netwrix

# NIS2: Safeguarding Data, Identity and Infrastructure

Evgenia Izotova,

Sales Team Leader Netwrix

# NIS2

Entered into force on January 16, 2023

Achieve a high level of cyber security

Address the change in cyber security threat landscape

# Who is covered?

EU member states

All companies with

> 50 employees
> 10 MIL EUR revenue

18 sectors

# What covered entities need to do?

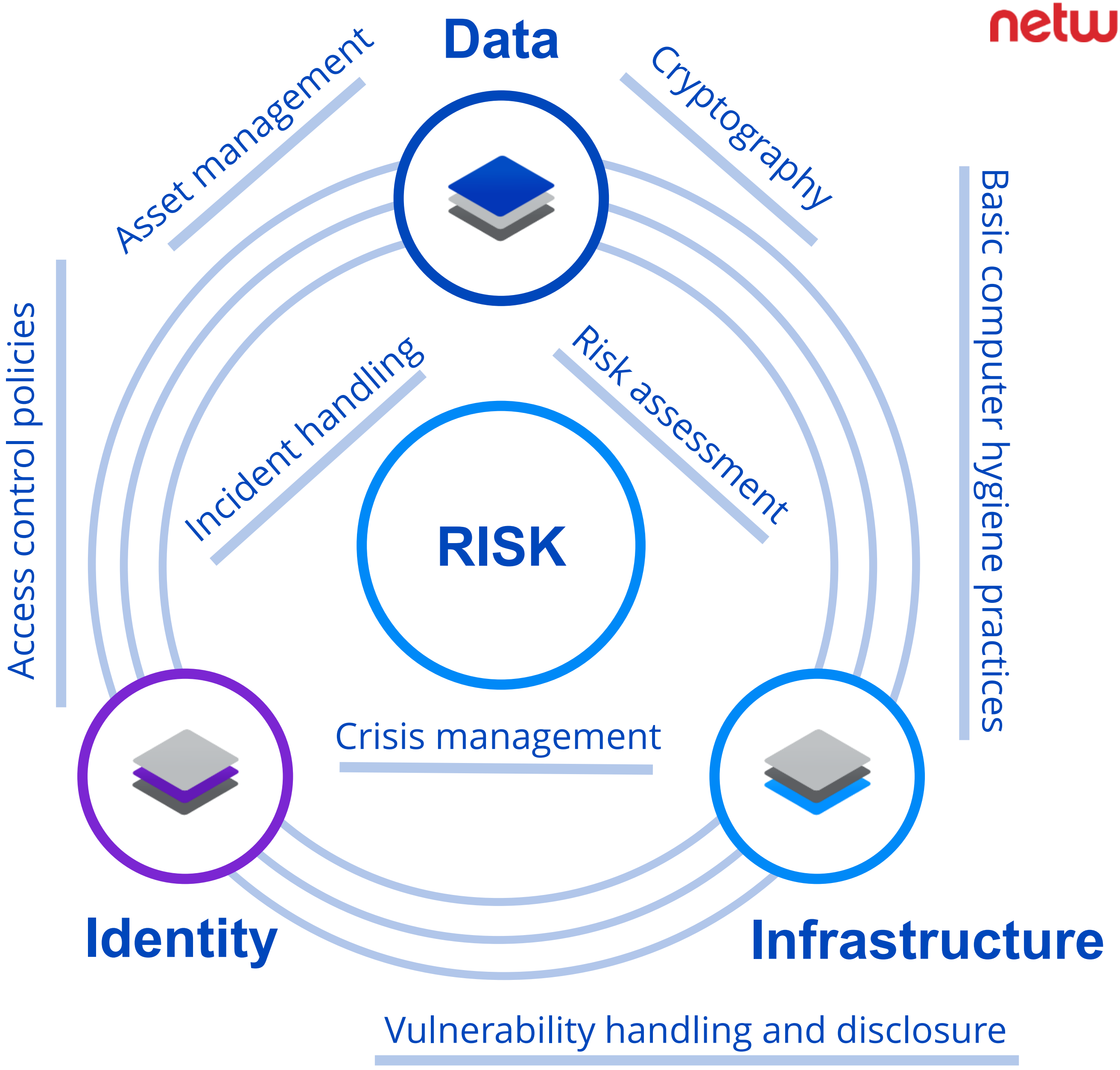
- Incident handling
- Crisis management
- Vulnerability handling and disclosure
- Risk assessment and management
- Asset management

- Basic computer hygiene practices
- Cybersecurity training
- Cryptography
- Human resource security
- Access control policies

