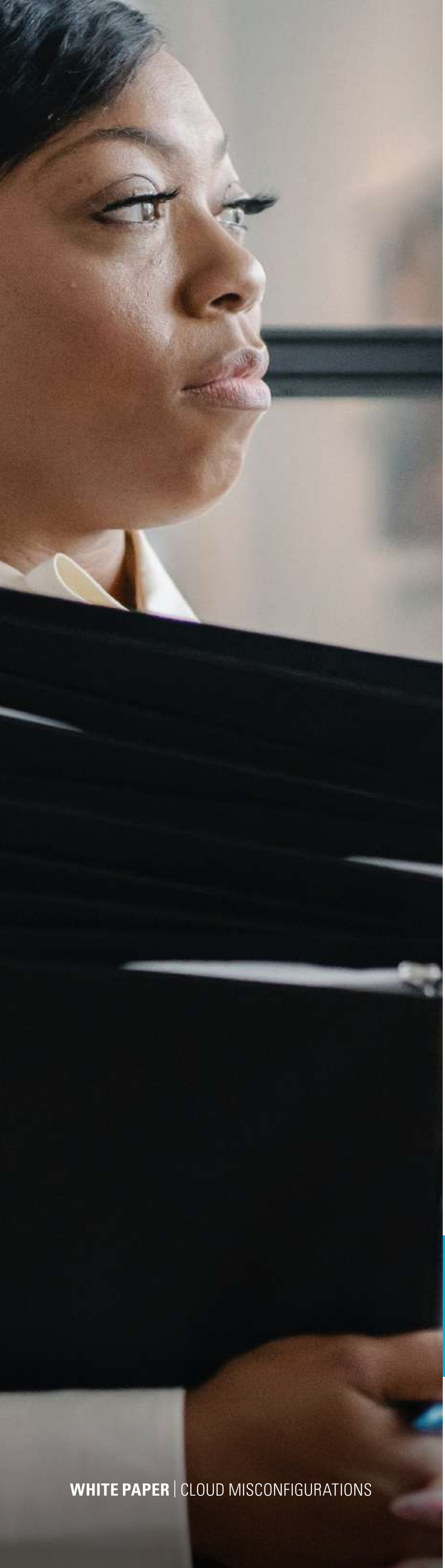
HOW TO OVERCOME CLOUD MISCONFIGURATIONS

IDENTIFYING CLOUD CONFIGURATION RISK FACTORS IN SaaS, INFRASTRUCTURE AND DevOps ENVIRONMENTS

MOTOROLA SOLUTIONS



EXECUTIVE SUMMARY

Organizations of all sizes find it challenging to implement security controls across their various cloud environments. In this white paper, we discuss configuration risk factors for cloud infrastructure, SaaS and DevOps and how to identify and prioritize them.

INTRODUCTION

Organizations are going through a transition in today's evolving technology landscape. The old information technology model has shifted sharply to a wide-open terrain of platforms and environments that can take businesses in any direction they want to go.

In particular, the cloud has changed the traditional technology business model. There are three core areas that have been disrupted: traditional software delivery (now turning into more of an "as-a-service" model), infrastructure delivery (now turning into more of a "infrastructure-as-a-service" model or IaaS) and the intersection between development and operations, known as "DevOps." There are security risks associated with each of these models.

The first model, Software-as-a-Service (SaaS), is often adopted by organizations without being sanctioned by the security team. Then there is cloud infrastructure, which is vital to any organization that is trying to build applications faster or deploy applications more efficiently. Finally, there are challenges associated with DevOps automating this infrastructure to help organizations move faster.

One of the biggest threats to cloud security is the misconfiguration of cloud platforms. In one recent survey, misconfiguration was ranked by organizations as the single biggest threat to public cloud security (62 percent). This is followed by unauthorized access (58 percent), insecure interfaces/APIs (52 percent) and hijacking of accounts (50 percent).[1]

In this white paper, we discuss specific risk factors for each of these models and how to prioritize these risks.

ONE OF THE BIGGEST THREATS TO CLOUD SECURITY IS THE MISCONFIGURATION OF CLOUD PLATFORMS.

CLOUD SECURITY CHALLENGES OVERVIEW

Most security professionals agree that cloud services themselves are secure. However, maintaining security best practices when using these services falls onto the organizations themselves.

What are some of the major challenges organizations face in maintaining these security practices?

Security teams struggle to apply the right controls across cloud environments largely due to a lack of understanding and a lack of visibility. This stems from non-security practitioners taking the lead on configuration steps.

