vital
TECHNOLOGY GROUP

Cloud Security Threats in 2022

Strengthening your Cloud environment with Azure Sentinel

The 2022 Cloud landscape

The flexible, scalable and powerful potential of the Cloud has led to a dramatic increase in adoption in recent years. As the COVID-19 pandemic spread across the globe, and remote working became the new normal, the adoption of Cloud computing accelerated rapidly. Modern businesses are now relying on the Cloud for a variety of solutions including data backup and storage, accessing applications and data analytics. As a result, more sensitive information is now hosted on the public Cloud than ever before.

While Cloud computing comes with a range of benefits for individual users and entire enterprises alike, when a Cloud environment is improperly managed, it can make a business vulnerable to a range of cyber threats.

A comprehensive understanding of the current Cloud landscape and the most effective methods of defence are vital to effectively protect your business from pervasive Cloud security threats.

Our eBook collates all the crucial information you need to operate securely within the Cloud in 2022, including:

- The frequency of Cloud attacks
- The challenges of Cloud security
- The different types of Cloud threat
- The primary victims of Cloud threats
- The security benefits of Microsoft Sentinel

vital
TECHNOLOGY GROUP

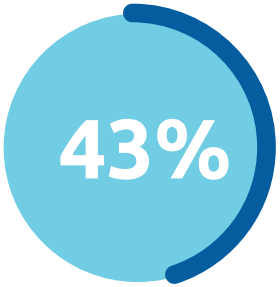
The frequency of Cloud attacks

The unexpectedly rapid Cloud adoption process that many businesses went through in the last few years has led to a myriad of security issues. As businesses attempted to efficiently facilitate remote working, in many cases Cloud setup and provision was prioritised over security. The majority of organisations (54%) used tools or applications that were moved from on-premises environments and were therefore not purpose-built for the Cloud, limiting their scalable security capabilities.

The significant increase in Cloud adoption has been mirrored by a major uptick in Cloud threats and Cloud data breaches. In the last eighteen months, the majority of businesses leveraging Cloud capabilities have experienced some form of data breach.

of organisations are hosting at least some of their IT environment in the Cloud.

of companies have experiences at least one Cloud data breach in the last 18 months.



of companies have reported 10 or more Cloud data breaches in the last 18 months.

While these statistics are shockingly high, they are more a reflection of the inadequacy or utter lack of Cloud security measures implemented by most businesses, rather than the implicit dangers of the Cloud environment. With the correct management and security provisions, the benefits of the Cloud can far outweigh the potential risks.

vital TECHNOLOGY GROUP

The challenges of Cloud security

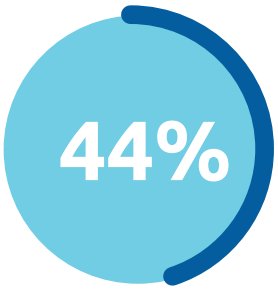
While there are many advantages to Cloud adoption, securing a diverse Cloud environment can present many challenges. To maximise the potential of the Cloud, it is essential that you properly prepare for any and all potential threats.

A survey from IDG has found that of the top five challenges associated with public Clouds, three are related to Cloud security. Data privacy and security challenges, protecting Cloud resources and lack of Cloud security expertise were cited as primary issues. The most commonly reported issue with the public Cloud was controlling Cloud costs, which perhaps contributes to many businesses' insufficient investment in Cloud security provisions.

What are the top Cloud security concerns?

Data loss and leakage

Data privacy and confidentiality



Accidental exposure of credentials

How are businesses currently preparing?

Despite struggling against the challenges of Cloud security, the majority of businesses are not adequately strengthening their security posture in response.

Only one in five businesses assess their security posture in real time.

One in five businesses conduct weekly evaluations of their security posture.

58% of all businesses only evaluate their security posture once a month, or less frequently.

In addition, despite 93% of businesses citing concern about human error causing the accidental exposure of data, 22% of organisations still assess their security posture manually. Rejecting automation in this manner is a significant drain on resources and enhances the possibility of human fallibility affecting valuable data.

Common Cloud security threats

There are three primary forms of Cloud security threat currently dominating the cyber sphere. Understanding these attacks is the first step towards protecting your business from a data breach.

So, what do these threats look like?

