Implement Security For Cloud Superiority

An IDC Infographic, sponsored by ExtraHop

THE CLOUD IS MAINSTREAM

Based on IDC surveys:

As many as **70% OF BUSINESSES** are now using public cloud services.

Companies adopt public cloud to:

- Improve business agility
- Enhance IT security
- Simplify and standardize IT infrastructure and application platforms

Security divides organizations when it comes to cloud:

40.5% say security is a leading **driver** for public cloud adoption

But

46% cite security concerns as the top **inhibitor** of public cloud adoption

REALITY CHECK: CLOUD SECURITY IS UNCHARTED TERRITORY

Threats are adapting to the cloud era:

- **Infrastructure vulnerabilities**
- **Unauthorized access**
- **Misconfigurations**
- **Insecure APIs**

Cloud breaches leave an impact:

"Uber leaks data for 57 million users, fined $460,000"

"Organizations undergoing a major cloud migration at the time of a breach saw a cost increase of $300,000, for an adjusted average cost of $4.22 million."

Ponemon Institute, Cost of a Data Breach Report 2019

Cloud creates organizational challenges:

- Loss of centralized control/visibility of data and workloads
- Inconsistent policies and protections
- Overburdened IT staff can't keep up with security incidents

Not all data/workloads are appropriate for cloud due to privacy, security, or regulatory considerations:

80% of organizations report cloud repatriation activities

19% cite security as the leading reason for cloud repatriation

CLOUD SECURITY: LESSONS LEARNED

Organizations' initial approach to cloud security analytics misses the mark:

47% initially extended an existing on-premises solution to the cloud or purchased a solution from a current vendor

ONLY 16% bought a new product from a new vendor specifically for cloud architecture

Course corrections are required:

- **34% of organizations** have changed how security analytics are applied to cloud architecture at least once
- **23%** have changed their approach multiple times
- **Only 6%** are **NOT** considering a change

Cloud security must be practical:

- **57% of organizations** change cloud strategies to standardize on-premises and cloud security analytics tools

Top considerations for making cloud security decisions:

EASE OF USE: 33% **COST: 28%**

THREE STEPS TO CLOUD SECURITY SUCCESS

1 Adopt a cloud-native approach

70% of new enterprise applications will be developed cloud-native by 2021. Security tools balancing cloud-native functionality with support for multiple cloud services will be required to fully protect future computing environments.

- **39% of organizations** rated security analytics as the most popular new technology for cloud security. Cloud-native security analytics tools are emerging as a vital capability for SOCs.

2 Integrate and consolidate tools to enable automation

To secure the cloud, organizations favor flexible solutions that fill more than one purpose (36%) and ease of integration (32%).

- In making cloud security decisions, important considerations are access to similar information as provided on-premises **(29%)** and reducing the number of security tools **(19%).**
- **Only 12% of organizations** are clearing all alerts—many worry about what they may be missing.
- **18% of respondents** rated automation and orchestration as one of the most important new security technologies.

3 Align to security frameworks

The NIST Cybersecurity Framework (CSF) helps enterprises evaluate and assess the strength of their security programs.

- IDC estimates that **over half of Fortune 500 companies** are adopting NIST as their primary control framework.
- The Center for Internet Security (CIS) Controls are a set of practices that align to NIST CSF and **define concrete steps to mitigate cybersecurity risk.**
- **CIS Benchmarks provide secure configuration guidelines** for over 140 platforms including cloud providers such as AWS, Azure, and Google.

THE CLOUD SECURITY FORMULA

Comprehensive cloud security requires the combination of 3 data sources:

Network/NDR
- Offers network traffic analysis for complete visibility
- Provides inside-the-perimeter security

Endpoint/EDR
- Provides deep insights into system activities and events taking place on endpoints
- Detects incidents on the perimeter

Logs/SIEM
- Collects and analyzes log data
- Consists of very mature tools

Sources: IDC Cloudview, May 2018; IDC Cloud and AI Adoption Survey, January 2018; IDC FutureScape: Worldwide Cloud 2019 Predictions, Nov. 2018

US45635619TM