
ORACLE
Cybersecurity From Strategies
to Digital Resilience

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

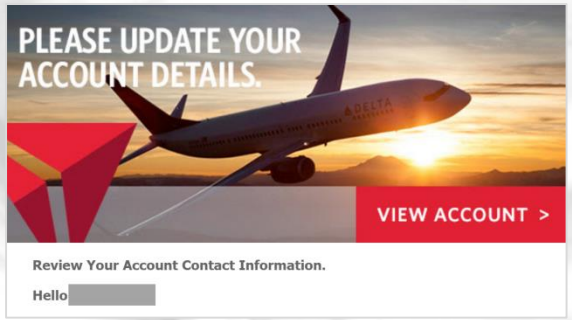
Today's Agenda

1. The Impact of the Cloud-enabled Workplace on Cybersecurity Strategies
2. Cybersecurity Best Practices for Modern IT Environments
3. In Summary: Closing the Gap
4. Cybersecurity Improvement Project

Attackers Are First to Use Emerging Technology

Millions of Records Lost

Stealing legitimate credentials through phishing attacks underscores need for User Behavior Analytics



Global Internet Down

Most sophisticated global denial of service exploits IoT vulnerabilities; hackers bring down prominent web sites

Financial Network Exploited

$80M stolen from Bangladesh Bank

ORACLE

Business Imperatives

> 80% believe digital transformation, underpinned by strong security, will boost their business and improve customer experience.
>
> – A Secure Path to Digital Transformation, Oracle Cloud Survey, 2016

Workloads Are Everywhere

Cloud is not just SaaS. Workloads are moving rapidly to PaaS and IaaS

71% of large enterprise will shift some workloads to cloud by 2018

Enterprises plan to use an average of **6 clouds** to run their workloads

2016 McKinsey, 2016 Right Scale

ORACLE

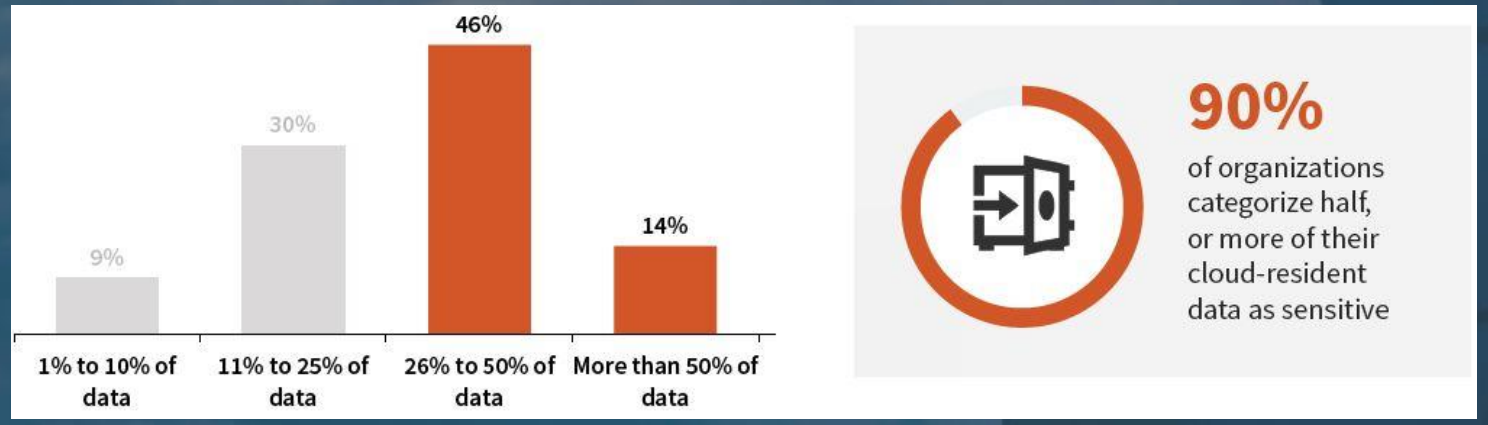
Oracle and KPMG Cloud Threat Report 2018

- Survey research of 450 global security leaders/practitioners
- Security, compliance issues that impact orgs on their cloud journey
  - **#1 challenge**: managing security events in cloud
  - **85%** cite more than half of cloud data is “sensitive”
  - **89%** concerned employees violate cloud policies
  - **100%** say GDPR impacts their cloud service provider(CSP) strategy

www.Oracle.com/CTR

Broad Cloud Adoption Puts the Spotlight on Cybersecurity

Cloud Agility - Which enables rapid deployment of cloud application, it's causing a "PACE GAP" between how fast business are scaling up in the cloud and their ability to keep up with commensurate security measures.



