panoptica

The Future of Cloud Security

Attack Paths and Graph-based Technology

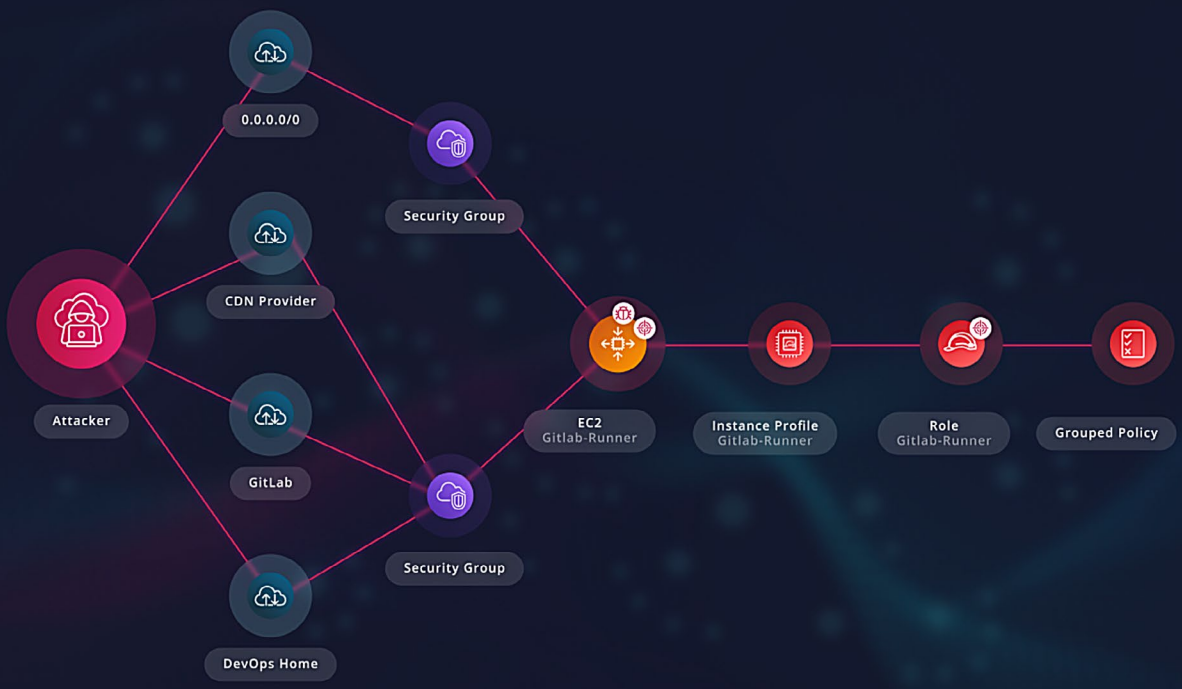


Table of Contents

Introduction

In this whitepaper we will dive into:

Section 1: The current approach to cloud security management

Section 2: Beyond the typical CSPM

Section 3: Graph-based technology and using context to build attack paths

Section 4: The attack path differentiation and attack path analysis

Cloud security risks and vulnerabilities are on the rise and 30%[1] of businesses fail to apply adequate security controls or provide the tools Security and DevOps engineers really need to solve this problem. Unprecedented and rapid expansion to the cloud, prompted by many organizations' digital transformation also means that cloud services are expanding faster than ever before. AWS alone has experienced over 1000% growth in services since 2013.[2]

Cloud security engineers are tired. Their current legacy tools and practices cannot securely scale with the requirements of today's ever-shifting environments, and engineers are suffering daily from meaningless alerts in the tens of thousands – the cloud security posture management (CSPM) industry average for false-positive alerts is 45%. Duct-taped and siloed solutions are not able to prevent breaches. Cloud misconfigurations account for 15% of initial attack vectors in security breaches.[1] This problem is only getting worse—between multi-cloud and various flavors of Kubernetes, the market requires a depth and breadth of expertise that is hard for organizations.

Two primary causes of cloud misconfigurations in most companies:[10]

62% Lack of security visibility and monitoring capabilities

49% Lack of knowledge and expertise in cloud security best practices

Security breaches:

99%

Through 2025, 99% of all cloud security breaches will have a root cause of customer misconfigurations or mistakes.[4]

Cloud account compromises:

~$6.2 million

In a 12-month timeframe, organizations lost ~$6.2 million to cloud account compromises.

3.5%

Data shows that cloud account compromises average out to roughly 3.5% of organizational revenue in a 12-month period.[5]

So how can organizations solve this problem?

Next generation cloud security, based on the graph

To meet these dynamic changes and increased cloud sprawl, organizations need a next-generation solution. ` Having a legacy CSPM provider isn't enough to protect businesses from fast changes to their multi-cloud environment and potential vulnerabilities across their cloud stack.

