Phoenix AzGuardian

Fortify your Azure cloud security and protect yourself against cryptomining fraud and other security threats including insider attacks, privileged account escalation, and brute force attacks with Phoenix AzGuardian.

What is cryptomining fraud in Microsoft Azure?

Cryptomining fraud involves unauthorised individuals or groups gaining access to your Azure resources and using them to mine cryptocurrencies without your knowledge or consent. They leverage the processing power of Azure's high-performance computing resources to perform the complex calculations necessary for cryptocurrency mining, with your organisation responsible for this usage, and compromised Microsoft Azure tenancies are facing more frequent incidents of this type of fraud. It's a stealthy, illegal operation that, if left undetected, can lead to significant and unexpected Azure consumption costs that severely impact your organisation's ability to operate and deliver services.

Cryptomining fraud leads to:

Financial implications:

unauthorised cryptocurrency mining activities consume considerable amounts of processing power, leading to the generation of significant unauthorised cloud consumption costs. Unfortunately, the organisation that owns the Azure environment that is compromised has to bear these costs, not the service provider.

Loss of service:

cryptomining fraud activities can lead to service degradation if legitimate Azure resources are impacted or terminated, and entire subscriptions can be completely hijacked or even cancelled during an attack.

Regulatory risks:

unauthorised data access and data loss can result from the same breaches that enable unauthorised cryptomining to take place, as the same access can also be used by attackers to access your confidential data, causing serious compliance and regulatory issues.

The challenges of maintaining your Azure cloud security

Due to the unique characteristics of cloud environments and the evolving nature of cryptomining fraud techniques, managing your Azure cloud security to reduce the risk of cryptomining fraud in Microsoft Azure often presents several challenges, including:

Dynamic nature

Cryptomining fraud techniques constantly evolve to bypass existing security measures. Attackers adapt their code, utilise obfuscation techniques, and leverage new vulnerabilities to evade detection and continue their unauthorised mining activities.

Visibility and monitoring

Traditional security measures may struggle to detect cryptomining fraud activities within Azure. The nature of cloud resources and the decentralised architecture make it crucial to have robust monitoring and visibility solutions in place.

Scale and complexity

Azure environments encompass a vast array of resources, making it challenging to identify and mitigate cryptocurrency fraud incidents effectively. The distributed nature of cloud infrastructure further complicates the detection and prevention process.

Rapid deployment

Once an organisation's Azure environment has been compromised, the resources required for cryptomining can be provisioned and up and running in a matter of minutes, with the resulting unauthorised costs being generated immediately.

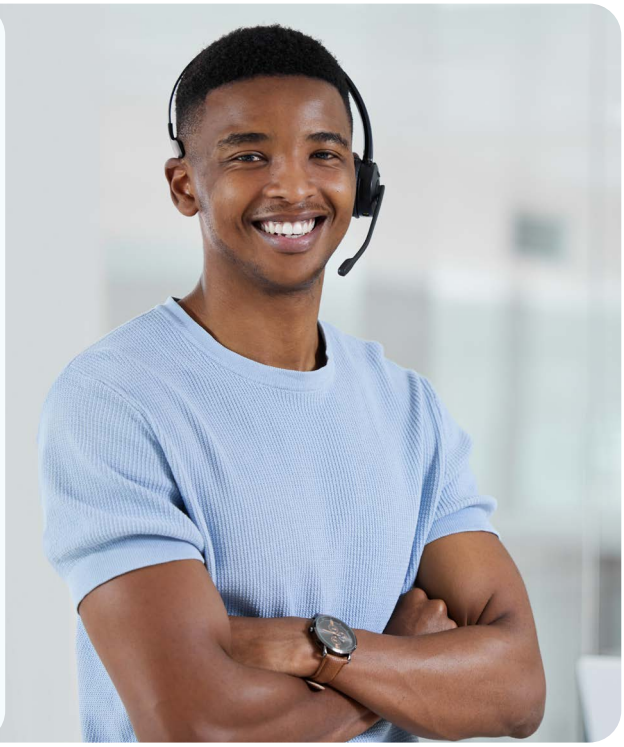
Addressing these challenges requires a comprehensive approach to combine robust security configuration with monitoring and detection mechanisms, and maintaining up-to-date knowledge of emerging malicious and unauthorised access techniques that could enable cryptomining fraud to be committed.

Phoenix AzGuardian: fortifying your Azure cloud infrastructure

To combat these increasing threats, Phoenix have developed AzGuardian – a powerful, proactive defence mechanism, delivered as a managed service, and designed to safeguard your Azure infrastructure from being exploited for fraudulent usage by proactively implementing a combination of Azure security best practice, threat detection, and a dynamic response.

As well as protecting against cryptomining fraud, our service secures your organisation against several other security scenarios including insider attack, privileged account escalation, initial access (preventing sign-ins from outside the UK or approved country of origin), and brute force attack.

The Phoenix AzGuardian Managed Service features a three-stage approach, described as **Prevention**, **Slowdown**, and **Stop** with each stage providing an additional level of proactive risk mitigation.



Prevention

The service supports the deployment and adoption of Microsoft best practice methodology to reduce the risk of unauthorised privileged access to an organisation's Azure environment by a malicious actor.

Slowdown

The service places further controls within the environment to restrict the activities available to a malicious actor, and deploys monitoring and alerting for real-time visibility of potentially unauthorised events that can be investigated and acted upon to stop an attack before it progresses.

Stop

The service includes a proprietary kill-chain stage designed to automatically terminate Azure resources that meet specified criteria that are suspected to have been created by an unauthorised or malicious actor. This prevents any further resources being created, effectively stopping the attack.

As the world's first proprietary solution of its kind, Phoenix AzGuardian has a proven track record in safeguarding Azure environments by protecting against and neutralising cryptomining attacks and helping preserve the integrity of your Azure cloud infrastructure.

Join the growing number of organisations who continue to experience the benefits and peace of mind of our Phoenix AzGuardian Managed Service first-hand.

Why Phoenix?

As one of the most recognised and accredited world-leading Microsoft partners with a focus on transforming organisations across the UK, you can trust in Phoenix, our skills, and specialist knowledge.

Microsoft Partner — 2021 Partner of the Year Winner United Kingdom

Microsoft Partner — Winner — 2023 Partner of the Year — Modern Endpoint Management Award

Microsoft Solutions Partner — Data & AI — Azure

Microsoft Solutions Partner — Microsoft Cloud

Microsoft Solutions Partner — Security

Microsoft Partner — 2019 Partner of the Year Winner — Modern Workplace Transformation Award

Microsoft Partner — Azure Expert MSP

Microsoft Solutions Partner — Infrastructure — Azure

Microsoft Solutions Partner — Digital & App Innovation — Azure

Member of Microsoft Intelligent Security Association

Get started with Phoenix AzGuardian

Don't let malicious threat actors gain access to your Azure environment. Adopt our Phoenix AzGuardian Managed Service and fortify your defences against this threat, supporting the security of your Azure infrastructure and the safety of your organisation.

Get in touch now

01904 562200
www.phoenixs.co.uk
hello@phoenixs.co.uk