panoptica

Cisco Cloud Application Security

Context-Driven Security

How Graph-Based Technology Builds Context in the Cloud

Table of Contents

Introduction

Cloud security is a critical concern for businesses today. As enterprises adopt cloud-native technologies and deploy to the cloud, they encounter countless new security challenges. The traditional security methods that once protected their applications are now inadequate for protecting complex cloud environments. This leaves them in a tough spot: either vulnerable to threats or bogged down by a disparate set of cumbersome security tools.

Stuck in this predicament, many enterprises struggle to find their way out. With current security strategies proving inefficient, they run up against operational challenges and ever-increasing risk.

In this white paper, we'll explore a new approach to cloud security: using graph-based technology to provide the context that your security stack can use to determine potential attack paths. Enterprise security teams will only be adequately equipped to prioritize security alerts effectively once they have the proper context around their cloud infrastructure and vulnerabilities. We'll examine the following:

- The Pain Points of the Current Approach to Cloud Security
- The Impact of the Current Approach on Your Enterprise
- How Graph-Based Technology Transforms Cloud Security
- The Integration of Attack Path Analysis with Your CNAPP

Let's start by reviewing the challenges faced by enterprises that try to use traditional security tools for their cloud security.

The Pain Points of the Current Approach to Cloud Security

Although many businesses have transitioned their applications to the cloud, their security approaches and tools have been slower to adapt. As a result, they come up against several pain points.

Siloed and Disparate Security Tools

Many enterprises use a variety of security tools, each designed for specific tasks. In simpler times, an enterprise may have started with a single tool. But as its infrastructure becomes more complex—multi-cloud deployments, containerization, more endpoints, more data, etc.—what began as a one-tool security stack balloons into dozens of disparate tools.

This piecemeal approach fragments an enterprise's view of the security landscape. Each tool operates in its own silo, making it challenging to establish a comprehensive view of the security posture. Without tight and easy integration between tools, enterprises deal with gaps in security coverage and inconsistencies in data reporting.

A study conducted by Forrester surveyed 200 North American IT security and operations decision makers. Over 50% of the cyber-security respondents reported using at least 10 different tools in their organization. Nearly 30% reported using at least 20 different tools.

Inefficient and Slow Response

Disparate tools not only make it difficult to understand your security posture, but they also require additional time and expertise for proper management. For most enterprises, this added burden can stretch IT resources to a breaking point. As a result, enterprises see inefficiencies related to incident detection and response. Ultimately, security incident response time slows.

Chronosphere's 2023 Cloud Native Observability Report surveyed 500 engineers from U.S.-based companies. Barely 1% of respondents said that their company met or exceeded their goal for mean time to repair (MTTR).

Lack of Visibility

Traditional security tools are often unable to provide organizations with a complete view of their cloud environment. They either don't have all the information, or they can't properly correlate the information to establish a comprehensive view. Lack of visibility into your cloud environments creates blind spots, and this is how vulnerabilities go unnoticed. Without modern cloud security tools that leverage context to provide a complete view of your cloud, an enterprise leaves its cloud infrastructure exposed to potential threats.

Overwhelmed by Alerts

Every security tool is equipped with an alert feature. When a tool detects something awry, it alerts you. This includes false positives. But, when enterprises have multiple, disjointed tools—some of which may have overlapping functionality—it's no surprise that security teams are frequently overwhelmed with a high volume of alerts.

The best-case scenario of alert fatigue is that a security team becomes minorly annoyed and inconvenienced. Perhaps team morale takes a hit. However, it's not uncommon for alert fatigue to lead to critical alerts being overlooked or delayed. This could result in an ineffective security response or, worse, a full-blown security breach.

Being overwhelmed with alerts causes more than just overlooked alerts and a slow security response. Constantly bogged down with triaging alerts, teams have little margin left to focus on work that brings higher business value.