Even large organizations with vast security expertise are having trouble implementing security controls across their various cloud environments. The scale and complexity can be daunting. Whether they are maintaining multiple cloud infrastructure or SaaS workloads, learning these new platforms and keeping up with the rapid flow of new features is challenging for any organization.

From a production standpoint, different business units do not want to take accountability for what is going on in individual production environments in the cloud. They view production environments as separate entities. For instance, what takes place in the research and development (R&D) production environment is R&D's responsibility.

However, compliance checks from auditors have created greater sense of urgency around testing and development of applications that is taking place in R&D's sandbox, the isolated computing environment software developers use to test new programming code.[2] That test data cannot be ignored, especially to maintain compliance with regulations like the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry (PCI), personally identifiable information (PII) and Human Resources (HR) information.

SOFTWARE-AS-A-SERVICE ACCESS CONFIGURATION CHALLENGES

Many organizations have adopted SaaS applications in some form or fashion to streamline their business processes and replace traditional on-premises applications. Often, the people using these applications are the administrators for the accounts, not the security team. These business professionals are buying the applications; they are not federating these applications out of a directory. Their focus is creating and managing individual user accounts.

One of the key challenges organizations face with user accounts is controlling access when employees leave a company. For instance, many organizations do not have policies in place to govern when access to critical applications is denied.

Another major challenge companies face is gaining visibility into potential account takeovers. Applications sit outside of the network, so it can be difficult to maintain control of these environments. There is not a traditional firewall around these environments to indicate when someone is logging in from a different country or a different location.

When there is an alert for potential account takeover, it is more likely that the account credentials of these applications have been compromised in some other way. However, if individuals have used a different site maliciously or from a different location, it is difficult to determine the source since the device is not sitting inside of an organization's network under tighter security controls.

The final risk factor to be aware of is users integrating their SaaS applications with other applications. For example, the sales teams may be entering their Office 365 credentials into customer relationship management (CRM) applications like Salesforce or sales-enablement applications. Other examples of SaaS applications that could create integration challenges include Box, G Suite, ServiceNow and Dropbox.

OFFICE 365

The most popular cloud app of 2019.[3]

57%

Percentage of respondents who say their organization uses multi-factor authentication to secure access to data in the cloud environment.[4]

Many security executives said they are hesitant to adopt software as a service (SaaS) in some critical domains due to potential cybersecurity risks.[5]

CLOUD INFRASTRUCTURE CONFIGURATION CHALLENGES

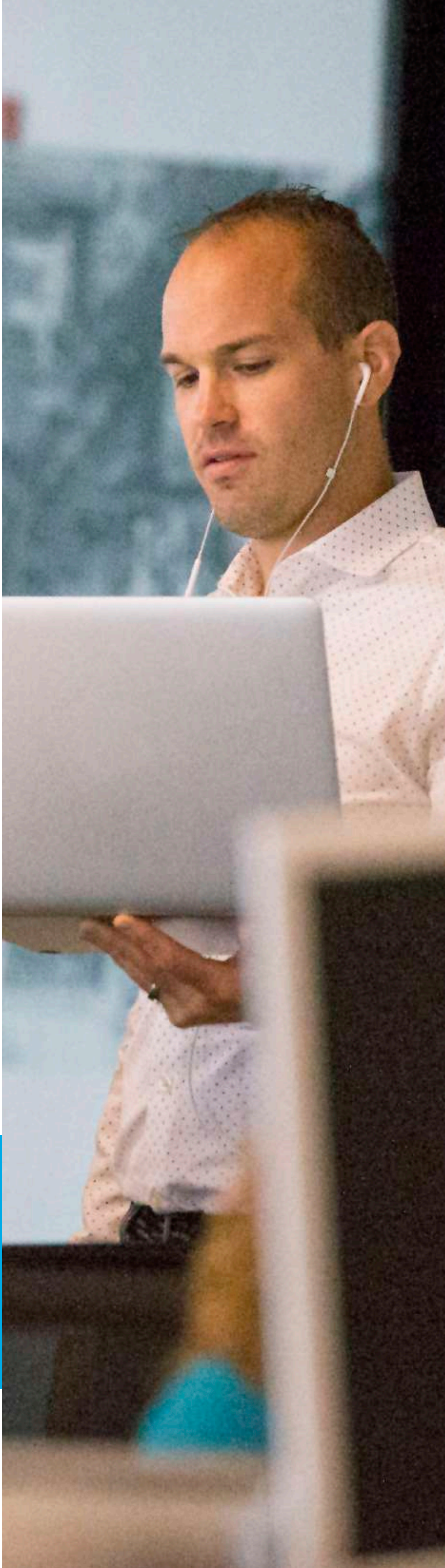
The second cloud model, cloud infrastructure, is structured around workloads running on Amazon Web Services (AWS), Microsoft Azure or Google Cloud, in most cases. The interesting part about cloud infrastructure management is that developers are taking the lead. They do not need IT anymore to deploy new servers. They can take code and start writing it as a Lambda process (a serverless method to run code) in AWS without any infrastructure or administration whatsoever, for example.

