Elastic Security for Cloud – The Next Step in Securing Cloud and Hybrid Environments

EMA IMPACT BRIEF

elastic

Abstract

Elastic, an American technology company specializing in search-powered solutions and enterprise observability, recently announced the release of its cloud security product. This product will help organizations solve their visibility and observability challenges when working with cloud or hybrid environments.

Background – The Cloud Visibility Challenge

One of the biggest challenges in the shift to cloud and hybrid environments is maintaining visibility. Within three years, public cloud hosting is expected to increase from today's 40% of application workload to 70%. As the amount of processing in the cloud increases, so do the threats of cloud data breaches with the increased cloud attack surface. Organizations can't secure what they can't see, and traditional EDR/XDR platforms don't translate well to cloud containers and applications. The result for hybrid environments is typically two separate platforms: one for on-prem computing and another for cloud computing. Obviously, this isn't ideal, and results in the inability to cross-correlate events between on-prem and cloud, splitting the organization's visibility and observability in two.

Observability becomes even more challenging when organizations have hybrid or multi-cloud environments. Elastic Security for Cloud solves the observability challenge by centralizing multi-cloud and hybrid environments in a unified single pane of glass. This results in reduced workloads and easier tracking of threats across the entire environment, saving organizations staffing costs while improving incident response times. After all, adversaries don't care when their attacks traverse cloud boundaries and organizations can't assume that an attack in one environment won't be leveraged to attack the other.

Key Ramifications

The following are the key ramifications of Elastic's release of their cloud security product:

- Full visibility and observability for multi-cloud and hybrid environments allow full tracing of attacks across an organization's entire environment without the need to switch between SIEM or XDR interfaces.

- Reduced workload and faster response time through a single-pane-of-glass interface for reduced costs, not only in staffing, but also potential costs for response and remediation of incidents.

- Organizations can leverage data beyond security applications, using the data for availability and performance monitoring and improvements. This provides additional value to organizations while eliminating the need to purchase separate tools for performance monitoring.

These features and the corresponding impact to customers make Elastic Security for Cloud an extremely important investment for any organization with a cloud or hybrid environment.

EMA Perspective

You can't secure what you can't see, and lack of comprehensive visibility of the full environment is where many cloud security products fall short. Organizations leveraging multiple products to secure cloud and on-prem environments separately may encounter gaps in visibility, and in the process, gaps in security coverage. Elastic's release of their cloud security product fills the visibility gaps of complex cloud and hybrid environments, providing a comprehensive picture of the true attack surface.

Cybersecurity should be considered an investment, not an expense, and technologies that help reduce staffing costs and improve response time are a worthy investment. As the cybersecurity industry continues to struggle with a lack of experienced workers and a predicted increased demand by 33% over the next 10 years, reducing the workloads of existing staff is more critical than ever. Organizations with cloud or hybrid environments can't afford not to invest in these unified interfaces.

EMA believes that simplified, single-pane-of-glass interfaces for security of cloud and hybrid environments, such as the interface offered by Elastic, are critical to the future of cloud security and an important investment for any organization with a cloud presence.