Cross-Cloud Visibility: Essential to Secure Victory in the 21st Century

Prepared by L. Murphy
NetCentrics Technologies and Solutions Team

July 2023

CONTACT US

(703) 714-7345

info@netcentrics.com

www.netcentrics.com

205 Van Buren Street
Suite 420
Herndon, VA 20170

NETCENTRICS

The Fence and the Guardian

In the realm of cybersecurity, complexity is always an issue in regard to articulating a problem. Specialists struggle to explain the fine details of the problem to the lay person, and the lay person doesn't have the background knowledge to accurately understand what the problem is, much less how to solve it.

To that end, imagine a fortress encircled by a fence, representing the very essence of security. This fence stands as the first line of defense, shielding a coveted domain from the relentless advances of malevolent forces outside its borders. These external entities, representing cunning adversaries, persistently probe and test the fence's fortifications, seeking any weakness to exploit. However, the threats do not end there. Imagine that in addition to threats outside the fence, there are threats within taking the form of well-intentioned allies unwittingly contributing to the vulnerability of the domain by leaving valuable ordinance or intelligence plans in the open. Not through malice, but simple carelessness. Like artisans of unintended sabotage, friendly actors within the enclave unknowingly carve hidden passages into the very structure they seek to protect.

But a fence is useless without someone to patrol it. In this nuanced tapestry, the vigilance of the a chosen cybersecurity tool becomes paramount as the embodiment of diligent security guards. They *must* be able to see and identify threats anywhere they might occur, or else the fence serves no purpose. The tool must have as much visibility as possible to effectively patrol the inner landscape, scrutinizing each nook and cranny for signs of compromise either from bad actors or careless friendlies. The tool must operate unobtrusively, with an ever-watchful eye for any anomaly that might undermine the fortress's defenses. This is the intricate dance between external threats and internal missteps, highlighting the indispensable role of a proactive cybersecurity tool to maintain the integrity of any digital environment.

Trading Convenience for Compromise

To complicate matters, imagine that this fence is not just a simple rail and wire, but a state-of-the-art smart fence that requires specialized knowledge to operate as well as repair. Now imagine your fortress has three or more of these fences, all of different make and model, and they must operate together in harmony to ensure the integrity of your fortress. Do you believe that just any tool can not only effectively monitor the fences themselves, but also the threats probing the outside of the fence, the admin troop who left the keys to the nuclear case on their desk, and address these both of those threats in a timely manner?

Now we can see the problem. A tool is needed to give organizations this critical visibility because as the cyber terrain becomes more complex, their potential vulnerabilities also multiply.

But this reality isn't stopping organizations from sprinting headlong into multi-cloud environments. More than half of all workloads are now hosted on public clouds, which is consistent across global regions. The trend toward multi-cloud environments is driven by the desire for increased flexibility, scalability, resilience, security, regulatory compliance, cost optimization, and provider diversity, and this trend is only increasing. With 77% of organizations adding new or updated code by the week, organizations are recognizing the benefits of leveraging multiple cloud providers to build robust, adaptable, and secure infrastructures that align with their specific needs and objectives. However, they are not fully realizing all the threats this choice brings.

Mutiplying Vulnerabilities

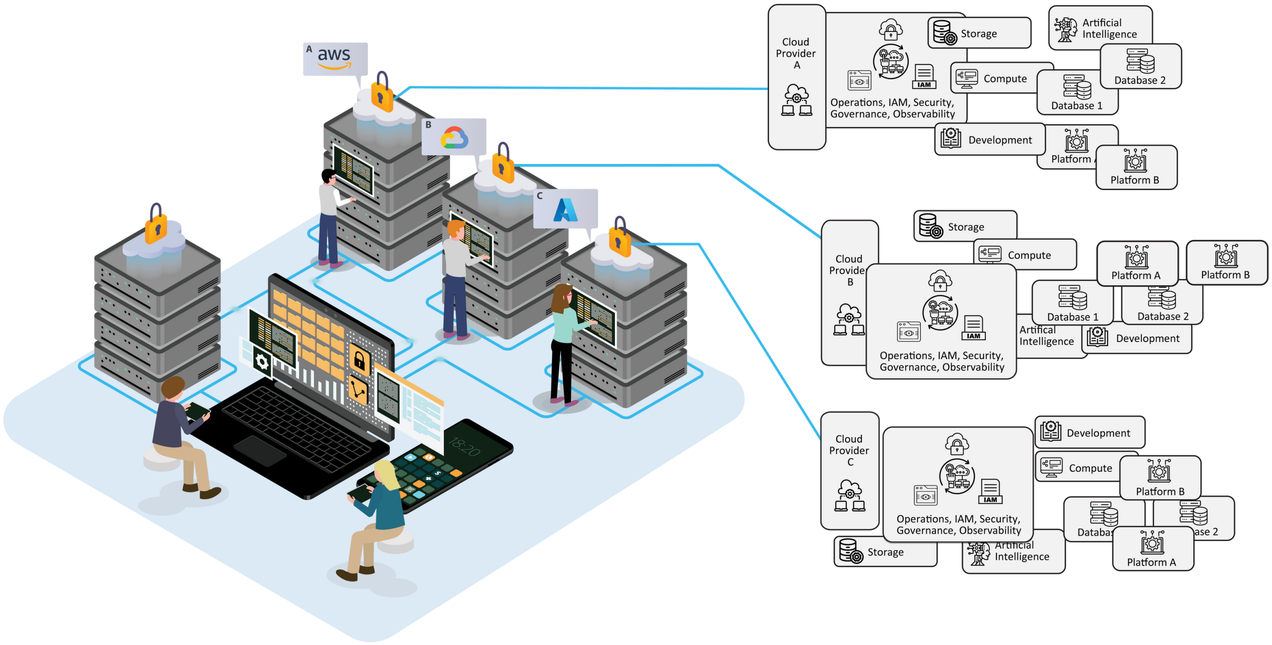
Many organizations believe that multi-cloud environments provide an additional layer of security. This is not true. Spreading assets across different Cloud Service Providers (CSPs) increases the risk of failure for organizations due to heightened complexity and a larger attack surface inherent in multi-cloud architectures.

