Evaluating Cloud Security Solutions
Evaluating Cloud Security Solutions

Executive Summary

Enterprises are rapidly adopting cloud services that range from applications to infrastructure. Applications such as Salesforce, Microsoft Office 365, and Box enhance collaboration and improve productivity. Cloud-based infrastructure such as Amazon Web Services (AWS) enables agility. Integrations between cloud services using APIs drive efficiency. However, the cloud presents challenges in the areas of threat visibility and compliance.

Information Technology (IT) teams are finding that the cloud creates gaps in their security architectures. On-premise and endpoint security solutions do not address the security of critical corporate data in the cloud. Integrations between cloud services and Security Information and Event Management (SIEM) technologies are limited and require manual data collection and analysis. The volume of cloud usage and the relentless efforts by hackers outpace the efforts by IT to secure the cloud environment. Defensive measures to secure the cloud are not enough; hackers are getting past these defenses, generally by using compromised credentials.

If you have similar challenges, you can use this Buyer’s Guide to identify capabilities that you need to address the security of your organization’s cloud services. Specifically, this guide describes key issues that you need to consider as you select a solution:

- Security compliance
- Threat visibility
- Incident response
- Ease of use

This guide also describes how to prepare for investment in a new solution, and provides a comparison checklist to document your findings.
Security Compliance

The recent spate of high-profile breaches has prompted cloud service providers to build security configurations into their platforms. These configurations allow enterprises to tune the cloud service to meet their compliance needs. However, manual monitoring and auditing of these configurations is labor-intensive and error-prone.

Consider these issues when assessing a cloud security provider:

- Does the solution let you define all security configurations for a specific cloud service at a glance?
  
  Example: Does the solution let you define hundreds of security configurations across AWS Elastic Cloud Compute (EC2), Simple Storage Service (S3), and Identity and Access Management (IAM) with a single click?

- For the hundreds of security configurations in each cloud service, does the solution provide guidance for each configuration?

- After you define your configuration for each cloud service, does the solution monitor these configurations in real time?

- In the event that a configuration is directly changed in the cloud service, does the solution reset the configuration to the defined preference?

Threat Visibility

Enterprises must protect their data from hackers and insiders. Your provider must be able to detect breaches and predict risks with precision.

Here are some questions to ask during the evaluation process:

- Does the solution let you define threat scenarios that are custom to your environment?
  
  Example: Can the solution detect when an employee opens a non-sanctioned port on your AWS VPC deployment?
Does the solution incorporate real-time intelligence feeds from proprietary and commercial sources?

Can the solution detect malicious activity if a hacker infiltrates the cloud service by using compromised credentials?

Can the solution detect risky activity performed accidentally or intentionally by an insider?
Example: Can the solution detect if an employee adds new members to a privileged AWS administrator group?

Does the solution assess risk based on anomalous user and application behavior?
Example: Does the solution correlate failed logins to Salesforce with an unusual number of file downloads in Box by the same user?

Does the solution establish user- and application-specific behavioral baselines?
Example: Does the solution create a behavioral fingerprint for an employee’s Salesforce activity and another one for their AWS activity?

Does the behavioral analysis address false positives, that is, can it determine legitimate deviations from normal behavior?
Example: Will the solution flag activities from a San Francisco-based employee who travels to New York for business once a year?

Does the solution apply machine learning to assess risk events and provide an actionable threat summary?
Example: Can the solution correlate seemingly disparate events such as failed login attempts from suspicious locations with unusual file downloads during non-business hours and identify potential account hijacking?

Does the solution provide insight into cloud activities across all cloud services?
Example: Does the solution provide reports that highlight users with the most downloads or how frequently AWS keys are rotated?
Incident Response

A good security solution lets you track all identified threats and perform incident response, thus closing the loop.

Your provider needs to support these capabilities:

- Does the solution automatically generate incident tickets to ensure that all risk events are tracked?
- Does the solution provide built-in capabilities to manually remediate incidents?
- Does the solution provide built-in capabilities to automatically remediate incidents?
  
  Example: In the event of an AWS account hijacking, can the solution disable the user’s AWS account?
- Does the solution integrate with other enterprise applications or change management processes?
  
  Example: When login failures are detected from suspicious IP addresses, can the solution trigger the network firewall to blacklist them?

Ease of Use

For a security solution to be viable, it must be easy to deploy and maintain. Installation of hardware, software, and agents can impede the user experience and are tedious to maintain. Inline solutions such as proxies impede the user experience and can cause business disruption as a result of down time. At a minimum, you should ask:

- Does the solution require the deployment of any hardware, software or agents?
- Is the solution inline to my Internet traffic?
Readiness Planning

After you select a solution, you will need stakeholder buy-in and management approval. To do this, you will need the following information and a clear understanding of the proposed solution’s value.

- **The buying process**
  - The stakeholders in your organization who are involved in the decision-making process
  - The approval and procurement processes
  - Budget availability

- **Understanding of the current solution**
  - All components of existing cloud security solutions
  - Network topology
  - The staff required to support this solution

- **Benefits of the proposed solution**
  - Automation of the entire security lifecycle from threat detection through remediation
  - Threat visibility in a single pane of glass across your entire cloud footprint—applications to infrastructure
  - Compliance through monitoring and enforcement of security configurations
  - Incident response with automated forensics, incident tracking, and remediation
  - Ease of deployment and maintenance
  - No impact to user browsing experience

- **Business case**
  - Return on investment based on the benefits of the proposed solution
  - Implementation plan
  - Impact analysis to stakeholders
  - Customer references
## Appendix: Cloud Security Solution Checklist

<table>
<thead>
<tr>
<th>SOLUTION CRITERIA</th>
<th>Current Solution</th>
<th>Option 1</th>
<th>Option 2</th>
<th>Palerra LORIC™</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SECURITY COMPLIANCE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the solution let you define all security configurations for a specific cloud service at a glance?</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>For the hundreds of security configurations in each cloud service, does the solution provide guidance for each configuration?</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>After you define your configuration for each cloud service, does the solution monitor these configurations in real time?</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>In the event that a configuration is directly changed in the cloud service, does the solution reset the configuration to the defined preference?</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>THREAT VISIBILITY</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the solution let you define threat scenarios that are custom to your environment?</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Does the solution incorporate real-time intelligence feeds from proprietary and commercial sources?</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Can the solution detect malicious activity if a hacker infiltrates the cloud service by using compromised credentials?</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Does the solution assess risk based on anomalous user and application behavior?</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Does the solution establish user- and application-specific behavioral baselines?</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Does the behavioral analysis address false positives, that is, can it determine legitimate deviations from normal behavior?</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Does the solution apply machine learning to assess risk events and provide an actionable threat summary?</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Does the solution provide insight into cloud activities across all cloud services?</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>In addition to detecting existing threats, does the solution predict risks to your assets?</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>INCIDENT RESPONSE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the solution generate incident tickets to ensure that all risk events are tracked?</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Does the solution provide built-in capabilities to manually remediate incidents?</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Does the solution provide built-in capabilities to automatically remediate incidents?</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Does the solution integrate with other enterprise applications or change management processes?</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>EASE OF USE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the solution require the deployment of any hardware, software or agents?</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Is the solution inline to my Internet traffic?</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>