REDSCAN
A KROLL BUSINESS

Redscan e-book

How to successfully build a cloud security monitoring strategy

2020 Computing Security Awards WINNER

SC 2020 awards highly commended

CYBER SECURITY EXCELLENCE AWARDS WINNER 2020

teiss Awards2020 WINNER

Cyber Security Awards Winner 2019

Contents

1. Introduction

The importance of cloud monitoring

If, like many others, your business is migrating an increasing number of workloads to the cloud, security considerations should never be far from your thoughts.

The benefits of leveraging cloud infrastructure and services are well-documented. However, if not managed correctly, these can significantly increase cyber risk.

Cloud computing broadens the available surface for cybercriminals to attack, making it harder to protect your estate against the latest threats. The recent shift to support remote working means that assets are also more readily accessible and exposed than ever before.

Guidance to improve your resilience

Given the substantial increase in cloud breaches, it is clear that protecting critical assets cannot be achieved with preventative controls only. Enhancing your cyber resilience now also requires the ability to quickly detect and respond to threats which could bypass your defences.

Achieving the monitoring capabilities required to identify the latest adversarial tactics, however, can be a challenging prospect. Evolving threats and cloud architectures mean that there is a lot to consider.

This e-book outlines the key factors to think about when planning your strategy and the steps you can take to improve overall monitoring success.

Cloud security statistics

- Nearly 80% of companies have experienced a cloud data breach in the past 18 months.

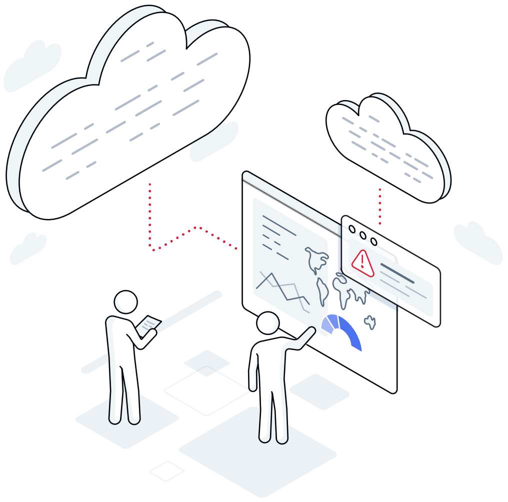
  Source: IDG

- 87% of IT professionals fear that a lack of cloud visibility is obscuring security threats to their organisation.

  Source: Dimensional Research

- 93% of cyber security professionals say they are moderately to highly concerned about public cloud security.

  Source: Synopsys



2. Why proactive monitoring is essential

How quickly can you detect and respond to cyber attacks?

Protecting on-premises and cloud workloads against the latest cyber security threats is a continuous task. With more exposures than ever to keep on top of, as well as more skilled attackers to exploit them, proactive threat monitoring is now considered essential to enhancing resilience.

At some stage, threats may evade your organisation's defences – the challenge now is to identify how quickly you can detect and respond to them to minimise potential damage and disruption.

Evolving approaches

Approaches to monitoring on-premises and cloud environments differ greatly, influenced by contrasting architectures and technologies. When it comes to the cloud, strategies can also be influenced by cloud deployment and services models.

Devising a strategy that is flexible enough to meet your needs, both now and in the future, is key.

87% of enterprises have adopted a hybrid cloud strategy

Source: Flexera

3. Common cloud detection use cases

Considerations for security monitoring vary widely between cloud and on-premises environments. With employees accessing cloud infrastructure and services remotely, the definition of the corporate network is evolving. Users are now being granted direct access to cloud-hosted systems, often via unsecured and unmanaged internet connections.

To better secure cloud environments, organisations have begun adopting elements of zero-trust networking. This shift changes the use cases that organisations need to focus on for effective security monitoring.

Five high-level cloud use cases are outlined below.

3.1. Privileged account access

Broadly speaking, detections for cloud environments need to focus more on Identity and Access Management (IAM) and Privilege Access Management (PAM), placing more importance on anomalous user behaviour and credential abuse.

