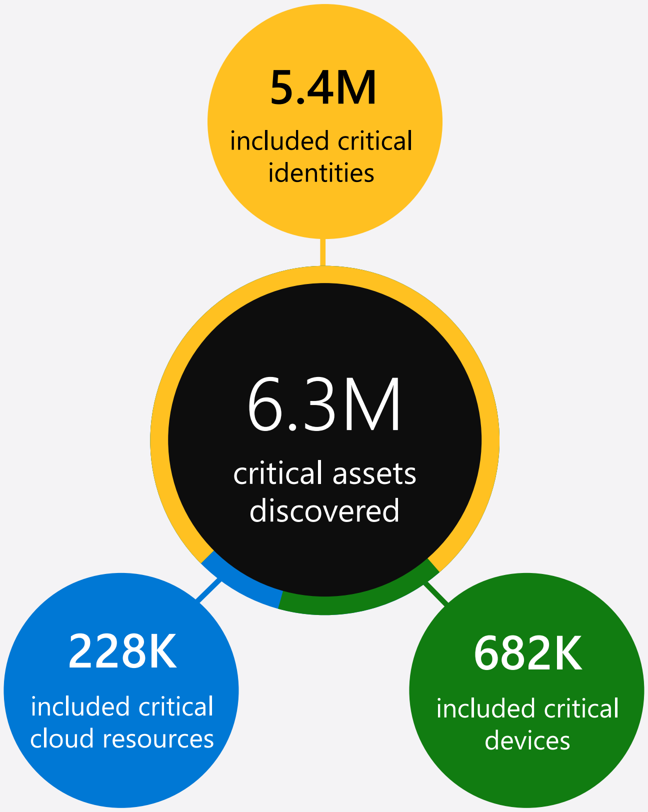
Attack path:

Exploitable paths that attackers might use to breach your environment and access high-impact assets

Attack path analysis:

A pre-breach analysis performed by correlating security risk in and across environments to provide visibility into how an attacker could infiltrate and move through your multicloud estate

88% of Microsoft Security Exposure Management public preview customers had an attack path that led to a critical asset



Without attack path analysis to illuminate these exploitable paths, many organizations may not even be aware that their critical assets are at risk. Among Microsoft Security Exposure Management public preview customers, 88% had an attack path that led to a critical asset and more than 6.3M exposed critical assets were discovered, including identities, devices, and cloud resources.

Microsoft Security Exposure Management is an attack surface management tool designed to help organizations identify, prioritize, and remediate critical exposures by collecting and normalizing asset data, mapping assets and their relationships, and providing comprehensive visibility into the attack surface.

Unaddressed attack paths can also lead to significant damage across multicloud environments, including compute abuse, data exposure, and user credential exposure. These attack paths are widespread, in some cases occurring across multiple cloud environments.

49% of attack paths could result in compute abuse, such as the unauthorized use of cloud computing resources

24% of attack paths could result in data exposure to the internet or unauthorized users

20% of attack paths could result in credential exposure such as improperly secured passwords or keys

7% of attack paths could result in sensitive data exposure like personal information or company secrets

1% of attack paths were cross-environment, such as across clouds or from code development to cloud runtime environments

Attack paths are by no means uncommon. More than half of organizations were exposed to at least one attack path in 2023, with the average organization containing 351 attack paths across their multicloud environment. These attack paths can occur for a variety of reasons, with the most common causes being internet exposure and insecure credentials.

