Thinking Autonomous

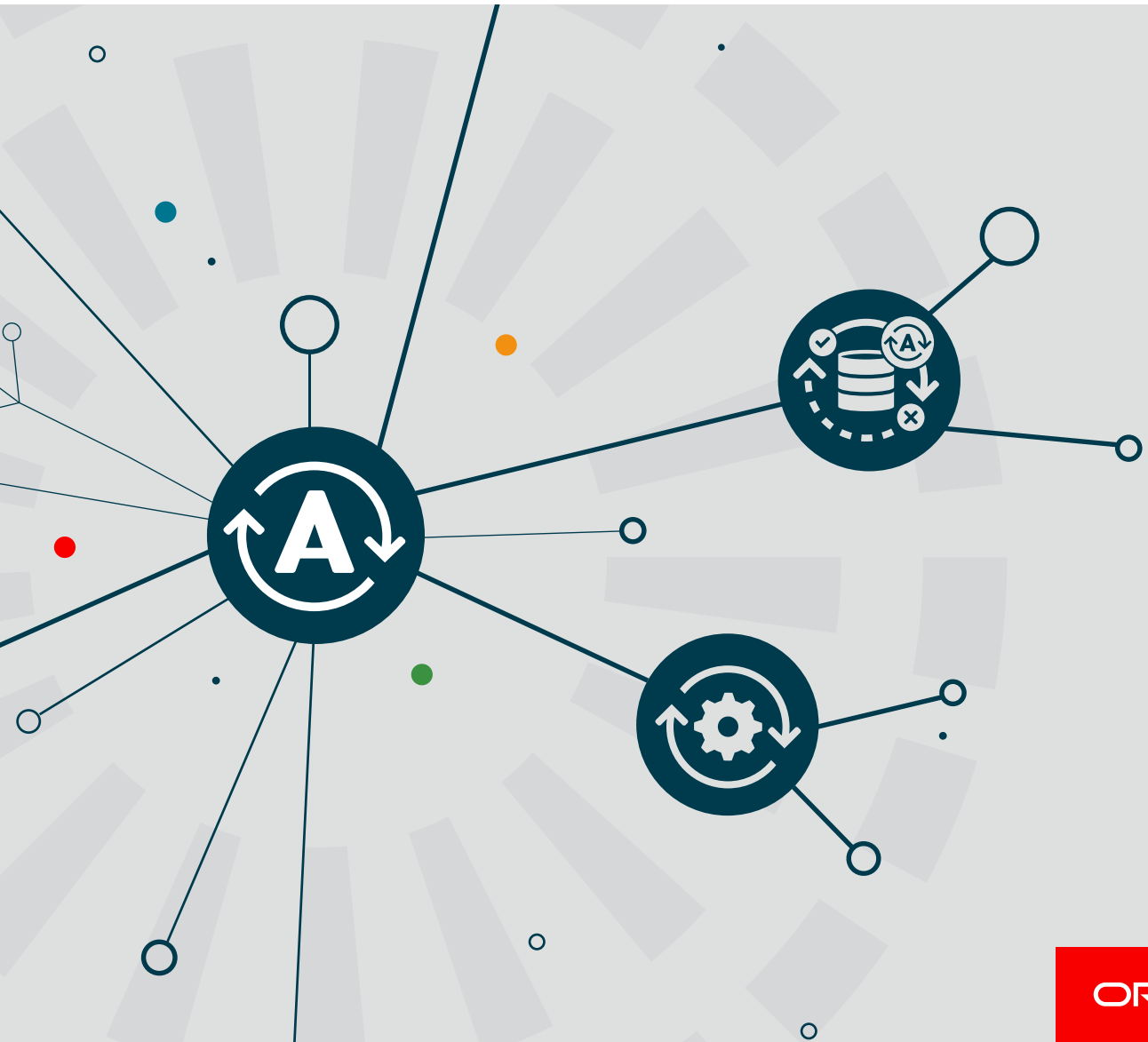
Longitude
A Financial Times Company

IT security and risk: Intelligent automation eases the burden

ARTICLE

ORACLE

Contents



Introduction

It's time to think differently about IT security.

The World Economic Forum recognizes the growing threat to cybersecurity, ranking it alongside extreme weather and natural disasters among the top five risks facing the world today, with a "massive incident of data fraud/theft" fifth and "large-scale cyberattacks" fourth on the list. Moreover, Cybersecurity Ventures calls cybercrime the greatest threat to every company in the world and predicts that by 2021 it will cost US$6 trillion annually, double what it cost in 2015.

"There are multiple threat vectors, both internal and external," says Greg Jensen, senior principal director of cloud security at Oracle. "And it's impossible to manually address all these threats."