Sensitive Data Is Migrating Upwards to the Cloud

Sources: Oracle and KPMG Cloud Threat Report 2018

At the same time, Cyber threats are becoming more complex and sophisticated.

45%

have experienced one or more of these three types of exploits

Zero-day exploits that take advantage of OS/app vulnerabilities unknown to the victim

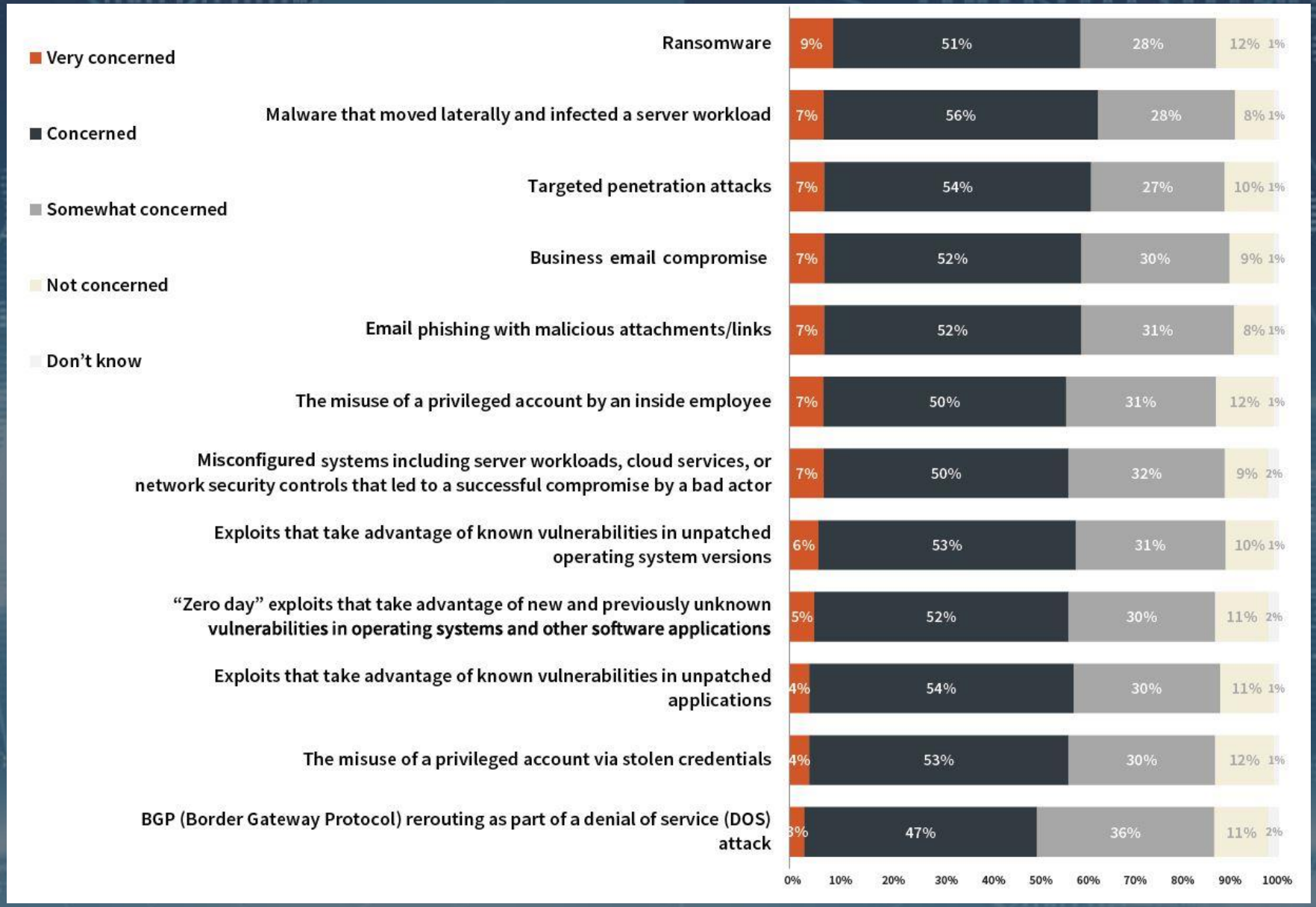
Exploits that take advantage of known vulnerabilities in unpatched applications

Exploits that take advantage of known vulnerabilities in unpatched operating system versions

Sources: Oracle and KPMG Cloud Threat Report 2018

ORACLE

Top Concerns over the Next 12 Months



Sources: Oracle and KPMG Cloud Threat Report 2018

Cyber Attacks Have Operational and Financial Impacts

66%

experienced at least one of these types of interruptions to business operations

Standard business ops, ability to provide services, lost employee productivity, delayed another IT project

