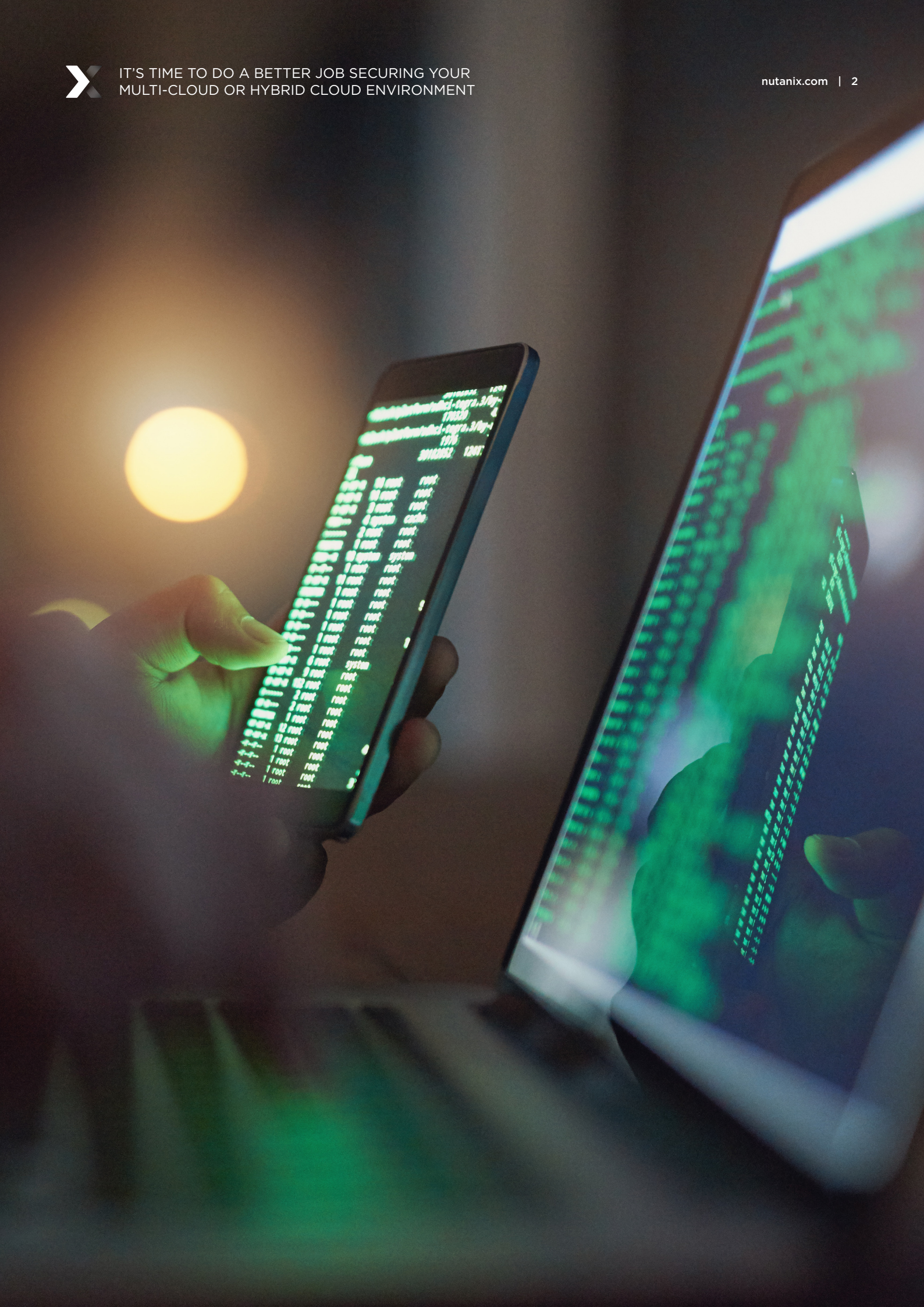
CXO FOCUS

IT'S TIME TO DO A BETTER JOB SECURING YOUR MULTI-CLOUD OR HYBRID CLOUD ENVIRONMENT

—

BY GENE KNAUER

NOVEMBER 2019



Cars and roadways have numerous safety features, yet if an inexperienced driver is behind the wheel, the chances for a mishap rise dramatically. Such is the case with public cloud, hybrid cloud, and multi-cloud environments. Security features are abundant, but when user errors lead to misconfigured cloud resources, data breaches and failure to maintain regulatory compliance can be the result.

Businesses are increasingly adopting multi-cloud architectures to benefit from the freedom to choose the appropriate cloud platforms for various workloads with differing requirements. But despite all of the great security features available from cloud providers, securing critical applications and data and staying in compliance with regulatory mandates requires an all-encompassing, automated approach that goes beyond human limitations.

