N2WS

MONTHLY WEBINAR SERIES

Episode 6:

DORA COMPLIANCE DEMYSTIFIED!

HOSTED BY

Sebastian Straub

Principal Solutions Architect

Jessica Eisenberg

Senior Global Campaigns Manager

Let’s start with a meme to set the tone...

What is the Digital Operational Resilience Act (DORA)?

1

What is it?

an EU regulation aimed at strengthening cybersecurity and digital resilience

2

Why was it created?

to ensure financial institutions can withstand, respond to, and recover from disruptions

3

When does it start?

DORA will be enforced starting **January 17th 2025**

TL;DR on N2WS

get.n2ws.com/tldr

Is DORA a burden or a necessity?

FOR EVEN MORE INFO...

Check out our **Ransomware TL;DR** episode: https://youtu.be/ST2N2m-5fI4

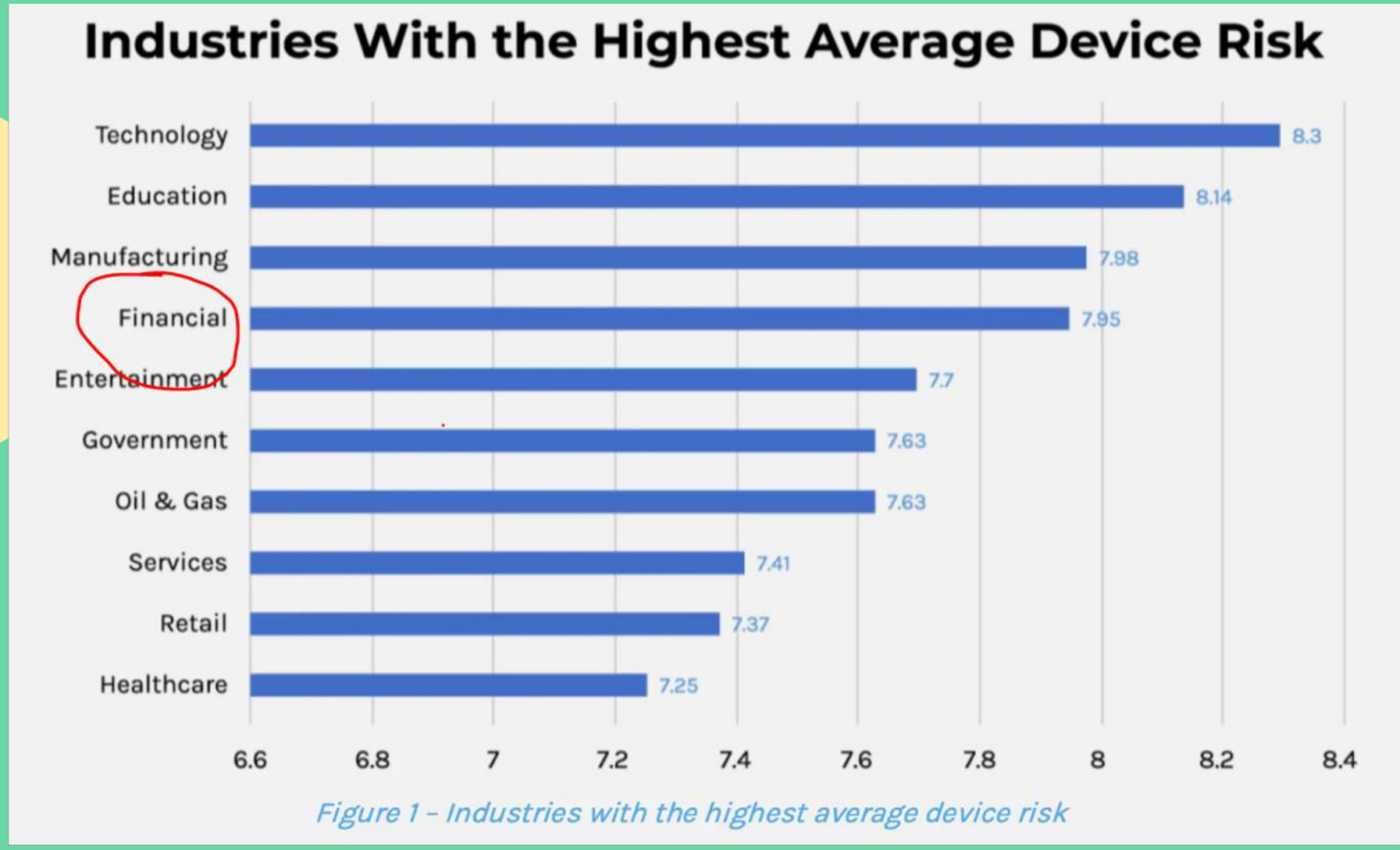


Figure 1 - Industries with the highest average device risk

TL;DR on N2WS

get.n2ws.com/tldr

Is my organization affected? Maybe ↓

✅ EU FINANCIAL INSTITUTIONS

Like banks, insurance, crypto-assets, and other financial entities physically located in the EU

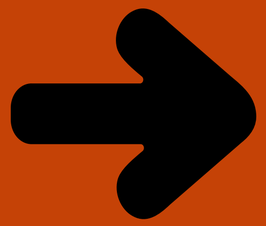
✅ NON-EU FINANCIAL ENTITIES

Even if your organization is NOT headquartered in the EU, but you do business there

✅ NON-FINANCIAL INSTITUTIONS

Are you an ICT provider who manages a financial company's data? Make sure you're keeping clients compliant

What even is an ICT (and why does DORA regulation keep mentioning it)?



Information and Communication Technologies that enable the management, processing, storage, and communication of information in organizations.

This can be any outsourced tech provider:

➡️ INTERNET SERVICE PROVIDER
➡️ CLOUD SERVICE PROVIDER
➡️ TELECOMMUNICATIONS COMPANIES

TL;DR on N2WS
get.n2ws.com/tldr

And, as if you need another headache, there are penalties

Unlike many other regulations, DORA also allows regulators to impose personal fines. And, in some cases, even criminal penalties.