What is concerning is that not only are these processes not sanctioned by security teams, the R&D team are typically configuring these environments on their own. They are not security professionals, yet they are spinning up workloads daily at an accelerated rate.

It is not typically the production environment itself that causes issues for organizations. Issues arise when the R&D group wants to run through tests in the production environments and they end up making the data world-accessible. They fail to realize that if they do not secure those machines, the data will get breached. In these instances, it is more of an issue of the R&D team not properly following configuration steps versus the full production environment not being secure.

Getting visibility into these environments can also be difficult because the teams create multiple AWS accounts or organizational structures and they do the same thing on the Azure site with subscriptions. For instance, they could end up with five or six different groups to manage and maintain control over. Organizations often struggle to understand where all of the new development is coming from.

Machine-to-machine communication is another major challenge that comes up for cloud infrastructure security. Organizations must determine how many applications they need to use. Typically, there are multiple services interacting with each other that provide value to an application. What that means is that users are authenticating across machines. It is not a single person who is handling the authenticating; they are authenticating on users' behalf into multiple systems. It is important for security teams to understand that the inner workings of this workflow, which is why monitoring machine-to-machine communication is a real challenge.



1K

Number of insurance policy holders exposed when AgentRun's Amazon AWS S3 storage bucket wasn't password protected[6]

3.2 MILLION

Number of files left exposed at Los Angeles non-profit on an unsecured AWS S3 bucket[7]

33%

Percentage of cybersecurity professionals that are struggling with visibility into infrastructure security[8]

4 WAYS THAT CLOUD SECURITY CAN IMPACT ORGANIZATIONS

Organizations need to pinpoint the risk of cloud breaches and security incidents in four critical areas:

DATA LOSS

First and foremost, data can be stolen or exposed. Clearly, businesses handle plenty of sensitive information and this information is moving to the cloud. In many cases, breaches occur because data has been exposed to the public or it becomes accessible through a configuration error. The loss of data has a domino effect if confidentiality and privacy terms are violated.

DATA INTEGRITY

Secondly, data in the cloud can be manipulated. Many workloads that get moved to cloud environments require a lot of processing, such as large catalogs or pricing data or customer information. This is data that directly influences decision-making. If someone tampers with that data, it can have a direct impact on business performance. For instance, if pricing data is changed in an e-commerce environment, there can be a residual impact on profitability.

DATA AVAILABILITY

Ransomware is a perfect example of a threat that can compromise data access and impair overall availability if downtime occurs. Ransomware does not only impact work stations, though. It can get into cloud environments and encrypt storage buckets, preventing users from gaining access to critical data.

RESOURCE ABUSE

Managing all the workloads in a cloud environment (or environments) is a complex process. There can be many people who have legitimate access to these environments to turn on different resources. What if an employee went rogue and realized they could make extra money by running workloads in a different environment that is not monitored closely? For example, in the case of a cloud data breach that impacted Tesla, a Model S owner accessed one of the company's AWS accounts and built a cryptocurrency mining rig in his electric car.[9] These individuals do not have to be internal staff – it can be a contractor. In fact, more and more contractors are gaining access to privileged accounts because companies need added expertise or to complete time-sensitive projects. However, they also gain access that can be used to abuse resources.

DevOps CONFIGURATION CHALLENGES

The final model that deserves plenty of attention is DevOps, which includes tools such as Jenkins, Splunk, Kubernetes and GitHub. DevOps is largely a new model for automating the production infrastructure at a faster rate than traditional software development and infrastructure management practices. In these environments, production workloads are orchestrated. When deploying a new application, rather than users logging in to that machine with privileged access management or putting patches on it, a new gold image can take its place.

Still, from a security standpoint, even if those individual touchpoints are removed, security teams need credentials to interact with these machines. Organizations require an orchestration console that provides access keys or the ability to turn machines on or off, affecting network resources.