A **report** conducted by International Data Corporation found that companies with 1500 to 4999 employees ignore or do not investigate 30% of the security alerts they receive. It also found that false positives took nearly as much (or sometimes even more) time as actionable alerts to investigate.

Inability to Prioritize Threats

The infrastructure to support a globally distributed cloud-native application can be massively complex. We're no longer in the days of maintaining a handful of servers, a database, and a CDN for serving up a static frontend. With cloud-native applications, enterprises now need to manage hundreds of workloads and services, and they're ephemeral—continually spun up, spun down, or replicated based on the need of the moment.

With so many digital assets interconnected in different ways, a clear understanding of those connections is essential for knowing how to prioritize threats. Traditional security tools may identify vulnerabilities, but they often fail to convey the potential impact of a given threat on the broader system. Security vulnerabilities are legion, so prioritization is key. Without proper prioritization, the result may be inefficient or misguided security efforts.

The Impact of the Current Approach on Your Enterprise

The current approach to cloud security—with disjointed tools and without adequate cloud environment context—falls short in its ability to ensure an efficient and effective security posture. The impact of these shortcomings is significant. Let's consider some hard numbers.

Mean Time to Repair (MTTR)

When an enterprise uses multiple, siloed tools, the results it receives are fragmented. A lot of additional time and effort are needed to piece the information together, and this directly impacts a security team's MTTR. When tools don't integrate seamlessly with one another, cloud visibility is obscured, and your team will take longer to identify and respond to threats. As the clock continues ticking, the window of vulnerability expands. As threat identification and mitigation are delayed, the potential damage inflicted by that threat grows.

Alert Fatigue

As we've noted, the current approach to cloud security is prone to inflicting alert fatigue on security teams. Every day, teams face a barrage of alerts—many of which are false positives. As if dealing with threats wasn't enough, security professionals need to expend energy on discerning genuine threats from meaningless noise. Critical alerts result in delayed responses, or they're missed altogether. Over time, alert fatigue will strain resources, damage morale, and reduce the overall effectiveness of your teams.

Tool Sprawl

The tool sprawl that comes with the current approach impacts an organization in obvious and subtle ways. As the cloud security landscape grows complex, organizations add more tools to cover those complexities. Not long after, they have inadvertently created a disjointed and unwieldy security environment. The results of tool sprawl include:

- Complicated management of tools
- Increased maintenance costs for tools
- Resource allocation issues
- Additional training or expertise needed for each new tool
- Low team morale or burnout among the security team

In summary, the current approach to cloud security, characterized by its reliance on multiple, siloed tools, presents significant pain points for businesses. These challenges are enough to compromise the effectiveness and responsiveness of teams working to secure their cloud environments.

An alternative approach to cloud security—one that incorporates graph-based technology—offers a promising solution. This method provides a more integrated and insightful way to manage cloud security.

How Graph-Based Technology Transforms Cloud Security

Graph-based technology offers a fresh approach to cloud security, focusing on interconnectivity and relationships within the cloud environment.

Mapping Cloud Environments with Graph-Based Technology

Cloud environments can comprise a complex and intricate stack of digital assets and resources, including identities, computing, databases, storage, and more. Layer on the complexity of enterprises that use multiple cloud providers to support their cloud-native applications, and you have a potentially tangled web.

With such complexity, how might an enterprise gain an accurate and comprehensive view of its cloud infrastructure? The answer is the graph-based map. Graph-based technology uses a network of nodes and edges to map out relationships and dependencies in a cloud environment.

By **using graphs to map the relationships between cloud assets**, an enterprise enjoys **improved visibility**. This approach provides a unified, clear, and comprehensive view of the entire cloud environment, revealing connections between assets—*and* potential vulnerabilities. A graph-based visualization of your cloud environment provides **contextual insights** that yield a deeper understanding of your security landscape, which is critical for informed decision-making.

Beyond Potential Vulnerabilities to Potential Attack Paths

Graph-based technology not only pinpoints vulnerabilities among your cloud asset connections, but it facilitates the mapping of potential attack paths.