Businesses require a single, complete platform for all their cloud security needs to provide maximum security and true prioritization while improving efficiency and the effectiveness of their internal teams. Having all resources under a single platform requires that all facets of cloud management are contextually correlated. To be able to ascertain all context required, a solution based on graph theory is the only way forward. This will be discussed later in this paper in greater detail. Graph technology positions companies to garner more in-depth information about their platforms through the insight generated by graph databases. It provides businesses with the ability to leverage the voluminous data at their disposal and use it to reveal patterns and deeper insights. By leveraging the power of graph databases, graph technologies provide the ability to create and map relationships with dynamic assets, while visually depicting their interdependencies. Without the context provided by graph theory, it is impossible to get your arms around this massive and ever-evolving problem.

Cloud security management basics – setting the stage

Cloud security and security risk in organizations require a myriad of roles and responsibilities across multiple kinds of security teams. The breakdown of specific organization functions within security, often called responsibilities or "jobs to be done" spreads the onus of responsibility and ownership across multiple levels and sections of the organization.[6]

The diagram below represents an ideal view of a complete security team in best case scenarios where there are ample resources and budget. Integral to this risk management is **posture management** – which includes the ability to monitor and remediate risks.

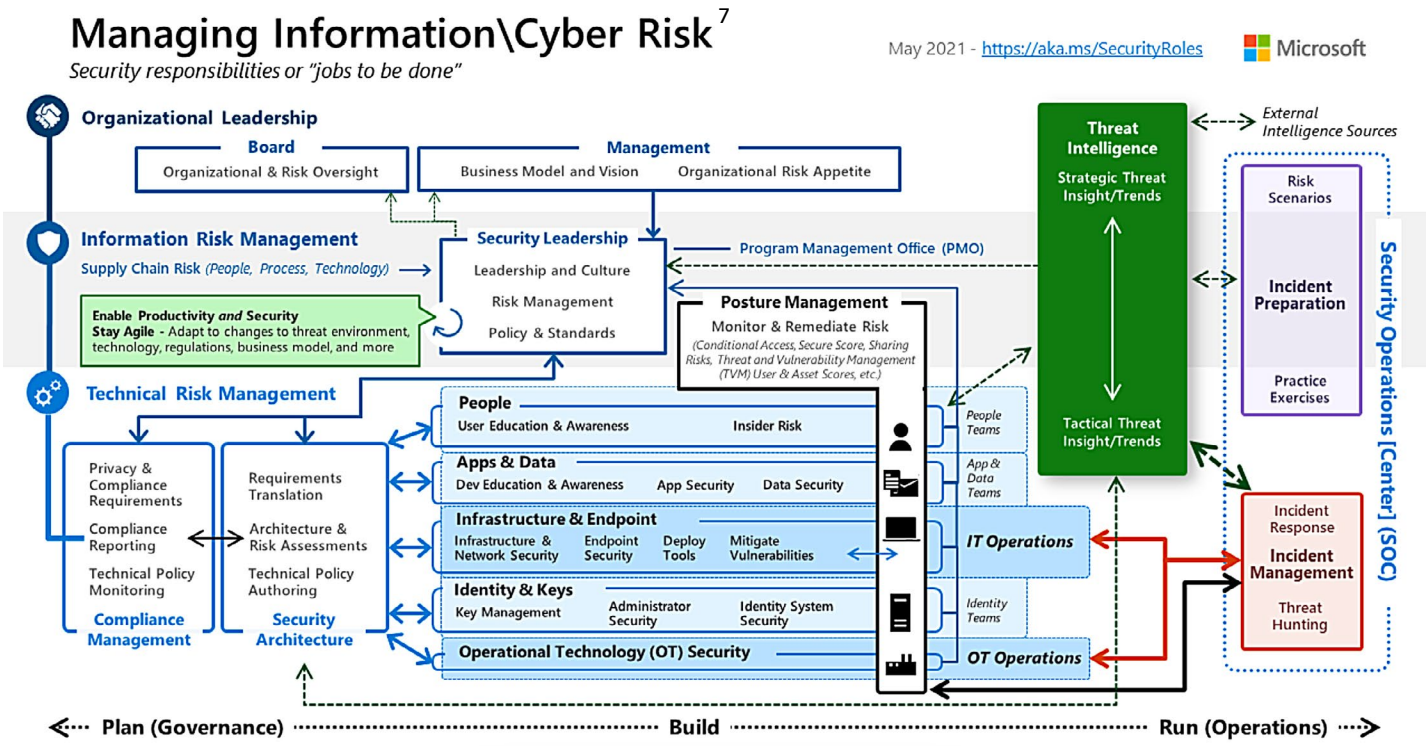


Image courtesy of Microsoft

As denoted in the above diagram, the concept cyber risk management is wide and requires distinct expertise cross-functionally to be best executed. The "jobs to be done" as it were, requires individuals to wear multiple hats and work seamlessly across systems and technological areas. Often this creates friction across teams, and it prompts questions of ownership and responsibility.

Section 1:

The current approach to cloud security management

Legacy cloud security posture management (CSPM) solutions

Cloud Security Posture Management (CSPM) can help organizations discover misconfigurations and vulnerabilities that can open their businesses to potential attacks. Most organizations, whether they are migrating to the cloud or cloud-native must have a CSPM tool in place to help them manage and mitigate potential risks.

