



NETCENTRICS
SECURE OUR NATION

Securing the Multi-Cloud:

The Imperative of Unified Security Solutions



Table of Contents:

Introduction	3
Cloud and Multi-Cloud Adoption Trends	4
The Multiplying Challenges of Cloud Security	5
Prevalent Types of Cloud-Based Cyber Attacks	5
Trending: Cloud as a Vector for Disruptive Attacks	6
Key Cyberattack Trends to Watch in 2025	7
Beyond IT: Intensifying Threats to OT and Industrial Infrastructure	7
Cloud Security Trends: 2025 and Beyond	8
Comprehensive Visibility: Crucially Important But Difficult to Accomplish	9
Strategies to Improve Security in Multi-Cloud Environments	10
Cross-Cloud Threat Hunting: Visibility is Imperative	12
How Wraith Secures Multi-Cloud Environments	13



Introduction

As organizations increasingly migrate to cloud environments, the landscape of cybersecurity is undergoing a profound transformation. As cloud adoption continues to accelerate, it is imperative for security leaders to stay abreast of evolving threats and leverage emerging technologies to safeguard their digital environments. This white paper aims to provide Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and Security Operations Center (SOC) and cloud security professionals with a comprehensive overview of the current challenges, prevalent threats, actionable strategies and best practices to enhance cloud security posture in 2025 and beyond.

Cloud and Multi-Cloud Adoption Trends

Migrating to the cloud allows organizations to reduce the amount of hardware and people needed to run their enterprise.

94% of enterprises are using cloud services in 2025,

with 90% of large enterprises using multi-cloud infrastructure. 60% of the world's corporate data is now stored in the cloud. Cloud infrastructure spending is expected to grow to \$1.35 trillion by 2027, while the global SaaS market is projected to reach \$900 billion by 2030.



AI as a Driver of Cloud Migration

Enterprises have recognized that deploying AI applications requires renewed emphasis on cloud migration. To use a metaphor, if data is the fuel for AI, then the cloud is the freeway. Large-scale investment in both cloud and AI infrastructure remains a defining theme of the market in 2025. Meanwhile, AI-driven migration tools have become widespread, simplifying cloud migration processes.



The Multiplying Challenges of Cloud Security

The rapid adoption of cloud services has introduced an additional layer of security challenges. One of the foremost issues is the complexity of managing security across multi-cloud environments. Each cloud platform comes with its own set of tools, configurations, and security paradigms, making it difficult to enforce uniform security policies. Additionally, the accelerated pace of cloud adoption often leads to misconfigurations, which remain a primary vector for breaches. Today's cybercriminals have adopted AI tools that can reverse-engineer binary code to find vulnerabilities at a much faster rate than humans. The integration of generative AI and serverless computing further complicates the security landscape, requiring robust, real-time threat detection and response mechanisms.



Prevalent Types of Cloud-Based Cyber Attacks

Cloud environments are increasingly targeted by sophisticated cyberattacks. Ransomware and multifaceted extortion remain among the most disruptive forms of cybercrime, affecting various sectors globally. Distributed Denial of Service (DDoS) attacks continue to be a significant threat, leveraging botnets to overwhelm cloud infrastructure. Additionally, the rise of AI-driven attacks, including sophisticated phishing and social engineering tactics, poses a growing risk. These attacks exploit vulnerabilities in cloud configurations and identity management systems, leading to data breaches and service disruptions.



Trending: Cloud as a Vector for Disruptive Attacks



1.AWS Misconfiguration Attack:

In December 2024, AWS business customers experienced a significant cyberattack that exposed their sensitive data. By conducting widescale scanning of misconfigured customer sites, the attackers were able to steal login credentials, API keys, and proprietary source code. This breach affected millions of websites and resulted in the stolen data being stored in an unprotected AWS S3 bucket. The attackers, linked to the Nemesis and ShinyHunters hacking groups, sold the stolen data on a dedicated Telegram channel, earning hundreds of euros per breach. This incident highlighted the critical importance of secure cloud infrastructure management in the customer portion of the shared responsibility model between AWS and its client base. It also underscored the need to incorporate defensive AI tools that can detect signature-based and behavioral-based anomalies.



