PREPARING YOUR BUSINESS FOR THE THREAT LANDSCAPE

2023: Cloud Security Trends

Download

NET3 TECHNOLOGY

Trends Overview

What will 2023 hold for organizations in the cloud?

01 Rapid Adoption of Cloud

02 Cloud First

03 Hybrid Cloud

04 Artificial Intelligence

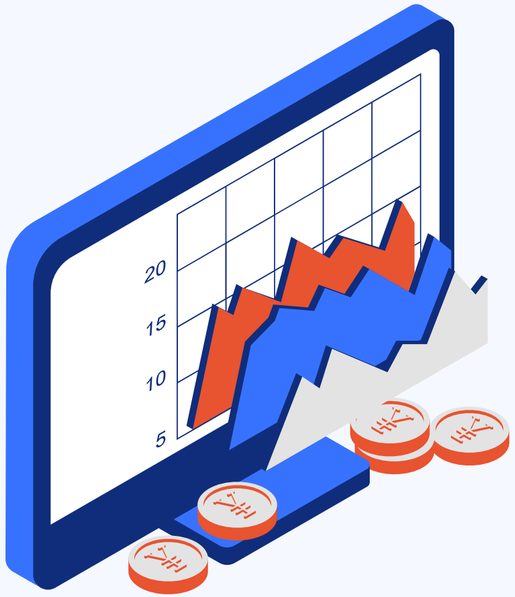
05 Zero Trust Model

06 EDR

07 Immutable Storage

Sources: Computer.org, Gartner.com, Analyticsinsight.com

The Rapid Adoption of Cloud and How Companies Can Improve Their Strategy



Throughout the past decade, many companies made the switch from hosting data on premises to the cloud, now that those companies have migrated - how can they keep their data secure and continue to improve their data protection strategy?

Some companies have still neglected the advantages the cloud has to offer, but 2023 will continue to demonstrate rapid adoption of the cloud.

NET3 TECHNOLOGY

Cloud First

- 92% of organizations currently host their IT environment in the cloud with the goal of increased flexibility, productivity, and reduced costs.
- The COVID-19 pandemic proved that cloud strategy and business strategy go hand-in-hand, according to Gartner.
- Companies who fail to adopt the cloud first mindset will risk languishing in an on-premises data center.

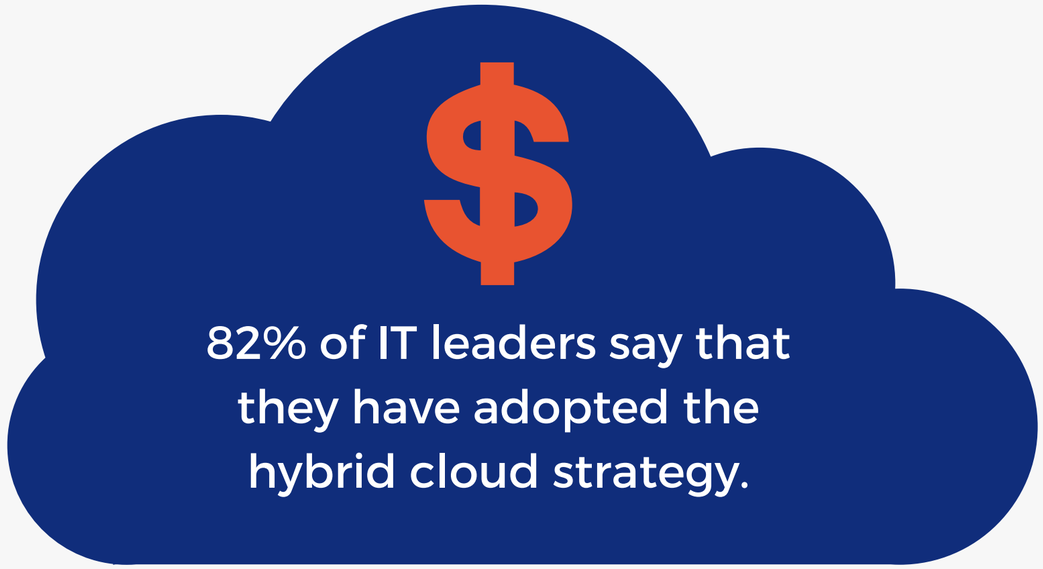
"The cloud was able to demonstrate that you can continue to run your business globally, during a pandemic with minimum glitches, when employees had to shift to work from home practically overnight."

-Milind Govekar, Research VP at Gartner

NET3 TECHNOLOGY

Hybrid Cloud

- Hybrid cloud allows organizations to elect which data is hosted on premises, or in the cloud - dependent on the nature of the data.
- More sensitive data can be kept on premises to maintain under close watch, while data that requires immediate availability and accessibility may be kept in a public cloud.
- Hybrid cloud offers organizations the scalability and adaptability that their individual needs require.



Artificial Intelligence

How machine learning can offer your organization top of the line security

Artificial intelligence has the ability to scale and adapt to the changing business requirements and needs. It offers extra security to organizations with the ability to learn user behavior and detect unusual behavior and stop the action BEFORE damage is done.

By implementing artificial intelligence into your cloud security strategy, policies can be developed and taught to control data access and prevent unusual behavior.

The cybersecurity workforce has slimmed dramatically, highlighting the demand and need for artificial intelligence and machine learning.

Zero Trust Model

The core principles of the new security model

A strategic security model that restricts everything and anything from gaining access to systems without first having their identity authenticated. The implementation of this model will continue to increase due to the rising threat of cyberattacks.

LEAST PRIVILEGE ACCESS

At the core of the Zero Trust Model is the idea that you should only grant access to users on a case-by-case basis and only grant access to data they need to complete tasks.