Over the years, CSPM technologies have evolved, and they continue to change as the market shifts. In their earliest stages – what can be referred to as the first generation of CSPMs[8] – these tools were typically focused on identifying where there were instances of non-compliance primarily in AWS environments. The tools were built to meet specific security requirements and benchmarks mandated by different regulatory bodies and to fulfill general security functions.

Second generation CSPMs further expanded upon this by adding capabilities in Google Cloud Platform (GCP) and Azure, Common Vulnerabilities and Exposures (CVEs) scanning from a known-list and other benchmarks to say whether enterprise cloud environments are secure. It was during this stage that suddenly asset and resource hygiene began to be problematic, coupled with the question of which team owns what resource, Security or the evolving role of DevOps?

Third generation CSPMs saw the development of “auto-remediation” - basically identifying issues of non-compliance and remediating if a particular set of conditions were met. However, compliance alone is not enough to ensure a secure environment, even more so as assets and objects are being added or modified on a consistent basis within these environments. While auto-remediation has the potential to save time and improve the efficiency of security operations, it can also be risky and cause more headaches for your DevOps teams if not implemented carefully.

Legacy CSPMs are not able to accommodate these requirements, creating the following challenges for Security and DevOps teams:

CHALLENGES OF THE CURRENT APPROACH:

Lack of knowledge and expertise in cloud security.
Lack of knowledge and expertise in cloud security best practices (62%) as well as a lack of security visibility and monitoring capabilities (49%) were identified as two primary causes of cloud misconfigurations in most companies.[10]

Lack of visibility / inability to view holistically the cloud environment or cloud stack of the business.
Nearly 60% of CISOs and other security decision makers who participated in a survey consider lack of visibility as well as inadequate identity access management pose a major threat to their organization's cloud infrastructure.[11]

Teams suffering from a lack of prioritization in security alerts, and thereby alert fatigue.
Among IT security professionals, 40.4% say that the alerts they receive lack actionable intelligence to investigate and another 31.9% report that they ignore alerts because so many are false positives.[12] Furthermore, the average enterprise generates 2 billion cloud-related events a month, which could result in many unnecessary alerts.

Only meeting compliance benchmarks which means meeting the bare minimum from a security perspective. Being compliant doesn't necessarily mean that your environment is secure. Compliance deals with anticipated threats – the ones we know. But attackers don't necessarily take the road most traveled, they see through compliance to locate weaknesses within. They take advantage of configuration vulnerabilities caused by weak configurations and misconfigurations in the cloud, akin to the exploitation of application vulnerabilities due to oversights and bugs in code.[13]

Multiple tools to manage.
A survey by the Cloud Security Alliance found that half of enterprises have six or more tools that generate security alerts.[14] Not only is it problematic to juggle multiple tools, but in addition, these tools operate in silo – meaning that there is no way of efficiently leveraging the tools simultaneously and understanding which alerts or notifications from which tool should be dealt with first.

Keeping up with changes to cloud environment and managing dynamic environments.
17% of organizations reported that their most difficult challenge was cloud sprawl – unmanaged or unaccounted for resources. 15 AWS alone has experienced a nearly 1000% growth in services since 2013.[16]

Balancing the security requirements of a multi-cloud environment as your organization grows poses a significant challenge. Simply checking the box of compliance requirements is not enough to ensure your cloud is secure or following best practices to avoid common misconfigurations and security vulnerabilities.

Regardless of the size of your organization, making cloud security scalable should be a number one priority. The only way to do so accurately as your business grows and launches new products and features to market is through a graph-based and comprehensive approach to security.

Organizations require a fourth (or next) generation CSPM which provides more context, deeper insights into present vulnerabilities, agentless functionality, and the ability to connect between otherwise siloed and disparate tooling to surface the most critical and highly prioritized potential exploitable assets or set of assets.

Section 2:

Beyond the Typical CSPM

Fourth generation (or next generation) CSPM tools look to go further, creating a holistic, and proactive rather than reactive approach to handling misconfigurations, vulnerabilities, or over-permissive policies. Compliance is not enough to secure your environment, especially when new assets and objects are continually adjusted. But if you do security right, approaching it in a more holistic manner by surfacing the necessary context, there's a very low chance that you won't also be compliant along the way.

Organizations should be looking for forward-thinking vendors with innovative technology that can bring them a dynamic and proactive solution to meet today's challenges.

The need for a graph-based approach to cloud security

Through a modern approach to cloud security, wherein all risks are calculated through graph-based algorithms, cloud security engineers can unlock true prioritization and access only the critical security alerts that matter most. The graph provides the ability to glean the much-needed insights that connect all the assets in an attack graph and overall risk from disparate security findings, risky roles and configurations (IAM), malware, public exposure points, and more, to flesh out a more complete picture of the environment. Graphs are invaluable to security teams due to their ability to provide a detailed and three-dimensional overview of cybersecurity infrastructure and attack paths. In so doing, they illuminate security issues that exist and how these can impact the cloud network. The use of graph databases to create graphs of activity and behavior is especially useful to uncover anomalous behavioral patterns.