Moreover, DevOps teams need to understand how the orchestration works because many service accounts use orchestration tools. They also need to make sure default passwords are updated. Oftentimes, that's where the configuration issues arise.

In DevOps, resources often get turned up and down. For example, DevOps teams may not have to deal with a traditional server that is driving the resources – it could be a Lambda set of code in AWS that individuals need to understand. This is a new world in security that introduces a new set of issues. Since Lambda offers a serverless approach, developers can simply upload their code to AWS without having to provision a server. In these instances, developers are not exactly following the soundest coding practices and they can sidestep steps like patching the OS. The smallest of code errors can quickly escalate into a security liability.

SUMMARY

The 2020 Flexera State of the Cloud survey on cloud security trends shows cloud has become mainstream. More than half of the organizations surveyed (53 percent) said they use cloud heavily and have reached the advanced cloud maturity level. Thirty percent are at the intermediate level with apps running in the cloud.

As cloud adoption continues to accelerate, cloud configuration errors will remain a central issue that organizations must confront and ultimately overcome if they want to get the most out of their cloud capabilities. Without sound configuration practices in place, companies will continue to leave themselves vulnerable to risk factors that can expose their data and open the door for abuse of privileges and resources. With the lessons learned in this white paper, security teams will stand a better chance to help their organizations take a shared responsibility approach to protect their SaaS, cloud infrastructure and DevOps environments.

65%

Percentage of IT professionals saying they plan to deliver 10 or more apps and 38% planning to deliver 25 or more apps in 2019[10]

50%

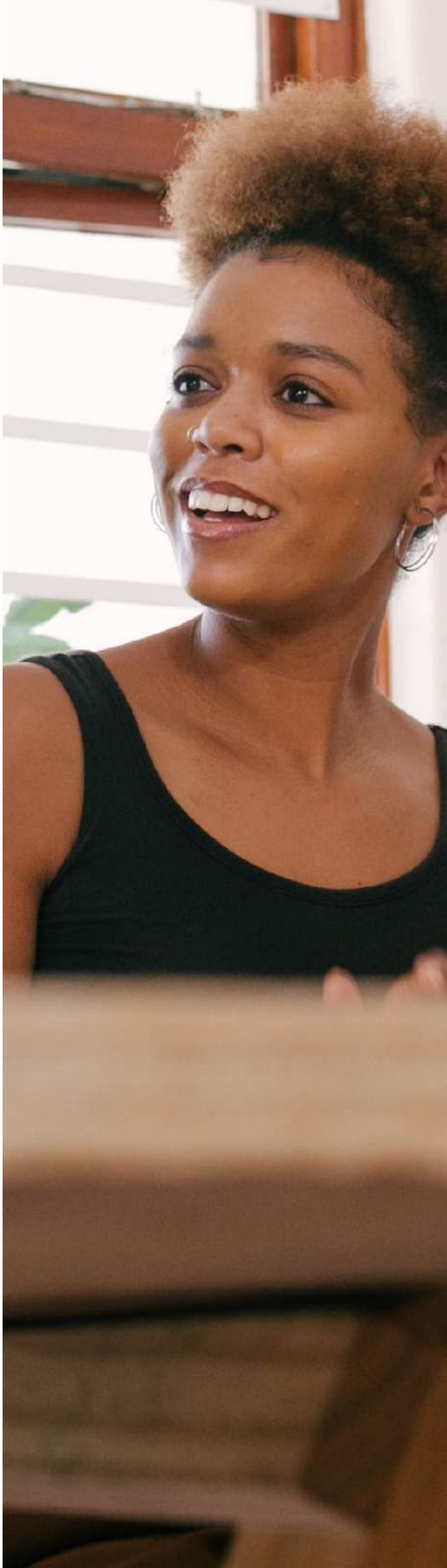
Percentage of AWS customers who did not ever use the built-in AWS CloudTrail service for DevOps[11]

50%

of AWS Users have adopted Lambda[12]