Phishing attacks targeting remote workers are increasingly sophisticated and, without proactive monitoring, there is a risk that users could fall victim to attacks. Having comprehensive visibility of who is accessing your information and why is vital.

Suspicious activities to identify include:

- Account access from unexpected regions or unknown IP addresses
- Credential abuse attacks, e.g, password stuffing, password spraying and bruteforce attempts
- Use of unknown applications and services
- New and modified infrastructure, indicating resource abuse

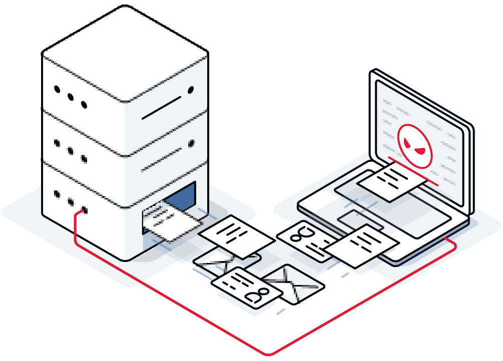
3.2. Data exfiltration

Cloud environments often process a wide range of sensitive information. Given the nature of the cloud, this data is likely to be highly accessible, putting it at greater risk of falling into the wrong hands. Maintaining confidentiality of data on these platforms is critical.

Data exfiltration use cases should identify the confidential or unknown data leaving your organisation's cloud environments. System monitors should also account for situations where cloud services may act as a conduit for exfiltrating data from on-premises environments as attackers can use these services to circumvent detection.

Behaviour-based analytics can help to identify and block suspicious activity, including:

- File downloads via anonymous users or APIs
- Large volumes of data being transferred via non-standard protocols, ports or policy groups
- Unauthorised use of file sharing sites such as Dropbox, Box, iCloud and Google Drive
- Data re-classification of marked sensitive documents before a download and/or export operation



80% of organisations say they are unable to identify excessive access to sensitive data in IaaS and PaaS environments.

Source: IDC

3.3. Suspicious network connections

Monitoring your networks for SQL injection, Command and Control (C2) communications and other indicators of compromise should be imperative, regardless of where your environments are located.

However, doing so within a cloud native environment poses additional challenges. Most cloud services leverage encryption protocols (like SSL), making traffic inspection and analysis harder. Because attackers are savvy about this, the number of attacks which leverage encryption protocols to obfuscate activity is increasing.

Suspicious network activity that can be observed includes:

- C2 and/or botnet activity
- Malicious code execution (such as SQL injection)
- Privilege escalation and elevation
- Unusual data flow to and from devices

3.4. Man-in-the-cloud attacks

Man-in-the-cloud attacks work by compromising authentication tokens held on an endpoint. Legitimate tokens are replaced with tokens which will instead direct users to the attacker’s own infrastructure where they are able to harvest credentials and steal data. This form of attack is usually executed via spear phishing and can be very hard for users to detect.

To enhance identification of the latest man-in-the cloud attacks, consider integrating your detection controls with SSL decryption tools and Cloud Access Security Brokers (CASB). Cloud security monitoring can help to detect evidence of token tampering and data interception by identifying:

- Anomalous DNS traffic
- Connections to unknown cloud instances
- Evidence of website domain impersonation
- Signals relating to process injection

3.5. Unsecured storage containers

Poorly secured cloud storage buckets and databases which lack authentication or authorisation protocols are a well-recognised source of data breaches.

Monitoring, managing and governing the configuration of these cloud resources, and having mechanisms in place to alert and take actions when misconfigurations are identified, is crucial to protecting your data and assets.

Cloud security monitoring can help to ensure that your organisation doesn't unknowingly expose assets by identifying:

- Misconfigured policies and security groups
- Large and unexpected amounts of incoming and outgoing data
- Indicators of API abuse
- Containers and storage buckets with 'risky' configurations

95% of cloud breaches are due to human error

Source: Gartner

4. Key considerations when building your monitoring strategy

There’s a lot to consider when developing and executing your monitoring strategy. If poorly conceived and implemented, it could fail to provide the level of threat detection coverage and visibility you need to comprehensively protect critical assets.