To ensure the best cloud security practices are in place, organizations should be looking for vendors who can:

- **Bridge the gap between Security and DevOps teams** – closing the gaps in expertise and augmenting the resources of the current team **without requiring additional hires.** Providing a "shift left" concept of security, from code to cloud with Infrastructure as Code (IaC) scanning.
- **A platform able to comprehensively illuminate vulnerabilities and gaps across the cloud stack while providing visualization to the entirety of the organization's business assets.** Visualization of entire cloud stack – across GCP, AWS, Azure, and K8s – using graph database.
- **Graph-based technology to provide the prioritization required to reduce alert fatigue and false positives – ensure that only the most critical alerts are being handled and being handled quickly.** Ensure your team is working more effectively and efficiently, minimizing the number less than critical, one-off security alerts, and instead connecting the dots between findings to surface the critical attack paths that matter most.
- **Businesses require a vendor that can provide the compliance benchmarks the business requires, but also should be adaptable and dynamic enough to offer 1) customized compliance and 2) security beyond benchmarks.** The best approach is using a solution that can bring them the compliance and posture management required, while closing the security gaps you may not have been able to detect with your legacy CSPM provider.
- **Provide a unified platform to orchestrate and ingest all aspects of cloud security, management, and long-term protection and reduce the need to manage multiple disparate tools.** The ability to unify CSPM, CWPP, and CIEM capabilities under the umbrella of a singular, integrated, and comprehensive platform – from build to production.
- **Stay one step ahead of cloud security trends – a proactive security research team that searches for vulnerabilities or potential misconfigurations across cloud providers.** Cloud security is complicated, and things change quickly. To stay one step ahead of opportunistic hackers, you need a proactive security research team that can anticipate threat trends to cloud environments and fluid changes to code & applications.

To bring forward true prioritization at scale, organizations require a tool that can provide the context they need to connect the dots between disparate security findings.

Section 3:

Graph-based technology and using context to build attack paths

Using graph-based technology to understand and prioritize risk

Through graph-based algorithms, it is possible to reveal all steps that happen during an attack itself, to visualize it, and reveal the remediation for how a user could mitigate such an attack. Through graph- based technology you can map the entire topology of your cloud environment and then overlay the complete flow of a potential attacker – from the network entrance point of the cloud environment all the way through to the workload risk and relevant permissions / identities – to reveal the final impact.

A graph-based approach to cloud security makes it possible to visualize and map:
- Network Access: Private vs public settings
- Identity: Permissions and privileges
- Workload Hygiene: Workload configurations, patching and stored credentials

And then, surface how to fix / remediate discovered risks across multi-cloud environments. This is only possible through mapping the relevant connections within the environment and providing the context engineers need to better understand what is important and what is not.

What is “context?”

The power of context to accurately provide prioritization

Why does context matter and what does it mean?

When it comes to cloud security and ensuring that your cloud stack is secure across all layers and cloud providers, understanding the context behind the surfaced security findings matters. Without the broader context of how disparate security findings may be impacted or connected to other findings, vulnerabilities, or issues across your cloud stack, the ability to accurately prioritize the findings that matter most is skewed.

Old school CSPMs typically only provide a list of security findings. They do not necessarily consider the following categories which are essential to establishing the context behind each finding itself.

Types of Context

Identity context

Identity context basically asks the question: “Who is allowed to access what asset and what is this asset authorized to do?”

Understanding this context provides you with the ability to consider the environment and circumstances a particular identity’s access or request to access a particular resource or asset. It also considers the limitations or lack of limitations regarding what a particular asset is authorized to do.

Network context

Network context provides the required details about the environment itself in which the asset or resources exists. It likewise asks the questions:

- Who has access to this network?
- Who else is in the network?
- To what is the asset attached within this network?

By asking these questions, we are better able to assess the level of risk or vulnerability associated with assets within the context of the network / environment itself.

Workload hygiene

When we look at security findings, we also must consider the workload hygiene.

Here, it is important to review the configuration of the asset itself - i.e. Is the asset up to date with its security patches? Is the asset "clean?" Best practice dictates that assets within workloads should be as "clean" as possible and should have the proper encryption and necessary security precautions in place.

Threat intelligence

When we think about threat intelligence from the perspective of context, it is important to understand many different facets of what could potentially increase risks to your environment. With more innovative solutions, threat intelligence should be approached by asking the following questions:

- What information can be seen from outside of the environment about the asset?
- What does the asset contain?
  Data, PII, etc.

Threat intelligence should be used as an enrichment to a platform – meaning that these additional feeds as they are integrated into platform, will be overlaid across security findings to provide additional detail regarding what potential threats could exist to the asset in question - i.e. Is it connected to any critical CVEs, is it a public-facing asset, etc.

Malware & CVEs

As mentioned in the previous category regarding threat intelligence, potential threats can be viewed both from the exterior POV - how would an attacker potentially exploit an asset, and what makes it vulnerable from the outside looking in - but also approached by looking at threats and risks from the inside looking out. In other words, are there any CVEs or malware running on the asset from within the environment?

Real-time events

The platform your organization uses should look at real-time events across your applications, network, and infrastructure. This ranges from GuardDuty events to data exfiltration, and more.

