Guide

THALES
CYBERSECURITY

# The Day Access Stopped

## A practical guide to identity resilience for security leaders in UAE & KSA

cpl.thalesgroup.com

THALES

CYBERSECURITY

## When authentication fails, everything fails

Earlier this year, a single regional infrastructure disruption knocked more than 60 cloud services offline at once. Banks issued emergency notices. Payment platforms went dark. For some organizations, recovery stretched into weeks.

Incidents like this show how quickly systems can become inaccessible: not because they're gone, but because users can't authenticate. When identity fails, it becomes a business continuity issue – and a direct test of an organization's cyber resilience.

Whether identity is cloud-based or on-prem, the question is unavoidable: if your primary environment went offline today, how long before access comes back - and how do you know for sure?

## The identity blind spot

Identity usually isn't where business continuity or digital resilience planning starts. Most focus on keeping systems running and data protected – and assume access will still be there when its needed.

But identity is the layer everything runs through. If it's down, nothing else really matters. That gap shows up differently depending on how identity is deployed:

- **Cloud IAM** depends on hyperscaler availability: when regions go down, identity goes with them, and failover isn't always an option due to data residency rules
- **On-prem IAM** gives more control but still creates a single physical point of failure if that environment is disrupted
- **Across both**, IAM continuity is often assumed, not designed or tested with a true backup layer in place
- And some solutions go further, **bypassing security controls** entirely when connectivity is lost, trading protection for availability

## Where do you stand today?

Before addressing the gap, it is worth pressure-testing whether identity resilience and business continuity readiness is already a hidden risk in your environment. These are not technical questions, but operational ones that determine how quickly your organization can recover when access is disrupted.

- How quickly can your organization restore authentication if your primary identity system becomes unavailable?
- What contingencies are in place to maintain access during a disruption, and are they independent of your main environment?
- Has identity continuity planning been formally reviewed as part of your broader risk and compliance programs?

## What a resilient identity architecture looks like

Identity resilience doesn't come from a single deployment model - it comes from removing dependency on any one system, location, or provider. The goal is simple: ensure identity can continue operating even if the primary environment cannot. Here are a few key resilience measures to put in place:

### Cloud backup environment

A secondary cloud environment allows identity to shift if a primary region goes down, avoiding total dependency on one provider or location, ensuring business continuity during identity disruption

### Second on-premises installation

A second on-site or geographically separate installation protects against outages, damage, or loss of connectivity at a single facility

### Sovereign identity layer

A regionally compliant environment ensures identity can fail over without violating data residency regulations

### Hybrid identity architecture

A combination of cloud and on-prem environments removes dependence on any one system, ensuring continuity even during large-scale disruption and strengthening overall digital resilience

## The regulatory reality

This shift isn't temporary - and it isn't optional. Regulatory frameworks across the region are moving beyond policy and into enforcement, requiring organizations to prove that identity systems can withstand disruption and support business continuity and cyber resilience requirements.

- **NCA ECC-2 (KSA)** mandates data residency and backup strategies for identity and access control systems
- **SAMA CSF** enforces IAM and continuity requirements across the financial sector, with high audit failure rates highlighting execution gaps
- **UAE NESA IAS** requires organizations to implement and regularly test identity-related disaster recovery plans
- **DESC ISR** requires continuity of critical business processes, including identity as a core control domain

## Start the conversation before you have to

You don't need a complete strategy to get started. But waiting until identity fails is the most expensive time to figure it out. Across UAE and KSA, organizations are already asking the same questions - and the ones moving early are the ones avoiding reactive decisions later.

The next step is simply getting clarity on where you stand. Thales works with organizations across the region to assess identity resilience, surface continuity gaps, and help you understand what needs to change - without overcomplicating the path forward.

## About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

cpl.thalesgroup.com

**Contact us –** For contact information, please visit cpl.thalesgroup.com/contact-us