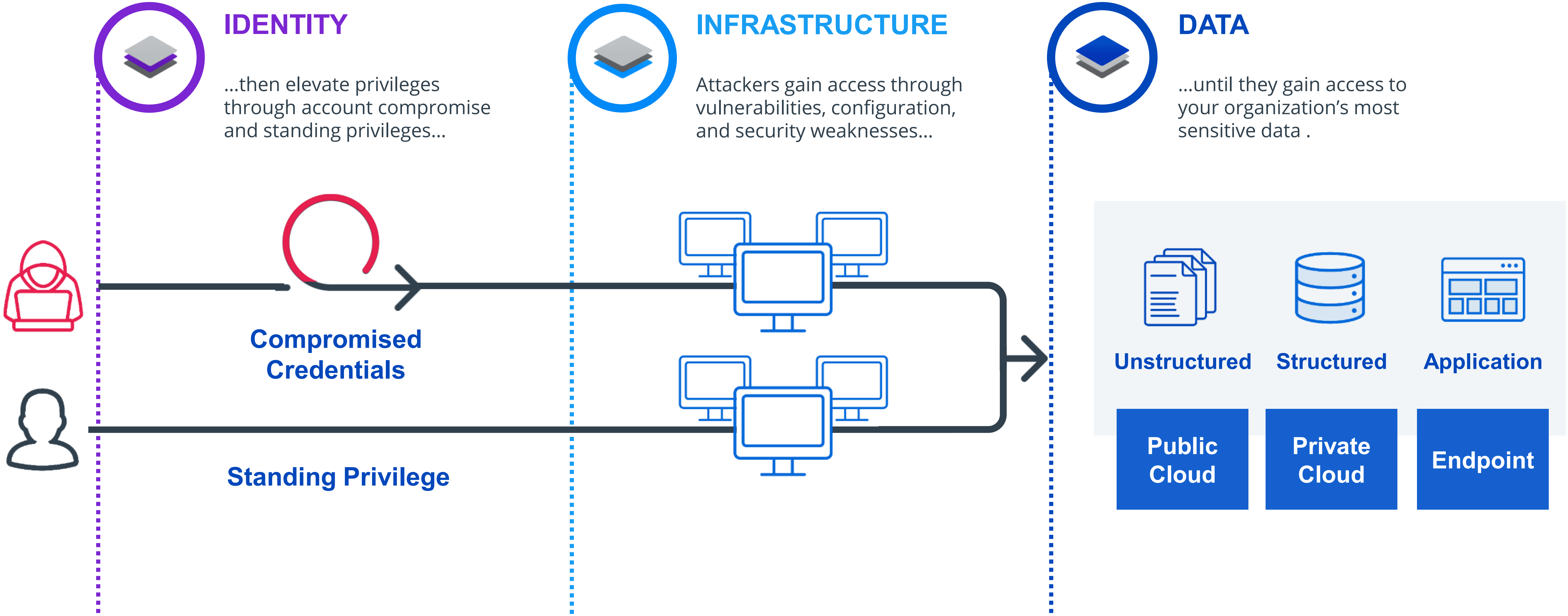
ORGANIZATIONAL MEASURES → PROCESSES

TECHNICAL MEASURES → HARDWARE AND SOFTWARE

# A Multi-Layered Approach is Required



# Secure All Three Attack Surfaces



## IDENTITY

...then elevate privileges through account compromise and standing privileges...

## INFRASTRUCTURE

Attackers gain access through vulnerabilities, configuration, and security weaknesses...

## DATA

...until they gain access to your organization’s most sensitive data .

Compromised Credentials

Standing Privilege

Unstructured

Structured

Application

Public Cloud

Private Cloud

Endpoint

# Measures: Organizational ► Technical

| | | MITIGATE | | REMEDIATE | | |
|---|---|---|---|---|---|---|
| | | IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER |
| ATTACK SURFACES | **DATA** | Which data is sensitive? | Who should have access to sensitive data? | Who is accessing sensitive data? | Do I have to report a data breach? | What data needs to be recovered? |
| | **IDENTITY** | Which accounts pose risk and why? | How do you secure privileged access and govern identities? | Is there any improper user activity? | How to respond to a threat faster? | How to undo improper AD changes? |
| | **INFRASTRUC-TURE** | What makes us vulnerable to threats? | How to prevent unwarranted changes? | What configuration changes were not approved? | How did an incident occur? | How could an incident have been stopped? |

