The bridge to possible

The Cisco Cloud Application Security Attack Path Engine

Monitor, prioritize, and dynamically remediate your most critical cloud risks

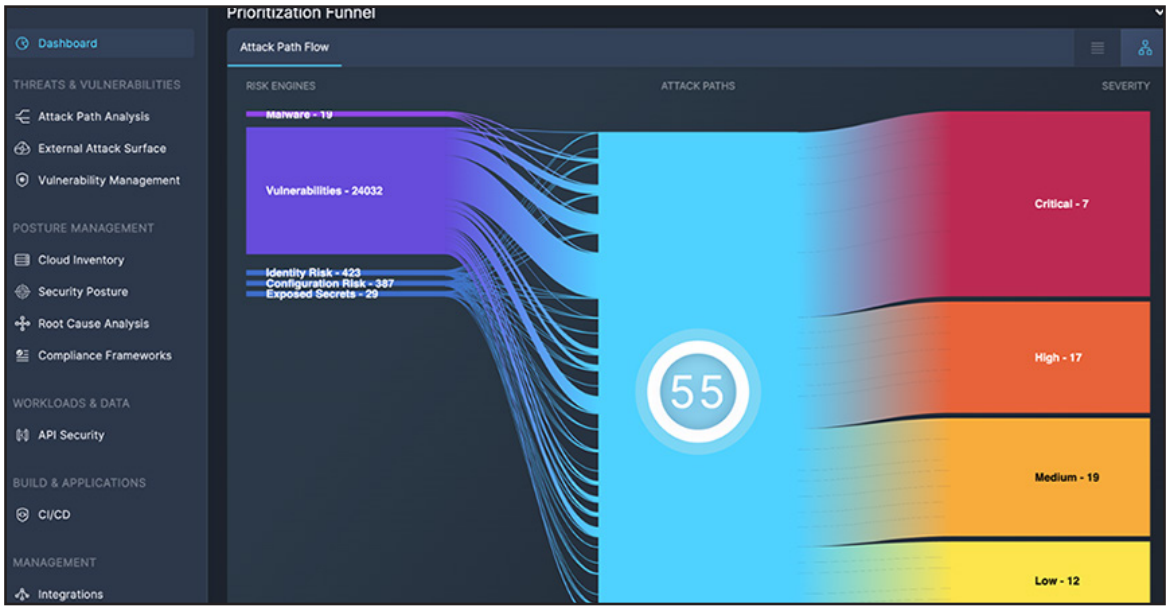

Figure 1. Attack Path Analysis Prioritization Funnel, view risks like vulnerabilities, secrets, and misconfigurations through the lens of attack path to prioritize remediation.

Traditional Cloud Security Posture Management (CSPM) tools identify cloud risks but fail to deliver the context, prioritization, and remediation required to quickly address issues without straining resources or budgets.

Cisco Cloud Application Security is different. It enables organizations to not only meet multicloud compliance but also monitor, prioritize, and remediate a wide range of threats. It provides code to cloud protection from development to runtime, and empowers organizations to safeguard their APIs, serverless functions, containers, and Kubernetes environments. Where Cloud Application Security shines is its advanced attack path analysis capabilities which include the attack path engine. The attack path engine actively analyzes misconfigurations, network exposure, secrets, vulnerabilities, malware, and overly permissive identities to identify exploitable paths that could be used to get into an environment and move laterally. These attack paths are prioritized by severity to clearly show the biggest threats without overwhelming operators in countless alerts. Security teams can focus on the risks that matter most by viewing their environment from an attacker's point of view.

Challenges

Cisco's Attack Path Engine helps you address key cloud security challenges:

- **Lack of context and visibility leads to a reactive security posture.** A lack of context into an organization's cloud environments leads to a reactive security posture, the inability to prioritize security alerts efficiently, and increased efforts in managing assets, complex systems of applications, and data across environments.
- **Alert fatigue**. Security engineers and DevOps teams are overwhelmed with thousands of alerts per day. **More than 31% of IT security professionals ignore incoming alerts**, resulting in critical security vulnerabilities going undetected. Among IT security professionals, 40.4% say that the alerts they receive lack actionable intelligence to investigate, and another 31.9% report that they ignore alerts because so many are false positives.[1]
- **DevOps and Security resources are tight, and teams are short-handed.** The current constellation of security engineers and DevOps teams are juggling a lot. They need to maximize their manpower and their ability to stay one step ahead of market cloud security trends to better secure their code and their environments.

Figure 2. Attack Path Analysis, see how an attacker can exploit risks including secrets and excessive permissions to get into an environment and move laterally.

Core Capabilities

Cisco's Attack Path Engine provides complete code to cloud protection, empowering you to:

- **Uncover the critical risks that matter most and proactively protect your cloud environment** Graph theory technology is at the heart of Cisco Cloud Application Security solution. This technology powers Cisco Cloud Application Security ability to accurately map out the entirety of your cloud stack but also provide the correct prioritization of security findings and connected assets, resources, and identities. Cisco Cloud Application Security scans and prioritizes exploitable gaps in your environment, even prior to deployment, delivering the proactive security posture your organization requires.
- **Determine the root cause of an issue and prioritize accordingly** Improve your team's efficiency and efficacy. With Cisco Cloud Application Security Attack Path Engine, reduce lists of non-critical security findings to instead make the right connections between risks and map the critical attack paths that matter most. Easily identify, prioritize, and dynamically remediate critical risks.
- **Reduce the time required for fixes through dynamic remediation** Dive straight into remediations with ready-made Terraform Infrastructure as Code (IaC). Cisco Cloud Application Security saves your team time and resources by providing your team with out of the box recommendations to help resolve the vulnerabilities discovered in your environment. These recommendations are applicable to discovered attack paths and can be dynamically customized to best suit your organizations' requirements.

For more information on how Cisco Cloud Application Security can help you secure your environment from code to cloud, please visit https://www.cisco.com/go/cloud-application-security.

Sources

[1] https://www.mcafee.com/blogs/enterprise/cloud-security/alert-fatigue-31-9-of-itsecurity-professionals-ignore-alerts/