51%

experienced at least one of these types of financial impacts

Any financial impact, capital expenditures, shareholder value, financial loss

Data loss

Reputation damage

Sources: Oracle and KPMG Cloud Threat Report 2018

Cybersecurity Best Practices for Modern IT Environments

ORACLE

A Modern IT Environment comprised of:

- Cross-generational application stacks that require a reorientation around the definition of the perimeter.
- The use of multiple cloud providers across the entire stack of SaaS, PaaS, and IaaS.
- A pragmatic approach to securing the use of cloud applications.
- An ongoing focus on awareness training.
- A need to retool technical cybersecurity skills and roles.
- A characterization of patching as a configuration management best practice.
- The implementation of a defense-in-depth approach to protecting mission-critical applications.

Sources: Oracle and KPMG Cloud Threat Report 2018

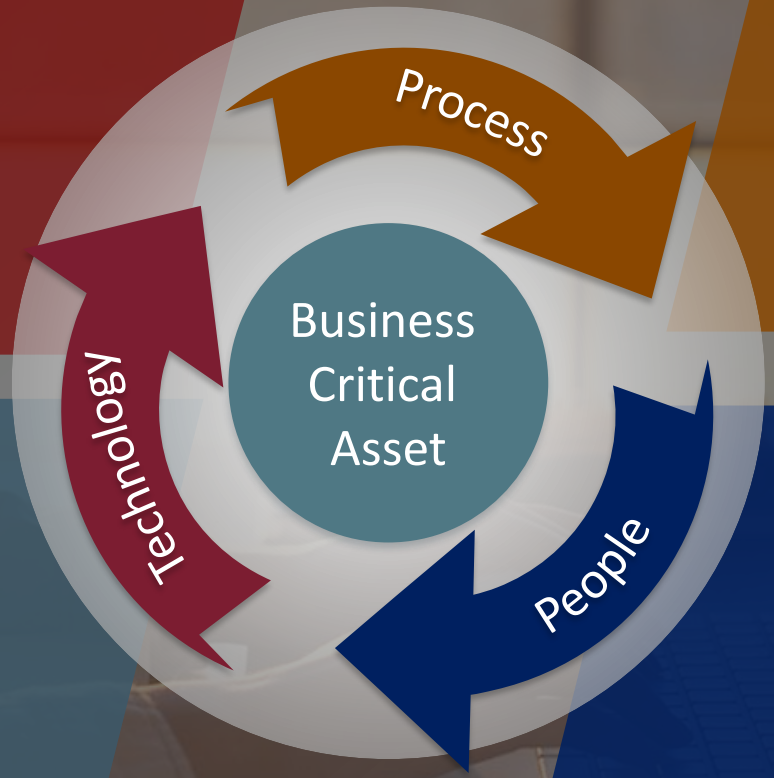
Securing the cloud-enabled workplace requires a holistic and integrated approach

Technology

Push security down the stack and include layers of defense across IaaS, PaaS, and SaaS.

Process

Employ stringent security policies and controls across people, technology and business critical asset.



Business Critical Asset

Design access controls to secure access to Business Critical Asset.

People

Hire highly talented cybersecurity resources and train them on Security Assurance methodology.

Think Beyond Perimeter Defenses

Adopt a Dose of Cloud Security Pragmatism

Coverage across cloud services, including SaaS properties and IaaS services, so that visibility and control policies can be applied across the breadth of services being used.

Contextual visibility that goes beyond the discovery of shadow IT applications to allow organizations to assess the risk associated with each app and service in use.

Data discovery and classification, another aspect of visibility, to provide insight into what types of data assets are being stored in conjunction with the use of cloud services.

Maintenance of system integrity by monitoring for configuration drift and automating the remediation of non-conformant workloads and cloud services, including, for example, the ACLs on object stores.