Misconfiguration and human error

Cloud misconfiguration is the act of setting up Cloud assets incorrectly, meaning that they can be exploited by malicious activities. Misconfiguration can cause security breaches to take longer to detect. Misconfiguration of access permissions can leave privileged accounts vulnerable to attack, and critical corporate data unsecured. In the last two years, the compromise of privileged accounts has made up 34% of all identity-related breaches. However, only 38% of organisations are using multi-factor authentication to secure their privileged accounts, and more than 90% of Cloud identities are using less than 5% of their granted permissions. This heightens the chance of a data breach, as it creates a golden opportunity for cyber criminals to gain access to sensitive data by exploiting accounts with misconfigured permissions.

Account takeover attacks

According to a 2021 report from CISCO, phishing attacks account for over 90% of all data breaches. During a phishing attack, a cyber criminal will pose as a legitimate or trusted source and send targeted correspondence designed to manipulate victims into revealing sensitive information or downloading malware to their device.

Cyber criminals can leverage the Cloud to aid phishing attacks by directing users to phishing pages that use legitimate domain names, such as docs.google.com. These content delivery networks and Cloud file share services allow users to host their content on a legitimate domain. This allows cyber criminals to host malicious files more easily. This is a successful phishing tactic as victims are more likely to click on a link that appears to come from a legitimate source. It is also extremely difficult to block these domains without removing all the content hosted on them, including any legitimate content.

Ransomware

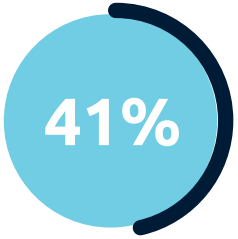
59% of ransomware incidents in which data is successfully encrypted involve the public Cloud. The public Cloud is both the platform from which the data is stolen, and where the attacker stores it while they exploit their victim for ransom. Typically, cyber criminals send exfiltrated, encrypted data to a legitimate Cloud storage service, such as Google Drive, Amazon S3 or Mega.nz. This makes it more difficult for the target to locate their stolen data.

The victims of Cloud attacks

Organisations of all sizes can be targeted by Cloud attacks, from small start-ups to large-scale enterprises. If a business is hosting data in the Cloud, then they are automatically at risk of attack. However, different sized businesses have been reported to struggle with different forms of Cloud threats. The primary Cloud security concern for enterprises is data privacy and protection, while SMBs are reported to also struggle with migrating data to the Cloud, securing Cloud resources and dealing with a lack of Cloud security skills.

There is some differentiation between industries, with certain sectors seeing a larger volume of Cloud threats.

Of the total number of breaches caused by Cloud misconfiguration:



