PULSEMETER

Techstrong Research

Risk and Threat Management Strategies

SPONSORED BY

tenable

IN THE CURRENT DIGITAL ERA, the role of the cybersecurity team has extended beyond traditional boundaries, confronting an environment marked by increasing attack surfaces, escalating complexity and continuously evolving threats. The challenge lies not just in managing the dichotomy of cloud and on-premises infrastructures but also in navigating a comprehensive security landscape characterized by a plethora of security tools, the need to dive deeper into application and API security and applying least-privileged access to better align individuals with appropriate permissions for their roles.

In addition, the rise of microservices, APIs and the interconnectivity of digital services introduces new layers of potential vulnerabilities. Identity management remains a critical focal point. The software supply chain, traditionally underemphasized in security strategies, now presents a significant threat vector, necessitating a more comprehensive approach to security.

A pivotal aspect of this complex security terrain is the management of security vulnerabilities. The importance of an effective vulnerability management program cannot be overstated. Such a program is essential for identifying, evaluating, prioritizing and mitigating vulnerabilities, thereby reducing the window of opportunity for attackers.

In early 2024, Techstrong Research polled our community of security, cloud and DevOps readers and viewers to understand their perspectives on scaling security across cloud and on-premises. This report uncovered

Key Takeaways

1. Consolidate and integrate security data: Simplify security management by reducing the number of disparate data sources and fostering integration for improved control and visibility.

2. Leverage CNAPP for more complex architectures: Security teams may not possess the full depth of knowledge of microservices, service mesh, containers and serverless, but cloud-native application protection platforms (CNAPP) can readily fill this security gap.

3. Increase governance across cloud identities and entitlements: Look to increase controls over access permissions for both human and machine identities as a way to reduce breaches.

4. Focus on Kubernetes and container security: Apply container best practices, including creating secure container base images and utilizing runtime security. Implement Kubernetes best practices by utilizing ingress and egress policies, restricting access to secrets, etc., and utilizing role-based access controls.

5. Embrace automation as a way to scale cloud security: Adopt security automation across the cloud SDLC as a way to enhance threat detection, response and overall efficiency in security processes.

6. Continuous training and upskilling of security teams: Invest in ongoing education and training to ensure security teams are equipped to handle evolving technologies and threats.

many challenges, offering insights into effectively managing the array of security tools and strategies for mitigating the expanding attack surfaces. Our aim is to equip cybersecurity engineers and leaders with the knowledge and tools necessary to fortify their defenses against a diverse array of threats in this intricate and constantly evolving digital landscape.

TECHSTRONG RESEARCH ANALYST VIEW

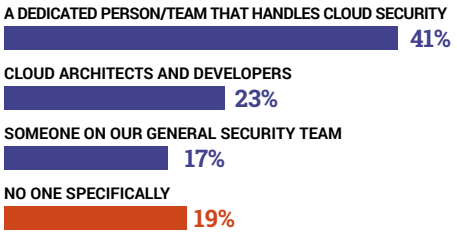
Many security organizations grapple with the complexities of rapidly evolving digital projects, expanding and scaling cloud environments operating in multi-cloud or hybrid cloud models and cloud-native software architectures.

The crux of the challenge lies in risk management across cloud operating models, web applications, APIs, identity, access management and more. These challenges are further magnified by the burgeoning array of security vulnerabilities, with the ever-present threat of zero-day exploits. In addition, the convergence of cloud and on-premises security requires a unified strategy that can adapt to the distinct needs of each environment while maintaining a consistent security policy across all platforms.

Organizations must take a multifaceted approach to risk and security management to tackle these challenges effectively. A comprehensive, integrated view of the security attack surface

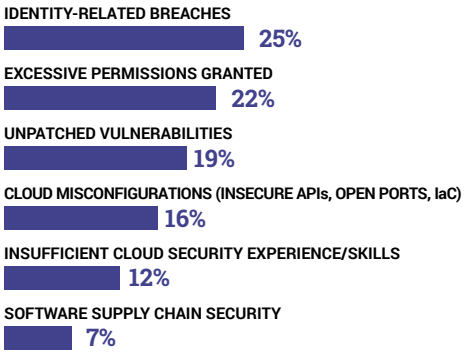
Who in your organization is responsible for cloud security?