A holistic view of the environment

Through an approach of breaking down the different layers of context, it is possible to get a more holistic view of the entirety of an organization's multi-cloud environment. Looking at the many layers and facets which could potentially impact the risks to an environment, builds a more comprehensive story to flesh out the significance of otherwise disparate security findings. This allows the platform to ingest these multi-layer feeds and provide the output of prioritized attack paths which connect the singular security findings.

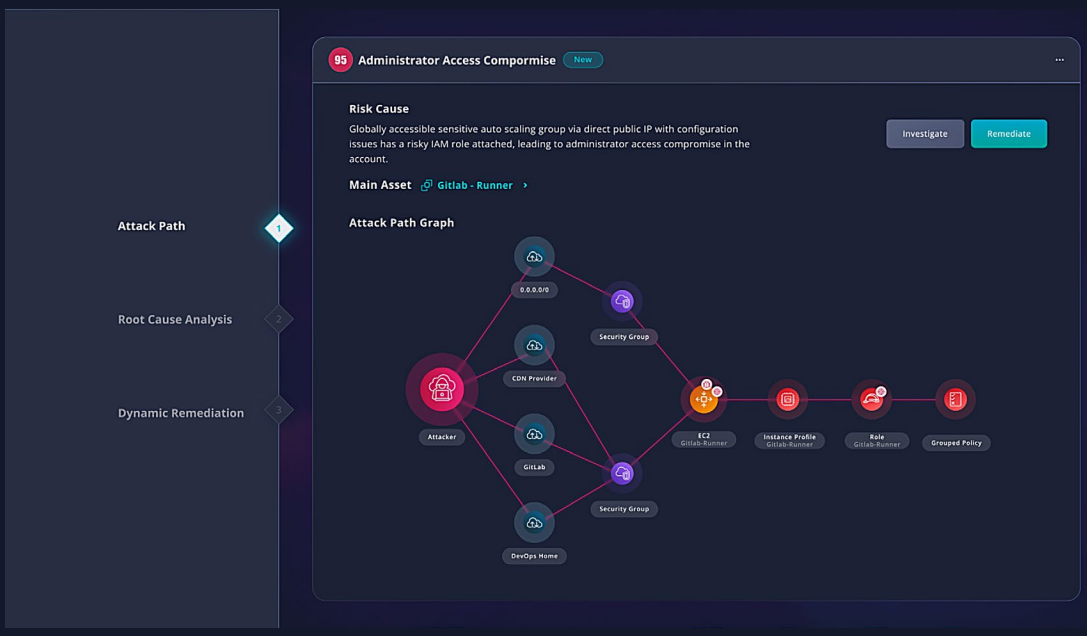


Figure 1.

An attack path that starts with a potential attacker having global access to sensitive auto scaling groups via direct public IP that can lead to an Administrator Access Compromise.

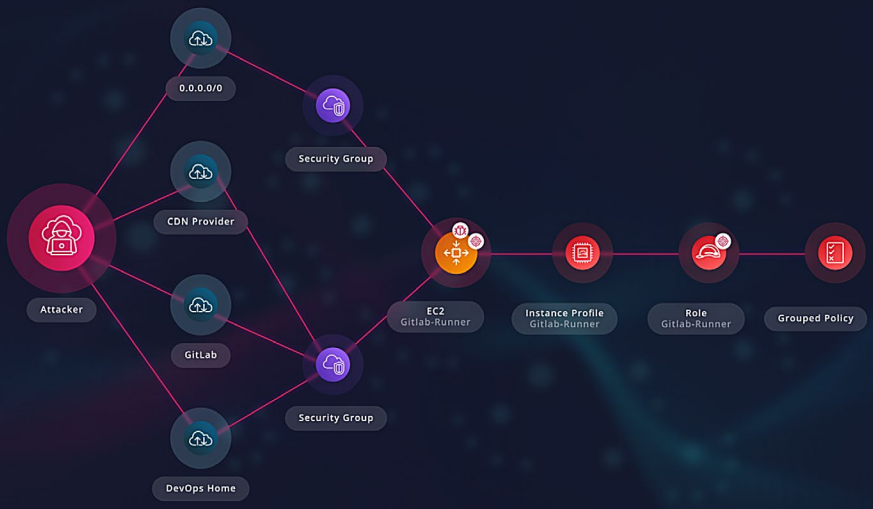


Figure 2.

Close up view of attack path details featured in Figure 1.

How do graph-based algorithms work when applied to cloud environments?

First, you need to form a graph

To get an accurate view of your cloud infrastructure, you need a map. Cloud mapping is completed by assessing the relationships between cloud assets; this can be most efficiently represented as a graph. To create the graph, you'll need to build an explicit and well-defined relationship table stating all the possible links between the assets, and then how these can be deducted from the data collected. Panoptica tackles this based on basic permissions to an organization's metadata, and the result is a topological graph containing all cloud entities, including the links between one another.

Each link is created with two elements in mind. First, direction. This means we would ask, "Is asset A connected to asset B or vice versa?" Next, the type. The question here is more complex and could be, "Is asset A contained in asset B, attached to it, exposing it?" and more. A graph database specializes in identifying not only the assets themselves, but more importantly, the relationships between those assets.