2019: A Great Year for Hackers

By late summer, 2019 was already declared a banner year for hackers. According to the 2019 MidYear Data Breach Report, the first six months of 2019 have seen more than 3,800 publicly disclosed breaches, exposing 4.1 billion compromised records. 2019 has been called the worst year on record for data breaches.

Why is this happening?

One reason is that despite sophisticated, multi-layered security technology and services that are available on-premises and in clouds, using hybrid cloud and multi-cloud architectures has added to the complexity and number of separate technologies IT administrators have to manage. So it isn't surprising that by 2022, at least 95% of cloud security breaches are expected to be due to misconfigured resources, contributing to security vulnerabilities in public and private cloud environments, according to research by Gartner. >>

95%

By 2022, at least 95% of cloud security breaches are expected to be due to misconfigured resources

A Facebook-integrated app called "At the Pool" exposed over 22,000 user passwords through a backup in an Amazon S3 bucket that stored the passwords as plain text

In one case this year, email data from the medical device company Zoll Services, archived by a third-party service provider, was exposed during a server migration. That medical information included patient names, addresses, dates of birth, Social Security numbers, and more. In another case, over 108 million records of bets made at websites belonging to an online casino group were stored on a cloud storage server that hadn't been secured with a password. The database contained information about players' names, email addresses, home addresses, phone numbers, bets, wins, deposits, and withdrawals. The data left the players vulnerable to extortion schemes by hackers who had data on their wins and losses.

The targets of breaches and revealed vulnerabilities this year include governments, public and private corporations in a wide array of industries, and even large technology companies like Facebook via third-party apps that access user information. A Facebook-integrated app called "At the Pool" exposed over 22,000 user passwords through a backup in an Amazon S3 bucket that stored the passwords as plain text.

Automated, Cloud-Scale Security for all Your Clouds

Hurrah for organizations that are embracing public cloud, hybrid cloud, or multi-cloud architectures. You're enjoying tremendous benefits. But now it's time to re-evaluate your cloud security and to consider deploying more sophisticated, automated lifecycle management and security features that not only detect risks in real-time, but also help to fix them immediately.

Imaging being able to detect and fix security misconfigurations in near real-time across all cloud environments. Or gaining real-time visibility and control over the security health of all your cloud environments by automating hundreds of security audits — network, infrastructure, database, access, server, data — based on industry best practices. Or providing security risk posture tracking and proactive remediation of potential security blind spots via a single, multi-cloud security posture management solution regardless of what hypervisor you're using. Picture a recommendations engine that continuously helps your company improve your cloud infrastructure security posture.

All of these features are available today on cloud-scale management platforms.

108 million

Over 108 million records of bets made at websites belonging to an **online casino group** were stored on a cloud storage server that **hadn't been secured with a password**.

Automating Regulatory Compliance

Helping companies maintain regulatory compliance isn't an afterthought with these distributed, cloud-scale security platforms; it's integral. The same security platform tools to improve overall cloud security posture in multiple cloud architectures can be used to address very specific local and international security mandates across all of those clouds.

An API-driven app can run an array of security audit checks whenever an "event" happens anywhere within cloud domains. Events might include a cloud services configuration change, the onboarding of new users, or changes to compute instances. If the app detects infrastructure-level security issues, it alerts cloud security teams so they can react and fix the issue before the business is impacted. Event-driven detection of cloud security vulnerabilities is becoming absolutely critical in multi-cloud and hybrid cloud environments if the benefits of the cloud are to be enjoyed and security standards and mandates adhered to.

For example, a user accidently leaves a storage repository configured with global read/write permissions. The app detects the issue in real-time and alerts the user as soon as the storage resource is spun up, thereby protecting the data. Another example is the use of audits to check the security policies of virtual machines (VMs) or VMs that may be exposed to public or external IPs over TCP or UDP ports. The app checks to make sure that data encryption has been enabled or not and if there are too many users with admin privileges. It raises the alarm if something isn't right.

These cloud security and management platforms also include process, documentation, and configuration checks to ensure that the cloud environments follow mandated regulatory policies.

Many Clouds, Single Pane of Glass

Having a single solution to help you detect and remediate security issues across your company's multi-cloud or hybrid cloud environment in real-time is the way to go. And it's available. These platforms provide broad visibility, detection, remediation, auditing, and compliance features that quickly identify security risks and the steps to fix them before anyone outside of your IT department is the wiser.

KEEP UP TO SPEED
WITH THE LATEST CONTENT

NUTANIX.COM/CXO

POWERED BY

NUTANIX