58% of organizations are exposed to at least one attack path

7% of organizations are exposed to more than 1,000 attack paths

351 attack paths at the average organization

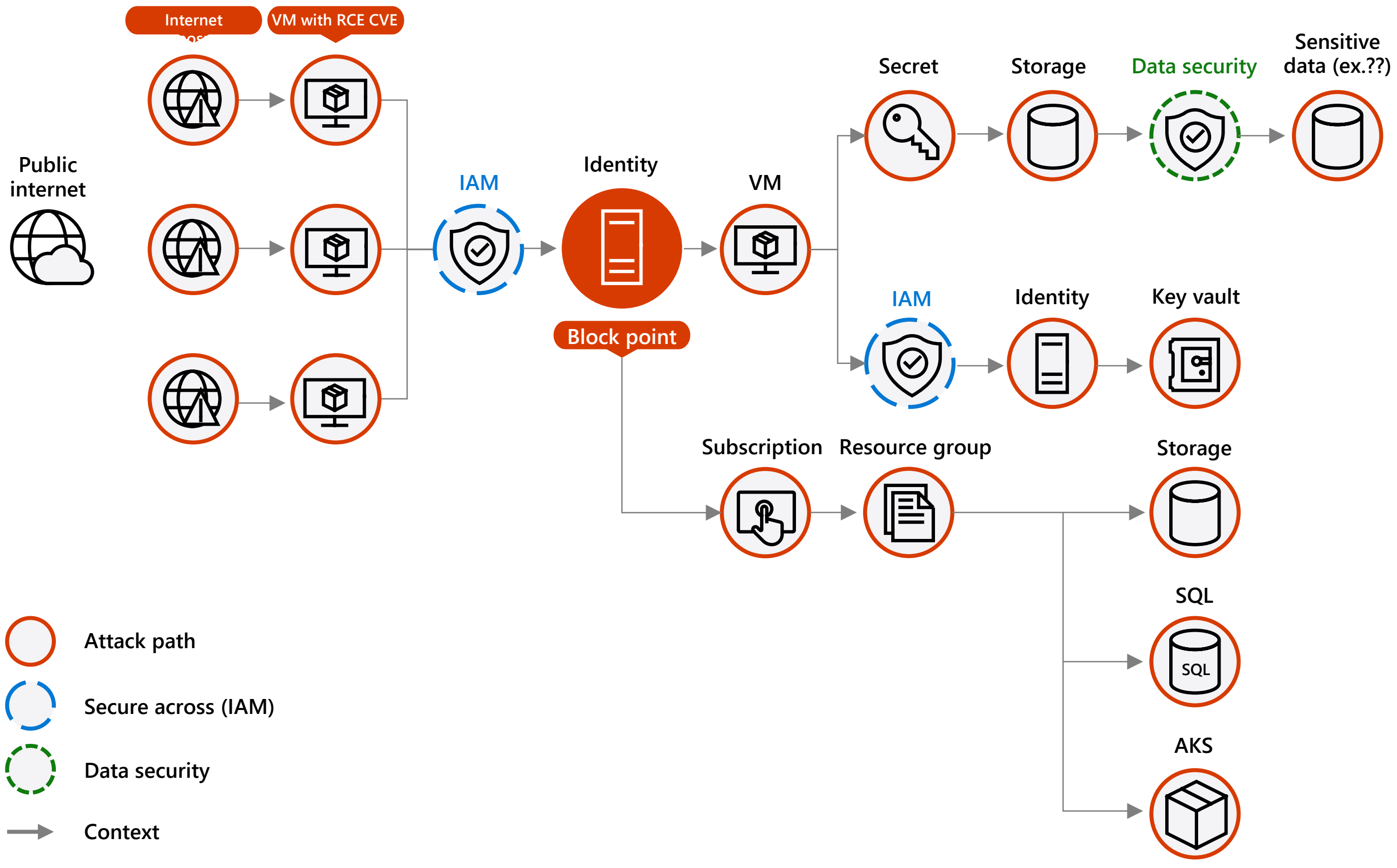
84% of attack paths originate because of internet exposure

66% of attack paths involve insecure credentials

By taking a shift-left approach to security, organizations can proactively identify and remediate these attack paths before threat actors have a chance to exploit them.

Did you know that just a fraction of the resources used in multicloud environments are responsible for a larger percentage of attack paths?

Attack path block point



This is because of the proliferation of block points, or areas in the cloud network where most of the network traffic flows through. If compromised, these points allow attackers to branch out and access more resources within your network.

The diagram above shows multiple attack paths originating from the public internet. In this example, there are three virtual machines (VMs) with a remote code execution (RCE) CVE. Adversaries can take advantage of these CVEs to gain access to an identity, establish a foothold in your environment, and move laterally to access sensitive data, a key vault, or an AKS cluster. Threat actors can target all of these potential attack paths, even opting to pursue one attack path at a time so that, if detected in one path, they can pivot their strategy and maintain a foothold in the environment.

Organizations can secure these block points by implementing CNAPP to prevent adversaries from progressing along the attack path.

Reduce complexity with threat protection

In addition to DevOps security and attack path analysis, organizations also need to consider how the growing use and variety of cloud workloads impact their exposure to cyberthreats.

When cloud workloads span across multiple cloud environments, that creates a larger, more complex attack surface for security teams to contend with. These intertwined workloads create additional complexities and dependencies that require proper configuration and monitoring to secure. Many companies also rely on individual point vendors to manage a piece of their workload protection. However, this approach misses the bigger picture and overlooks the potential cross-workload risks in multicloud environments.

For example, consider a company that uses two different cloud security solutions for API and data storage protection. Suppose a compromised API links to data storage, but the two point solutions can’t communicate or integrate. The complexity between these different types of workload interactions can increase your attack surface. This is why comprehensive threat protection is such a critical focus in multicloud security.

There are three main challenges with multicloud threat protection.

The first is the growing sophistication of attack tactics and the use of AI by threat actors. As cloud adoption grows, traditional threat surfaces are expanding and network perimeters have disappeared. This introduces novel attack scenarios and techniques. For example, threat actors like Charcoal Typhoon have been known to use large language models (LLMs) to support tooling development and scripting, understand various commodity cybersecurity tools, and generate content that could be used to social engineer targets.[5]

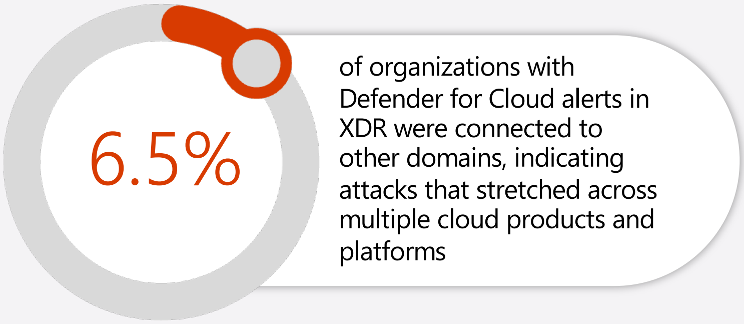
Charcoal Typhoon is a Chinese state-affiliated threat actor with a broad operational scope. They are known for targeting government, higher education, communications infrastructure, oil and gas, and information technology sectors.

