Guide

Top Capabilities for End-to-End Public Cloud Security

The shift to the public cloud has resulted in applications – and their underlying environments – being exposed to a larger attack surface and an expanding array of vulnerabilities. When combined with breakneck application development speeds, it's becoming increasingly important that application and cloud security is kept in lockstep.

For these reasons, ensuring end-to-end protection of public cloud environments, development platforms and applications is critical. Organizations must ensure consistent, frictionless and automated protection of cloud workloads and applications.

Here are the capabilities organizations must consider when evaluating public cloud security solutions.

Requirements for Comprehensive, "Frictionless" Security Across Hybrid Cloud Environments

Ultimately, complexity is the enemy of security. Every cloud has its own security capabilities, APIs, management and reporting. Relying on these disparate, native tools can result in "security silos" that cause varying levels of protection and inconsistent reporting. This makes it nearly impossible to detect sophisticated threat actors that understand how to evade these tools.

Overcoming these challenges requires a comprehensive security solution that combines several key high-level requirements:

- **Consistency**
  Maintain uniform levels of security across different environments, platforms and clouds
- **Comprehensive**
  Protect every threat surface, both at the application level and the cloud infrastructure level

- **Adaptive**
  Leverage advanced behavioral-based and machine-learning algorithms to manage frequent changes in the application itself or in the underlying environment
- **Frictionless**
  Integrate security into the development cycle, without getting in the way of DevOps

Cloud-Native Application Protection

Cloud applications face unique, cloud-native attack vectors. Comprehensive, 360-degree protection is critical to safeguard every attack surface of cloud applications and requires the following capabilities and integrations:

- **Multi-Layered Protection**
  Multi-layered protection for application infrastructure and workloads hosted in public cloud environments to prevent accidental exposure, misconfigurations and malicious activity in the cloud environment
- **Integration with Application Development**
  Tight integration with CI/CD lifecycle and DevOps orchestration platforms to ensure application security from development through launch and update
- **Bot Management**
  The ability to distinguish malicious bots from good bots
- **API Protection**
  API protection against exposure and abuse that leverages automated API discovery and full parsing of JSON and XML objects

Cloud-Native Capabilities and Tools

Multi-layered protection for computing infrastructure and workloads hosted in public cloud environments is critical. Any cloud-native application protection platform should provide the following tools and capabilities to safeguard against every attack surface.

- **Cloud Security Posture Management**
  CSPM that provides one-click compliance reporting and detection of cloud misconfigurations for protection, compliance and governance of the overall cloud account
- **Cloud Infrastructure Entitlement Management**
  CIEM with detection and remediation of excessive permissions to prevent them from being exploited by malicious actors
- **Cloud Threat Detection and Prevention**
  CTDR for detection of potentially suspicious activity in your cloud and an AI-based correlation engine to show the step-by-step progression of attacks
- **Advanced Attack Detection and Response**
  Advanced threat detection capabilities to automatically identify suspicious activity in your cloud environment, as well as correlate individual events into streamlined attack storylines and automatically block malicious activity before it results in data breach

- **Cross-Cloud Reporting and Visibility**
  A 360-degree view of everything that is happening in your public cloud account from a single dashboard
- **Agentless**
  Cross-cloud solutions shouldn't require installation of any software or hardware in the customer's environment, which provides easy and seamless deployment of the solution with no additional overhead
- **Detailed Compliance Reporting**
  Out-of-the-box, built-in and one-click compliance reporting across a variety of common industry standards, with detailed, visual reports on exactly where you are successful and where you are not
- **Misconfiguration Detection and Enforcement**
  Protection against a wide array of cloud security misconfigurations such as public exposure
  of assets, authentication misconfigurations, password policy, logging, networking, monitoring and encryption
- **Smart Permission Hardening**
  Unique permission hardening, which analyzes the gaps between defined and used permissions and eliminates excessive permissions without impacting business operations