Enterprise Strategy Group™

BRIEF

JUNE 2025

AWS Shield Network Security Director Provides Mapping for Contextual Understanding to Mitigate Risk and Speed Response

Melinda Marks, Practice Director, and John Grady, Principal Analyst

Abstract: As organizations increasingly move workloads to the cloud and security responsibility becomes decentralized, the difficulty in maintaining visibility across network resources and configuration hygiene rises. AWS Shield network security director can help organizations understand network security in place and make needed changes to mitigate risk for better security and compliance.

Key Highlights

- 32% of organizations that experienced an attack on their public cloud infrastructure said it was due to an exploit of misconfiguration.
- Understanding network configurations and connections can help security teams mitigate risk and respond faster to threats
- AWS Shield network security director helps security teams effectively manage network security to protect their cloud applications

Dynamic Applications and Related Resources in the Cloud Cause Security Challenges

With organizations under pressure to increase productivity, they are leveraging cloud services and modern development processes to rapidly release their applications in the cloud. While this provides opportunities for more accessibility and business for companies of all sizes and industries, security teams need to ensure they can secure their cloud applications that have complex connections to other applications and resources.

Unfortunately, basic network security hygiene remains a key issue. In fact, Enterprise Strategy Group research shows that 43% of organizations have experienced an attack on their public cloud infrastructure environment in the last 24 months.[1] In many cases, these incidents are the result of unforced errors rather than sophisticated adversaries using advanced tactics. Specifically, 32% experienced exploits of misconfigurations, 26% experienced exploits of open ports, and 23% saw unauthorized access by internal users.

Making efficient and effective use of the tools offered by cloud services providers (CSPs) should be a top priority for any security team. But it is critical that the CSPs enable this usage, prioritizing proactive visibility, insights, and context to help security teams identify the most critical risks and close the associated gaps in their security posture.

Introducing AWS Shield Network Security Director

AWS Shield network security director, now released in public preview, helps customers manage network security to better understand their vulnerabilities to attack and take needed actions to mitigate risk. It helps security teams:

- **Visualize network resources and configuration issues** in one dashboard, showing the network topology of compute and networking connections in their environment.

[1] Source: Enterprise Strategy Group Research Report, *The Evolution of Network Security*, October 2024. All Enterprise Strategy Group research references in this brief are from this report.

- **Improve security posture,** assessing and remediating configuration issues by severity level based on AWS best practices.
- **Quickly respond to critical security issues** with remediation recommendations and step-by-step instructions.
- **Assist developers via Amazon Q** so they can easily analyze and report on their organization's security posture.

Analyst Insight

While the scale, speed, and agility afforded by public cloud infrastructure can significantly improve business outcomes, security can suffer. Getting a clear, real-time understanding of the network topology within a cloud infrastructure provider has historically been a manual process. AWS Shield network security director can help organizations simplify and accelerate obtaining visibility, along with important context around what should be addressed first based on criticality. Leveraging Amazon Q for natural language querying and remediation recommendations can also help non-security team members benefit from this solution.

> "AWS Shield network security director can help organizations simplify and accelerate obtaining visibility, along with important context around what should be addressed first based on criticality."
>
> **- John Grady,** *Principal Analyst, Enterprise Strategy Group*

AWS Shield network security director is a good first step and will meet most customers where they are now. As organizations' comfort level with generative AI and AI-led automation continues to grow, it will be important for AWS to expand the offering to include these capabilities as well. This will help further democratize security and enable non-security personas to benefit.

Conclusion

Too often, organizations overlook the basics when it comes to security. High-profile, sophisticated attacks generate headlines, but simple, avoidable errors are often what lead to problematic incidents. This is understandable, as security teams are stretched thin, identifying critical issues remains difficult, and responsibility for protecting corporate applications is often distributed across multiple teams. AWS Shield network security director is a good example of how CSPs can help their customers take better advantage of the security tools they offer, prioritize what's most important, and better enable a strong security foundation across the organization's cloud footprint.

About Enterprise Strategy Group
Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com