New Tools for a New Battleground

Legacy tools can still prove highly effective in on-premise environments against advanced persistent threats (APTs) and new tactics, techniques, and procedures (TTPs) specifically designed for these settings. Their reliability in such scenarios stems from their historical development to counter prevalent threats in traditional on-premise setups.

However, legacy tools often operate in isolation and lack the ability to integrate and share data with other security solutions. This lack of integration limits visibility across the entire security infrastructure, making it difficult to correlate and analyze data from different sources. As a result, security teams may miss important indicators of compromise or fail to detect coordinated attacks that span multiple systems. Their limitations arise when transitioning to cloud environments, where everything is code-based and legacy tools lack crucial visibility. In the cloud, they become incapable of gaining visibility into network flows, or any activities, authorized or unauthorized. They are effectively blind to threats outside the particular terrain in which they are operating.

Remember: a security team patrolling a fence is ineffective if they discover a hole hours after it has been made.



To this end, a tool is needed that gives us full visibility into a multi-cloud environment to detect threats across boundaries.

Further Complications

One of the common misconceptions among organizations, as they move toward cloud environments, is that they no longer have to be as concerned with their security as before. They believe that the provider will do the heavy lifting in that area through the Shared Security model. This is not true.

Furthermore, organizations in the federal space have to be concerned with whether their chosen solutions meet stringent requirements, representing yet another wrinkle in an increasingly complicated security mandate.

The adoption of cloud technology continues to surge, with 39% of respondents indicating that more than half of their workloads have migrated to the cloud. 58% have plans to complete this transition by 2023. A forecast by Gartner suggests that by 2025, an astonishing 95% of new digital workloads will find their home on cloud-native platforms.

Notably, the Department of Defense (DoD) is taking significant strides in this direction with the implementation of the Joint Warfighting Cloud Capability (JWCC), a foundational element for enabling the Joint All Domain Command & Control (JADC2) framework. Concurrently, the Air Force and the Army are actively developing and deploying their specific components of JADC2: the Air Battle Management System (AMBS) and the Tactical Intelligence Targeting Access Node, respectively. Additional cloud initiatives in the pipeline include the Army's multi-vendor Enterprise Application Migration and Modernization deal (EAMM) as well as the Department of the Air Force's comprehensive modernization plan for Cloud One, known as Cloud One Next (C1N). These collective efforts underscore the evolving landscape of cloud integration across defense sectors.

