

HyperBUNKER

When attackers reach your backups, what still works?

Restarting operations after ransomware

hyperbunker.com



When Recovery Fails

Ransomware **doesn't end when systems are breached.**

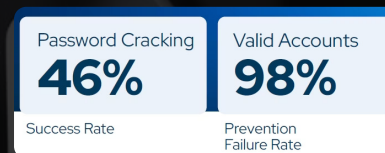
It ends when **you can't restart operations.**

In real incidents, nothing can be trusted.

Attackers Don't Stop at Access

Attackers are not breaking in anymore. **They are logging in.**

- *46% of environments had password hashes cracked*
- *98% of attacks using valid credentials succeed*



Once inside, they move to:

- identity systems
- backup infrastructure
- control planes

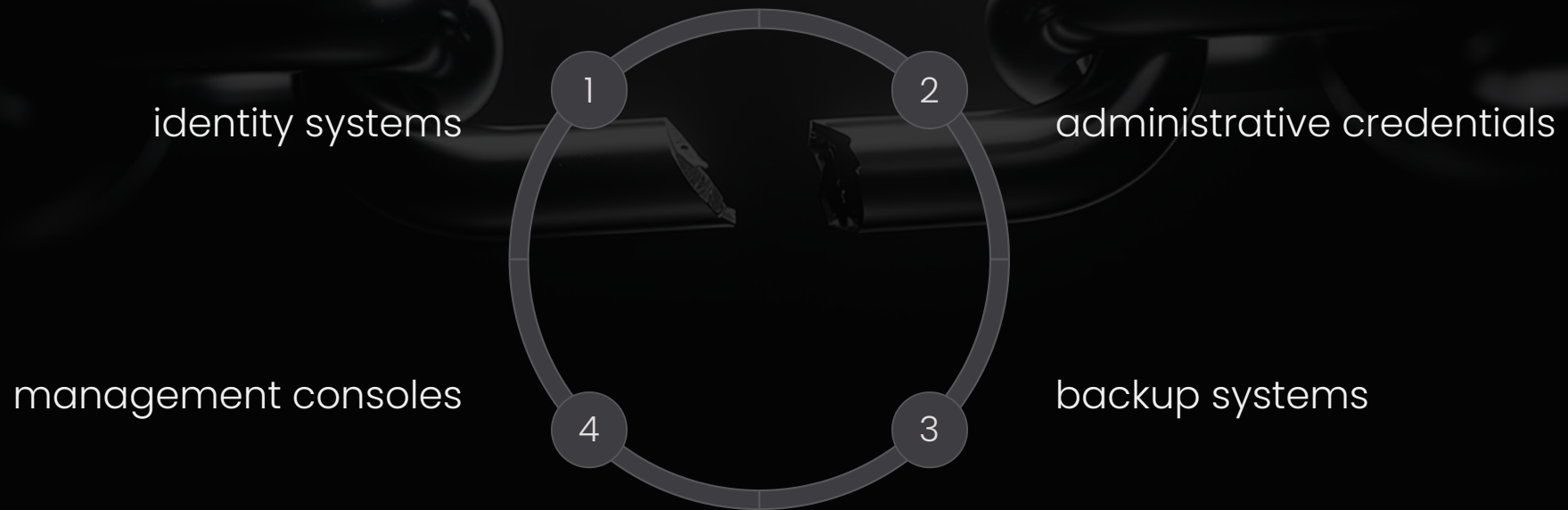
Some don't negotiate. They wipe (NotPetya - WhisperGate - AcidRain - ICS destructive malware).

The only question : Can you restart?

Why Recovery Breaks

Recovery doesn't fail because tools are missing.

It fails because it **depends on systems under attacker control.**



The Architectural Problem

Recovery fails for a structural reason.

It runs inside the same environment that gets taken over.

Recovery must exist **outside the attack surface.**

If recovery depends on compromised systems, it will fail.

A Different Recovery Model

Recovery must not depend on identity.

It must not be reachable from the network.

The attacker must not be able to touch it.

Principles:

physically isolated

**not reachable from the
network**

**independent from
identity systems**

stored as offline copies

The attacker is removed from the recovery path.

What Actually Allows you to Restart

The question is not how much data you protect.
It's what you need to restart.

You can rebuild infrastructure.

You can redeploy applications.

But without a trusted baseline, you can't restart.

To restart, you need a minimal trusted baseline:



Identity

- Active Directory
- Domain Controllers



System Configuration

- OT configs
- Network setup



Access

- Privileged accounts
- Credentials



Business Data

- Transactions
- Records

If this is missing, systems may exist — but operations do not.

HyperBUNKER

HyperBUNKER is build for this.

A physically isolated recovery system outside the operational environment.

Not reachable from the network.

No credentials.

No remote access.

Nothing to log into. Nothing to take over.

This is **not another backup system.**

This is what remains when backups are gone.



How HyperBUNKER Works



Capture

A minimal operational baseline is captured from production on a defined schedule.



Isolation

Transferred through a hardware-enforced one-way path.



Offline Immutable Copies

Physically disconnected and unreachable from the network.



Recovery

Systems rebuilt from a trusted pre-incident state.

Restore does not depend on:

identity

backups

control systems

This is what allows you to restart when everything else fails.