are from tech companies

are from healthcare organisations

are from government agencies

are from finance companies

are from hospitality businesses

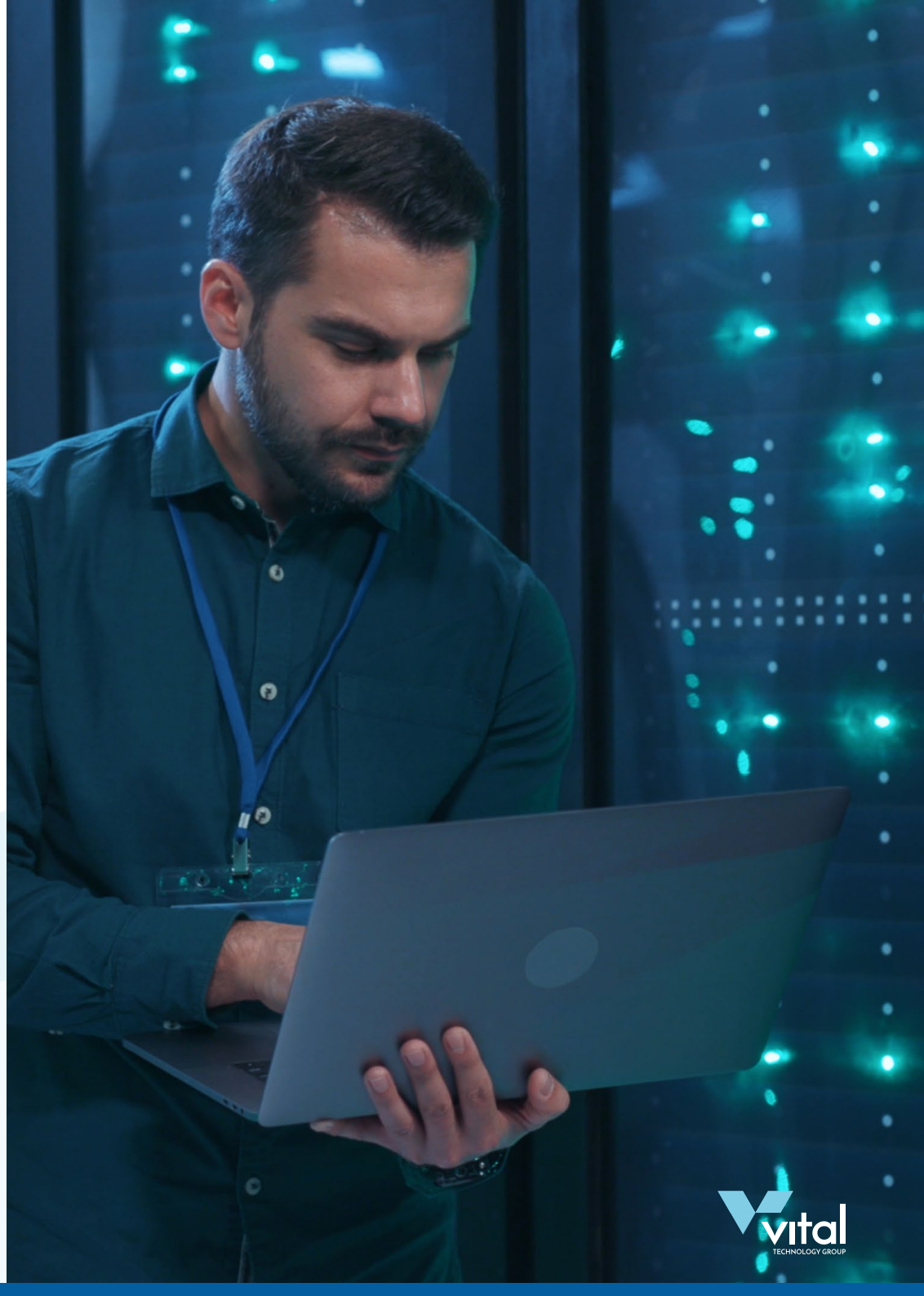
Introducing Microsoft Azure Sentinel

Microsoft Azure Sentinel is a Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) solution, native to the Azure Cloud.

Sentinel harnesses the power of Azure to deliver intelligent security analytics and threat intelligence across entire organisations. Attack detection, threat visibility, proactive hunting and threat response are combined in one highly scalable security solution.

Microsoft Azure Sentinel provides you with a unique and comprehensive bird's-eye view of the security of your business, minimising the complexity of threat detection, increasing the volumes of alerts and providing long resolution time-frames.

The Cloud-delivery of Sentinel eliminates hardware expenses while ensuring efficient deployment. If you need an advanced security solution for the Cloud, you can roll Sentinel out across your entire organisation in mere minutes.



Access

Collect data at Cloud scale across all users, devices, applications and infrastructure, both on-premises and in multiple Clouds. With impressive flexibility you can configure Sentinel's data capture capabilities according to your unique requirements.

AI threat investigation

Leveraging Azure's Artificial Intelligence capabilities, you can use Sentinel to investigate threats and hunt for suspicious activities at scale. Becoming more advanced and intelligent with prolonged use, Azure Sentinel can identify previously undetected threats and minimise false positives.

App integration

Sentinel is configured for all Microsoft Cloud solutions meaning it can instantly support and optimise Microsoft 365 and SharePoint environments. Additionally, Sentinel builds on the full range of existing Azure services, meaning it can natively incorporate with proven foundations like Logic Apps and Log Analytics.

Rapid incident response

With built-in orchestration and automation of common tasks, Sentinel can rapidly respond to and resolve incidents or threats. By automating any recurring or predictable enrichment, response and remediation tasks, Sentinel frees up time and resources for more in-depth investigations of advanced threats.

Hybrid-friendly

Sentinel is designed to fully support and secure businesses operating with a hybrid Cloud model. No matter how much of your data is stored within the Cloud, Sentinel can protect the user, application, device and infrastructure. With Sentinel, hybrid workplaces are just as defended as those fully based in the Cloud.

Customised responses

Users can implement business-specific rules and policies for Sentinel to abide by. These rules aid threat detection and resolution. This helps to make Sentinel more bespoke to your company, better protecting you from the threats that concern you most.

Transform your Cloud security today

As businesses continue to migrate to the Cloud, new and increasingly advanced threats will continue to dominate this space. Leveraging a Cloud-based and scalable SIEM solution like Microsoft Azure, Sentinel can provide effective protection against these emerging security risks.

Vital have the Cloud expertise, security specialisms and Azure fluency to help you harness the powerful potential of Microsoft Azure Sentinel. If you're exploring your security solutions, or are taking your business to the next stage of its Cloud-empowered journey, we're here to help.

Get in touch with a Vital representative today to discover we can facilitate your adoption of Microsoft's transformative Sentinel solution.

BOOK A MEETING