It's also impossible to hire and train enough staff to deal with these increasing security vulnerabilities. According to Enterprise Strategy Group, more than half of IT and business decision-makers report a problematic shortage of security skills today.

Oracle's research supports that conclusion, citing the lack of skills and qualified staff as the second-biggest cybersecurity challenge. And this skills gap is expected to get worse. By 2021, Cybersecurity Ventures predicts there will be more than 3.5 million open cybersecurity jobs.

> *"There are multiple threat vectors, both internal and external"*
>
> **Greg Jensen, Senior principal director of cloud security, Oracle**

ORACLE

> *"Fast-forward to databases supporting a number of different applications in a corporate environment owned by multiple divisions or locations, autonomous security is the key."*
>
> **Brian Jensen, Application risk consulting sales leader, KPMG**

Even if there were enough trained security professionals, that isn't really the solution to the increasingly complex and common threats. "We can't do it by the human factor alone," says Greg Jensen. "We can't school enough people or hire our way out of this problem."

On one side, there is an increasing threat landscape; on the other side there is the evolution of organizations' internal IT infrastructures. In the past, IT assets and systems were in one location, protected by fortifications, like a castle behind its walls and moat.

"Anything inside the castle wall was protected by the same infrastructure," says Brian Jensen, Oracle application risk consulting sales leader at KPMG. "Now there is no castle—every application and associated database has to stand alone and be protected on its own."

Intelligent automation is changing how we think about security infrastructure and where to build defenses. "Fast-forward to databases supporting a number of different applications in a corporate environment owned by multiple divisions or locations," says Brian Jensen. "Autonomous security is the key."

ORACLE

The solution to the security conundrum

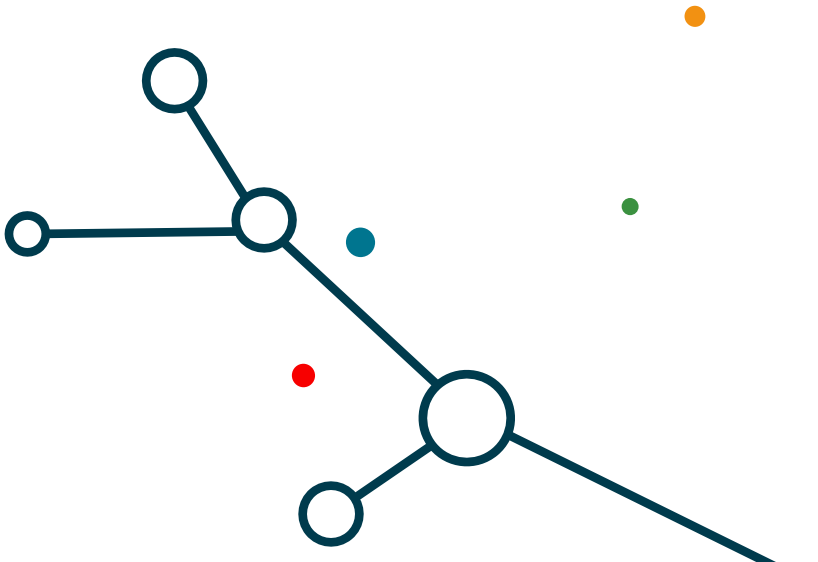
There are several challenges to securing organizations' data and applications, andnot least is the sheer number of security-related events. "Organizations face 3.2 billion events each month," says Greg Jensen. "Out of that 3.2 billion today, on average only 31 are actual security threats." That's a lot of noise to deal with, and poring over that many records is not humanly possible.

A second security challenge is keeping pace with patches. Microsoft alone issues dozens of patches every month. Add to that patches from every other vendor and it's no surprise that IT officers are struggling to keep up. It isn't just the volume of patches that causes delays in updating systems; companies have a variety of reasons for not deploying security patches, including the fact that many organizations have hundreds and possibly thousands of databases. Running a patch can take thousands of hours to perform, often requiring downtime or business disruption.

"There are legitimate operational issues why sometimes organizations don't patch as quickly as they ought to when they become aware of a vulnerability for which there is an available patch," says Doug Cahill, senior analyst and group director, Enterprise Strategy Group. "Sometimes patching requires rebooting the system, which would impact an SLA [service-level agreement]; sometimes the business does not yet support the version of the OS it would be upgraded to by the patch, or the patch would impact system performance and that would affect SLA response time."

Cloud computing is a third challenge organizations are dealing with. The very element of the cloud model that brings value to adopters—the fact that it's remote and distributed—causes administrative issues that impact security. "IT has become increasingly decentralized," says Cahill. "Business units are making their own IT decisions, including doing their own application development and delivery."