What is an Attack Path?

An attack path helps to show how multiple security vulnerabilities may be exploited in coordination by an attacker seeking access to a specific asset. The attack path is a "**visual representation of the ongoing flow that occurs during the exploitation of such vectors by an attacker.**"

An attack path is not the same as an attack vector. Often these terms are used interchangeably, but an attack vector is a single method used by an attack to compromise a cloud environment, while an attack path can be defined as the following:

- **It's like a map or recipe.** An attack path is a visual representation of exploitable attack vectors. Think of it as a "map" or "recipe" that an attacker could use to compromise a cloud environment. The attack path gives emphasis on "connecting the dots" and looking at the entire context of an imposed risk.
- **It's contextual.** This context incorporates elements from a variety of risk categories—starting 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 exploitation of sensitive data.
- **It's like looking through the lens of the attacker.** Attack paths can uncover new and unknown risks, rather than those originating from known attack vectors. How can this be done? By analyzing your attack surface and looking at it through the lens of the attacker. Attackers map security findings by identifying them in a cloud environment. Then, they see how each aspect of a finding could potentially impact another if it was compromised.

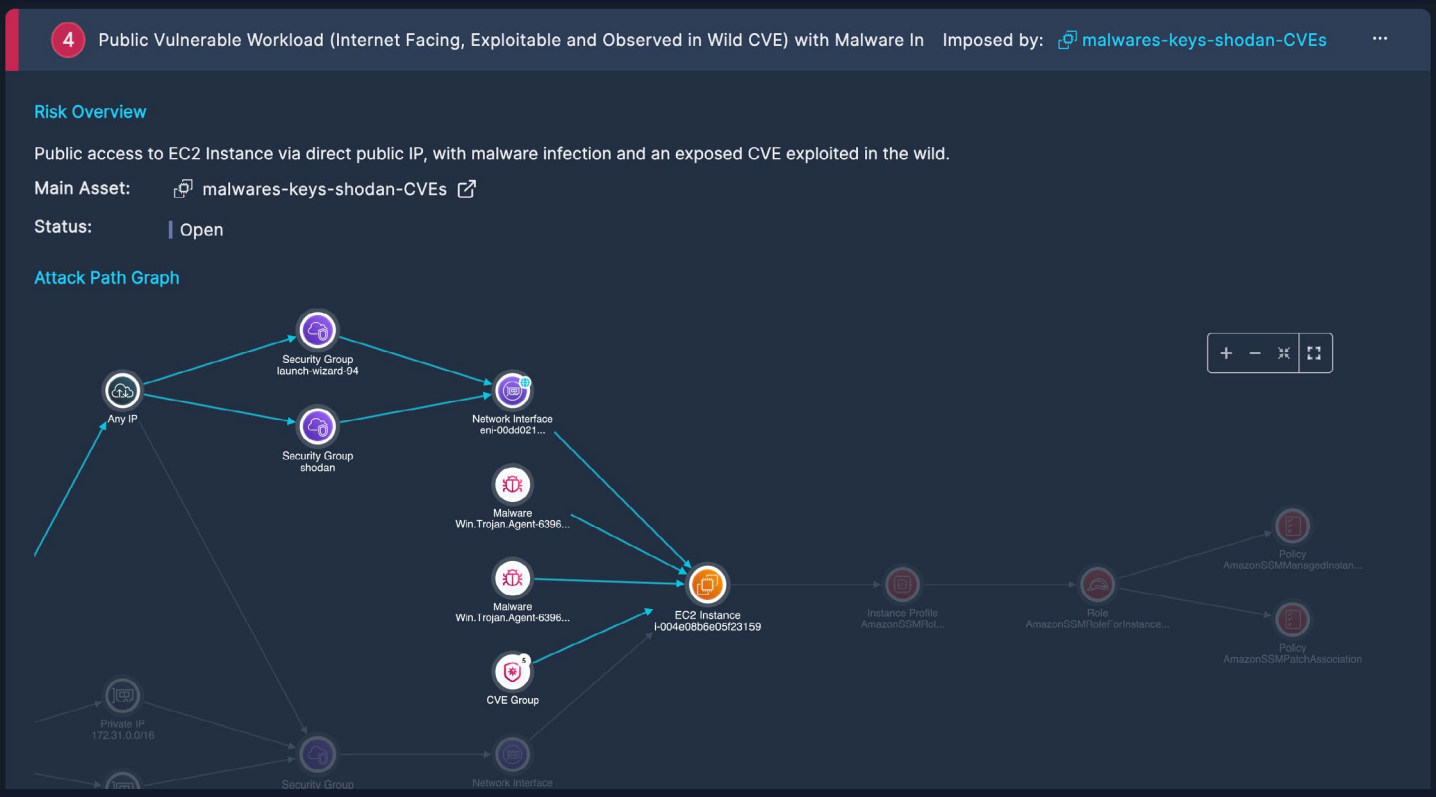
  This is how critical attack paths are constructed and eventually prioritized. Which assets could be compromised? How easily? What connected accounts or identities or permissions could an intruder access if they breach asset X? Where are there the most exploitable gaps in your cloud's surface area?