Secondly, organizations may have resources across different cloud providers, each of which can connect to different identity providers. This expands the organization's overall attack surface. Consider the example of a cross-cloud supply chain attack. In this scenario, developers build pipelines in Azure DevOps (ADO). They then build Docker containers and put them in a registry, with images being picked up from anywhere. Kubernetes workloads may be deployed in a certain cloud provider, such as Azure Kubernetes Service (AKS), while also using images stored in a different cloud provider, like AWS's Elastic Container Registry (ECR). Because these images are stored in ECR but deployed in AKS, attackers could potentially target them to execute a cross-cloud supply chain attack.

In total, roughly 10% of Azure clusters use cloud services from a different cloud provider. For example, a workload running on AKS might use AWS's S3 storage to store data.

Finally, because modern IT environments spread across multiple platforms, many organizations lack strong visibility into what is going on across all their different clouds. They need a better way to centralize and contextualize findings across their various security approaches.

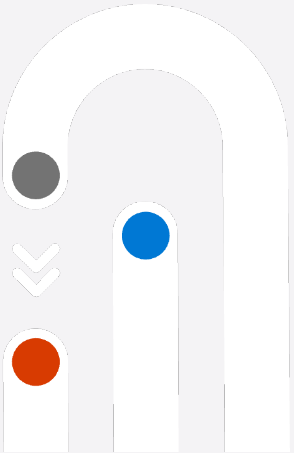
For example, Microsoft's CNAPP solution, Defender for Cloud, has an extended detection and response (XDR) integration that provides richer context to investigations and allows security teams to get the complete picture of an attack across cloud-native resources, devices, and identities. Roughly 6.5% of Defender for Cloud alerts were connected to other domains—such as endpoints, identities, networks, and apps and services—indicating attacks that stretched across multiple cloud products and platforms.



6.5%

of organizations with Defender for Cloud alerts in XDR were connected to other domains, indicating attacks that stretched across multiple cloud products and platforms

This number will only increase as additional correlation logic is added, which can help identify and link related security events to detect potential threats.



[5] "Staying ahead of threat actors in the age of AI," Microsoft Threat Intelligence.

Recommendations

Ultimately, protecting cloud-native applications and infrastructure starts with adopting a shift-left approach to security. This ensures that the development and deployment process is secure from the very start. A CNAPP solution can help enforce security best practices in the earliest stages of development and promote a holistic software development lifecycle (SDLC) for all cloud-native applications. However, for this to work, you must ensure that your application security is developer-friendly.

At Microsoft, we offer native security tooling with GitHub Advanced Security for both GitHub and Azure DevOps. This allows developers to work within their native tools while still enforcing security best practices across the code and application development lifecycle. By eliminating or fixing security alerts earlier in the development process, the development cycle can move much faster and be less costly.

Additionally, security teams should leverage attack path analysis within a CSPM as the first line of defense when managing cloud security posture as part of an organization-wide proactive attack surface and risk management continuous threat and exposure management program.[6] For both attack paths and threat protection, it's important to maintain Zero Trust best practices by assuming breach and limiting exposure by adding multiple layers of protection across the environment.

For example, we found that internet-exposed VMs have a 6.5 times greater chance of compromise compared to non-exposed machines. Furthermore, 15% of internet-exposed machines are targeted by brute force attacks. This indicates that attackers are attempting to gain access to someone's identity through password spraying, which, if successful, would provide initial access to their cloud computing resources. That is why avoiding exposing management ports to the internet is essential. Instead, use a closed management interface to gain connection without exposing potentially sensitive resources to the internet.

☑ Leverage a holistic CNAPP solution to integrate security checks and controls into the DevOps pipeline and implement comprehensive cloud-native workload monitoring and protection

