DARKReading

TOP TIPS

Safeguard Your Cloud Journey With A Comprehensive Security Solution

The transition to remote work environments, increased cloud adoptions and new technology deployments (AI, IoT, robotics, etc.) highlights the need for a comprehensive approach to security.

As organizations rapidly expand their remote workforces due to the pandemic, they face unprecedented threat levels and resource vulnerabilities. Growing reliance on cloud services such as Infrastructure as a Service (IaaS) and runaway Shadow IT deployments further compromise the legacy safeguards currently in place.

Security professionals need to know the status and location of all their resources and workload deployments from end to end. Using effective risk analysis, connectivity visualization and inventory visibility within an "exposure first" security approach, they can identify key vulnerabilities and prevent costly breaches. Along with adopting cloud security best practices, organizations can then accurately identify all the resources deployed across their public cloud and on-premises environments.

As CISOs and IT leaders confront vastly expanded and complex networks while migrating more assets than ever to the cloud, these Top Tips offer guidelines for strengthening cloud security and remediating the riskiest vulnerabilities:

Understand Exposure Risks

Unintended access and Shadow IT can expose critical resources, expand attack surfaces and create new vulnerabilities. For example, IT leaders need to expand awareness of "runaway inventory" beyond their monitoring capabilities and harden any resources that have been exposed.

To truly understand deployment risks, IT and business leaders should know what resources are exposed and then redesign their cloud networks to reduce risk by aligning with a service provider's best practices.

Ensure End-To-End Visibility

It's not uncommon for organizations to lose track of their VPC/VNET/VCN deployments over time. Gain a comprehensive overview of your cloud footprint and reduce the overall attack surface. Assemble a complete inventory of assets and resources across cloud and physical sites to understand the interconnections and block potential incursions.

Identify resources in the Internet and employ dynamic visualizations for all cloud environments (AWS, Microsoft Azure, Google Cloud Platform and Oracle Cloud) to provide timely, comprehensive and accurate views of your infrastructure.

Create Cloud Segmentation Policies

Minimize your cloud-based attack surfaces and prevent lateral incursions into your infrastructure. Using segmentation policies and continuous monitoring, organizations gain insights and detailed information to accelerate their remediation efforts and meet compliance goals.

Prevent Data Leakage/ Exfiltration

Acquire immediate intelligence once information has leaked or a breach has occurred. Avoid unnecessary losses, regulatory fines and brand damage through 24/7/365 threat awareness and monitoring. Educate business end users on data safety protocols, particularly as remote workplaces become the norm.

Adopt Best Security Practices

Employ industry standards such as Center for Internet Security (CIS) Benchmarks and Cloud Security Alliance frameworks to confirm best practices and eliminate security misconfigurations.

Evaluate Cloud Vulnerabilities

Prioritize remediation of Internet-facing access and identify the possible downstream impacts of these lapses. Employ a vulnerability management solution that can generate a severity score to help you gauge risk, but also consider where the vulnerabilities exist in the context of your network and access points.

Control Shadow IT

Harness cloud deployments that don't comply with security mandates. Today, numerous business teams across an organization can deploy cloud services at will, however there's typically a single security team for oversight. CISOs and IT leaders require capabilities that can help them identify the resources that they need to safeguard along with the most effective ways to ensure airtight protection.

Adopt A Single Security Solution

Gain a detailed security assessment and visual representation of your multi-cloud environment using a unified view from an outside vendor that can provide clarity on how and where resources are connected. A unified solution will compensate for multiple disparate consoles and tabular views that offer only fragmented, partial assessments of security strengths.

Find Out More

RedSeal helps government agencies and Global 2000 companies measurably reduce their cyber risk and show where their resources are exposed to the Internet. Only RedSeal's award-winning cloud security solution can bring all network environments– public clouds (AWS, Microsoft Azure, Google Cloud Platform and Oracle Cloud), private clouds, and on premises – into one comprehensive, dynamic visualization. RedSeal verifies that networks align with security best practices; validates network segmentation policies; and continuously monitors compliance with policies and regulations. It also prioritizes mitigation based on each vulnerability's associated risk. Visit RedSeal to find out how to get started:

Visit RedSeal to find out how to get started

VISIT NOW

Sponsored by

REDSEAL