CLOUD SECURITY GLOSSARY

- **Amazon Web Services (AWS):** a subsidiary of Amazon.com that provides on-demand cloud computing platforms to individuals, companies and governments.[14]
- **AWS Lambda:** AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second.[15]
- **Google Cloud:** a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products, such as Google Search and YouTube.[16]
- **Machine-to-Machine (M2M) Communication:** used for automated data transmission and measurement between mechanical or electronic devices. The key components of an M2M system are: Field-deployed wireless devices with embedded sensors or RFID-Wireless communication networks with complementary wireline access.[17]
- **Microsoft Azure Cloud:** a cloud computing service created by Microsoft for building, testing, deploying and managing applications and services through a global network of Microsoft-managed data centers.[18]
- **Multi-Factor Authentication (MFA):** a security mechanism in which individuals are authenticated through more than one required security and validation procedure.[19]
- **On-premises applications:** on-premises is the software and technology that is located within the physical confines of an enterprise as opposed to running remotely on hosted servers or in the cloud.[20]
- **Ransomware:** a subset of malware in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access returned to the victim.[21]
- **Sandbox:** isolated computing environment software developers use to test new programming code.[22]
- **Security Operations Center (SOC):** a facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis.[23]
- **S3 bucket:** Amazon Simple Storage Service (S3) is storage for the Internet. It is designed to make web-scale computing easier for developers.[24]
- **World-readable storage:** files on a file system that can be viewed (read) by any user.[25]



TRUSTED CYBERSECURITY SERVICES

Motorola Solutions Cybersecurity Services bring together an integrated portfolio aligned to the National Institute of Standards and Technology (NIST). As a trusted business partner, we help you develop roadmaps to safeguard your information, employees and systems.

With more than 90 years of experience managing mission-critical technologies and more than 20 years of developing cybersecurity solutions, Motorola Solutions is well-positioned to be the ‘one service provider’ for your cybersecurity needs.

With best-in-class people, process and technology we bring scalable operations that can help organizations manage cyber risk awareness, detection, response and recovery. Our cutting edge security automation and orchestration platform delivers 24/7 insights on security management, system performance and service delivery, enabling a 100 percent co-managed approach to security management.

We provide a purpose-built and integrated approach to end-to-end resilience.

SOURCES:

[1] 2020 Cloud Security Report, Cybersecurity Insiders

[2] Definition of Sandbox, TechTarget,
https://searchsecurity.techtarget.com/definition/sandbox

[3] Okta 2020 Businesses at Work
https://www.okta.com/businesses-at-work/2020/#most-popular

[4] 2019 Global Password Security Report by LastPass

[5] Securing software as a service,
https://www.mckinsey.com/business-functions/risk/our-insights/securing-software-as-a-service#

[6] Insurance Startup Leaks Sensitive Customer Health Data, ZDNet,
https://www.zdnet.com/article/insurance-startup-leaks-sensitivecustomer-health-data/

[7] 3.2 Million Files Revealed on AWS S3 Bucket, InfoSecurity Magazine,
https://www.infosecurity-magazine.com/news/3-2-million-files-revealed-on-aws/

[8] 2020 Cloud Security Report, Cybersecurity Insiders

[9] Tesla Cloud Resources are Hacked to Run Cryptocurrency-Mining Malware, Ars Technica,
https://arstechnica.com/informationtechnology/2018/02/tesla-cloud-resources-are-hacked-to-runcryptocurrency-mining-malware/

[10] The State of Application Development, 2019/2020, OutSystems

[11] The Dev-Ops Adoption: A Clear View on the State of Affairs, Hackernoon

[12] State of the Serverless https://www.datadoghq.com/state-of-serverless

[13] Cloud Computing Trends: 2020 Flexera State of the Cloud Report

[14] What is AWS, Amazon Web Services,
https://aws.amazon.com/what-is-aws/

[15] Amazon, “What is AWS Lambda?”
https://docs.aws.amazon.com/lambda/latest/dg/welcome.html

[16] What is Google Cloud, Google Cloud,
https://cloud.google.com/what-is-cloud-computing/

[17] Machine-to-Machine Communication Definition, Gartner IT Glossary

[18] What is Azure, Microsoft Cloud Services,
https://azure.microsoft.com/en-us/overview/what-is-azure/

[19] Multi-Factor Authentication Definition, Techopedia

[20] What is On-Premises, Webopedia,
https://www.webopedia.com/TERM/O/on-premises.html

[21] Ransomware Definition, SearchSecurity

[22] Definition of Sandbox, TechTarget,
https://searchsecurity.techtarget.com/definition/sandbox

[23] Security Operations Center (SOC) Definition, Digital Guardian

[24] What is Amazon S3?”Amazon,
https://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html

[25] World readable definition, Juniper Systems,
https://www.juniper.net/documentation/

Learn more at: motorolasolutions.com/cybersecurity

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**