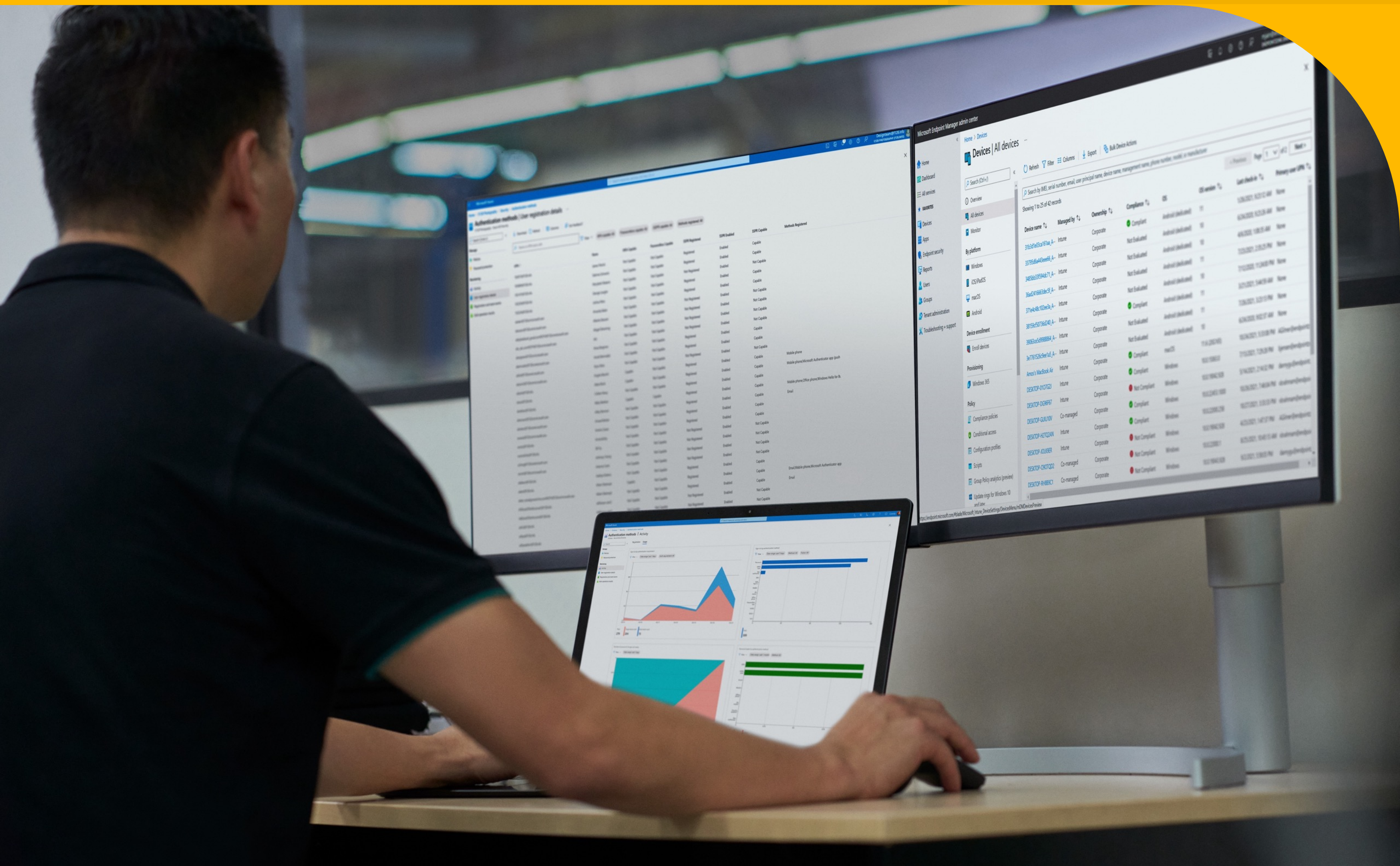
☑ Focus on a preventative, risk-based approach by leveraging attack path analysis to proactively identify and remediate potential attack paths before they can be exploited. CSPM enables you to reduce attack surface and manage risk in your multicloud environment, and Exposure Management extends your proactive program across your whole organization

☑ Follow Zero Trust best practices by assuming breach and limiting internet exposure unless absolutely necessary, especially in the case of management ports. Instead, use a closed management interface to establish a connection without risky internet exposure

[6] "How to Manage Cybersecurity Threats, Not Episodes." Gartner.

Secure human and workload access across multicloud

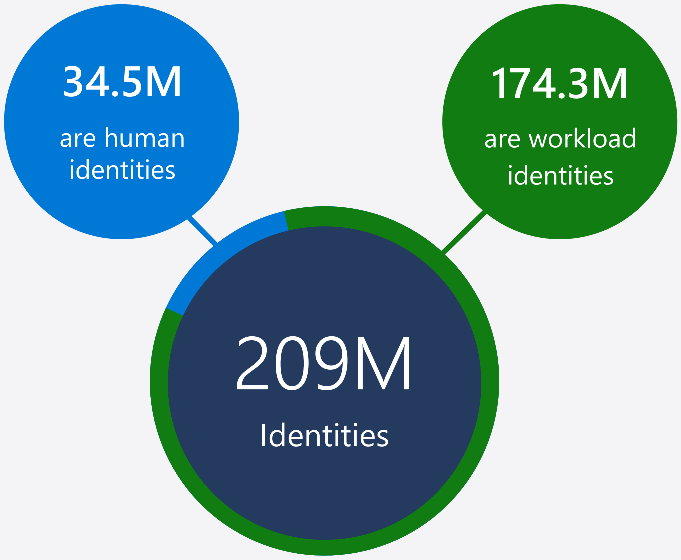
Another foundational element of multicloud security is identity and access management. Not only do security teams have to monitor and secure user identities, but they also must account for workload identities. This is especially challenging given how quickly identities and their access to cloud resources have grown in recent years, with more and more workload identities gaining increased access to cloud resources. Workload identities currently outnumber human identities, and that gap is only growing.



Protecting workload identities is of critical importance

As more and more companies move their workloads to the cloud, we're seeing a rapid growth in the number of workload identities being created. Today, there is one human identity for every 10 workload identities. This problem is even more acute among small- and medium-sized businesses, which have one human identity for every 50 workload identities.

Of the 209M identities Microsoft Entra Permissions Management discovered across its customers' clouds in 2023:



As the number of workload identities continues to far outpace the number of human identities, it's important to consider the relative risk of each. Fewer solutions can adequately protect workload identities compared to how these solutions can protect and secure human identities. This is because the majority of identity and access solutions in the market today have primarily focused on safeguarding human identities rather than workload identities.