NEVER TRUST

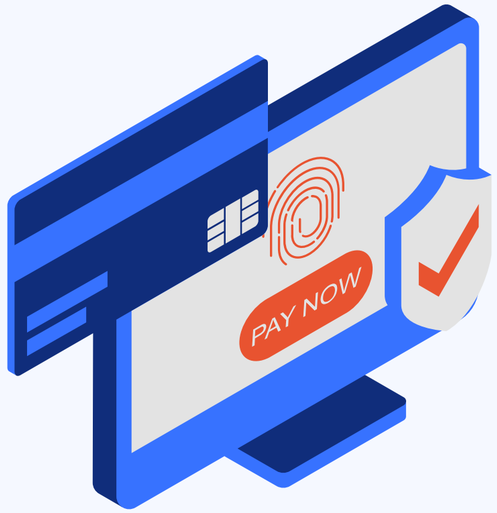
No trust should be given to any user or action by default. Every single request or new entry should require identification verification before access is granted.

ALWAYS MONITOR

The Zero Trust Model will not be effective without consistent and precious monitoring of user behavior and any unusual changes to the data or network.

n3t
NET3 TECHNOLOGY

Endpoint Detection & Response (EDR)



The first line of defense. When a user makes a risky click, you need a toolset to prevent & react.

In 2022, we saw an astronomical amount of cyberattacks, resulting in hefty ransom payments, critical data loss, and most importantly - the distrust and abandonment of customers.

Although a vast majority (54%) of ransomware attacks come from phishing, we are increasingly seeing a phenomenon known as whale hunting. When whale hunting, extensive reconnaissance is done by the threat actors to determine a target with enough cash and a big enough vulnerability to make it worth it.

Possible the most important metric with regards to ransomware and malicious activity is dwell time, the length of time a threat actor has had in the network before being detected. During dwell time, a threat actor is busy exfiltrating data, establishing a foothold in the environment, and escalating their privileges.

Early detection is critical to an organizations disaster response. Carbon Black, Darktrace, and Acronis all provide agent level EDR capabilities to provide process level anti-malware and exploit prevention.

NET3 TECHNOLOGY

Immutable Storage

With cybersecurity threats evolving and increasing, how can we ensure out backup data is secure?

We rely on backups to keep our data secure in the event of a disaster event. Unfortunately, we can no longer assume data backups are secure and protected from attacks.

Immutable storage gives another layer of protection for your backups by not allowing that data to be modified, encrypted by another process, or deleted.

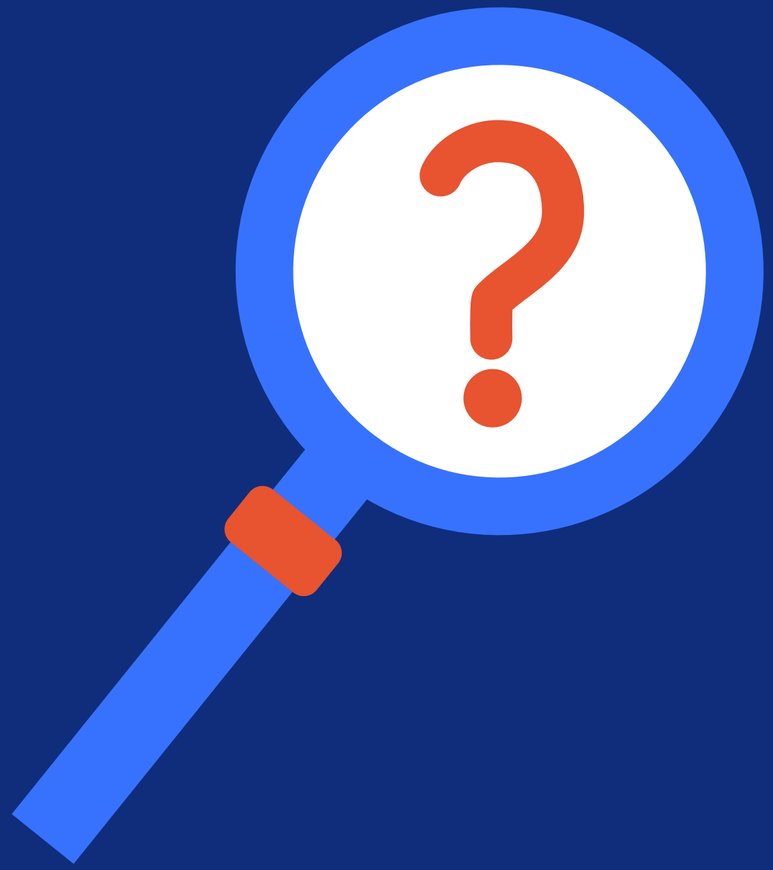
- According to Veeam's 2022 Ransomware Trends report, immutable storage was the #1 contributor to organizations being able to successfully recover from a backup instead of paying the ransom.
- 1 in 4 organizations were able to recover from their ransomware event from backups instead of paying the ransom.
- The three most important contributors to being able to successfully recover from a ransomware event using backups instead of paying the ransom are:
    1. Immutable/air-gapped backup repositories
    2. Verifiably recoverable and assuredly "clean" data
    3. Orchestrated workflows for recurring testing & reducing the time of remediation

NET3 TECHNOLOGY

Do you have any questions?

Contact us to learn how to prepare for these 2023 Cloud Security trends.

Our goal is to make customers ***confident*** in their cloud strategy. Speak with one of our engineers today!



www n3t.com

sales@n3t.com

Net3 Technology is a leading cloud services provider offering nationwide backup, disaster recovery, IaaS, Cybersecurity, and Ransomware solutions tailored to fit company requirements with flexible pricing options.

n3t NET3 TECHNOLOGY