2%

Fines are calculating according to your annual revenue – up to 2%

TL;DR on N2WS

get.n2ws.com/tldr

The 4 Main Pillars of DORA ↓

1. ICT Risk Management

Comprehensive frameworks to identify and mitigate ICT risks

2. Incident Reporting

Major incidents must be reported to competent authorities

3. Resilience Testing

Regular testing to ensure systems can withstand cyber threats

4. Third-Party Risk Management

Ensures resilience in third-party providers

TL;DR on N2WS

get.n2ws.com/tldr

IMPLEMENTING N2W FOR RAPID DORA COMPLIANCE

TL;DR on N2WS

get.n2ws.com/tldr

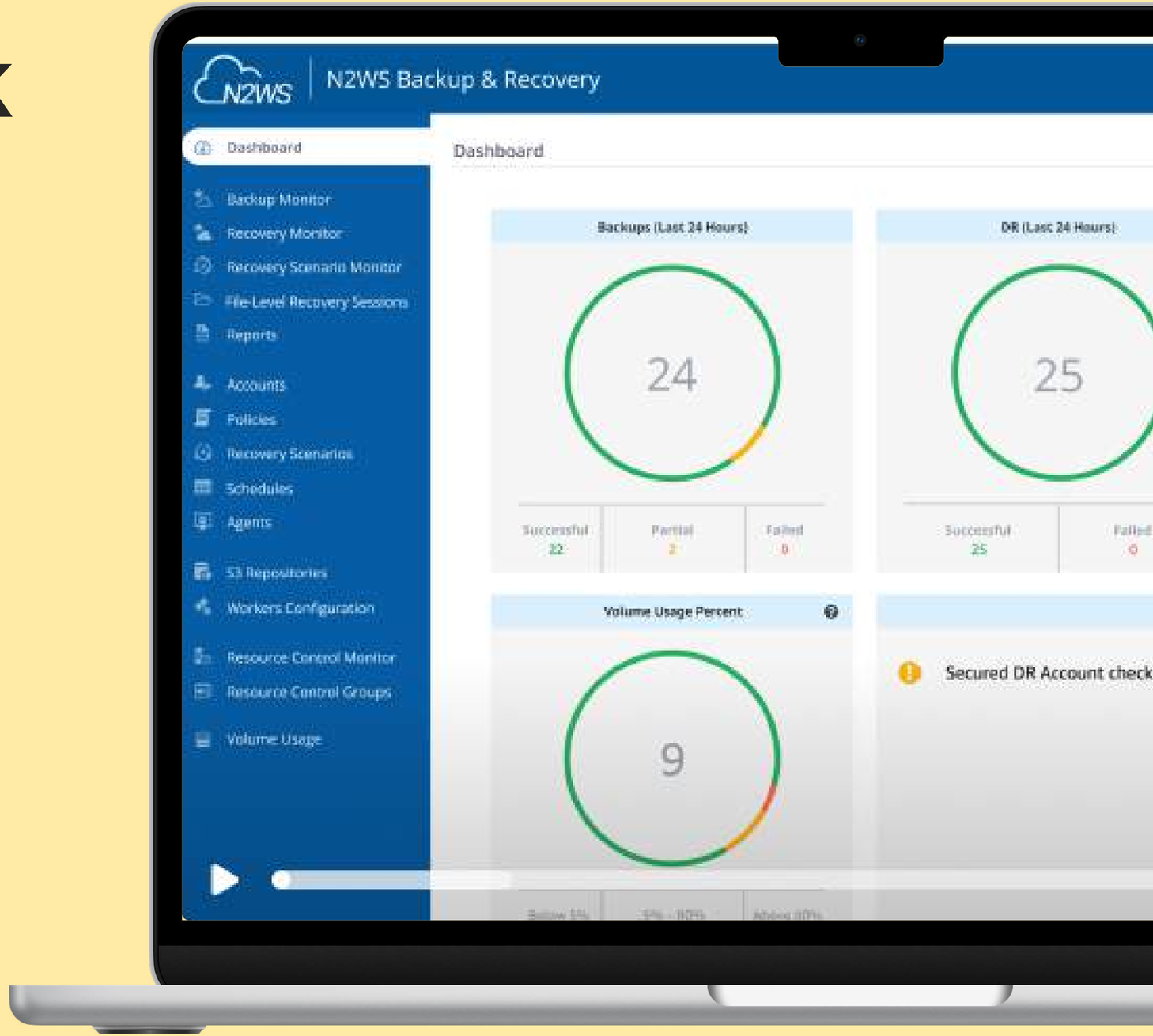
Pillar 1: ICT Risk Management

✅ Automate backups and copy to cross-region and cross-account

✅ Automate tagging of resources ensures that new resources are sorted into the appropriate backup policies