To better understand what’s required, some of the key aspects to factor in as part of your planning are outlined below.

4.1. Cloud, asset and data discovery

A key first step in planning security monitoring is to gain a complete understanding of the environments in use across your organisation, as well as the systems and data that reside within them.

Fully scoping your digital footprint is vital and can help to identify environments that have fallen out of use and could be targeted without anyone noticing.

4.2. Technology selection

It’s important to ensure that you have the right technology in place to fully monitor and respond to threats across on-premises and cloud environments. A good starting point is to evaluate any current tools in use and whether they offer the visibility and functionality your organisation needs. Many legacy technologies work less effectively in the cloud and lack more advanced features, such as behavioural monitoring, to identify the latest threats.

Native tools offered by some cloud providers can be a good option but may not support other infrastructure and services, which is not ideal if you operate across multiple environments and are forced to pivot between disparate systems. To help centralise visibility and respond effectively to threats, you may need to invest in additional technology.

4.3. Telemetry and intelligence required

Technology is important but if it’s not integrated with the right type of security data, the benefit of any investments can quickly be undermined. Obtaining the level of visibility needed to detect and respond to malicious activity as early as possible typically requires a range of log sources from networks, systems, applications and endpoints. Threat intelligence is also valuable in helping to enhance detection accuracy and confidence.

As well as identifying which log sources are required, it’s also a good idea to consider the costs of storing this data and how long it needs to be retained for. For example, to comply with the PCI DSS, logs need to be stored for a minimum of 12 months.

4.4. System tuning and maintenance

When investing in a security monitoring solution, it’s unrealistic to expect the technology to work straight out of the box. To achieve the best outcomes, it’s important to ensure that any technology you use is optimally installed and configured, plus kept constantly tuned to detect the latest adversarial behaviours.

The last thing that you and your security team need is high volumes of false positives, so make sure that you commit adequate resources to baselining systems and developing new detection rule sets.

4.5. Shared responsibility

Before using cloud infrastructure and services, ensure you have a clear understanding of the scope of your organisation’s security responsibilities in relation to them. Shared responsibility models aren’t always well understood and the dividing line between the requirements of providers and organisations varies.

In a traditional data centre model, you are responsible for security across your entire operating environment, including physical servers, applications and data. However, in a cloud model, a provider may only take responsibility for the security of infrastructure, making it your job to protect any data uploaded to it.

Confusion can also arise when it comes to outsourcing the management of cloud environments to third parties. In these circumstances, it is important to be aware that under the General Data Protection Regulation (GDPR), liability for security is still with your organisation as the data processor, rather than with the third party you contract.

4.6. Ensuring consistency

When devising a monitoring strategy, ensure that you consider how you will control access to each of your environments and achieve a consistent level of threat visibility across each one.

Attackers can move between environments, meaning that an insecure cloud instance could pave the way for data and assets located in an on-premises network to be compromised. Similarly, a single infected endpoint could result in breaches across multiple environments.

4.7. Compliance requirements

With cyber security and data protection requirements only increasing, it’s crucial to maintain a clear understanding of the full extent of your organisation’s responsibilities.

One key aspect to consider is data residency. To avoid falling foul of regulations, ensure that you understand where your organisation’s data is being processed, including from a security monitoring perspective.

Having your monitoring technology hosted in one territory but ingesting logs from multiple others could leave you at risk of compliance failures. This is a particularly important consideration in light of the invalidation of the EU-US privacy shield.

4.8. Incident response

Swift detection of threats is vital but if your organisation lacks the capability to respond quickly and effectively, any benefit of early identification could be cancelled out. Threat actors could slip through the net.

When thinking about your cloud monitoring strategy, consider any steps you need to reduce the time it takes to not only detect threats but also respond to them. This is likely to require having members of your security team on standby 24/7, developing and testing incident response procedures and using automation to help contain and disrupt threats.

4.9. Expertise required

People are an essential part of your security monitoring programme. Despite continuous advancements in security technology, having great talent on hand to help develop and execute it is essential. Does your organisation have the right knowledge in areas such as system implementation and configuration, alert analysis and incident response?