# NIS2 Cyber Challenges

CONTROLLING ACCESS TO SENSITIVE DATA

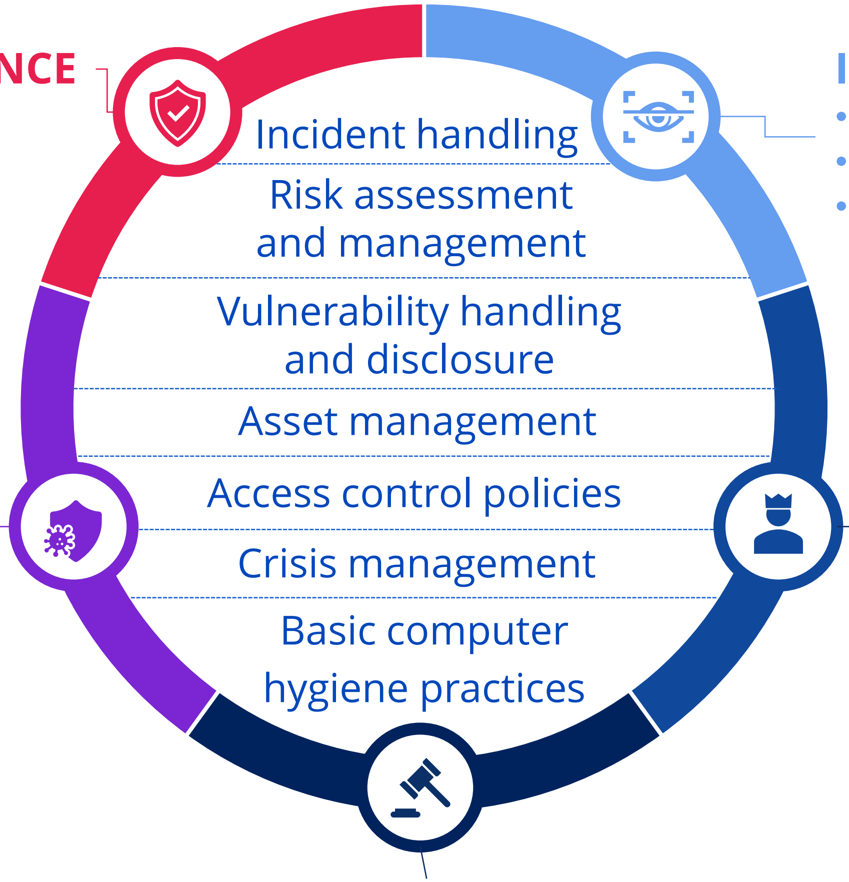
SECURING ALL IDENTITIES

RANSOMWARE THREATS AND OTHER CYBERATTACKS

PROTECTING ACTIVE DIRECTORY

COMPLIANCE REPORTING

# Solutions To Those Challenges



**DATA ACCESS GOVERNANCE**

**IDENTITY AND ACCESS MANAGEMENT**

- Privileged Access Management
- Identity Governance and Administration
- Access Management

Incident handling

Risk assessment and management

Vulnerability handling and disclosure

Asset management

Access control policies

Crisis management

Basic computer hygiene practices

**PROTECTION FROM RANSOMWARE AND OTHER CYBERATTACKS**

**ACTIVE DIRECTORY SECURITY**

**AUTOMATED COMPLIANCE REPORTING**

# NIS2 & Risk Assessment

An important aspect of NIS2 is the introduction of a **risk assessment** obligation for the companies involved, which must **assess and manage cyber risks** deriving from internal and external sources. This also involves considering the measures taken by your suppliers and monitoring your supply chain, carrying out regular and thorough checks on the third parties involved.

Based on the results of the risk assessment, the NIS2 Directive sets out a number of technical and organizational measures that companies classified as "essential" and "important" must comply with.