Workload identities are also much more difficult to secure than human identities because they don't have a clearly defined lifecycle. When a new employee or a third-party contractor joins your company, they have a clearly defined start date that's often accompanied by HR and other related processes. When their engagement with your organization ends—whether because they moved on to a new job or their contract ended—that final date is also clearly noted across multiple company systems.

However, the same is not true of workload identities, which can gradually taper out and become inactive. This is especially true when you consider the widespread use of shadow IT across multicloud environments. Inactive identities are not monitored the same way as active identities, making them an attractive target for adversaries to compromise as they can leverage the identity or credentials to move laterally throughout your environment. Workload identities can also be manually embedded in code, making it harder to clean them without triggering unintended consequences.

Workload identities:
Identities assigned to software workloads, such as apps, microservices, and containers.

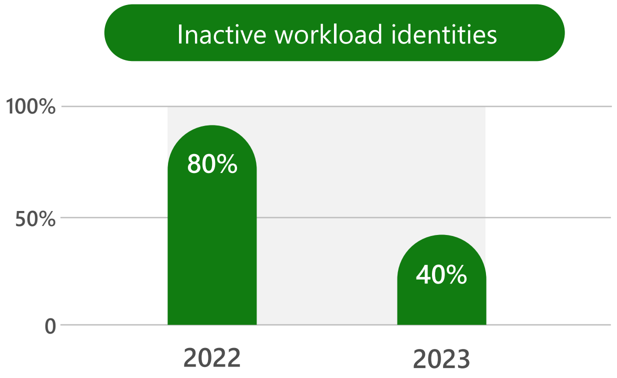
Inactive identity:
An identity that hasn't logged in or used any of its permissions in the last 90 days

Permissions:
The ability for an identity to perform an action on a resource

High-risk permissions:
Permissions that can cause data leakage, service disruption, or service degradation if misused or exploited

One bright note is that the number of inactive workload identities has dropped year over year according to data from Microsoft Entra Permissions Management.

Of the 174.3M workload identities identified



In 2022, 80% of workload identities were considered inactive whereas just 40% of workload identities were inactive in 2023. This shows us that Permissions Management helped organizations better manage inactive workload identities through increased visibility. Organizations are also beginning to realize the importance of securing workload identities. Once companies understand how crucial workload identities are to their overall risk posture, it becomes possible to secure them better.

Managing super identities is a crucial task for securing access

Further complicating identity security is the fact that the majority of identities are vastly over-permissioned. When an identity can access any permission or resource across your entire multicloud estate, it is known as a super identity.

A term originally coined by Microsoft in the 2023 State of Cloud Permissions Risks report, compromised super identities can allow attackers to gain access to all permissions and resources—putting them in a very powerful.[7]

Super identity:

A user or workload identity that has access to all permissions and all resources across your entire cloud estate.

Since last year, the percentage of super identities has remained the same, accounting for more than 50% of all identities. Ideally, this percentage would decrease so there is less opportunity for attackers to gain access to a wide breadth of permissions and resources—thus minimizing the blast radius from any potential breaches.

This problem is even more pronounced among workload super identities, which increased in 2023. In 2022, there were four human super identities for every six workload super identities. In 2023, that ratio increased to three human super identities for every seven workload super identities. Given the inactivity of workload identities in 2023, a significant number of workload super identities are likely not being managed—leaving them vulnerable to an attack.

[7] “2023 State of Cloud Permissions Risks report now published.” Alex Simons.

Unused permissions represent a significant risk

The problem of unused permissions stretches across human and workload identities in the cloud.

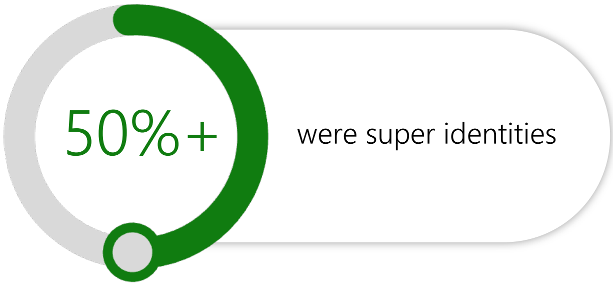
Microsoft Entra Permissions Management discovered more than 51,000 permissions granted to human and workload identities in 2023 (up from 40,000 in 2022). With more permissions come more access points for attackers. As evidenced by the continued prevalence of super identities, many of these permissions aren't even being leveraged fully.

2% of human and workload identity permissions were used in 2023

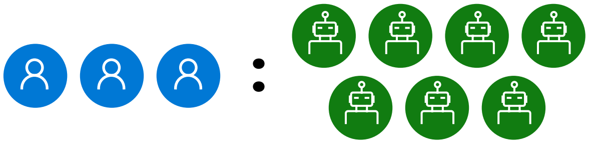
3% of workload identity permissions were used in 2023

Our data shows that just 2% of the permissions granted to human and workload identities in 2023 were used, and only 3% of workload identity permissions were used. While a slightly higher percentage of workload identity permissions are being used compared to human identity permissions, the remaining 97% of unused permissions still represent a valuable and attractive target for attackers. Too many identities continue to be far over-provisioned, increasing the number of identities that pose a potential security risk.