✅ Implement flexible backup schedules, 60 seconds to infinity

✅ Lock your backups using immutability

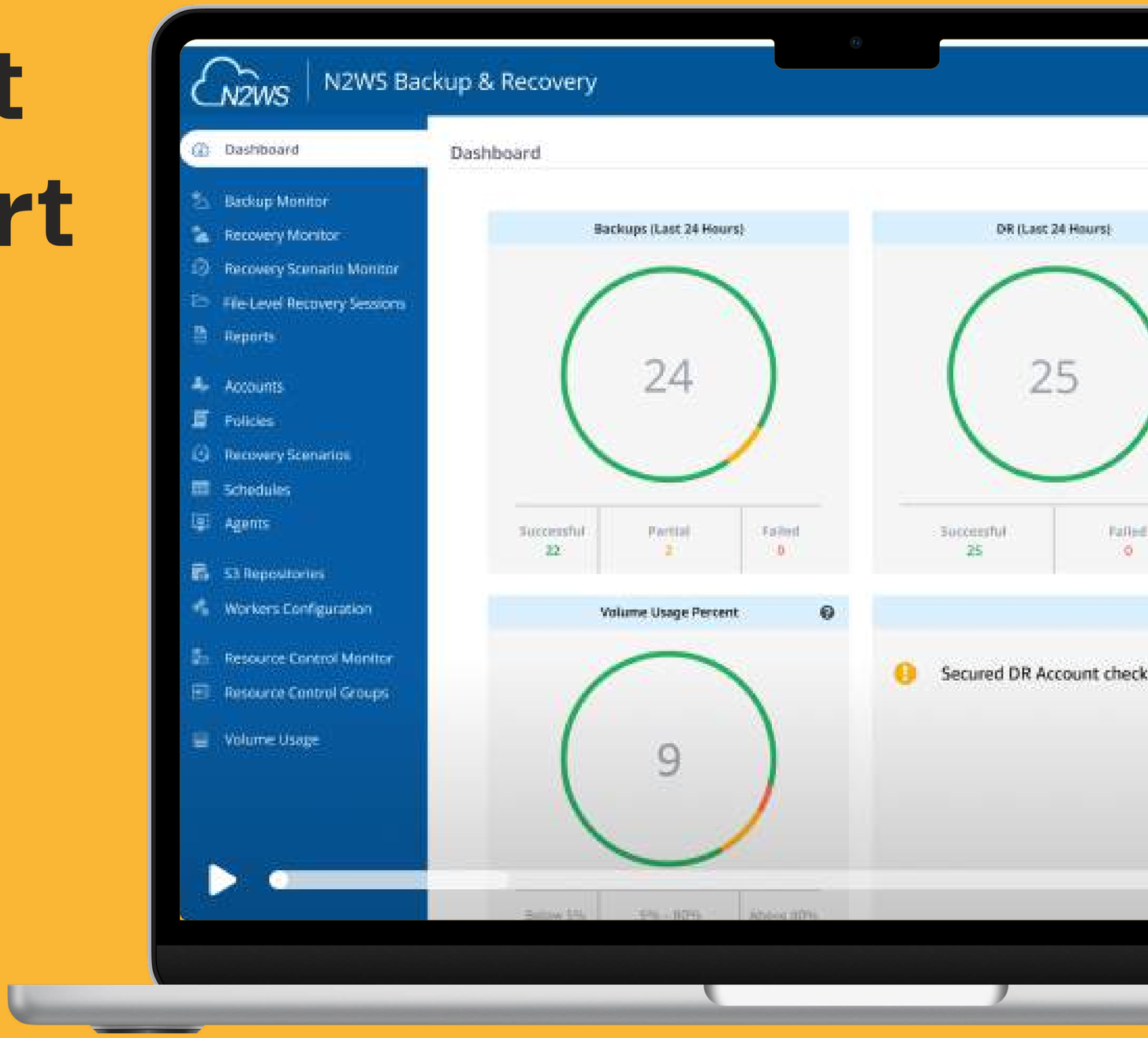


Pillar 2: Incident Response/Report

✅ **Encryption** to protect data (plus switching of encryption keys is simple and backup data is already encrypted).

✅ **Extensive audit trails** (Who? What? When? Where?)

