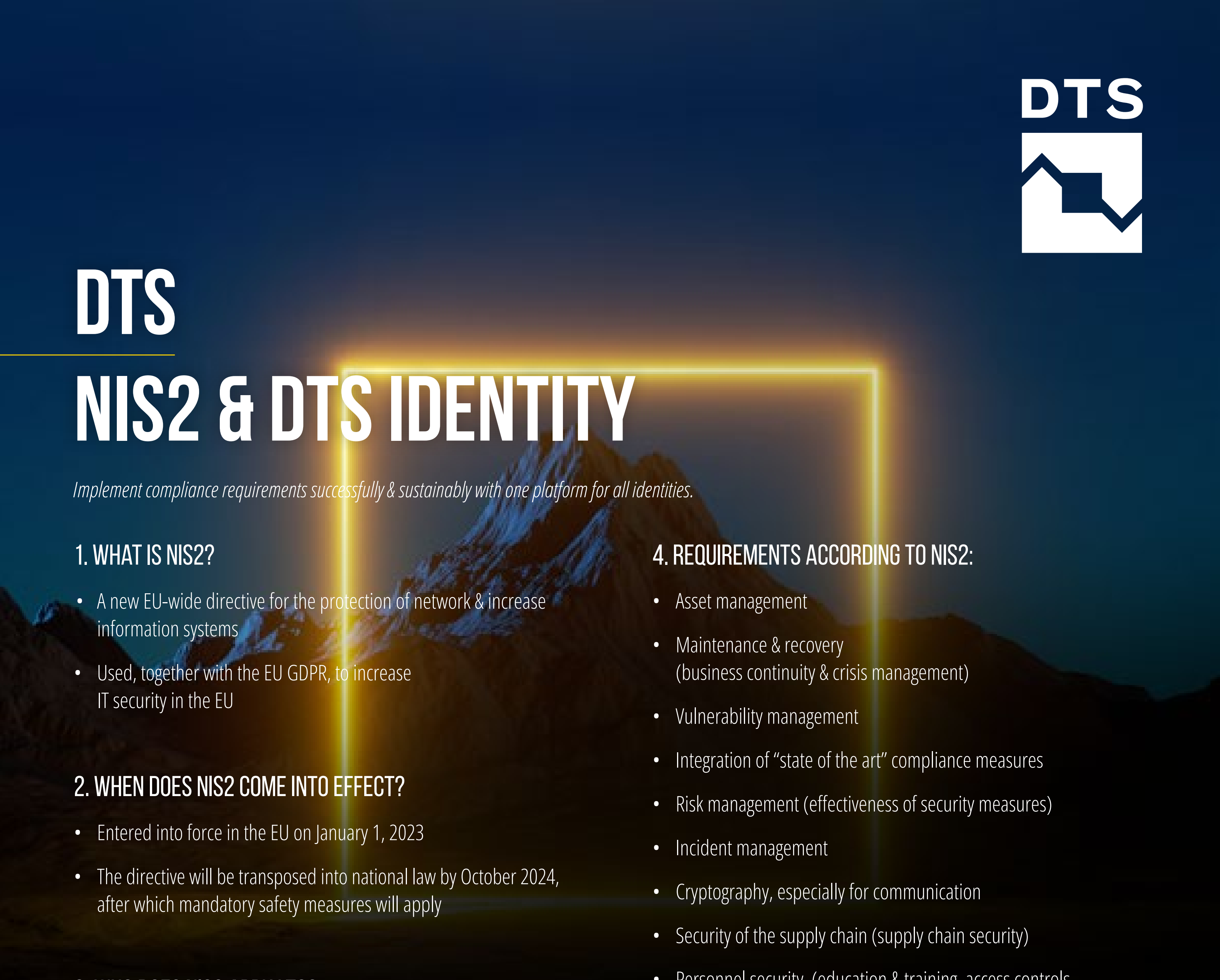


DTS

NIS2 & DTS IDENTITY

Implement compliance requirements successfully & sustainably with one platform for all identities.

1. WHAT IS NIS2?

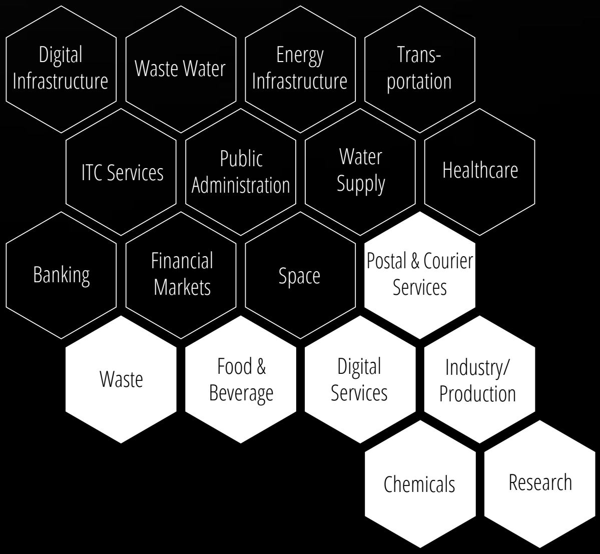
- A new EU-wide directive for the protection of network & increase information systems
- Used, together with the EU GDPR, to increase IT security in the EU