The graph should be a cross-platform graph, meaning it will contain assets from a multi-cloud environment, collected from various cloud providers (AWS, Azure, GCP), multiple orchestration platforms (Kubernetes, Rancher, Mesosphere), containerization platforms like Docker, 3rd party IP addresses, and more.

Assets can be linked in the graph regardless of their platform origin (for example, a Kubernetes service exposing an AWS load balancer), making the graph topology holistic and fully resemblant of the client's cloud architecture. The graph should be a cross-platform graph, meaning it will contain assets from a multi-cloud environment, collected from various cloud providers (AWS, Azure, GCP), multiple orchestration platforms (Kubernetes, Rancher, Mesosphere), containerization platforms like Docker, 3rd party IP addresses, and more.

Assets can be linked in the graph regardless of their platform origin (for example, a Kubernetes service exposing an AWS load balancer), making the graph topology holistic and fully resemblant of the client's cloud architecture.

Use graph analytics to extend the value of the data discovery capabilities in your analytics to represent relationships and node attributes – and to reveal hidden patterns and new insights.

Graph theory and graph databases

In graph databases querying languages are used to build upon concepts of graph theory. In so doing, variables can be assigned and referred to with types like nodes, edges, and even paths in the graph, which as it applies to cloud security, makes it perfect for threat modelling. Billions of nodes and edges can be held in a single database, making it fertile ground for research of social networks, consumption tracking, customer interest maps, and cloud architectures.

It is evident that using a graph theory-based approach to reduce cyber security risk on the cloud is a **requirement** rather than a "nice to have." Having continuous mapping of a cloud environment yields value in two different aspects. First, visibility – gaining a deep understanding of the environment's cloud architecture, and second, cloud risk management – identifying critical attack paths in the environment and mitigating the risk they present.

Graph theory algorithms can be used to ask questions about cloud topologies and the objects and assets found in them, including:

- How important is a node in a specific scenario?
- How many connections does it have, what types?
- Is it a node that links between different nodes from other accounts?

Using graph centrality theory, weight can be applied for each of these aspects. Then using a scenario-based system, we look for risk properties that may be shared across scenarios. This includes:

- High privileges / permissions
- Account access

Once completed, you can group findings by the risk cause. This same logic / algorithm can also be applied across organizations – this is what affords the system the ability to, at scale, discover potential attack paths.

Section 4:

The attack path differentiation and attack path analysis

What is an attack path?

An **attack path** is not the same as an attack vector. Often these terms are used interchangeably, but an attack vector is a method used by an attack to take advantage of a security mishap existing in a system – in this case, a cloud environment. In other words, it is the doorway through which an attacker can penetrate a given system. An attack path is the visual representation of the ongoing flow that occurs during the exploitation of such vectors by an attacker – which includes the attack vector as well as the damage that can be done once the attacker is inside.

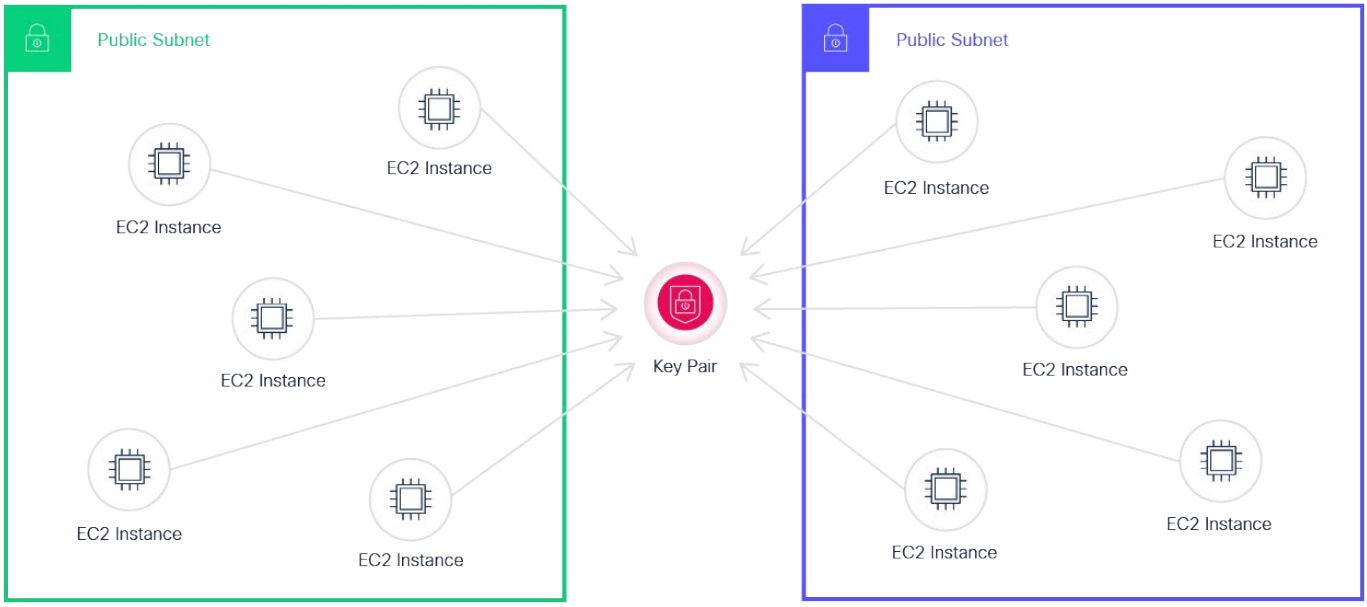
Attack path analysis

How does attack path analysis work?