✅ Internal data is protected by AES-256

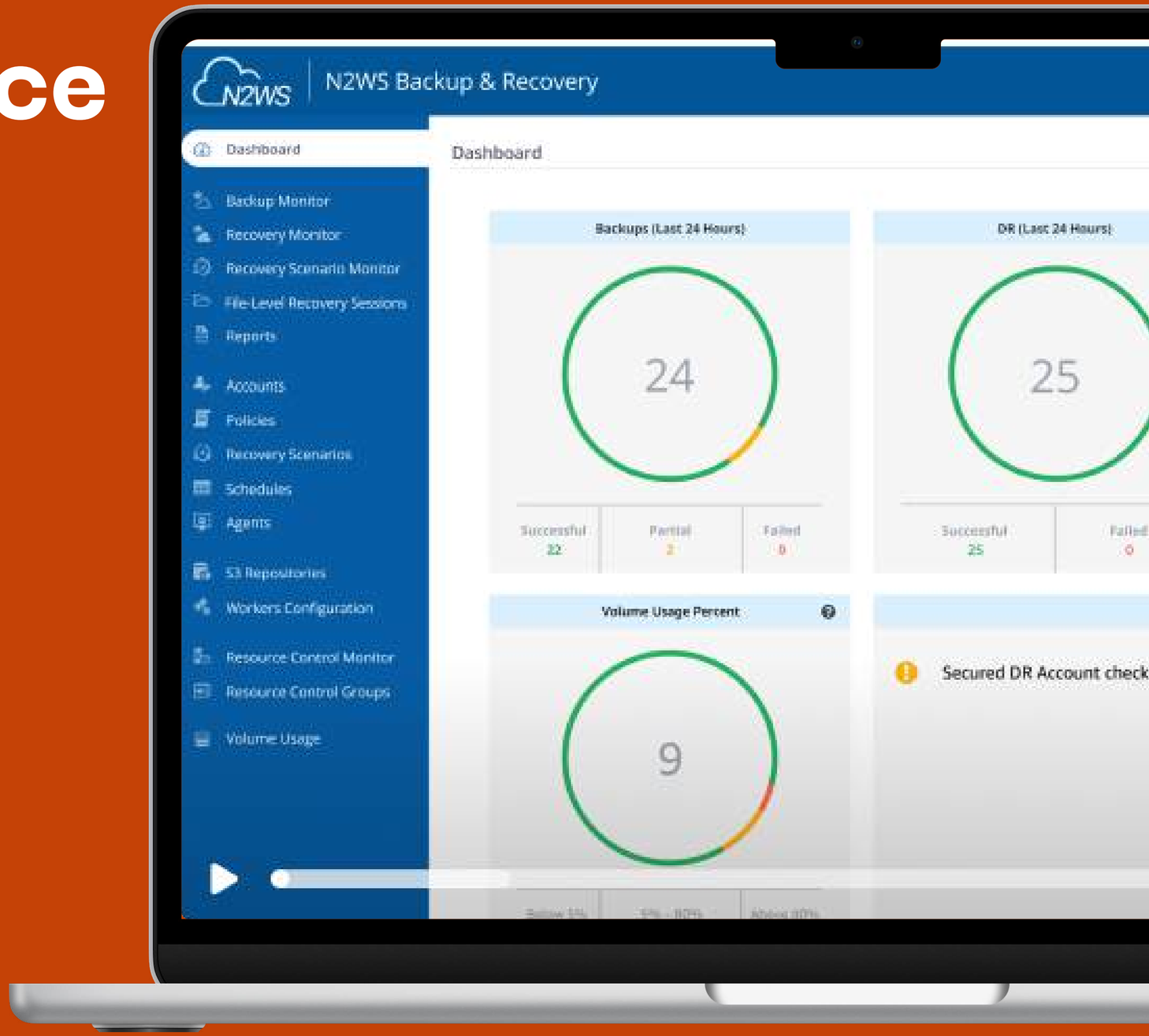


Pillar 3: Resilience Testing

✅ N2W has built-in tools for testing backup recoverability—saving your days of work

