UNDERSTANDING THE CHALLENGES OF CLOUD MONITORING AND SECURITY

HOW TO GET VISIBILITY INTO YOUR CLOUD INFRASTRUCTURE AND ENTERPRISE SaaS APPLICATIONS

WHITE PAPER | CLOUD MONITORING

MOTOROLA SOLUTIONS

EXECUTIVE SUMMARY

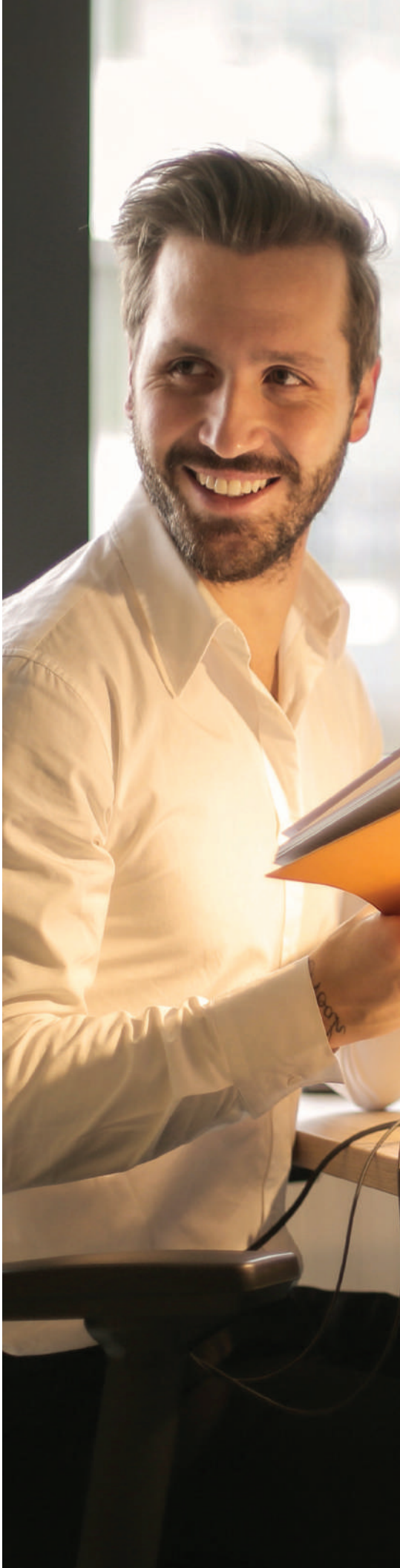
Although the benefits of moving to the cloud are clear – accelerated time to market, faster access to infrastructure, improved availability and business continuity – it presents new and unique security challenges. While cloud provider platforms are generally secure, each organization is ultimately responsible for properly configuring their own security controls to protect their data, applications and cloud infrastructure.

INTRODUCTION

With more than 97 percent of companies now using the cloud, more IT budgets and resources than ever are being dedicated to cloud solutions. Additionally, close to 50 percent of US government organizations are actively using cloud services, according to Gartner. Although the benefits are clear, moving to the cloud comes with new and unique security challenges.

In this white paper, we discuss key issues facing IT and information security professionals, including why cloud security requires a new approach compared to the traditional on-premises approach. We also examine how the cloud is being adopted across different industries; factors driving the cloud movement; what older cloud models looked like; how newer models have impacted business and security; and how organizations are adapting to these challenges.

While the concept of "single pane of glass" monitoring is ideal, we examine what that entails and the challenges involved in getting there. To conclude, we provide several real-world examples that illustrate the value of cloud access monitoring.



WHY COMPANIES ARE MOVING TO THE CLOUD

Cloud services are being used by 97 percent of organizations worldwide and, on average, 27 percent of IT security budgets are being allocated to cloud security.[1] Close to 50 percent of US government organizations are actively using cloud services.[2] Additionally, overall use of cloud services spiked 50 percent between January and April 2020, largely due to the COVID-19 pandemic and the shift to remote work.[3]

Whether through public, private or hybrid cloud deployments, some – if not most – corporate data is being hosted across multiple clouds. That includes sensitive data such as Protected Health Information (PHI), Social Security numbers, trading information and more.

Scalability and availability are two central reasons why organizations are moving to the cloud. By operating in a cloud environment, it is more feasible for organizations to scale back on operating expenses. In addition, given more availability and scalability, companies do not need to design their own internal network. Fully redundant circuits, servers and failover systems are expensive. In contrast, when one considers the cost benefit of pushing some of those critical systems into the cloud and adding those features that would otherwise have to be designed into an internal network, it can make a lot of sense to make the leap to the cloud.

An additional benefit of moving information to the cloud is reducing the amount of data that comes into the internal data center. With less back-and-forth traffic coming into the data center, organizations can scale back their data center storage requirements.

