ORACLE AND KPMG CLOUD THREAT REPORT 2019

EXECUTIVE SUMMARY

Executive Summary

Public cloud-hosted and -delivered services have become the centers of gravity for many organizations' information technology infrastructures. Cloud applications and platform services have enabled businesses to move faster than ever, intensifying organizational dependence on the availability, integrity, and security of those services. Last year's Oracle and KPMG Cloud Threat Report explored market research that revealed how organizations are struggling to keep pace with the speed and scale at which their businesses are using cloud services, creating a cloud security readiness gap. A year later, it is clear that the business-critical nature of cloud services has substantially raised the stakes for securing public cloud assets. IT organizations are operating with a strategic imperative to address a myriad of both old and new cybersecurity challenges, highlighting the need to retool the foundational elements of a cybersecurity program to bring the cloud into scope. We'll discuss both the challenges of and strategies for securing the business cloud by exploring the following key findings in the *Oracle and KPMG Cloud Threat Report 2019:*

- **The mission-critical nature of cloud services has made cloud security a strategic imperative.** Cloud services are no longer nice-to-have tertiary elements of IT—they serve core functions essential to all aspects of business operations.
- **Confusion around the shared responsibility security model has resulted in cybersecurity incidents.** A lack of clarity on this foundational cloud security construct has had real consequences for many enterprises, including the introduction of malware and loss of data.
- **Visibility remains the top cloud security challenge.** The fact that the infrastructure that hosts and delivers cloud services is managed by a third party can create a visibility gap that existing network-based security controls are ill-fitted to address.
- **Cloud adoption has expanded the core-to-edge threat model.** An increasingly mobile workforce accessing both on-premises and cloud-delivered applications and data dramatically complicates how cybersecurity professionals must think about their risk and exposure.
- **CISOs are too often on the cloud security sidelines.** The decentralized adoption of cloud services by line of business leaders who do not follow approval methodologies creates a visibility gap for the organization's cybersecurity leaders.
- **Shadow IT continues unabated.** SaaS consumption, empowered by the line of business, driven by the need for fast time-to-value, and enabled by the consumerization of IT, is here to stay, independent of attempts to control usage with policies.

- **Intelligent automation is gaining steam to address long-standing patching issues.** The operational obstacles to better patching practices are starting to be addressed by automating the never-ending patch cycle to help protect vulnerable systems against exploits.

- **Passwords are past due.** The headache of password management, poor password hygiene, and the friction of introducing a second factor of authentication are being replaced with new primary factors of authentication and adaptation for the secondary factors.

- **Machine learning is being employed to improve the fidelity and frequency of triaging security events.** Of the many use cases for machine learning, organizations are leveraging this important technology to bring some relief to security event fatigue, improving the accuracy and scale of security analytics.

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

1 in 10
Organizations can analyze 75%+ of their security events

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

53%
Are using machine learning for cybersecurity purposes

Save for younger, cloud-native companies, the use of public cloud services now represents a critical dimension of a hybrid and multi-cloud data center. As such, an appreciation and understanding of both the old and new is essential to evolve an organization's cybersecurity program that contemplates protecting traditional infrastructure as well as the increasingly critical set of cloud services.