  The ability to think like an attacker provides an edge; instead of reacting to breaches, it is possible to proactively determine which areas of your multi-cloud environment have the most "appealing" gaps.

This is why attack paths are important. It's a new representation, a new metric that leads to real risk reduction.

Attack Path Analysis

In attack path analysis, context is key, which is why graph-based technology is essential. Knowing about a security vulnerability here or there is useful to an extent; but with the entire cloud environment context afforded by graph-based technology, we can use attack path analysis to connect the dots between vulnerabilities. This provides crucial insights into the practical implications of a security weakness.



An added bonus of attack path analysis is the newfound opportunity for **focused prioritization**.
By identifying the various attack paths, one can determine the most critical threats. This approach helps security teams to concentrate their efforts where they are most needed, working down the list from there.

Technical Steps for Generating Stateful Cloud Environment Graphs

A detailed look at the process of mapping a cloud environment in order to analyze and prioritize attack paths is outside the scope of this white paper. However, we can summarize the major steps in the process, as outlined in this **technical deep dive**:

1. Data collection: Gather comprehensive data from the cloud environment—such as configurations, logs, and metadata—by sending requests to the API servers of cloud vendors, to form the basis of the graph.
2. Graph construction: Structure the collected data into a graph format, creating nodes and edges that represent the elements of the cloud environment and their interconnections.
3. Attack path detection: Determine what privileges attackers can obtain by accessing certain assets in the graph, and what other assets this can lead them to gain control of.
4. Risk analysis: Enrich attack path data with details to better understand attack scenarios, finally prioritizing the attack path among all others that were detected. Each attack path is given a risk name (concise path implication used as its title), risk cause (reason for path detection), and risk impact (potential result of the risk).

Improving Efficiency and Empowering Remediation

A Graph-based technology enhances the efficiency and accuracy of security teams by focusing on the most critical threats and providing actionable insights. This leads to more effective remediation strategies and a stronger overall security posture.

Attack path analysis is essential to the effectiveness of cybersecurity in the cloud-native era. And as we've seen, graph-based technology facilitates the cloud environment context that is foundational for attack path analysis. With this understanding in mind, let's turn our attention to the integration of attack path analysis within a cloud native application protection platform (CNAPP).

The Integration of Attack Path Analysis Within Your CNAPP

Integrating attack path analysis within a CNAPP marks a significant advancement in cloud security. In this section, we'll explore how graph-based technology and attack path analysis fit into the CNAPP framework, and how this coordination compares with traditional cloud security approaches.

