

ORACLE AND KPMG CLOUD THREAT REPORT 2019

Defining Edge Intelligence: Closing Visibility Gaps with a Layered Defense Strategy

[Read Full Report](#)

KEY RESEARCH FINDINGS



7 of 10
Use more business-critical cloud services YoY



3.5x
Increase in organizations with 50% of their data in the cloud 2018-2020



93%
Are dealing with rogue cloud app usage



45%
Plan to deploy automated patch management in the next 24 months



85%
Are interested in replacing passwords with new forms of authentication



82%
Of cloud users have experienced security events due to confusion over Shared Responsibility Security Models

Percentage of respondents at least somewhat concerned about threat type



91%
Email phishing



90%
Business email compromises



89%
Ransomware

“ Machine learning, automation, the speed at which we can execute security processes – it’s all resulting in minimal downtime for some customers and the enhanced ability for all to use cyber security as a business enabler.”



Shared Responsibility Security Model

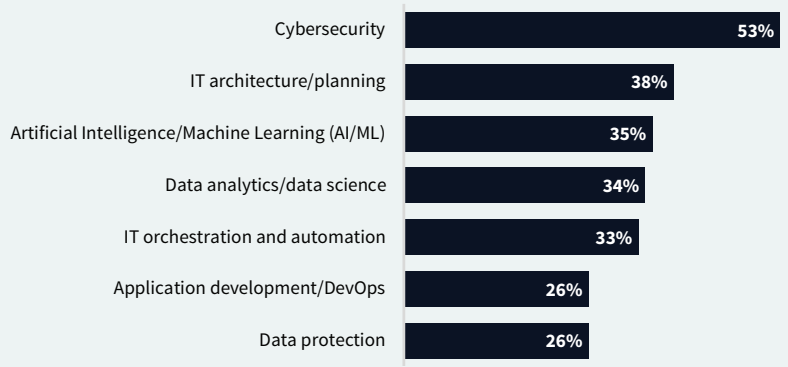
On-premises	IaaS (Infrastructure-as-a-Service)	PaaS (Platform-as-a-Service)	SaaS (Software-as-a-Service)
User Access/Identity	User Access/Identity	User Access/Identity	User Access/Identity
Data	Data	Data	Data
Application	Application	Application	Application
Guest OS	Guest OS	Guest OS	Guest OS
Virtualization	Virtualization	Virtualization	Virtualization
Network	Network	Network	Network
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

Legend: ■ Customer Responsibility, ■ Cloud Service Provider Responsibility



In which of the following areas do you believe your IT organization currently has a problematic shortage of existing skills?

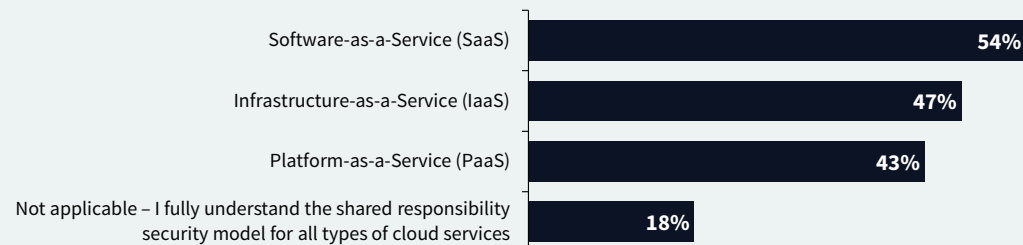
(Percent of respondents, N=586, multiple responses accepted)



“ Contributing to an inability to process security events is an acute shortage of cybersecurity skills.”

For which of the following types of cloud services do you find the shared responsibility security model the most confusing?

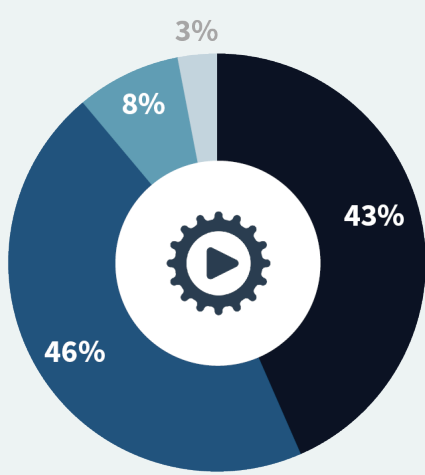
(Percent of respondents, N=456, multiple responses accepted)



Only 10% of CISOs state they fully understand the SRSM model (versus 25% CIOs)

Have or does your organization plan to deploy a solution that automates patch management for production environments?

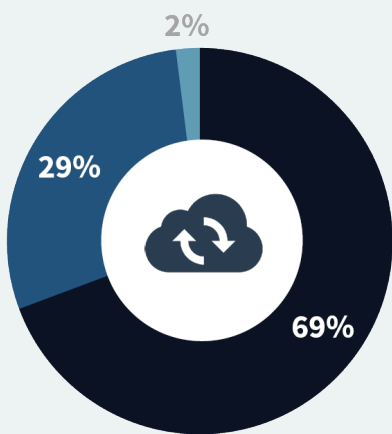
(Percent of respondents, N=456)



- Yes, we have implemented automated patch management
- Yes, we plan to implement automated patch management in the next 12-24 months
- No, but we are interested in automated patch management
- No plans or interest

How has the nature of the cloud services used by your organization changed, if at all, in the last 12 months?

(Percent of respondents, N=456)



- More of the cloud services we employ today are business-critical
- There has been no change in the business criticality of the cloud services we use
- Less of the cloud services we employ today are business-critical

[Read Full Report](#)