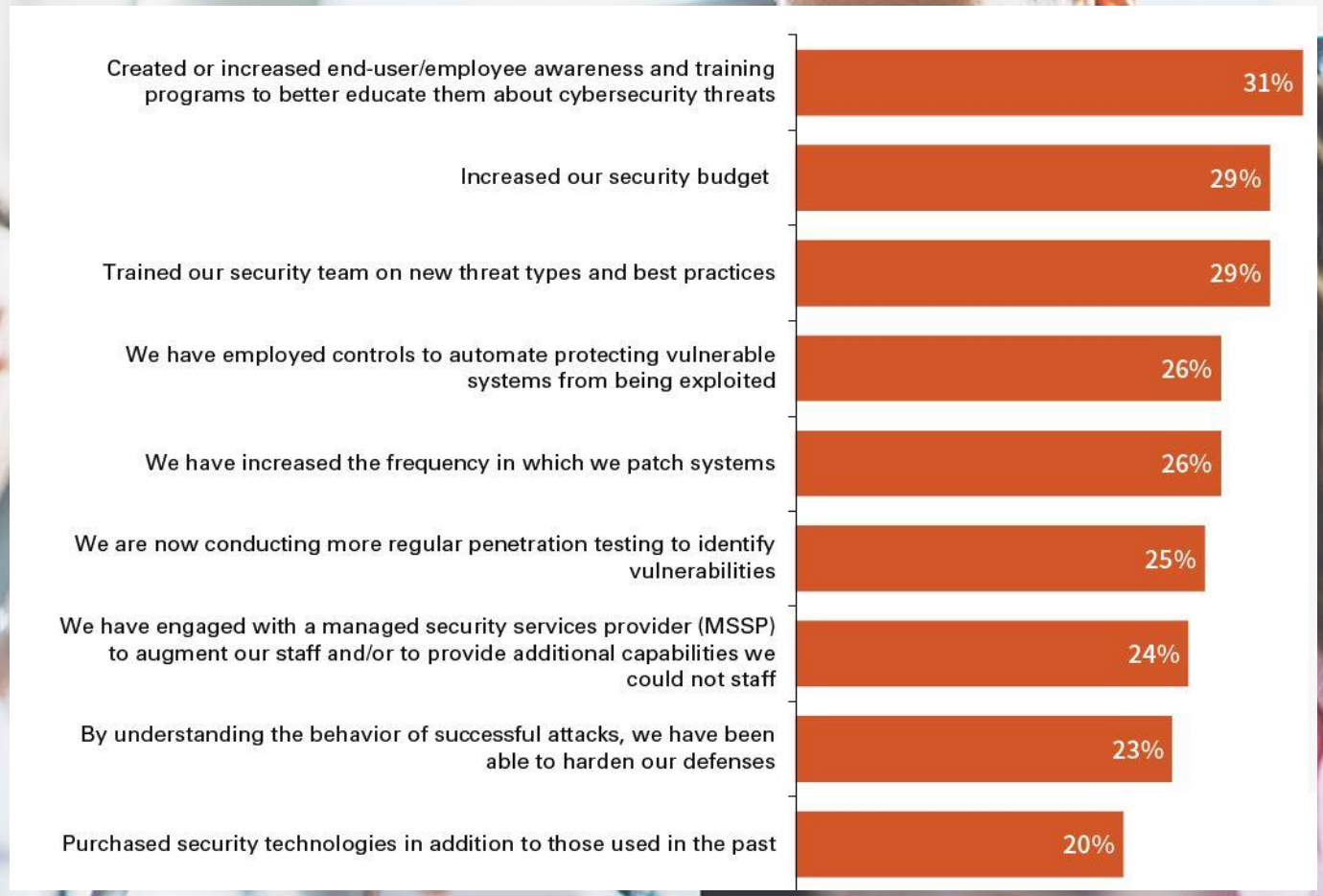
Threat prevention by inspecting in-transit traffic and at-rest content for malicious payloads to prevent cloud services from being employed as an attack vector.

Data loss prevention (DLP) policies to govern which users have access to classes of cloud-resident data.

Monitor user behavior for anomalous activity, such as non-standard login times and locations, as well as irregular data access actions.