While a cloud environment can deter the number of attacks on internal networks, organizations need to continue to be vigilant, ensuring they are configuring their security controls properly to protect their data, applications and cloud infrastructure.

In addition, since the cloud provider takes over the day-to-day responsibilities of ensuring that the infrastructure stays up and running, employees can work on other projects. Taking some of IT's tasks and pushing them to the cloud provider enables teams to focus on other, more important tasks.

DRIVERS OF CLOUD-BASED SECURITY SOLUTIONS[4]

WHAT ARE THE MAIN DRIVERS FOR CONSIDERING CLOUD-BASED SECURITY SOLUTIONS?

41%

Faster time to delpoyment and cost savings

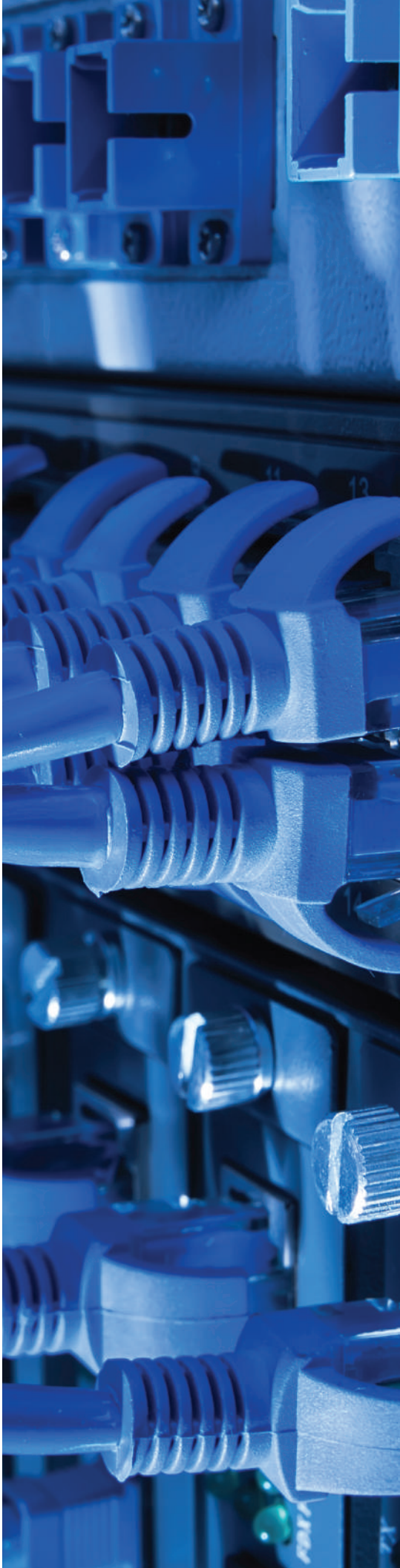
WHY CLOUD MONITORING REQUIRES A NEW APPROACH

The old cloud model focused on brick-and-mortar data centers. These were in-house data centers within companies' networks and buildings, or hosted at an offsite location in an outsourced data center model. It was concentrated between those two models, looking "inside the four walls." Being able to detect outside threats was the primary concern. If companies deployed a monitoring solution, it would monitor firewalls and endpoint protection, on their own internal servers. As those monitoring capabilities began to mature, companies could get better visibility into their data center.

Shifting from the old model to storing critical data in the cloud requires a new approach. It is important to remember that any server that is in the cloud and Internet accessible will have the same issues if it were in the cloud. Therefore, security professionals must carefully consider how they will monitor that data.

For example, there is a wealth of information that can be compromised in an email box. File transactions are another common process. Another example is bulk file transfers of sensitive information between organizations and their partners. In the past, they might have used File Transfer Protocol (FTP) or SSH File Transfer Protocol (SFTP) servers to handle secure transactions to move these files, but now that work may be pushed to the cloud.

In the new cloud model, corporate social media accounts should also be considered as an extension of the network. If an organization's corporate accounts were compromised and someone were to send out inappropriate posts, it could be very damaging.



MONITORING LOGS ACROSS THE CLOUD

The cloud model is part of the organization's overall infrastructure. Cloud providers are responsible for the core platform, but not for what organizations choose to deploy on it. While some of the larger providers may shut down malicious or dangerous behavior on their network, for the most part, organizations are generally free to operate as they like to meet business needs. However, corporate policies and regulatory requirements (Payment Card Industry Data Security Standard or PCI DSS, Health Insurance Portability and Accountability Act or HIPAA) still apply to all the systems deployed in the cloud. That includes any level of data retention, data protection or server system monitoring.

As more cloud services are added to the primary services, greater visibility is needed across the entire cloud environment. For instance, an organization may be using a Software-as-a-Service (SaaS) helpdesk solution like ServiceNow, a SaaS mobile management solution like AirWatch, a SaaS productivity suite like Office 365 and a SaaS HR solution like Workday. They may all be tied into a cloud presence, such as a federated Microsoft-centric model. Through cloud monitoring, organizations can view the logs and data associated with these environments.

