ARCTIC WOLF

BRIEF

Checklist for Cloud Monitoring

Small-to-midsized enterprises (SMEs) are increasingly reliant on cloud computing services. Many organizations have already shifted data from on-premises architectures to cloud alternatives, such as:

- Software-as-service (e.g., Microsoft Office 365, Salesforce, Google Apps)
- Platform-as-a-service (various solutions from Cloud Foundry, Oracle, IBM, et al.)
- Infrastructure-as-a-service (Amazon Web Services, Microsoft Azure, etc.)

Moving assets into the cloud, however, does not automatically guarantee their protection. Even in cloud data centers, the basic threats to data, infrastructure, and sensitive information remain: ransomware, malware, distributed denial-of-service (DDoS) attacks, and cryptocurrency-mining botnets can all compromise cloud-based systems.

The following checklist outlines features of a security operations center (SOC) that provide optimal protection for your cloud applications and infrastructures:

Hybrid Cloud Monitoring

Cloud security is often tackled through a DIY methodology that attempts to integrate native tooling, such as AWS CloudTrail and CloudWatch, with preexisting security tools and workflows. Alternatively, to the other extreme, some SMEs go all-in on cloud-specific security. Either approach is too limited to provide adequate coverage for today's complex hybrid environments.

A SOC securely aggregates and transports data from on-premises and virtual cloud sensors across different platforms. That lets you ensure full visibility of your vulnerable data and systems.

Predefined Best-Practice Security Alerts

Effective cloud security should feature specific alerts for common services like AWS and Office 365. In AWS, such predefined rules should meet the Center for Internet Security's recommended criteria for protecting IaaS instances. In Office 365, such rules should focus on granular monitoring of activities like authentication, mail and mobile, along with oversight of major components, including Active Directory, Exchange and SharePoint.

These rules should monitor security-relevant events, such as:

- Major resource deletions
- Creation of new user security groups
- Upload or deletion of certificates
- Brute-force login attempts
- Sign-ins from blacklisted IPs
- Termination of particular instances
- Concurrent access from multiple locations

Compliance Management

Sending data to the cloud can expose an organization to potential liabilities, stemming from both general and industry-specific regulations. PCI DSS (in the payment card domain), HIPAA and HITECH (in U.S. healthcare), and GDPR (the General Data Protection Regulation in the EU) are among these regulatory standards.

Managing the associated risk becomes an uphill struggle for firms strapped for IT personnel and other resources. A SOC provider, however, can help ensure that your organization deploys the proper security processes and requirements to meet or exceed compliance needs.

Trusted Guidance and Consulting

Over time, the security analysts at the heart of a SOC become well-acquainted with your cloud infrastructure. This knowledge helps them make informed suggestions for your security strategy and ensure that threat detection and response capabilities are fine-tuned for your environment, greatly reducing false positive alerts that can distract from truly legitimate threats.

Predictable Subscription Pricing

SOC pricing should be affordable and spare you the considerable expense you would shoulder for a comparable on-premises solution. Internal SOCs can rarely achieve this objective, since they rely on variably-priced software tools and create increasing management demands on IT teams. SOC-as-a-service has a fixed-price, subscription model, based on the number of users and sensors rather than the volatile volume of logs and monitored endpoints in your environments.

SOC2 Type II Certified

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com