ClamTech

CLAMTECH NEWSLETTER

ISSUE 04 | OCTOBER 2026

Security & Resilience



Malcolm Lungaro-Mifsud
Chief Operating Officer

A Note

As organisations become increasingly dependent on digital infrastructure, security is no longer only about preventing an attack. It is also about ensuring that systems remain available, data remains protected and businesses can continue operating when disruption occurs.

At Clamtech, we approach security and resilience as part of the wider infrastructure strategy. How systems are designed, deployed, monitored and maintained all contribute to an organisation's ability to respond when something goes wrong.

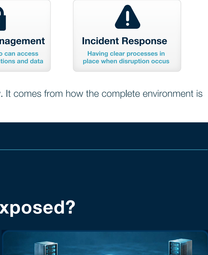
In this edition, we look at some of the practical considerations behind building resilient infrastructure, the role of modern security architecture, and the questions organisations should be asking about their own environments.

IN THIS ISSUE

- Designing for Disruption
- Where is Your Infrastructure Most Exposed
- Building Security into the Infrastructure
- Tech Insight: Zero Trust Explained
- How Resilient Is Your Business?

01

Designing for Disruption



Cybersecurity is often discussed in terms of preventing threats. For businesses, however, the wider question is what happens when disruption occurs.

A resilient infrastructure environment should be designed not only to reduce risk, but also to maintain critical services, protect data and enable recovery when systems are affected.

This requires organisations to consider security and resilience throughout their infrastructure, from cloud architecture and access controls to backup, monitoring and recovery.

At Clamtech, we work with organisations to identify potential points of failure and design environments that balance security, performance and availability.

Building Resilience

A resilient infrastructure strategy should consider:

Availability
Ensuring critical systems and services remain accessible

Redundancy
Reducing reliance on individual components or systems

Backup & Recovery
Protecting business data and ensuring it can be restored

Monitoring
Identifying issues before they develop into larger incidents

Access Management
Controlling who can access systems, applications and data

Incident Response
Having clear processes in place when disruption occus

Resilience is not a single product or technology. It comes from how the complete environment is designed and managed.

02

Where Is Your Infrastructure Most Exposed?

Modern IT environments are increasingly interconnected. Cloud platforms, remote access, applications, APIs and third-party services all create dependencies that organisations need to understand and manage.

Security therefore needs to extend beyond the traditional network perimeter.



Organisations should regularly review:

- Who has access to critical systems and data
- How applications and APIs are exposed externally
- Whether software and infrastructure are being kept up to date
- How unusual activity is identified and monitored
- Whether backups are isolated and regularly tested
- How quickly critical services could be restored following an incident

Understanding these dependencies and potential weaknesses is an important first step towards improving resilience.

03

Building Security into the Infrastucture

Security works best when it is considered from the beginning rather than added once an environment has already been built.

Clamtech works with organisations across cloud infrastructure, DevOps, security and managed IT to incorporate security into the design and ongoing management of their environments.



Through our partnership with Cloudflare, we can also provide technologies including:

- Zero Trust Network Access
- DDoS protection
- Web Application Firewall (WAF)
- API security
- Traffic management
- Application and network protection

The technology is only one part of the equation. How these services are configured, integrated and managed determines how effectively they protect the wider environment.

04

TECH INSIGHT

Zero Trust - What Does It Actually Mean?



Traditional network security was largely built around a defined perimeter: users and systems inside the network were trusted, while those outside it were not.

Zero Trust takes a different approach.

Rather than assuming that a user or device should be trusted because of where they are connecting from, access is continuously verified according to factors such as identity, device and the resource being requested.

In practical terms, this means giving users access only to the applications and resources they need, rather than providing broad access to an entire network.

For organisations supporting cloud environments, remote working and distributed teams, this provides a more appropriate security model for the way modern businesses operate.

05

How Resilient Is Your Business?

Security measures are important, but organisations should also understand how quickly they could respond and recover if something went wrong.

Ask yourself:

- Do you know which systems are critical to your business?
- Can you identify unusual activity across your environment?
- Do you know how quickly essential services could be restored?
- Are your backups regularly tested?
- Is access to critical systems properly controlled?
- Does your team know what to do in the event of a security incident?

If some of these questions are difficult to answer, it may be time to review your infrastructure from a security and resilience perspective.

Build security and resilience into your infrastructure.

Clamtech helps organisations identify risks and develop practical solutions across cloud, security, DevOps and managed IT.

LET'S TALK

LET'S CONNECT

hello@clamtech.com

www.clamtech.com