2.Snowflake data breach:

In a 2024 incident, attackers exploited stolen credentials to access customer environments hosted on Snowflake's cloud data platform. Using credential stuffing and brute-force attacks, the bad actors capitalized on weak or reused passwords and lack of multi-factor authentication (MFA) on customer accounts. Several Snowflake customers, including major financial and retail firms, reported data theft. The breach highlighted the shared responsibility model in cloud security, where customer-side misconfigurations can lead to major incidents.



3.Commvault Cloud Threat Activity:

In May 2025, CISA issued an advisory that data backup giant Commvault has been monitoring cyber threat activity targeting applications hosted in its Microsoft Azure cloud environment. CISA believes the threat activity may be part of a larger campaign targeting various software-as-a-service (SaaS) companies' cloud apps with default configurations and elevated permissions that lead to attackers stealing secrets. Thus, Commvault likely isn't alone in having its Azure clouds raided because of poor configuration. Commvault said the breach affected "all supported versions" of its software, suggesting the hackers' use of zero-days to get access to the data they want. The incident is thought to be linked to Salt Typhoon, the Chinese-backed hacking group targeting tech and telco companies and the U.S. Treasury.

Key cyberattack trends to watch in 2025

- The increasing speed of attacks: Attackers leverage AI and advanced tactics to reach data exfiltration within an hour, leaving minimal time to respond.
- Evolving attack techniques: 70% of incidents now span three or more attack surfaces, emphasizing the need for holistic security across endpoints, networks, cloud environments, and human factors.
- Key emerging threat trends: Disruptive extortion, supply chain vulnerabilities, insider threats and AI-assisted attacks are on the rise, impacting organizations across industries.

Cyberthreats are becoming more sophisticated and rapid.

Staying ahead of these challenges requires prioritizing rapid detection, swift response and robust security strategies.



Beyond IT: Intensifying Threats to OT and Industrial Infrastructure

Cyberattacks on industrial organizations surged by 87% in 2024, with a significant increase in threats to operational technology (OT) and industrial control systems (ICS), largely driven by geopolitical tensions and a rise in ransomware groups. These attacks are fueled by both state actors, such as the Chinese government-linked Volt Typhoon, and non-state actors who are increasingly targeting critical infrastructure due to its potential for disruption. The troubling trend of collaboration between nation-states and cybercriminal groups continues, leading to a proliferation of knowledge and capabilities that could significantly increase the frequency and severity of attacks on critical infrastructure.

Cybersecurity researchers report that cybercriminals increasingly targeted business operations in 2024, with 86% of major incidents causing disruptions like downtime and financial losses, marking a "third wave of extortion attacks." While encryption remains the most common tactic, seen in 92% of attacks, criminals are adapting by using operational disruptions to gain leverage and increase impact. The median extortion demand rose nearly 80% to \$1.25 million, highlighting the critical need for organizations to anticipate and defend against such evolving threats.



Cloud Security Trends: 2025 and Beyond

Looking ahead, several key trends are shaping the future of cloud security.

- The adoption of zero-trust architecture is becoming a cornerstone of modern cloud environments, emphasizing strict identity verification and minimizing implicit trust.
- AI and machine learning are set to dominate threat detection and response, enabling faster identification of anomalies and reducing false positives.
- Secure Access Service Edge (SASE) and Cloud-Native Application Protection Platforms (CNAPP) are expanding, offering comprehensive security solutions tailored for complex, multi-cloud environments.
- The democratization of cyber capabilities is lowering barriers to entry for less-skilled threat actors, necessitating advanced security measures to protect cloud assets.