Integration with CNAPP Technology

Modern CNAPPs bring a holistic approach to cloud security, consolidating the tools to cover various cybersecurity aspects that include:

- Vulnerability management
- Threat detection
- Endpoint detection and response
- Compliance
- Cloud posture security management (CSPM)
- ... and more.

A CNAPP integrates all of these tools together into a single, unified platform. No more disparate and siloed tools. No more alert fatigue from a sprawling set of tools that don't communicate with one another. No more fragmented visibility.

Through the integration of graph-based technology and attack path analysis within a CNAPP, users experience several key benefits:

- Enhanced visibility and context: Graph-based technology within a CNAPP provides a comprehensive view of cloud environments. This view illuminates the complex relationships between different assets and offers a context-rich perspective that is crucial for effective security management.
- Proactive security posture: The identification and visualization of potential attack paths enables enterprise security teams to shift from a reactive to a proactive security stance. This means much more than just responding to threats as they occur, but anticipating and preventing them before they materialize.
- Automated risk prioritization: Attack path analysis helps a CNAPP to intelligently prioritize risks. With risk prioritization automated, a CNAPP ensures that security teams focus on the most critical issues, improving response times and efficiency.

Contrasted with Traditional Cloud Security Methods

The graph-based approach within CNAPPs contrasts sharply with traditional cloud security methods in several ways:

- **Siloed to integrated**: Traditional methods often involve the use of disjointed and siloed tools. In contrast, CNAPPs provide an integrated platform that consolidates various security functions, offering a unified "single pane of glass" through which security teams can manage all aspects of their cloud security.
- **Reactive to proactive**: Traditional security is typically reactive, dealing with threats as they arise. CNAPPs, with the predictive capabilities afforded by attack path analysis, enable a proactive approach, identifying and mitigating risks before they become actual threats.
- **Generalized to contextualized security**: Traditional tools may identify individual vulnerabilities, but the resulting data lacks context. CNAPPs, through comprehensive graphs that visualize the cloud environment, provide a deeper, interconnected understanding of vulnerabilities and their potential impact.
- **Manual prioritization to automated risk assessment**: Where traditional methods rely heavily on manual processes for risk assessment, CNAPPs automate this process, leveraging advanced analytics to prioritize risks more effectively.
- **Attack path analysis**: Attack path analysis is the key to uncovering new (unknown unknown) and known risks. As the "map" or "recipe" that an attacker could use, the intuitive and easy-to-understand visualization of these attack paths is a game-changer for security organizations. Having a reliable attack path analysis system in place allows for a contextual and well-informed overview to combat security blind spots, helps with both tracking and prioritizing threats, achieves the goal of increasing the productivity of both risk reduction efforts and attack mitigation, and leads to more intuitive and improved decision making.

In conclusion, the integration of graph-based technology and attack path analysis in CNAPPs offers a more sophisticated, efficient, and proactive approach to cloud security. This modern method addresses the limitations of traditional security tools, providing businesses with the tools they need to protect their cloud environments more effectively.

The Future of Enterprise Cloud Security

Although the cloud security landscape is evolving, the use of graph-based technology and attack path analysis in CNAPP solutions introduces a shift toward more context-aware, interconnected, and intelligent security management. By embracing this approach, businesses improve cloud visibility and security efficiency while establishing a proactive security posture.

Corporate budgets are making room for cloud-native capabilities and security. Gartner's **report on worldwide cloud spending** forecasts over $350 billion to be spent in 2024 on cloud application or system infrastructure services, and an additional $50 billion spent on cloud management and security. Total worldwide cloud spending is projected to grow by 21%, from $597 billion in 2023 to $724 billion in 2024.

The CNAPP space will continue to trend toward more comprehensive solutions, incorporating advancements such as attack path analysis and more advanced tooling and feature capabilities to help cloud security engineers and developers further streamline their daily workflows. CNAPP solutions such as Panoptica are able to proactively adapt to complex cloud environments and service trends and respond to increasingly sophisticated threats.

Leveraging platforms such as these is essential for robust enterprise cloud security moving forward.