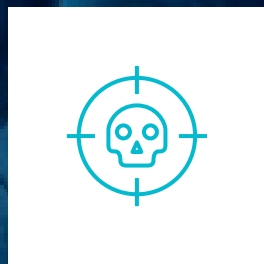


A ransomware attack will happen in the next 11 seconds...

Are you prepared?

Cyber Resilience is the Key: 5 Things to Consider



01

Detect attacks early

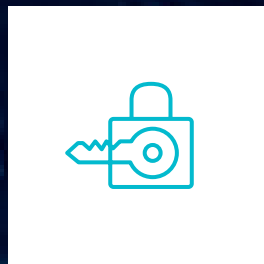
Early detection stops breaches in as little as 8 seconds. [cyberintelmag.com](https://www.cyberintelmag.com)



02

Isolate and Secure

An isolated and secured recovery environment prevents reinfection.



03

Store Immutable Images

Having an immutable backup ensures there is always the most recent clean copy of your data, safe and recoverable at any time. [phoenixnap.com](https://www.phoenixnap.com)



04

Scan Images for Anomalies

80% of ransomware victims suffer repeat attacks.




05

Accelerate Response and Recovery from Incidents

21 days is the average downtime organizations face due to ransomware attacks.

Don't be the next hostage

Persistent Intelligent Cyber Recovery (PiCR) Can Help




Detect Attacks Early

High-risk changes are detected and flagged on the Persistent Intelligent Cyber Resilience (PiCR) dashboard for review by the security team.




Secure and Isolate

Private IP address based internal network is used to prevent any direct exposure of the PiCR assets to the external public network.



Immutable Images

Using PiCR images can only be deleted by the retention manager based on a retention policy.



Scan for Anomalies

PiCR identifies the latest point-in-time images that can be recovery candidates. It re-analyzes images for anomalies that could indicate malware to prevent reinfection from corrupted images.