Of the 209M cloud identities identified in 2023,



There were 3 human super identities for every 7 workload super identities



If we are to properly secure identity and access as a collective defense community, we must focus on managing and lowering the number of super identities. The first step is establishing visibility into all super identities across your multicloud estate. From there, security teams can begin obtaining insights into unused permissions and right-sizing permissions in accordance with least privileged access principles.

Recommendations

In the realm of identity and access management, the handling of identities (both human and workload) and their access remains a formidable challenge. This is primarily due to the nature of their permissions, which are akin to root access. Managing these identities within a multicloud environment continues to be a significant hurdle.

Our observations indicate that customers are adopting various strategies to tackle this issue. Some focus on identity governance, while others establish automated access through Infrastructure as Code (IaC) services. Yet others rely on native cloud service providers to govern resource access authorization.

It's important to note that an Azure subscription, AWS account, or GCP project with multiple super identities signifies an elevated level of insider risk exposure. A cloud infrastructure entitlement management (CIEM) solution can provide visibility that eliminates the need for standing access for super identities, inactive identities, and unused permissions. Once the CIEM has identified entitlements, organizations can then take steps to revoke unnecessary permissions and ensure these identities are allocated just-enough permissions, just in time. This approach will significantly mitigate potential risks and enhance the overall security posture.

At Microsoft, we leverage our CIEM solution, Microsoft Entra Permissions Management, to establish visibility into who and what has access to which resources so we can ensure those access rights align with least privilege principles. Identities and their permissions are often the first entry point for attackers, so enforcing Zero Trust principles of least privilege access and explicit verification is crucial for hardening the overall security posture of cloud environments.

Permissions Management also provides remediation and monitoring capabilities, along with a permissions creep index (PCI) to measure how well an organization protects its permissions risks across multiple clouds. Among customers who have used Permissions Management since 2022, we've seen a 21-point improvement in their overall PCI score. Furthermore, by integrating Permissions Management, with other security postures through Defender for Cloud, organizations can better understand how unnecessary permissions create a vulnerability vector as well as its relative importance to the overall security of the environment.

- ☑ Define your vulnerable attack surface by gaining clear visibility into any identities, including high-risk permissions, inactive identities, and super identities
- ☑ Remove any unnecessary permissions from identities and replace with just-in-time permissions that the identity must inherit before it can perform a task
- ☑ Manage super identities by adhering to Zero Trust principles of least-privileged access and explicit verification

Safeguard growing data

In the expanding multicloud universe, data is being generated at an unprecedented rate. The rapid adoption of generative AI technology is only accelerating this trend. As per IDC, between 2023 and 2027, the amount of data created, captured, and replicated across the globe is expected to more than double in size, with an estimated 129 zettabytes generated in 2023.[8]

We've also seen a growth in data sources, making it challenging for organizations to secure sensitive data across their estate. To safeguard their most critical asset—their data—organizations must take a comprehensive approach to data security. An approach that helps them:

- ☑ Discover risks to their sensitive data, including employee and customer data, intellectual property, financial projections, and operational data across their multicloud universe
- ☑ Understand how users interact with data
- ☑ Protect and prevent unauthorized use of that data throughout its lifecycle with protection controls like encryption and authentication

[8] "Worldwide IDC Global DataSphere Forecast, 2023-2027." IDC.

Data security incidents have become both costly and frequent

From October 2022 to October 2023, a whopping 74% of organizations experienced at least one data security incident in which their business data was exposed.[9] Data security incidents pose an enormous risk to organizations. Not only can organizations lose business-critical data and customer trust, but these incidents can also be very costly in terms of prolonged downtime, reputational damages, lost business partnerships, and legal ramifications.

On average, organizations face 59 data security incidents every year. Depending on the severity of the incident, organizations could be facing millions in potential damages.

59 is the average number of data security incidents per year organizations face

74% of organizations experienced at least one data security incident in which business data was exposed

$15M is the average cost of data security incidents[10]

[9] "Data Security Index." Microsoft.

[10] "Data Security Index." Microsoft.

A fragmented solution landscape can increase the number of data security incidents

When tasked with managing data security across a complex multicloud environment, many organizations will opt to deploy and manage several distinct, un-integrated solutions to cover all the various use cases. However, our research found that a fragmented solution landscape weakened data security. For each tool an organization adopts, they must then dedicate staff and processes to maintaining and operating that tool. This is because each vendor provides a distinct portal with varying technological foundations.