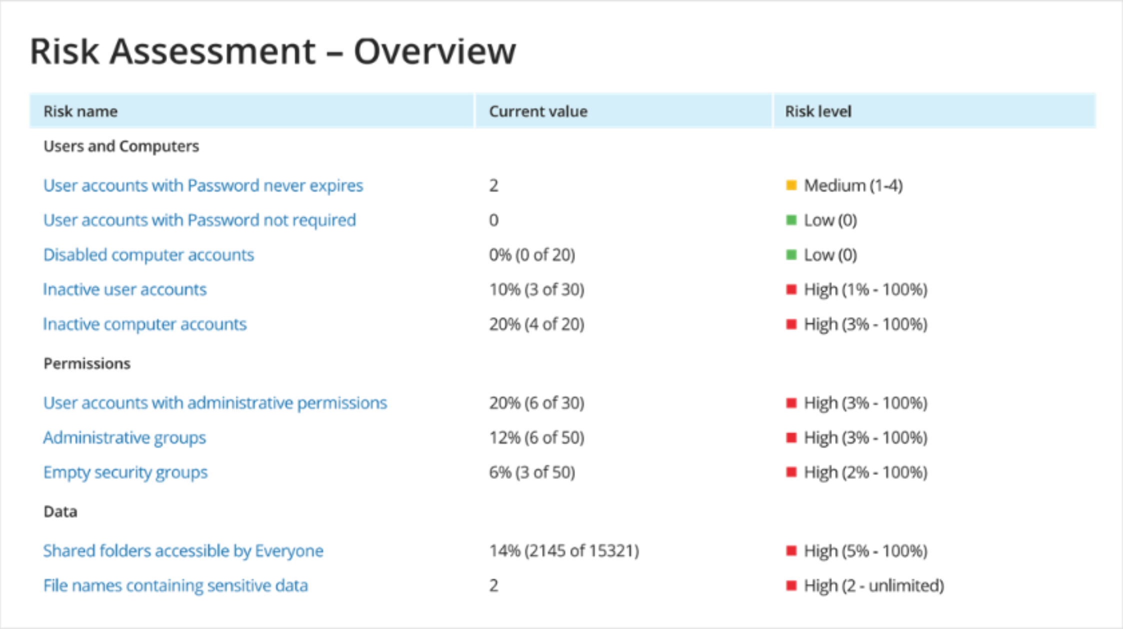
# Art. §21.2.a requires the implementation of risk analysis and security policies of information systems, what Netwrix Solutions can help organizations in this process?

# Risk analysis and security policies for IT systems

## Risk Assessment

Netwrix Auditor allows you to assess data, identity and infrastructure security risks as required by **Art. §21.2.a: Risk Analysis and Security Policies of Information Systems**

Data, identity, and infrastructure security gaps are identified, such as a large number of directly assigned permissions or too many inactive user accounts. These safety parameters are continuously evaluated and displayed through an intuitive, simple and interactive dashboard that allows you to intervene in real time on risks