✅ N2W Recovery Scenarios allows for automated failover and failback

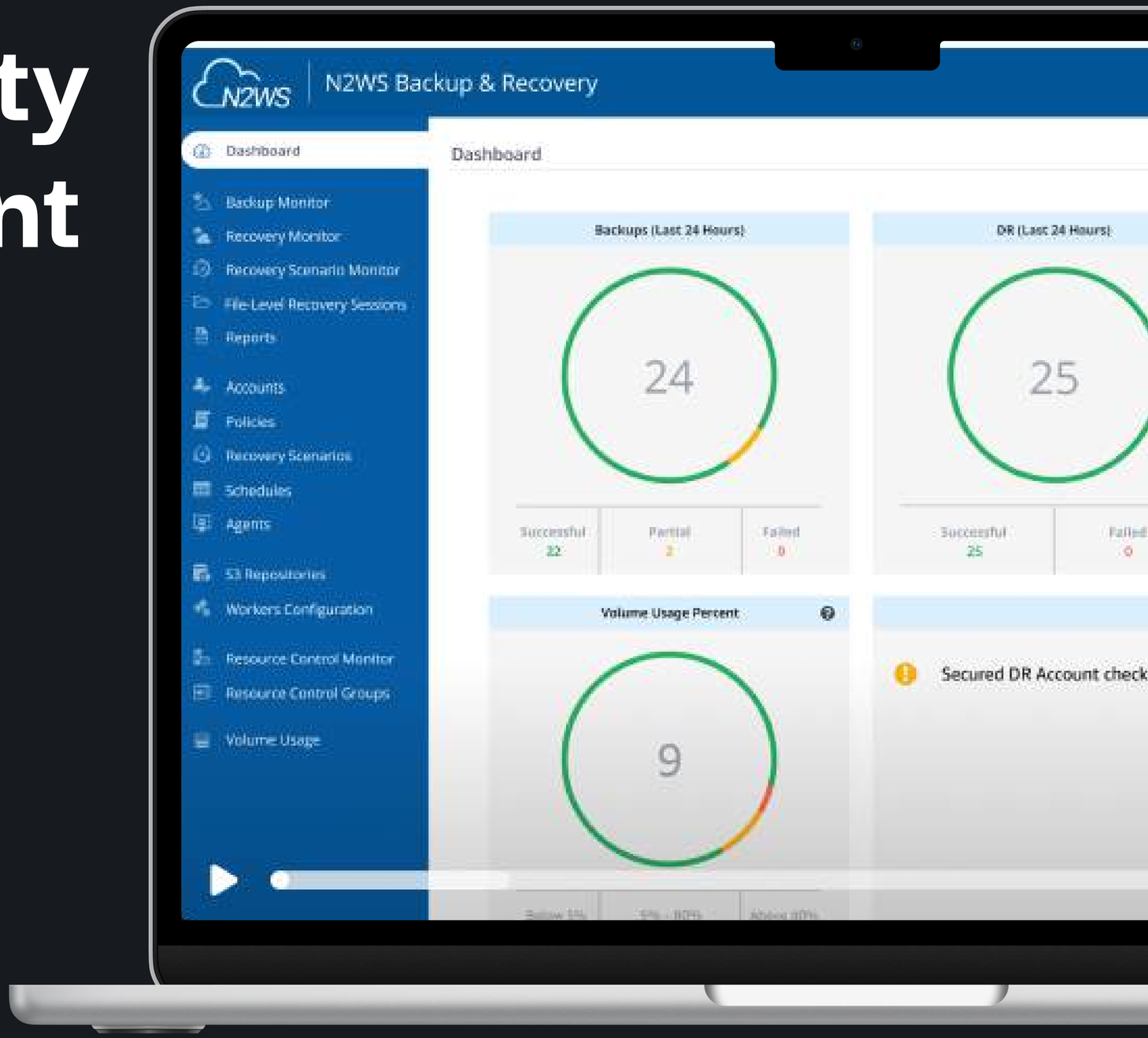
✅ You can also schedule customized recovery testing and DR “dry runs”



Pillar 4: 3rd-Party Risk Management

✅ Protect Resources in AWS and Azure in a single pane of glass

✅ Ensures resilience in third-party providers...



DORA = the perfect use for N2W

1

QUICK DEPLOY

which is important as the deadline is quickly approaching

2

STRONG SUPPORT

our professional services team is committed to your security

3

EASY COMPLIANCE

so you'll be ready for DORA!

Schedule a DORA compliance health check

email **info@n2ws.com**

TL;DR on N2WS

get.n2ws.com/tldr