Through asking context-related questions about risks imposed on a cloud environment and surfacing their responses, it is possible to surface attack paths in a visual, intuitive, and easy-to-understand manner.

Unlike signature-based attack analysis, the interesting and unique thing about attack path analysis is that they can uncover new and unknown risks, rather than those originating from known attack vectors. That means it's able to show you your attack surface in a much more helpful way. Beyond visualization, attack path analysis is a set of graph algorithms based on certain graph patterns, generating the most critical path for a certain asset based on several risk factors that meet a minimum score threshold.

Attack paths can find threats that are seen solely from the graph topology and the logical connections between the nodes within it. To take the simplest case, think of an access key shared by multiple EC2 instances, as seen in the diagram below. By running a degree centrality algorithm on all access keys that exist in the topology, we can detect attack paths that impose a serious risk and could potentially lead to attackers making lateral moves in the environment to reach sensitive data or any other payload.



The attack path analysis gives the cloud owner a comprehensive view on imposed risks and assets, and specifically those in concern or danger of attack. This view not only helps in mitigating current cases, but it also prevents attacks from taking place in the future.

An attack path is a **visual representation** of exploitable attack vectors. The attack path gives emphasis on “connecting the dots” and looking at the entire context of an imposed risk. This starts from the network exposure of the asset in question, continuing to the asset whose access privileges are elevated by risky roles and permissions attached, all the way to the “crown jewel” – the sensitive asset to be exploited or impacted if the attack is successfully executed by the attacker. Today, this crown jewel asset is often **sensitive data**, nd many cybersecurity technologies will start from this sensitive data, and then segment, isolate or protect to close any attack paths from being used. However, on the cloud-attack path analysis is not so simple.

Attack paths in action

While security findings and compliance policies / benchmarks are a good place to start to protect your cloud environment, singular findings can leave holes in the bigger picture. To better secure your cloud stack, attack paths are vital. To see how the attack path approach works, let's look at the following example:

The following two Security Findings are presented in the panel:

1. Usage of IMDSV1 (Low)
2. Highly permissive role attached to workload (Medium)

Without any context, these two singular findings can be considered as unrelated. But what if we add some context? Let's assume there is an EC2 instance in the AWS account which uses MDSV1 and has an "S3 read all" role attached.

Now we can understand the connection between these two otherwise seemingly unrelated security findings. We now can see that they are both related to the same EC2 instance. Now that we understand they are related, we need to better understand the real risk associated with them. Should these findings be marked as "Low Risk" or "Medium Risk?"

To answer this question and calculate the effective risk we need to look at the entire cloud environment. We need to answer some important questions including:

- Within which VPC this EC2 located?
- Is it private or publicly accessible?
- What are the effective permissions between the role and the buckets?
- and more...

Analyzing the identified security findings with context enables us to evaluate the real risk. In this scenario, if the EC2 is public to any IP and there is no deny from the bucket's resource-based policy, the real risk should be denoted as "High."

Attack paths vs security findings

An attack path is more sophisticated than a security finding because it includes context and evaluates the combined risk along several different variables:

	Attack Path	Security Finding
Findings	Combines multiple findings	Single finding
Context	Uses context	No context, presented in silo
View	Big picture	Narrow view
Risk	Presents real full risk	Presents partial-risk – disconnected from other factors in given environment

Relevant risk categories

- Public exposure
- Identity risk
- Account compromise
- Data at risk
- Credentials
- Config risk
- Asset at risk

Attack paths vs security findings

Why does prioritization matter?

When using legacy CSPM tools the most common feedback across the board is that users are overwhelmed with the volume of disparate and siloed security findings that their systems feed back to them. On a day-to-day basis, it was near impossible to ascertain which of the findings were most critical and which did not require imminent remediation. This ultimately leads to a flood of alerts but a lack of efficiency with how they are handled.

Using context to build prioritization

Looking at a variety of layers within multi-cloud environments builds the story behind each disparate finding. This multi-faceted approach builds the context or story by connecting between findings to surface what really matters. This provides the ability to accurately build prioritization of findings.

Looking through the lens of the attacker

By mapping each security finding identified in a hybrid cloud environment and looking across the entirety of this map to see how each aspect of a finding could potentially impact another if it were to be compromised by an attacker, provides a more sophisticated view of vulnerabilities.

This is how critical attack paths are constructed and eventually prioritized - which assets could be compromised, how easily, what connected accounts / identities or permissions could an intruder access if they breach asset X?

Where are there the most exploitable gaps in your cloud's surface area? Why are these gaps the most vulnerable? The ability to think like an attacker provides an edge - instead of reacting to breaches, it is possible to proactively determine in which areas your multi-cloud environment has the most "appealing" gaps.