When it comes to log monitoring, there are many different layers and levels to track. In Amazon Web Services (AWS), for instance, the first level is known as AWS CloudTrail logs. Through monitoring CloudTrail logs, organizations can get better visibility into their AWS presence and account activity. They can track who is logging in to manage the AWS account, who is creating instances, who is terminating instances and who is changing Virtual Private Cloud (VPC) firewall rules. This is important to monitor because there are costs associated with each instance that is deployed.

Virtual Private Cloud logs enable security teams to monitor the cloud equivalent of their firewalls. They can track data flows to and from different instances, determine whether these instances have succeeded or failed and conduct triage as needed. CloudTrail logs certainly offer deeper visibility, but they do not tell the whole story. Whether cloud providers are running a Windows Virtual Machine (VM) or Linux VM instance, there are still traditional instances running in the cloud that generate logs. To get the same level of visibility as they do from in-house systems, organizations must also monitor those logs.

ORGANIZATIONS STILL NEED TO KNOW WHO IS MONITORING THEIR CRITICAL SERVERS AND CUSTOM APPLICATIONS THEY HAVE MIGRATED TO THE CLOUD. ALTHOUGH THE CLOUD PROVIDER IS SUPPLYING THE PLATFORM, THE SERVERS AND DATA STILL BELONG TO THE ORGANIZATION. THEREFORE, THE ORGANIZATION IS RESPONSIBLE IF THAT DATA IS COMPROMISED.

CLOUD BUSINESS IMPACT

HOW ORGANIZATIONS ARE ADAPTING TO SECURITY CHALLENGES

While cloud providers offer many security measures, organizations are ultimately responsible for securing their own data, their own applications and their own services in the cloud. That hasn't changed. Security teams need to know that they are responsible for providing the same level of attention to their data in the cloud as they would if it were on-premise. In fact, once they adopt the cloud, the cloud becomes a part of their infrastructure. Corporate and regulatory requirements still apply.

How are organizations planning to handle their security needs when they move to the cloud? A cloud research study indicates that 61 percent of organizations that have adopted a cloud model are either training or certifying their IT staff to manage cloud security.[6] This means 39 percent of the other organizations are finding another solution, whether through partnering with a managed security services provider that can consolidate security software from independent vendors or hiring employees who already understand cloud security. Approximately one-third of respondents said they were planning to do a combination of both.

It is clear from the data that many organizations realize they cannot manage everything in the cloud and need additional help. Security teams need to know that they are responsible for providing the same level of attention to their data in the cloud as they would if it were on-premise. In fact, once they adopt the cloud, the cloud becomes a part of their infrastructure. Corporate and regulatory requirements still apply.

With all of that in mind, building the cloud presence into the overall IT infrastructure drives the need for a new approach. Many organizations wonder if they can get the same level of log detail from the cloud as they did when they managed the system 100 percent. Even though there are detailed logs from the cloud, a dedicated team needs to watch and understand them.

Organizations are beginning to recognize the limitations of current solutions and trying to solve the monitoring gap. For example, some of the cloud solution APIs are very new. If the API is not available, an organization cannot pull the data, and if they cannot pull the data, they cannot monitor it. Once the APIs become available, organizations must often play catch up to get back up to speed and get all the moving parts together. Next, they must go into a change management cycle before the next product release. All of this takes time, which means it can take a while to see the benefits of moving to the cloud.

What can organizations do to address this? There are generally three choices: manage it in-house, use monitoring tools offered via cloud providers or partner with a professional services provider. Each option has its own set of challenges and questions. If monitoring is brought in-house, it may require a new product to be integrated, with a costly learning curve. If the product doesn't support all the cloud providers an organization uses, who will be responsible for either developing the modules to monitor them, or will there be a gap?

If it is done in-house, does the organization have the development team that can help, or will the IT staff be savvy enough with the monitoring product to be able to roll their own? If the API changes, who will be responsible for making sure monitoring continues to work as desired and to fix it if it breaks?

The third choice is to partner with an MSSP that is focused on integrating cloud monitoring. Because MSSPs do this regularly, and interact with cloud platforms and applications daily, they can quickly adapt and add new services as needed. Additionally, MSSPs can do this more cost effectively, with a higher degree of expertise, than most organizations.

PATH TO STRONGER CLOUD SECURITY[5]

WHEN MOVING TO THE CLOUD, HOW DO YOU HANDLE YOUR CHANGING SECURITY NEEDS?