2. WHEN DOES NIS2 COME INTO EFFECT?

- Entered into force in the EU on January 1, 2023
- The directive will be transposed into national law by October 2024, after which mandatory safety measures will apply

3. WHO DOES NIS2 APPLY TO?

- For companies with at least 50 employees or at least € 10 million annual turnover
- In addition, companies must belong to one of these 18 affected sectors affected:



Digital Infrastructure
Waste Water
Energy Infrastructure
Trans-portation
ITC Services
Public Administration
Water Supply
Healthcare
Banking
Financial Markets
Space
Postal & Courier Services
Waste
Food & Beverage
Digital Services
Industry/ Production
Chemicals
Research

4. REQUIREMENTS ACCORDING TO NIS2:

- Asset management
- Maintenance & recovery (business continuity & crisis management)
- Vulnerability management
- Integration of “state of the art” compliance measures
- Risk management (effectiveness of security measures)
- Incident management
- Cryptography, especially for communication
- Security of the supply chain (supply chain security)
- Personnel security (education & training, access controls, authorization concept)
- Registration obligation, reporting obligations, sanctions & liability

5. NECESSARY MEASURES TO STRENGTHEN IT:

- Business continuity: Backup management, disaster recovery, crisis management
- Effectiveness: Specifications for measuring cyber & risk measures
- Purchasing: Security in the procurement of IT & network systems
- Incident management: Prevention, detection & management of security incidents
- Communication: Secure voice, video & text exchange
- Cryptography: Encryption wherever possible
- Policies: Guidelines for risks & information security
- Supply chain: Security in the supply chain
- Access control: Use of MFA & SSO

With DTS Identity, we can help you with the necessary measures! ⬇

6. THESE DTS IDENTITY FEATURES SUPPORT YOU IN FULFILLING THE REQUIREMENTS:

- ✓ Access control, access management & profile management:
  - Customer) Identity & Access Management (IAM & CIAM) ensures on a central platform that only authorized & entitled identities can access IT resources. In addition, DTS Identity protects your sensitive data (encrypted or hashed) & increases the overall level of security.
  - Multi-Factor Authentication (MFA) & Single Sign-On (SSO) for local or cloud apps: You log in once via your MFA for all approved apps and have access everywhere
  - Central, intuitive dashboard for all management & apps - as self-service, incl. CI customizing
- ✓ Policies:
  - Conditional access: Clear guidelines on who can access apps & information from where and with which MFA
  - Role-based Access Control (RBAC): A user can be assigned the appropriate role, with predefined access rights. This allows you to maintain an overview and control access to applications.
- ✓ Incident management:
  - Prevention & detection for traceability of access rights and logins → at a glance
  - Management: All access rights can be revoked directly
- ✓ Cryptography:
  - Encryption: None of the passwords are stored at DTS Identity & all are passed on in encrypted form
  - Breached Password Detection: Identification of breached users & passwords enables direct reaction
- ✓ Supply Chain: Security in the supply chain by integrating partners into DTS Identity via suitable B2B licenses
- ✓ Effectiveness: Evaluation of cyber & risk measures, as DTS Identity reporting is available at all times
- ✓ Communication: Secure voice, video & text communication through integration in DTS Identity
- ✓ More IT security in general:
  - Secure-by-Design architecture based on the Zero Trust principle (gclustered K8s environment that is resistant to brute force attacks as well as threats and DDoS)
  - Provided from our own certified & EU GDPR-compliant data centers

BUSINESS FLEXIBILITY

The cloud-native solution enables flexible adaptation to individual requirements. It can be implemented quickly and is scalable, making it easier to adapt to changes in the corporate landscape.

INCREASED SECURITY

The solution reduces the risk of cyberattacks and potential security incidents that could damage the company's reputation. This helps to strengthen the security posture and protect sensitive data.

COST & COMPLEXITY REDUCTION

he integration of security functions combines separate security products and makes the allocation of application licenses visible and easier to control. This leads to cost savings and a reduction in complexity.

INCREASE IN USER PRODUCTIVITY

The solution increases user satisfaction and efficiency by ensuring a consistent, fast and secure user experience from any location, regardless of the devices used and for all applications.

GET FREE & NON-BINDING ADVICE NOW!