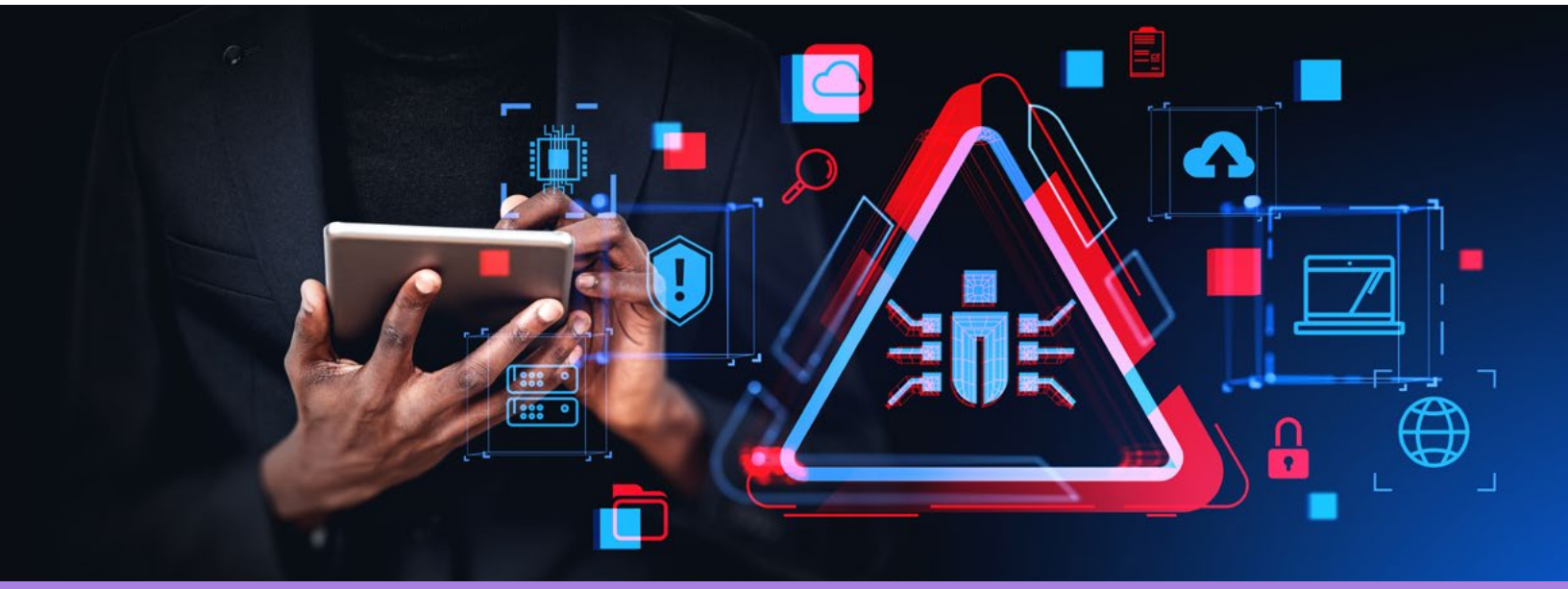
While no common group or role "owns" cloud security, different responsibility models work for each organization.



What are the biggest security threats to your cloud environment?

Identity management, over-provisioning and unpatched vulnerabilities continue to appear at the top of the security threat list.

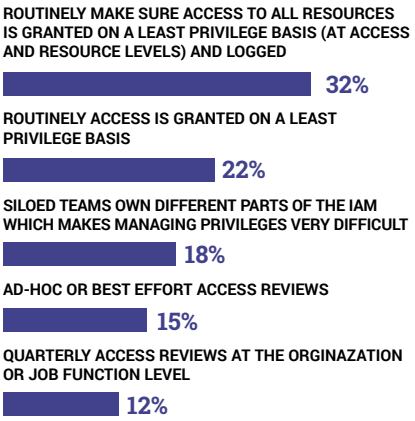




is necessary to recognize, assess and add context to security data to understand the interrelationship between systems, data sources and security management tools. This involves not only the consolidation of security tools but also the continuous training and upskilling of security teams to keep pace with the latest technologies and threats. Moreover, a strong emphasis on proactive vulnerability management and a shift toward automation and AI-driven security solutions can significantly enhance an organization's ability to respond to and mitigate emerging threats.

What best describes the identity and access management of your cloud environment?

Over 50% of respondents dutifully apply the principle of least privilege, but a sizable group still needs to tighten their provisioning processes.



Which is true regarding your company's experience scaling cloud adoption?

Nearly 50% operate in the cloud and are looking to expand, while others are evaluating on-premises solutions or just need help with the complexity.

What cloud concepts/ technologies do you want to learn more about in 2024?

The list of skills to be acquired in 2024 is extensive, leaving organizations with difficult decisions about where to invest in security teams' skills.