Comprehensive Visibility: Crucially Important but Difficult to Accomplish

Comprehensive visibility across multi-cloud environments is crucial for several reasons.

1. It enhances security by allowing organizations to detect and respond to threats more effectively, ensuring that no vulnerabilities are overlooked.
2. It improves operational efficiency by providing a unified view of resources, which helps in optimizing performance and reducing costs.
3. Comprehensive visibility supports compliance with regulatory requirements by enabling consistent monitoring and reporting across different cloud platforms.
4. It facilitates better decision-making by offering insights into usage patterns and trends, allowing businesses to strategically plan and allocate resources.

Overall, having a clear and comprehensive view across multi-cloud environments is essential for maintaining control, security, and efficiency in today's complex IT landscape.

Achieving comprehensive visibility in multi-cloud environments presents several challenges. One major issue is increased complexity; managing multiple cloud platforms requires additional expertise, processes, and tools to unify diverse systems. Security risks are also heightened, as ensuring consistent security practices across different providers can be difficult, potentially leaving vulnerabilities. Interoperability issues can arise, causing bottlenecks and data silos if seamless workload mobility isn't planned properly. Additionally, data transfer costs between cloud providers can be significant, especially with frequent migrations. Finally, choosing the right visibility tools is crucial, as the wrong tool can burden the environment with high resource requirements and may not provide the necessary insights. Addressing these challenges is essential for maintaining control and efficiency in multi-cloud operations.



Strategies to Improve Security in Multi-Cloud Environments:

Enhancing security in multi-cloud environments involves several key strategies:



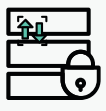
1. Implement Strong Identity and Access Management (IAM):

Use Single Sign-On (SSO) and Multi-Factor Authentication (MFA) to ensure secure access. Regularly review and update IAM policies for each cloud provider.



2. Secure Cloud Configurations:

Utilize Infrastructure as Code (IaC) and Cloud Security Posture Management (CSPM) tools to detect and correct configuration drifts.



3. Encrypt Data:

Ensure data is encrypted both at rest and in transit. Use centralized key management tools to maintain control over encryption keys.



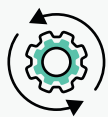
4. Monitor and Respond to Security Events:

Employ cloud-native monitoring tools and set up automated incident response policies. Conduct regular security audits to identify and mitigate vulnerabilities.



5. Maintain Visibility and Control:

Use unified management platforms to monitor all cloud environments. Configure alerts for security issues and ensure consistent policy enforcement.



6. Leverage Automation:

Automate repetitive security tasks to reduce human error and ensure consistency across multi-cloud setups.



7. Understand the Shared Responsibility Model:

Clearly define and regularly review the security responsibilities of both your organization and your cloud providers.



8. Tailor Security Policies:

Develop service-specific security policies and apply consistent controls across all cloud services.



9. Ensure Compliance:

Create a unified compliance framework and use tools that provide real-time visibility into compliance status across multiple clouds.



10. Develop an Incident Response Plan:

Establish procedures for responding to security incidents, including regular training and drills for your response teams.

By following these best practices, organizations can significantly enhance their security posture in multi-cloud environments, reducing the risk of breaches and ensuring robust protection of their data and resources.

Cross-Cloud Threat Hunting: **Visibility is Imperative**

Cross-cloud threat hunting has emerged as a vital strategy to secure organizations in today's threat landscape filled with sophisticated adversaries. As multi-cloud environments become standard, bad actors' attack tactics and techniques evolve, employing a gamut of vectors across multiple clouds. At present,

most organizations are not adequately prepared to defend themselves.

Cross-cloud threat hunting requires full visibility to be effective. Malicious actors 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 early threat detection and containment.