Compliance Requirements

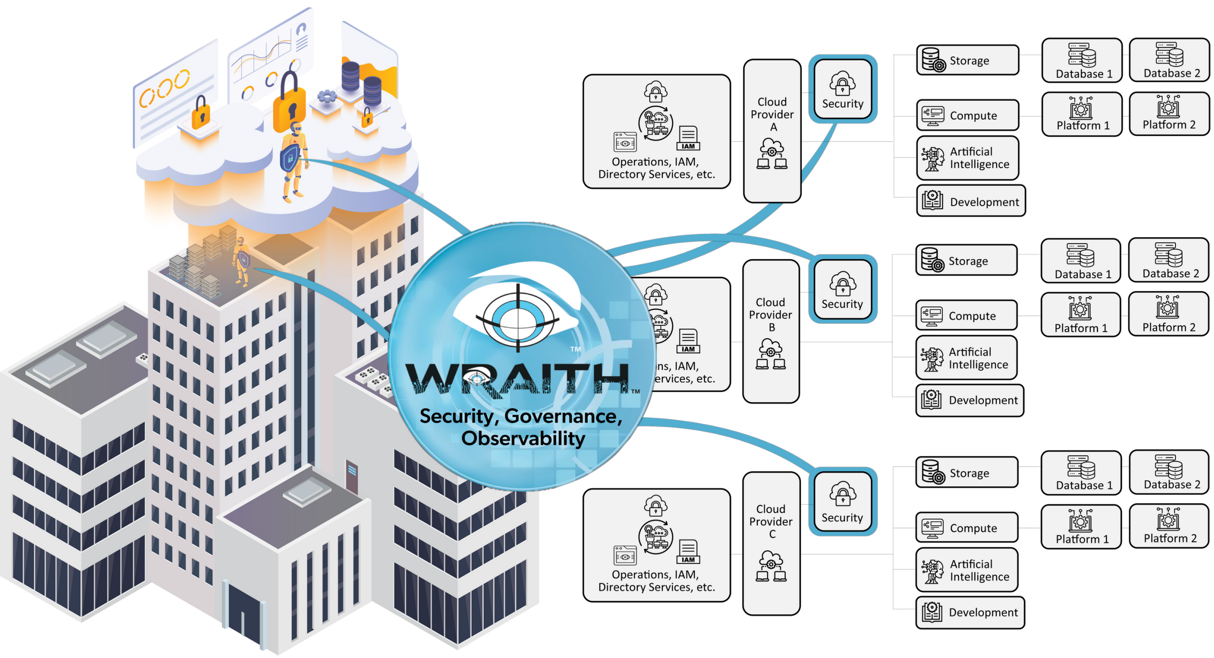
As many industries and sectors have specific compliance and regulatory requirements for data protection and privacy, moving to multi-cloud environments necessitates ensuring compliance with these regulations. Organizations must navigate the complexities of maintaining compliance while leveraging cloud services effectively, which makes the need for a tool that was designed with these regulations in mind all the more glaring.

The Decisive Element: Visibility

Visibility into the multi-cloud environment is critical, as a fence is useless on its own. If a security force patrolling the fence doesn't know when a threat is occurring or where, they are ineffective. Additionally, if they can't respond in a timely manner to threats, and their intelligence is stale by the time it reaches them, they are also ineffective.

Wraith provides that critical element: **visibility**.

It is a comprehensive solution that empowers organizations to safeguard their data, systems, and resources through continuous monitoring, evaluation, and management of cyber vulnerabilities across various clouds and on-premise terrains.



With its proactive approach, *Wraith* enables organizations to take timely action to mitigate risks and prevent potential breaches by providing actionable, easy-to-understand information to security teams so they can respond to threats across cloud environments quickly and efficiently.

The Name of the Game

Cross-cloud threat hunting has emerged as a vital strategy to win the conflicts of the 21st century, especially when facing near-peer adversaries. As technology advances into multi-cloud environments as the standard, adversaries' attack tactics and techniques are becoming increasingly sophisticated in turn, as they employ multifaceted attack vectors across multiple clouds. At present, most organizations are not adequately prepared to act. *Wraith* is a potential tool that enables them to act.

By utilizing cross-cloud threat hunting, cybersecurity professionals can effectively detect and mitigate threats across these diverse environments. This approach allows for a comprehensive view of the entire attack surface, enhancing the chances of early threat detection and containment.

Cross-cloud threat hunting needs full visibility to be effective. Near-peer adversaries possess vast resources and capabilities, making it essential to combine and analyze data from multiple terrains to identify patterns and uncover sophisticated attack campaigns. The ability to connect the dots and gain insights into the adversary's tactics and techniques is crucial for staying ahead in the cyber warfare landscape.

Collaboration is Key

The interconnectedness of various cloud environments means that an attack or breach in one cloud platform can potentially impact others. Cross-cloud threat hunting allows for swift response and containment, reducing the risk of lateral movement and the spread of attacks across multiple clouds. It requires security teams to collaborate and share threat intelligence seamlessly, leading to a more coordinated and effective defense against near-peer adversaries.

Proactive, Not Reactive

Cross-cloud threat hunting facilitates proactive and continuous monitoring of cloud environments. But this won't be as effective without maximized visibility. With a tool like *Wraith*, security teams can employ advanced analytics to continuously monitor and hunt for threats across multiple cloud environments and detect changes to the environment, bolstering situational awareness and enhancing the ability to respond swiftly to emerging threats which is the key to victory in our era.