2.8x

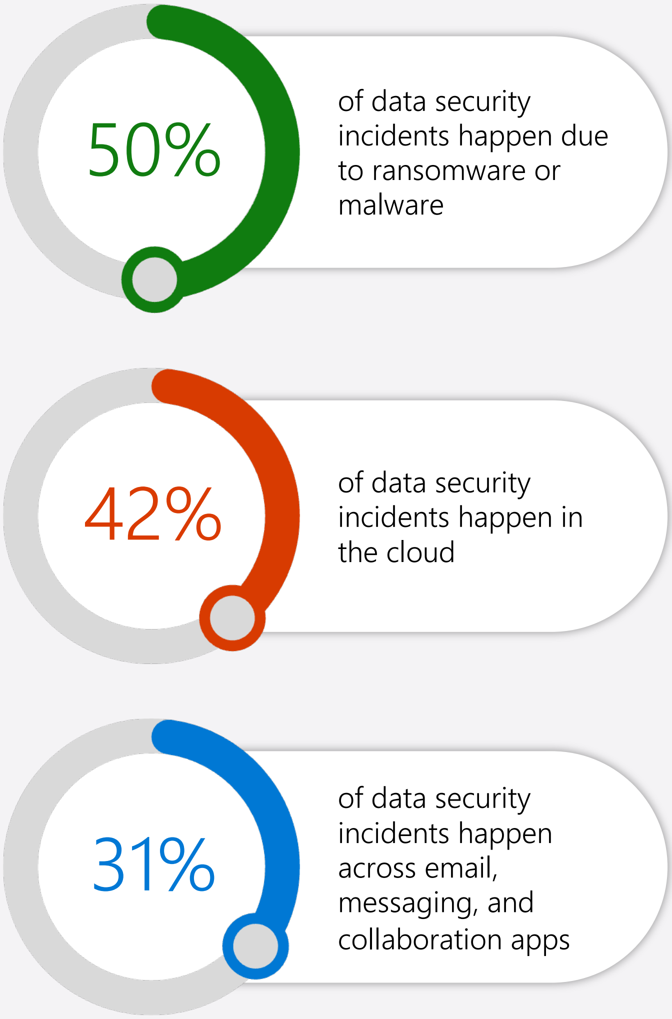
as many data security incidents are experienced by organizations with 16+ point solutions when compared to organizations with fewer tools

The proliferation of tools also leads to an increase in the number of alerts. At times, these alerts may be duplicated, creating more noise in the system. Organizations employing more than 16 tools to secure data face a staggering 2.8 times more data security incidents compared to those who use fewer tools. Moreover, the severity of these incidents tends to be higher as well.

Given the complexities of using disparate solutions, organizations should seek to reduce and refine the number of solutions they deploy to manage data security. We recommend leveraging an integrated set of solutions that work seamlessly and alleviate the complexities discussed above.

It is also important to understand the main sources of these data security incidents. Malware and ransomware are common causes, underscoring the need for a comprehensive data security solution to mitigate and prevent these kinds of attacks. Additionally, we are seeing a significant portion of data security incidents occur in the email, messaging, and collaboration apps that employees use every day to stay productive and work together. Enforcing extremely strict protection policies on all your users can disrupt the flow of data in an organization, which is crucial to getting work done. On the other hand, lack of protection poses significant risk to the data as discussed above.

Instead, organizations need a data security solution that is flexible enough so that they do not have to choose between protection and productivity and instead can achieve a sweet spot that works for them. An important part of achieving this balance is to apply restrictive policies only to high-risk users so that other users in the organization can maintain their productivity.



50% of data security incidents happen due to ransomware or malware

42% of data security incidents happen in the cloud

31% of data security incidents happen across email, messaging, and collaboration apps

A modern approach to data security is a proactive one

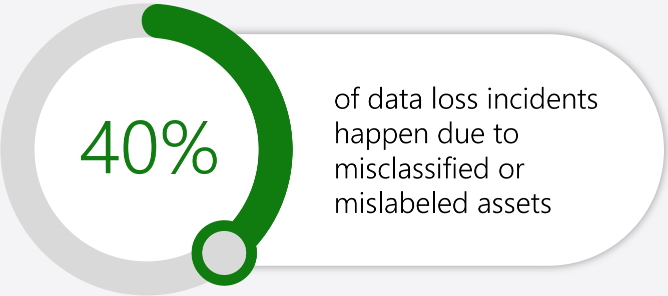
In addition to having too many tools, many organizations are in a reactive state of data security rather than a proactive one. In a reactive approach, organizations tend to play catch-up after the incident has occurred. A proactive approach is one in which organizations can prevent the data security incident from happening in the first place. For a proactive approach, organizations need to build multiple layers of protection for the data—one that combines the context of the data with the context of the user interacting with the data to provide comprehensive insights.

This multilayered approach becomes even more relevant when you consider the fact that misconfigured APIs were one of the leading causes of cloud data breaches in 2023. A multilayered approach to data security can help security teams proactively detect and monitor misconfigurations, so they can remediate as needed.

90% of data breaches in the cloud happen due to misconfigured APIs

The components of a multilayered data security strategy are:

- ☑ Create policies that prevent the unauthorized or unintentional use of data, including copying or printing sensitive information, sharing sensitive data through regular communications channels, or even uploading the sensitive data to personal cloud storage
- ☑ Understand how your users are interacting with the data to identify anomalies and prevent users from maliciously or negligently causing loss to the data
- ☑ Classify and label sensitive data. Depending on the level of security necessary, all business-critical data should be classified and then subsequently labeled to support appropriate protection such as encryption
- ☑ Leverage automation to ensure that policies can be automated adjusted based on the user's risk level and your security team does not have to manually add and remove users in and out of policy scope



Roughly 40% of organizations experience data loss because of misclassification or incorrectly labeled assets. To resolve this challenge, organizations need a robust data security solution that provides data loss prevention technology.