How Wraith Secures Multi-Cloud Environments



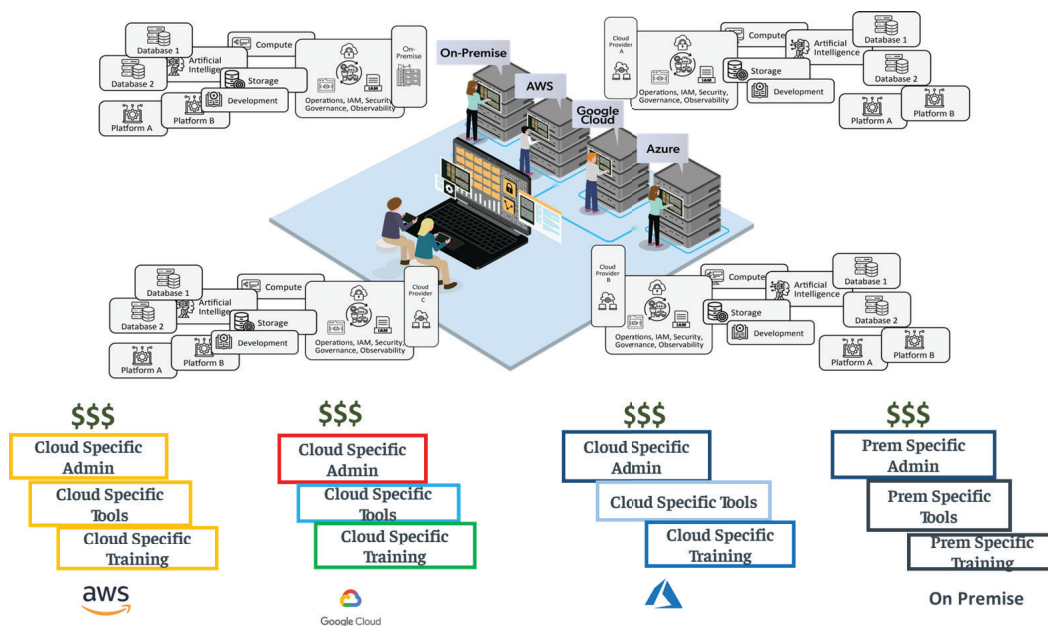
Wraith is an advanced cloud security solution that safeguards organizations' data, systems, and resources through continuous threat hunting, evaluation, and management of cyber vulnerabilities across multi-cloud, hybrid, and on-premise terrains.

These capabilities are enhanced by AI-enabled anomaly detection, making Wraith an essential tool for neutralizing hidden threats – whether it's unauthorized access, data exfiltration, privilege escalation, or unusual behavior patterns – to secure and defend IT environments.

By normalizing and centralizing security telemetry in one central dashboard, Wraith breaks down organizational and operational silos, leading to substantial savings through both workforce and tool rationalization.

By providing comprehensive, unified visibility across the entire attack surface, Wraith enables security teams to take timely action to mitigate risks and prevent potential breaches. It provides actionable, easy-to-understand information and collaboration tools to security teams so they can respond to threats across cloud environments quickly and efficiently.

Wraith is cloud provider-agnostic and can be configured to ingest data from any cloud or on-premise architecture. This eliminates the need to rip and replace existing tools and applications and spend resources to train and equip security teams differently for each cloud environment.




The interconnectedness of various cloud environments means that an attack or breach in one cloud platform can potentially impact others. Cross-cloud threat hunting with Wraith lets security teams quickly correlate alerts about changes and anomalous activities across multiple environments, allowing for swift response and containment. This reduces the risk of lateral movement and the spread of attacks across multiple clouds. With Wraith, security teams seamlessly collaborate and share threat intelligence, leading to a more coordinated and effective defense against the most dangerous attacks.




To learn more about Wraith, visit
www.netcentrics.com/wraith or
Request a 30-min live demo [HERE](#).



NETCENTRICS
SECURE OUR NATION

 (703) 714-7345

 205 Van Buren St. Suite 420
Herndon, VA 20170

 www.netcentrics.com

 bd@netcentrics.com