Sources: Oracle and KPMG Cloud Threat Report 2018

Focus on End-user Awareness Training

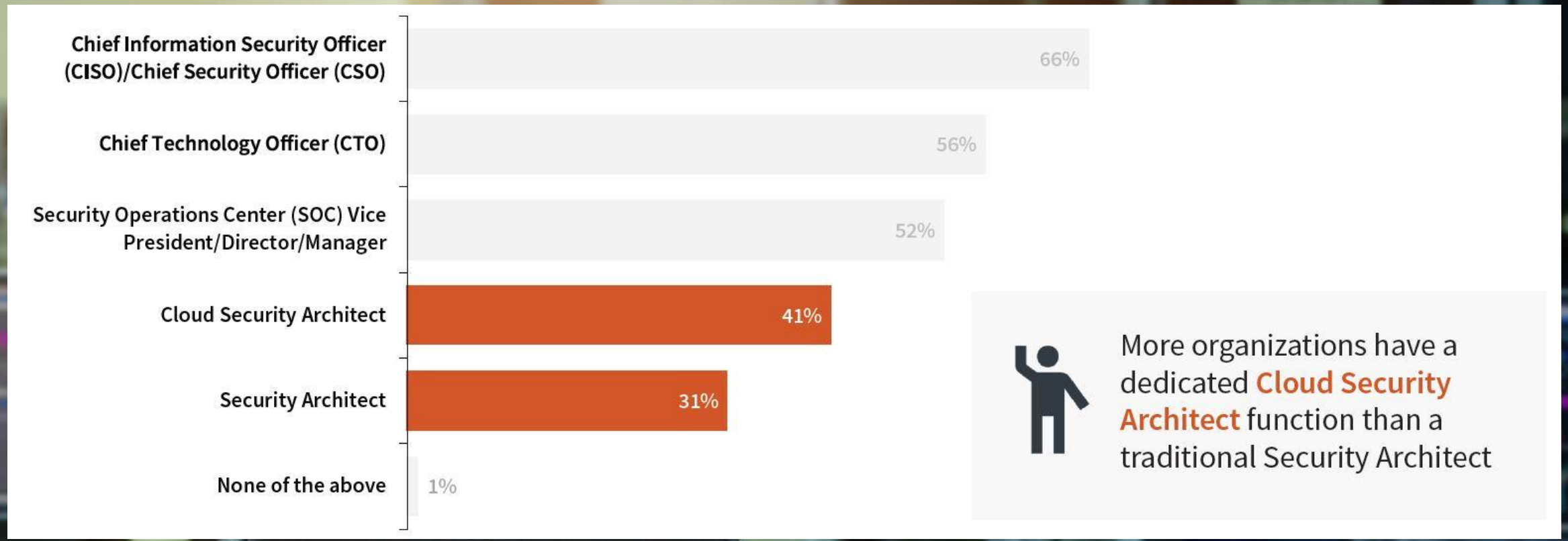


Top area of incremental cybersecurity budget prioritization:

Increase training

Sources: Oracle and KPMG Cloud Threat Report 2018

Retooling Cybersecurity Roles



Sources: Oracle and KPMG Cloud Threat Report 2018

Secure Application Stacks with Defense-in-Depth

The use of NPM and APM for cybersecurity use cases also fosters collaboration between IT operations management/Network Operations Center (NOC) teams who monitor network and application performance, and cybersecurity analysts in a Security Operations Center (SOC).

One View into All Data
Single pane of glass into all data collection and normalization

Artificial Intelligence Analysis
Machine learning to quickly remediate potential issues

Complete Threat Lifecycle
Prevent, detect, respond to, and predict sophisticated threats

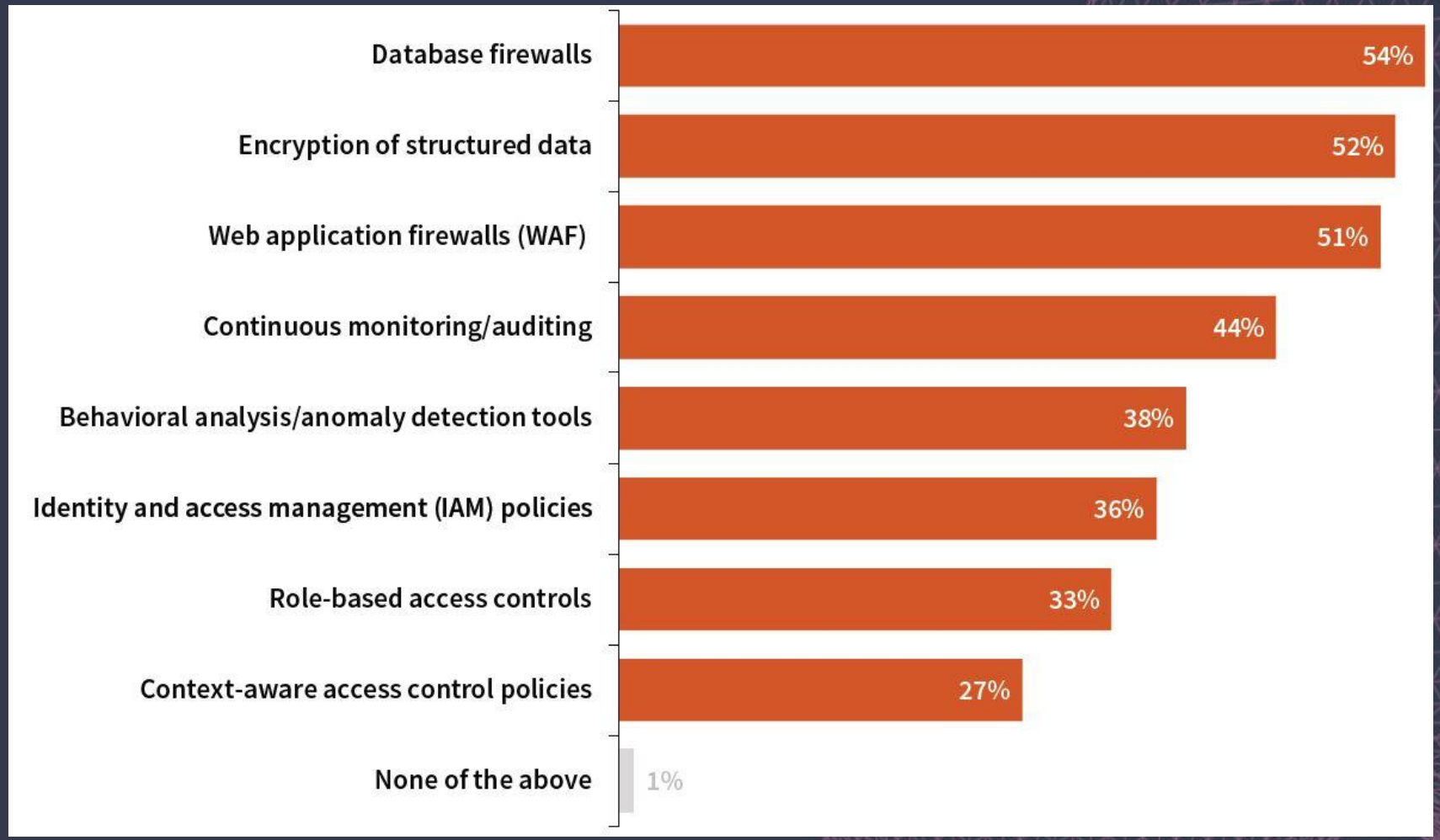
Adaptive Response
Step-up security controls based on anomalous user behavior