Are those people familiar with the complexities of managing converged infrastructure? And are they capable of bringing together your various stakeholders, third parties and technical resources in the case of a breach?

It is also important to assess whether you require this type of specialist personnel to be available around the clock and whether you need to establish a Security Operations Centre.

Almost a third of organisations have identified a challenge hiring staff with the appropriate skillset to manage converged infrastructures.

Source: 451 Research

5. Actionable advice to get started

To get up and running quickly and effectively, Redscan recommends the following steps:

5.1. Identify your crown jewels

As a starting point in the development of your cloud monitoring strategy, conduct an exercise to identify cloud infrastructure and services in use, as well as the data that they hold and their function. For most organisations this will include the use of SaaS services such as Microsoft 365 and Salesforce, in addition to any IaaS or PaaS provisions from cloud providers such as Microsoft, Amazon and Google.

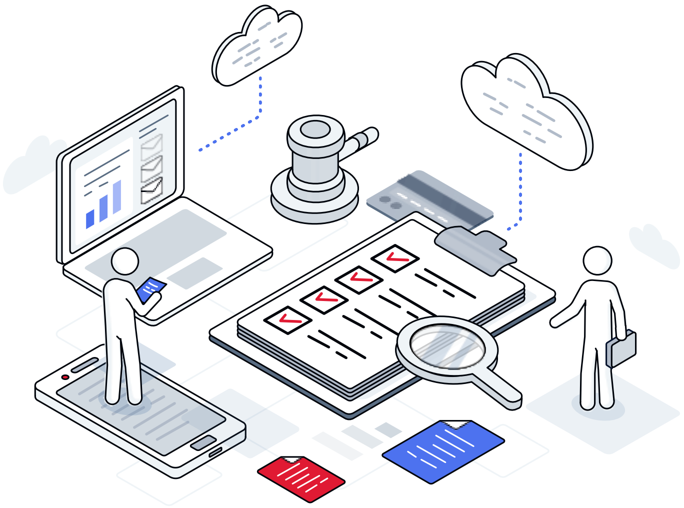
The level of assessment appropriate for your organisation will depend on your existing maturity status. This could involve compiling an asset inventory, distributing self-assessment questionnaires to internal stakeholders and engaging external consultants to provide independent insight.

5.2. Determine your cloud risk appetite

Risk appetite is the level of risk an organisation is prepared to accept in pursuit of its objectives. Setting tolerance levels for cyber security can aid your decision-making when it comes to choosing which environments and assets to monitor.

For cloud platforms, consider how the confidentiality, integrity and availability of your data (as outlined in the CIA Triad) could be affected and also factor financial, legal, operational and compliance risks as part of your decision-making.

For example, while closely monitoring an application processing sensitive customer data is likely to be deemed as important, a development server used solely for testing purposes might be considered as less of a priority.



5.3. Prioritise cyber security from the outset

Before migrating workloads to the cloud, make sure that you fully assess the associated cyber security risks. Rushing deployments without carefully analysing the potential security impacts can easily increase the likelihood of cloud misconfigurations, making it more complex to integrate new solutions.

Ensure that your digital and cyber security strategies go hand in hand to more easily facilitate your plans in the future and obtain greater value from your investments. The cost of retrofitting a security solution is often significantly higher than if it were implemented from the outset.

5.4. Utilise frameworks to aid use case development

Security frameworks are a good way to understand the tactics, techniques and procedures (TTPs) used by adversaries. Refer to frameworks such as MITRE'S Enterprise and Cloud ATT&CK matrices to help identify detection use cases, as well as the telemetry needed to observe them.

Complete detection coverage of all attacker behaviours is unlikely to be achievable from the outset, so focus on the TTPs that pose the greatest risk to your organisation and prioritise them accordingly.

5.5. Prioritise implementation

Comprehensive visibility across all your environments isn't likely to be achieved overnight. Adopt a phased approach to the implementation of your monitoring strategy by identifying the environments and assets at greatest risk, focusing on them in order of importance. A common place to start is monitoring SaaS applications such as Microsoft 365, Salesforce and Dynamics 365 for access and data exfiltration-related events.