This means there is little or no security oversight for these cloud applications, and organizations may not know which applications are running and where all their sensitive data is. This is a significant problem. Almost all (93%) of the respondents in the Oracle and KPMG Cloud Threat Report say they're dealing with rogue cloud application usage. And a quarter of them cite unauthorized use of cloud services as their biggest cybersecurity challenge today.



ORACLE

Automation holds the key to security

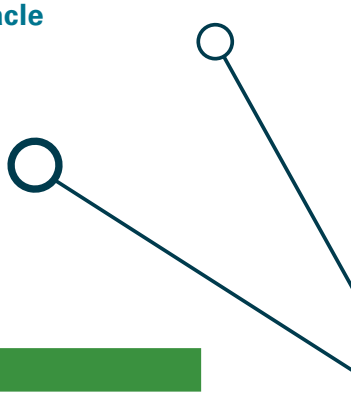
Organizations can deploy users, applications, devices, and infrastructure much more rapidly than ever before. Throughout all that activity, security practitioners have two main goals: To remove error-prone manual processes, and real-time detection and response to emerging threats. Intelligent automation gives them the power to do both.

Automated detection identifies vulnerabilities and threats in real time, enabling a rapid response to better mitigate both internal and external cyberattacks. "CISOs measure mean time to detect and mean time to respond," says Oracle's Greg Jensen. "Machine learning and artificial intelligence reduce false positives and false negatives and get to the real threats and reduce mean time to response."

Intelligent automation also manages security patches, saving time and human resources. This is critical to mitigating zero-day vulnerabilities before they're exploited. Because they recognize the value of patching, the majority of respondents to Oracle and KPMG's Cloud Threat Report said they had either implemented (43%) or are planning to implement (46%) automated patch management in the next one to two years.

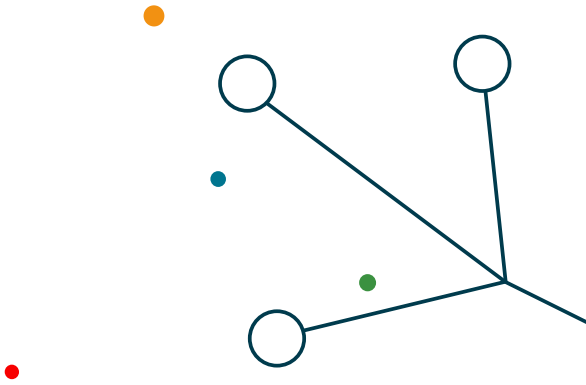
"Machine learning and artificial intelligence reduce false positives and false negatives and get to the real threats and reduce mean time to response."

Greg Jensen, Senior principal director of cloud security, Oracle



ORACLE

Autonomous is the future of data security



There will always be new security threats—as IT evolves, the bad actors look to exploit vulnerabilities and risks. To keep up, autonomous technology must be a key part of an organization's security playbook. It's the only way to ease the operational burden of patching known vulnerabilities and shortening the time to identify and mitigate both known and unknown exploits.

"We live in an application economy in which we interact with apps in both our personal and work lives every day," says ESG's Cahill. "This creates a continually increasing attack surface; new vulnerabilities are being introduced all the time. Organizations have to be on a "rinse and repeat" cycle to discover risks before they can be exploited. Autonomous security helps close that exposure window."

As business units make their own IT decisions and are doing their own applications and delivery, the decentralization of IT within an organization increases. That's why the future of IT is applications, all of which must work together, even when their underlying infrastructure is different and they aren't necessarily protected by the same mechanisms.

To protect the enterprise and its assets effectively, the security team must be internal decision-makers and providers—a council guiding the direction of IT within the organization. This entails using intelligent automation to secure the assets wherever they are deployed.

"The positives associated with this new automated world are amazing," says KPMG's Brian Jensen. "We're going to be a much more efficient US business economy because of that. However, we have to intentionally manage the risk, look at the risk reality, and take appropriate steps to mitigate it. We can't forget that we're here to enable and protect."

> *"The positives associated with this new automated world are amazing"*
>
> **Brian Jensen, Application risk consulting sales leader, KPMG**

ORACLE

Interviewees

Greg Jensen, Senior principal director of cloud security, Oracle

Doug Cahill, Senior analyst and group director, Enterprise Strategy Group

Brian Jensen, Application risk consulting sales leader, KPMG

Sources

Oracle/KPMG Cloud Threat Report 2019

Cybersecurity Jobs Report 2018-2021,
Cybersecurity Ventures

These are the biggest risks facing our world in 2019,
World Economic Forum

2019 Technology Spending Intentions Survey,
Enterprise Strategy Group

2019 Official Annual Cybercrime Report,
Cybersecurity Ventures

Try Oracle Cloud for free

cloud.oracle.com/tryit

Longitude
A Financial Times Company

ORACLE