Disparate Organizations
Heterogenous, on premises, cloud and multi-cloud coverage

Continuous Monitoring
Consistently assess suspicious activity; autonomous remediation

Sources: Oracle and KPMG Cloud Threat Report 2018

Secure the Database Tier with a Defense-in-depth Approach



How to prevent unauthorized access to your organization's sensitive and critical database servers?

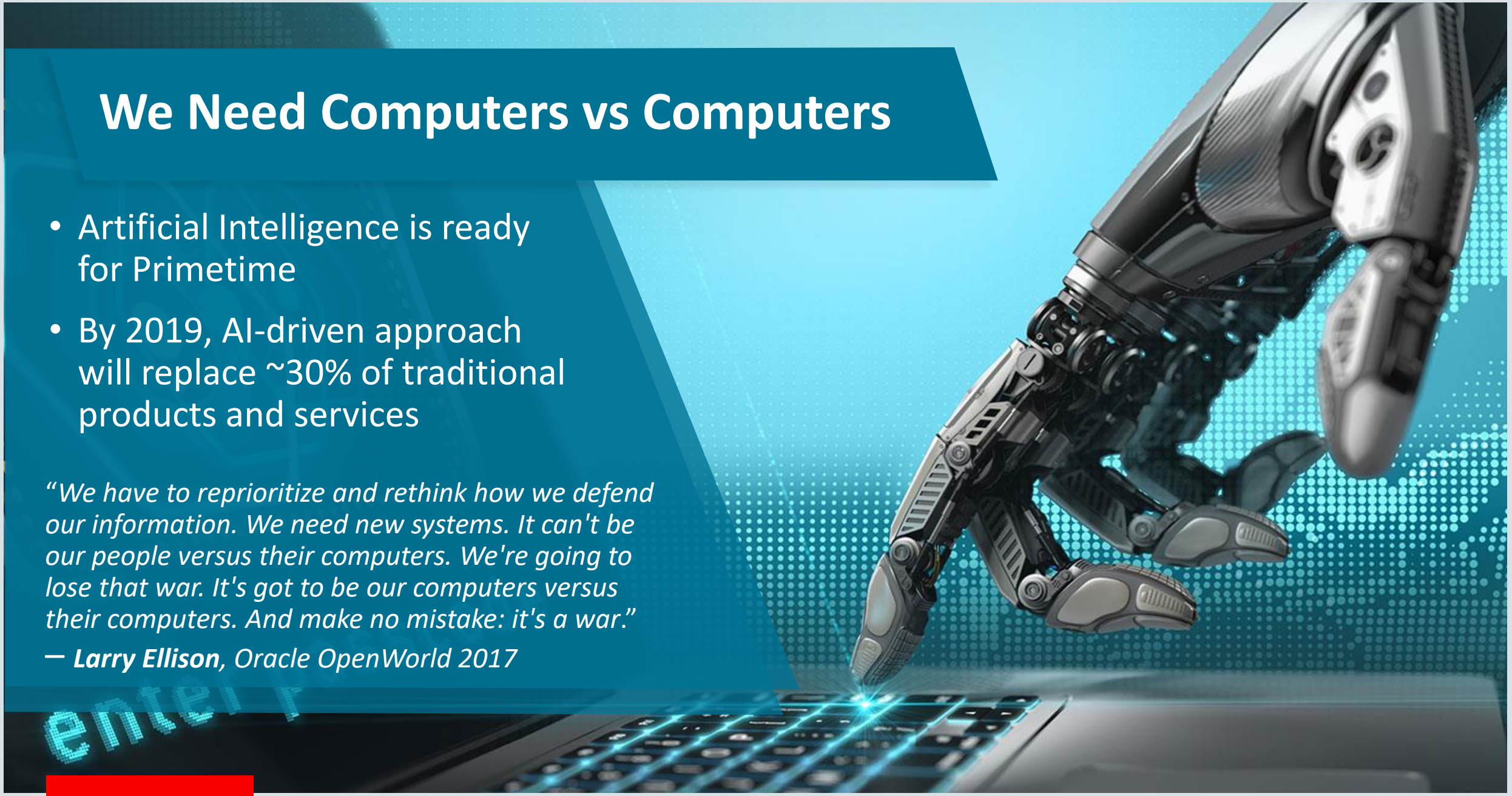
Sources: Oracle and KPMG Cloud Threat Report 2018