To power this capability, consistent and ongoing proactive cloud security research is required. In tandem with a graph algorithm team, cloud security vendors should have an expert cloud research team that is trying to understand how cloud security service work, how they are implemented, what functions are happening in the backend, and then going beyond that to test, "well, what would happen if I tried XYZ?" At the end of the day, the function of cloud security research is to better understand the services being provided to assist developers and users to work in their cloud environments more securely. Best-in-class providers will have a dedicated team that works alongside algorithm teams to ensure trends are continually updated and reviewed.

The insights you can gain from giving extra attention to the attack path and the contextual view are critical for the successful mitigation of imposed risks in any cloud environment. They go so much further than attack vector analysis can achieve.

Bringing it all together

Attack vector analysis alone doesn't offer a contextual view of your security risk, instead focusing on purely a single method that a bad actor might use to compromise your cloud environment. Even attack surface tools will only bring together any attack vectors that are a potential threat. Neither of these approaches allow you to quantize risk, or to uncover what needs actionable attention in your cloud. Using attack path analysis is a huge leap forward for cloud security, but you also need to ensure that you have a stateful view, not simply a one-time-only stateless approach where risks are seen and then forgotten. For the cloud security practioners, the Security and DevOps teams, this approach provides a welcome respite from the endless alerts and provides them the focus and clarity they need to make better informed decisions and work more efficiently and effectively.

Having a reliable attack path analysis system in place with a stateful cloud environment is a powerful combination that no cloud owner should resist – and that's exactly what you get with graph-theory-based approach. When implemented right, it allows for a focused and well-informed look into security blind spots, helps with both tracking and prioritizing threats, and achieves the goal of increasing the productivity of both risk reduction efforts and attack mitigation, leading cloud owners to overall improved decision making.

Conclusion

The Way Forward

A single, comprehensive platform to meet dynamic shifts in cloud security requirements

Cloud security is complicated and requires a dynamic application of technology to help manage risks and proactively prevent potential exploitations. The average cost for a hybrid cloud data breach is $3.61 million[17] . To avoid the potential risks that could lead to such a breach, organizations need to keep pace with ever-changing cloud security compliance requirements and constantly evolving risks through leveraging a proactive cloud security platform to protect and secure their cloud stack.

The view of said cloud stack should be holistic – from code, to buildtime, to operations – a continuous loop by which security is constantly at the center.

- Graph-based technology at the heart of the system
- Attack path analysis and approach
- Prioritization
- Remediation through dynamic guardrails
- Infrastructure as Code scanning – providing security from the earliest stages

Through the attack path approach

Ensure your cloud environments are safe and secure through a proactive security posture.
Protect your business from vulnerabilities and gaps while leveraging attack path-based detection to help prevent potential future attacks.

Mitigate the alerts that matter most.
Understand the 'why' behind prioritized cloud security vulnerabilities and receive only the most critical alerts and their remediation paths - delivered as Infrastructure as Code (IaC) - improving your team's efficiency and reducing their headaches.

Gain full security visibility across cloud environments.
Panoptica's patent-pending graph theory technology empowers your team with the end-to-end visualization they need to understand your entire cloud stack, effectively manage cloud assets, and identify the most critical security vulnerabilities and alerts.

Further enrichments to the attack path approach offer organizations the multiple layers of security and tools they need to ensure their business is protected from build to runtime. For Panoptica, the graph- based technology, powered by the continued fine tuning of expert researchers, is at the core of the solution – it's what makes it possible to surface attack paths and provide the value of prioritization and remediation of potential cyber risks along every stage of the cloud journey.

Sources

1. https://www.cybertalk.org/2021/10/20/key-cloud-security-statistics-that-will-reshape-your-cloud-perspectives/
2. https://cloudpegboard.com/servicecounts.html
3. https://www.gartner.com/smarterwithgartner/is-the-cloud-secure
4. https://www.gartner.com/smarterwithgartner/is-the-cloud-secure
5. https://www.cybertalk.org/2021/10/20/key-cloud-security-statistics-that-will-reshape-your-cloud- perspectives/
6. https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/organize/cloud-security
7. https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/organize/cloud-security
8. https://www.youtube.com/watch?v=cWYflFLOecA&t=1s
9. https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/what-is-a-cwpp.html
10. https://www.cloudhealthtech.com/blog/cloud-security-report-misconfiguration-risks
11. https://www.helpnetsecurity.com/2021/06/30/cloud-infrastructure-security/
12. https://www.mcafee.com/blogs/enterprise/cloud-security/alert-fatigue-31-9-of-it-security-professionals-ignore-alerts/
13. https://securityboulevard.com/2020/11/cloud-compliance-doesnt-equal-security/
14. https://www.mcafee.com/blogs/enterprise/cloud-security/alert-fa-tigue-31-9-of-it-security-professionals- ignore-alerts/
15. https://www.ibm.com/downloads/cas/L9K1MK1Y
16. https://cloudpegboard.com/servicecounts.html
17. https://www.forbes.com/sites/ibmsecurity/2021/09/21/want-to-avoid-a-multi-million-dollar-data- breach-you-need-these-three-things/?sh=28b2d61f94b2
18. https://neo4j.com/blog/reveal-hidden-patterns-healthcare-data-graph-analytics-opioid-crisis/