Additionally, consider enhanced detection and response capabilities for areas of your estate that are especially vulnerable to attack, such as servers and end-user devices.

5.6. Stay up to date with best practice

Industry bodies such as the Cloud Security Alliance (CSA) and National Cyber Security Centre (NCSC) are a great source of security information and advice to help inform your cloud monitoring strategy. Consider working towards standards such as ISO2700/1 and ISO27017 and keep a close eye on evolving industry compliance requirements too. For example, Version 4.0 of the PCI DSS is likely to introduce updated requirements for organisations operating in the cloud.

5.7. Commission scenario-based testing to identify gaps in threat coverage and visibility

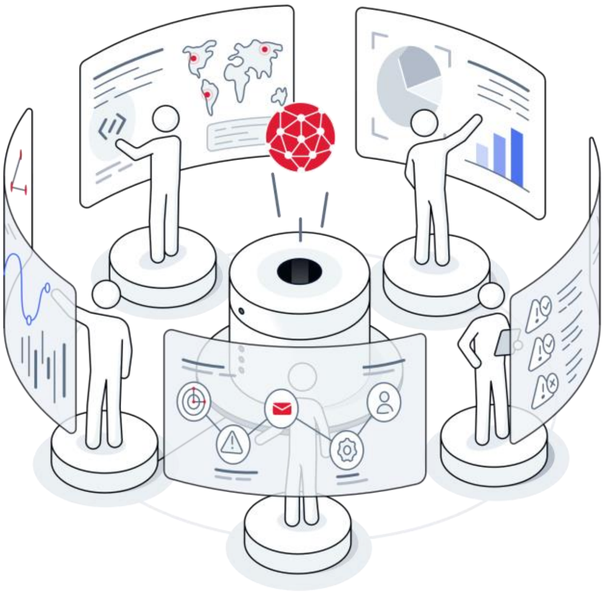
Ensuring that your security monitoring operation remains optimised to detect and respond to the latest threats is a continual process. To support this, commission scenario-based testing, a specialist form of security assessment designed to replicate a variety of the latest attack scenarios.

Scenario-based testing can help to identify gaps in threat coverage and visibility and provide valuable information to aid threat hunting and incident response.

5.8. Determine if you have the requisite skills in-house

Given the requirement for a range of specialist skills and the constant availability of personnel, consider whether your organisation has the right mixture of people to action your monitoring strategy effectively. Proactive monitoring of your organisation's infrastructure 24/7 is likely to require a large team of full-time security analysts and, potentially, a dedicated Security Operations Centre (SOC).

Perform a workforce calculation based upon the size of the network to be monitored, the number of assets and the amount of data generated and passing through it. Given the number of people required, consider whether it is worth outsourcing some or all aspects of security monitoring to a specialist third-party provider.



6. How Redscan can help

A turnkey solution for threat detection

As a provider of Managed Detection and Response services, Redscan is highly experienced at working with organisations of all sizes to alleviate the challenges of cyber security monitoring.

ThreatDetect™, our award-winning MDR service, integrates experienced SOC experts, a cloud-native technology stack and curated cyberoffensive intelligence to rapidly detect and respond to current and emerging cyber threats - 24/7/365.

Via our proprietary **CyberOps™** threat management platform, ThreatDetect™ supports proactive and centralised monitoring of networks, endpoints, applications and cloud environments. The service delivers actionable remediation advice and automated response actions to disrupt threats before they can cause damage and disruption.

Monitoring your infrastructure, platforms, services and endpoints

ThreatDetect is quick to deploy and supports monitoring of on-premises networks as well as cloud environments and workloads, including:

aws
Azure
Google Cloud Platform
salesforce
Microsoft 365
G Suite

Contact us to learn more about MDR or arrange an informal discussion about your cyber security needs

www.redscan.com
2 Throgmorton Avenue, London
+44 (0)203 972 2500

REDSCAN

A KROLL BUSINESS

0800 107 6098 ✉ info@redscan.com www.redscan.com