We Need Computers vs Computers

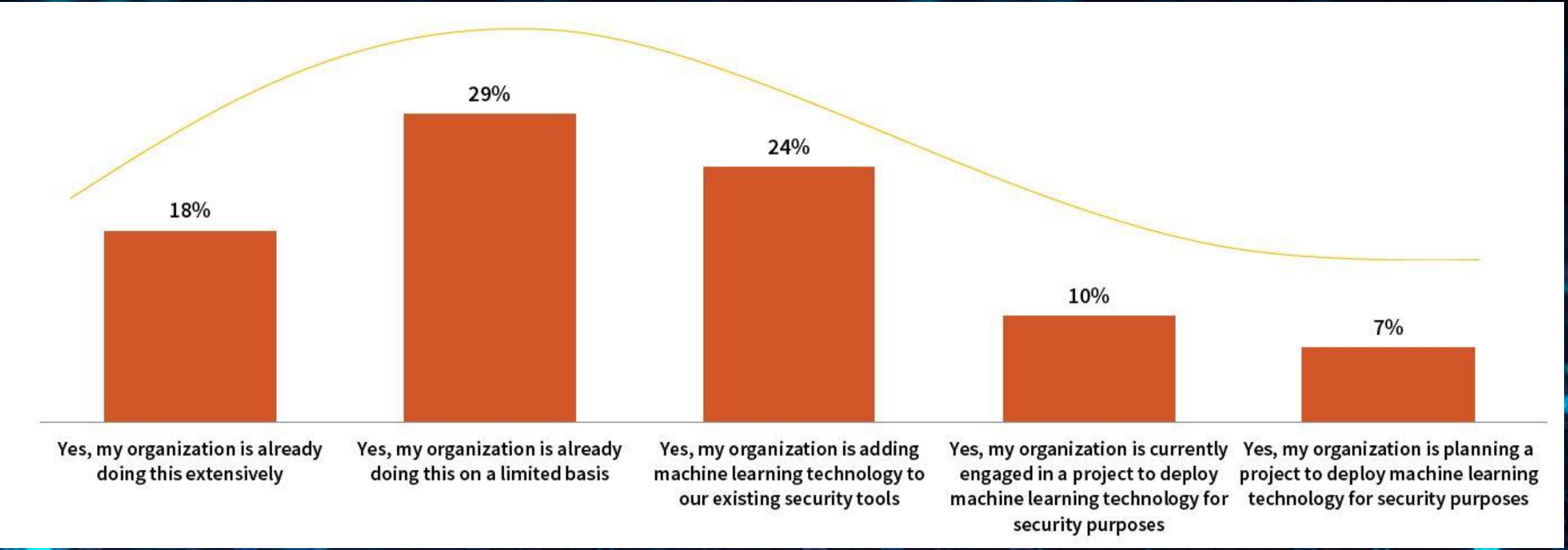
- Artificial Intelligence is ready for Primetime
- By 2019, AI-driven approach will replace ~30% of traditional products and services

"We have to reprioritize and rethink how we defend our information. We need new systems. It can't be our people versus their computers. We're going to lose that war. It's got to be our computers versus their computers. And make no mistake: it's a war."

