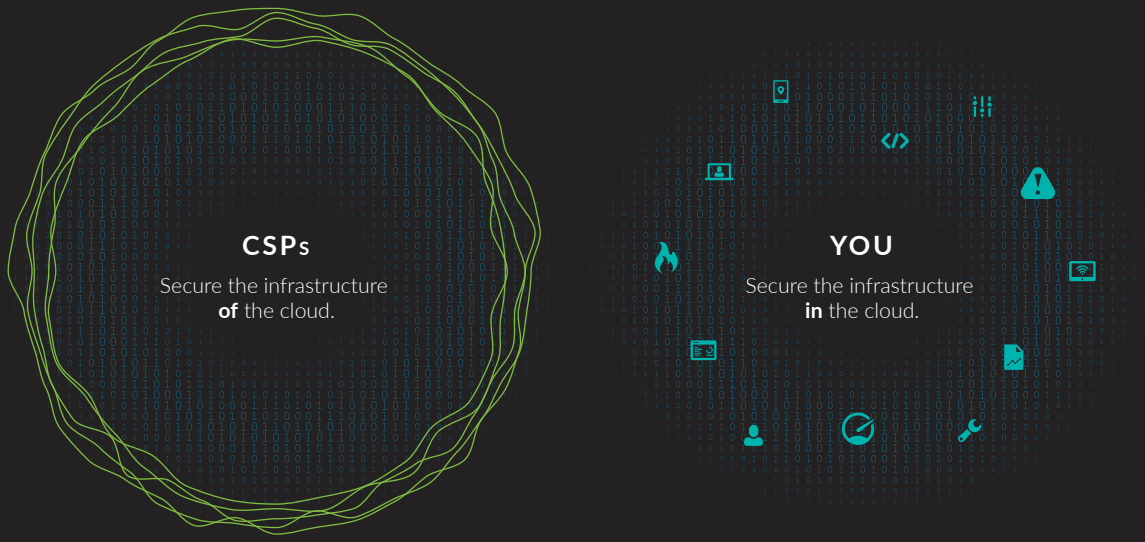
ExtraHop

Shared Responsibility in the Cloud

UNDERSTANDING THE ENTERPRISE'S ROLE IN CLOUD SECURITY

First things first, all cloud customers must know that Amazon Web Services (AWS) and Microsoft Azure are cloud service providers (CSPs). They are not security vendors. This is largely why they've tried to make it obvious that their security and compliance goes only so far. To help draw the line where the CSP's responsibility ends and the customer's begins, AWS and Azure have each developed shared responsibility models.



What does this mean?

Shared responsibility means that CSPs protect their assets (everything below the hypervisor), and the customer protects theirs (everything above the hypervisor)

The Shared Responsibility Model Doesn't Protect You

CSPs have yet to experience significant breaches. Because they are staffed with some of the world's best security researchers, they will likely get more secure over time. The same is not true for the average cloud customer. Gartner predicts that by 2022, at least 95% of cloud security failures will have occured in the customer's portion of the shared responsibility model.

This is a startling figure, but with a better understanding of your responsibility, and by unpacking the main threat vectors through which these failures might occur, enterprises can better understand what they can do to hold up their end of the cloud security bargain.

ExtraHop

SHARED RESPONSIBILITY IN THE CLOUD

APPLICATIONS & CONTENT

Azure Security Center events enrich network-based threat detection with on-box activity (disabled logging, suspicious processes, suspect file execution)

Full TLS 1.3 decode & transaction payload analysis in real time, for spotting threats and evaluating risk, even with PFS, deployments

NETWORK SECURITY

- Visibility into on-prem access to cloud infrastructure via private network connection to track lateral movement
- Accountability for remote access

INVENTORY & CONFIG

- Automatic discovery and classification of all cloud assets
- Track rogue instances even when logging is disabled
- Instantly flag exposed resources (i.e. Azure Blob Storage exposed to the Internet)

DATA SECURITY

- Full support for Azure SQL Databases and Azure Blob Storage protocols means visibility into behavior, not just activity.
- Machine Learning at the application layer provides immediate detection of exfiltration activity

ACCESS CONTROL

- Integration with Azure Activity Monitoring allows granular tracking of privilege manipulation
- Analysis of Active Directory payloads allows machine learning to flag suspicious behavior (credential harvesting, brute force)

Cloud-Native Security vs Cloud-Ready Security

Despite efforts to clearly delineate between their responsibility and the customer's, AWS and Azure still pitch cloud-native security solutions to their customers. For many enterprises–especially those new to cloud–these solutions offer immediate advantages, such as a familiar console, time-to-market acceleration, and turn-key readiness.

ExtraHop does it's machine learning in the cloud which has much more power to provide detectors. However, cloud-native security solutions, such as AWS Guard Duty, AWS CloudWatch, or Azure Monitor, all do their machine learning based on flow log data. Because AWS and Azure solutions rely on logs, the insights are largely surface-level and not based on behavioral patterns. They are not going to detect everything--including unreported rogue instances. An elastic load balancer will only tell you what it logs on your behalf, not a full accounting of its behavior.

HOW EXTRAHOP CAN HELP

By integrating and contextualizing cloud events with other infrastructure activities to create a unified analytics and investigation environment for SOC teams, Reveal(x) for Azure and AWS provides always-on, always-everywhere analysis of the application layer across the hybrid attack surface. With machine learning applied to over 4700 metrics, Reveal(x) detects late-stage attack activities with high confidence, presenting them in context for immediate investigation by cloud security teams.

ABOUT EXTRAHOP NETWORKS

ExtraHop provides enterprise cyber analytics that deliver security and performance from the inside out. Our breakthrough approach analyzes all network interactions and applies advanced machine learning for complete visibility, real-time detection, and guided investigation. With this approach, we help the world's leading enterprises rise above the noise of alerts, organizational silos, and runaway technology. Whether you're investigating threats, ensuring delivery of critical applications, or securing your investment in cloud, ExtraHop helps you protect and accelerate your business.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com