Recommendations

To comprehensively secure data, organizations need an integrated solution that can combine data context with user context across their multicloud estate. Without this multilayered approach, organizations will continue to be reactive in preventing unauthorized access to their sensitive data from external threats or mitigating the risk of insider data theft or accidental exposure.

Microsoft Purview—a comprehensive data security, data compliance, and data governance solution can help safeguard your data across your multicloud estate. Microsoft Purview can help discover hidden risks to your data wherever it lives or travels, protect and prevent data loss across your data estate, and quickly investigate and respond to data security incidents. It can also be used to help improve risk and compliance postures and meet regulatory requirements.

☑ Adopt a multilayered approach to data security

☑ Make data security a proactive conversation rather than reacting to an incident

☑ Focus on fewer tools and leverage an integrated solution to limit blind spots and reduce your risk of data security incidents

Executive conclusion

In closing, multicloud security can often be a complex endeavor, with multiple considerations and potential risks that security teams must account for. It starts in the earliest stages of cloud-native application and infrastructure development and extends throughout identity and access management, as well as data security.

Adopting a shift-left approach to security with a unified CNAPP solution can help integrate security checks and controls earlier on in the DevOps pipeline while also ensuring comprehensive cloud-native workload monitoring and protection. Meanwhile, attack path analysis enables organizations to achieve a more proactive state of security, especially when leveraged as the first line of defense for managing cloud security posture. When it comes to application and infrastructure threat protection, a Zero Trust mindset of assuming breach and limiting internet exposure can reduce an organization's overall risk posture.

In the critical area of identity, organizations must enhance protections for workload identities and manage the occurrence of super identities by adhering to Zero Trust principles around least privileged access and explicit verification. A CIEM solution can also help limit the number of individual point solutions an organization needs to deploy.

Finally, organizations must fortify their data security by adopting a multilayered approach. This enables organizations to be more proactive in their data security, while also safeguarding data and managing data compliance throughout the full lifecycle of the data.

To learn how you can improve security with code-to-runtime insights across multiple cloud environments and DevOps platforms, visit Microsoft Cloud Security.

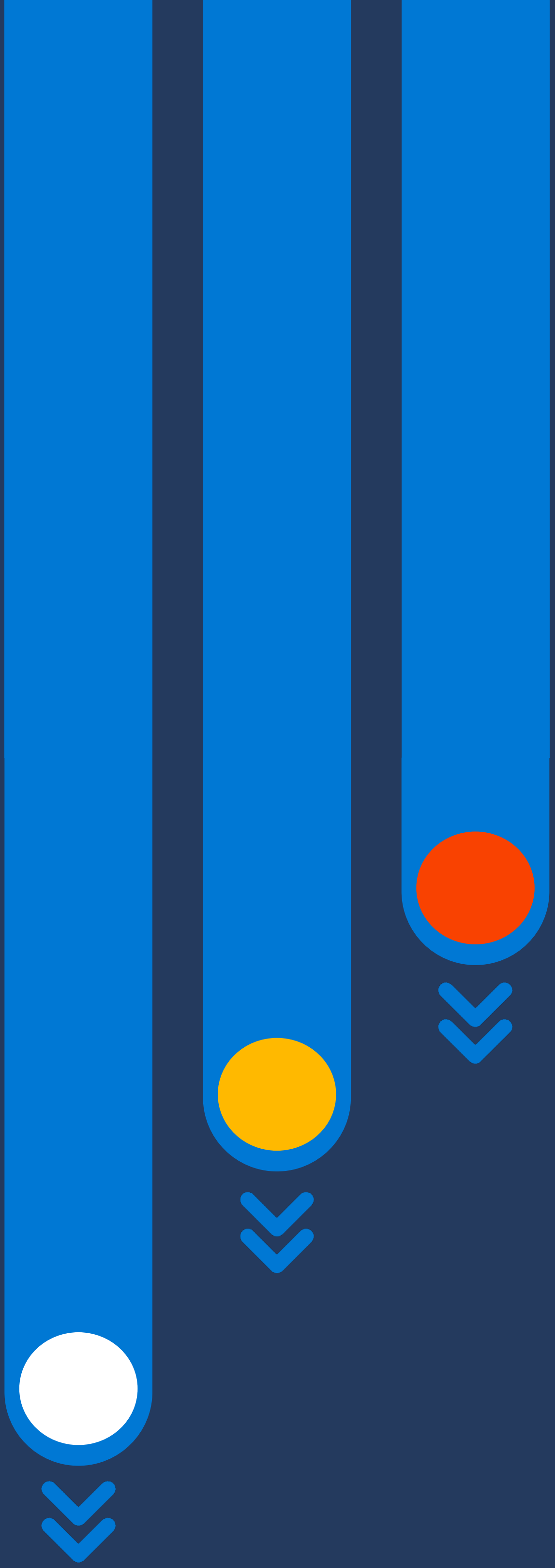
Learn more about Defender for Cloud »

To learn more about your multicloud identity and access vulnerabilities, sign up for a free trial of Microsoft Entra Permissions Management and receive your customized risk assessment report.

Try Permissions Management »

To gain deeper visibility into your multicloud data estate and understand what a comprehensive approach to data security could do for you, sign up for a free trial of Microsoft Purview.

Try Purview »



Microsoft Security