— ***Larry Ellison**, Oracle OpenWorld 2017*



The Use of Machine Learning for Cybersecurity



Sources: Oracle and KPMG Cloud Threat Report 2018

In Summary: Closing the Gap

- The rate at which cloud services are being adopted
- The diversity of the threat landscape, and the sheer volume of security event data that the expanded attack surface generates.
- IT and cybersecurity leaders are meeting the challenge by not only funding cybersecurity initiatives, but also retooling their skills and approaches for the dynamics of today's IT model.
- Many of the proven best practices to prevent these threats need to be adapted to secure a perimeter that is now as much about users and data as it is about physical demarcations.
- The emerging technologies discussed in this report—machine learning and security automation—promise to help cybersecurity teams be as agile as their line-of-business colleagues so they too can keep pace at scale.

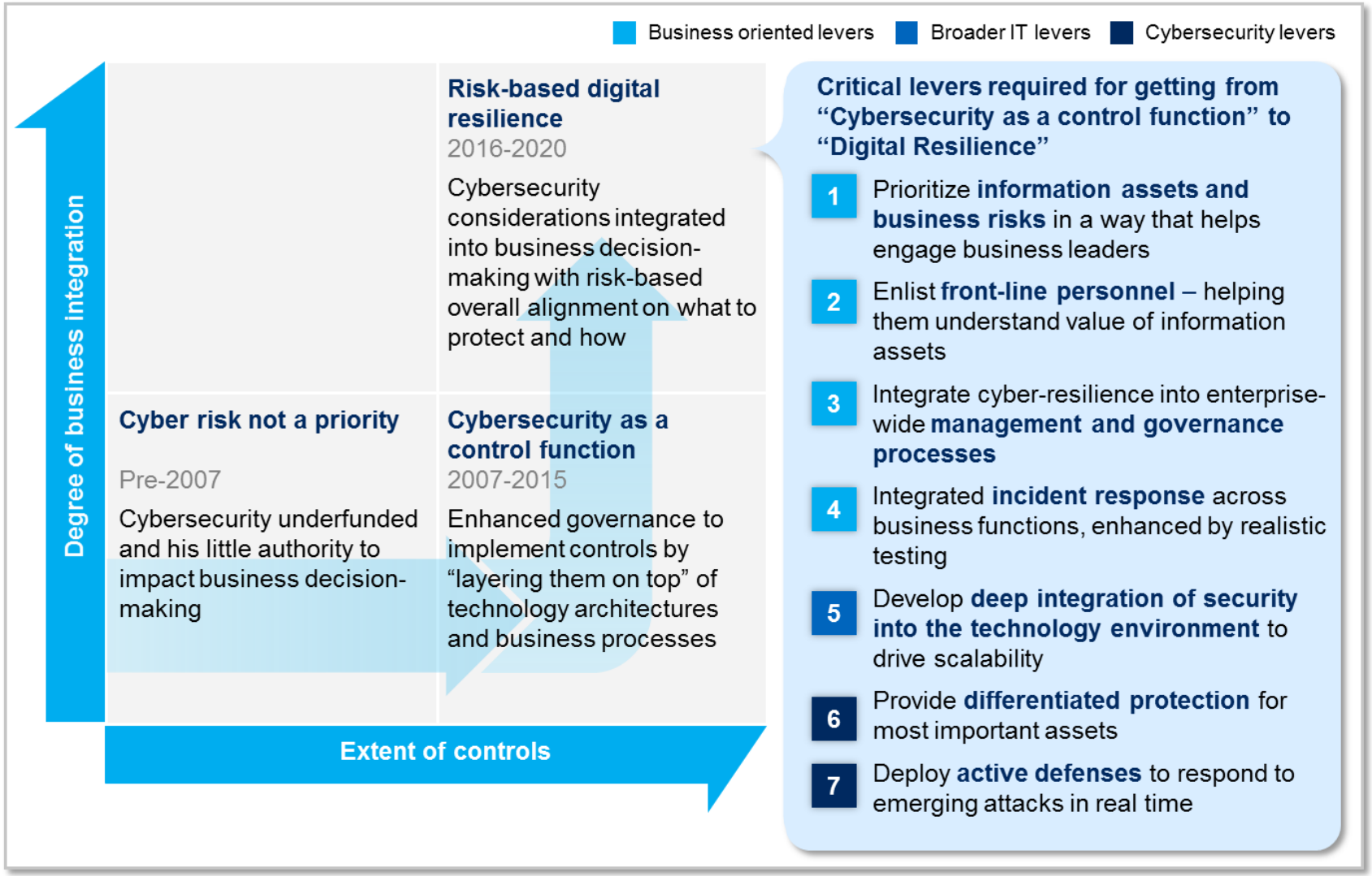
Sources: Oracle and KPMG Cloud Threat Report 2018

Cybersecurity Improvement Project with McKinsey & Company

McKinsey & Company

true

McKinsey's comprehensive framework to measures institutions' digital resilience along seven critical levers



Cybersecurity Improvement Project with McKinsey & Company

Overall workplan