61%

train and/or certify current IT staff

58%

use cloud provider security tools (e.g., Guard Duty in AWS)

30%

deploy security software from independent software vendor(s)

SINGLE PANE OF GLASS

WHAT IT MEANS AND CHALLENGES GETTING THERE

"Single pane of glass" monitoring means being able to look through a unified display to see what's happening in an organization's infrastructure, regardless of whether it is in-house or in the cloud. Seeing everything in one view is especially challenging in the new cloud model because data is stored between two environments. Ideally, both cloud and on-premises logs are going to the same security information and event management (SIEM) for a single view.

When data is moved to the cloud, it is not always a one-to-one move. Sometimes additional information is gleaned from the cloud that would not have been detected if the information was kept in-house. If there is any information that is unique to cloud monitoring that can be useful from a security perspective, either to help quantify events or make better security decisions when companies see events come in, that can be useful as well.

One of the benefits from a monitoring perspective is that gaps may show up in the log that wouldn't have been easy to see previously. Using cloud applications, employees can access information from anywhere in the world. Logs from these applications can show IP addresses and where people are connecting from because they're not going through the usual network firewalls and intrusion prevention systems.

REAL-WORLD EXAMPLES

MAKING THE CASE FOR CLOUD MONITORING

MONITORING MICROSOFT

For one company, monitoring access to Microsoft solutions was becoming increasingly complex. Although the Microsoft summary page offered some data, Motorola Solutions analysts captured more detailed information to show activity from employees logging into Microsoft Exchange, Office 365 and OneDrive. Using a single API offered more unified logging: instead of monitoring Microsoft Azure or Office 365 separately, these processes were combined into a comprehensive view.

Through a single interface, the business could see where people were connecting from, what the accounts were, who had accessed what data and when they logged in to various applications. They could also monitor access to SharePoint, including who uploaded and downloaded files within that environment. By monitoring all these access points, the company was better able to determine where the gaps were in their processes and policies and take immediate steps to remedy them.

MONITORING GEO PATTERNS

When Motorola Solutions analysts began monitoring a U.S. company's Microsoft Exchange account, the geographic data was one of the streams that was closely observed. Some of the metadata monitored included not only the contents of the logs, but other metadata, such as geo-fencing and the geographic data, which enabled the company to see any unusual activity.

In one instance, a user logged in from Kuwait, which raised some alarms. After investigating this anomaly, the company determined that the login was from a current employee working on a legitimate assignment. The company also saw many additional attempted logins from other countries, however, after further investigation, determined that they were from threat actors.

MONITORING AMAZON WEB SERVICES

In another instance, Motorola Solutions analysts began monitoring VPC logs from an Amazon instance for a U.S. company. The analysts could see a lot of traffic hitting SSH services that, for some reason, were exposed to the internet on one of the company's machine instances. This, of course, raised concerns as it was clearly someone with bad intentions trying to get into the SSH. After further investigation, it became clear that threat actors were trying to hit the root account or a blank named account. In this instance, the company quickly took steps to address the threat and ensure their systems were well-secured.

In many instances, it can take mere hours between a cloud service being deployed before threat actors find it and begin executing dictionary attacks using thousands of passwords. If an IP address is blocked, threat actors simply find another IP to use.

SUMMARY

The cloud movement is here to stay. Organizations that have not adopted the cloud yet will likely do so in the not-so-distant future. However, patience is essential for determining how to incorporate the cloud into an existing IT infrastructure. From a security perspective, cloud providers do not handle the implementation of in-house security policies and procedures, because it is impossible to implement each client's unique policies and procedures.

Ultimately, organizations are responsible for maintaining their cloud security. This means monitoring and rolling out policy requirements to the cloud that are within the company structure to ensure data is secure.

Lastly, it is important that organizations carefully evaluate which monitoring solution to deploy. Choosing a monitoring solution can be challenging and should be driven by an in-depth consideration of what your organization needs. Many organizations have found that partnering with a company that specializes in cloud security monitoring and has their best interests in mind can help them find and deploy the best solution for their needs.

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] Navigating a Cloudy Sky: Practical Guidance and the State of Cloud Security, McAfee. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-navigating-cloudy-sky.pdf

[2] Gartner

[3] Cloud Adoption and Risk Report, Work From Home Edition, McAfee. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-carr-wfh.pdf

[4] 2020 Cloud Security Report, Cybersecurity Insiders.

[5] Id.

[6] Id.

Learn more at: motorolasolutions.com/cybersecurity

MOTOROLA SOLUTIONS

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

CLOUD INTEGRATION

CHALLENGES AND SOLUTIONS

CHALLENGES

- Every cloud provider defines their own API
- Most (but not all) use OAuth and return JSON data
- Lack of log standardization, as log information and format is different for each cloud provider
- Some APIs are very new and evolving faster than developers can keep up

SOLUTIONS

- Evaluate in-house solutions that can also integrate cloud solutions
- Write your own modules
- Use the cloud provider's tools in the cloud
- Pick an outside partner or MSSP that is focused on integrating cloud monitoring