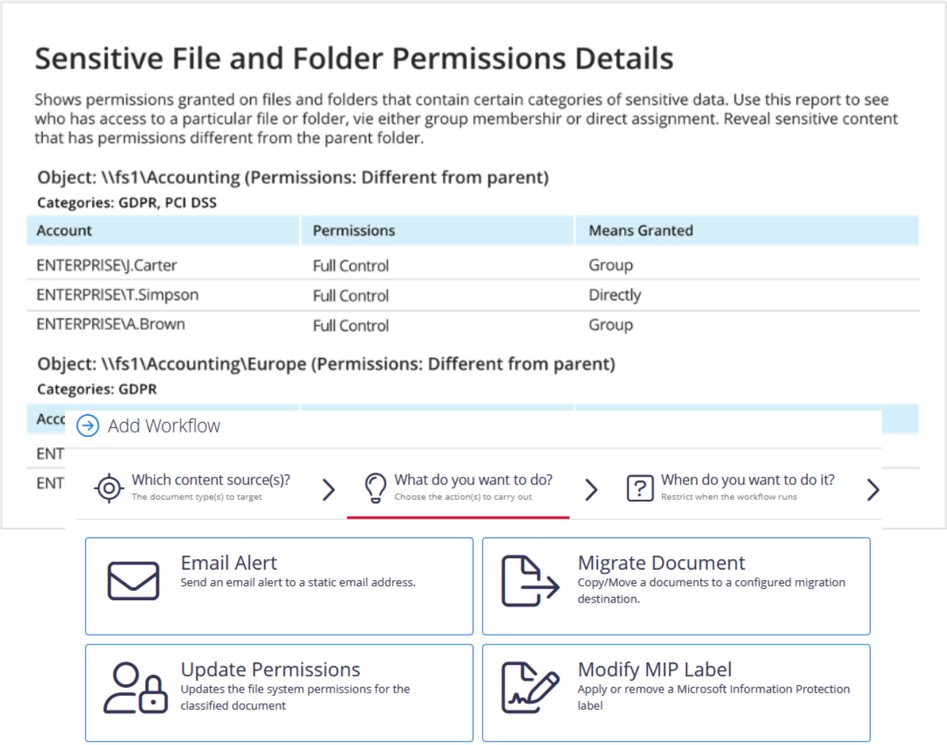


### Risk Assessment – Overview

| Risk name | Current value | Risk level |
|---|---|---|
| Users and Computers | | |
| User accounts with Password never expires | 2 | 🟨 Medium (1-4) |
| User accounts with Password not required | 0 | 🟩 Low (0) |
| Disabled computer accounts | 0% (0 of 20) | 🟩 Low (0) |
| Inactive user accounts | 10% (3 of 30) | 🟥 High (1% - 100%) |
| Inactive computer accounts | 20% (4 of 20) | 🟥 High (3% - 100%) |
| Permissions | | |
| User accounts with administrative permissions | 20% (6 of 30) | 🟥 High (3% - 100%) |
| Administrative groups | 12% (6 of 50) | 🟥 High (3% - 100%) |
| Empty security groups | 6% (3 of 50) | 🟥 High (2% - 100%) |
| Data | | |
| Shared folders accessible by Everyone | 14% (2145 of 15321) | 🟥 High (5% - 100%) |
| File names containing sensitive data | 2 | 🟥 High (2 - unlimited) |

Netwrix Auditor

# Risk analysis and security policies for IT systems



## Sensitive File and Folder Permissions Details

Shows permissions granted on files and folders that contain certain categories of sensitive data. Use this report to see who has access to a particular file or folder, vie either group membershir or direct assignment. Reveal sensitive content that has permissions different from the parent folder.

Object: \\fs1\Accounting (Permissions: Different from parent)

**Categories: GDPR, PCI DSS**

| Account | Permissions | Means Granted |
|---|---|---|
| ENTERPRISE\J.Carter | Full Control | Group |
| ENTERPRISE\T.Simpson | Full Control | Directly |
| ENTERPRISE\A.Brown | Full Control | Group |

Object: \\fs1\Accounting\Europe (Permissions: Different from parent)

**Categories: GDPR**

| Acc |
|---|
| ENT |
| ENT |

Add Workflow

Which content source(s)? The document type(s) to target › What do you want to do? Choose the action(s) to carry out › When do you want to do it? Restrict when the workflow runs ›

Email Alert
Send an email alert to a static email address.

Migrate Document
Copy/Move a documents to a configured migration destination.

Update Permissions
Updates the file system permissions for the classified document

Modify MIP Label
Apply or remove a Microsoft Information Protection label

### Regular Claims of Privilege Are Simplified

Netwrix Auditor and Data Classification allow you to find out who has access to what sensitive data and how they have gained that access, enabling data owners to regularly verify that those rights align with business needs. This makes it easier to understand which excess permissions to remove to enforce the principle of least privilege and keep risk at an acceptable level.

### Ability to automatically quarantine sensitive data to reduce the risk of a breach or loss

If a sensitive document is in an unexpected location, it is automatically moved to a quarantine area until it is determined where it should be stored and who should access it.

### Immediately block overexposed sensitive data

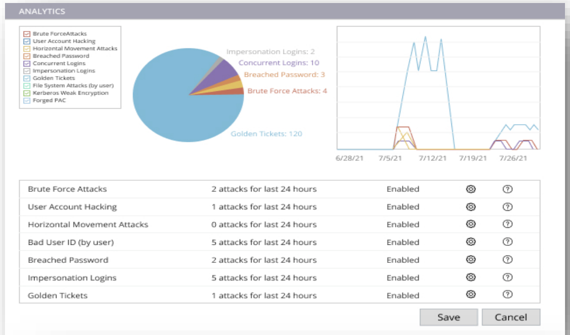
If access controls for sensitive data aren't appropriate for the risk, automatically remove all rights or change the permissions of global access groups, such as Everyone.

**Netwrix Auditor** **Netwrix Data Classification**

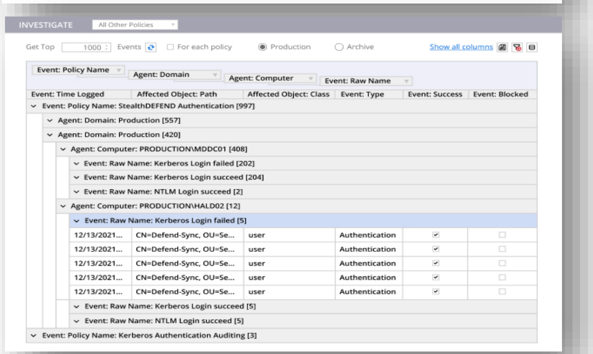
# What Netwrix solutions help to comply with ART. §21.2.b for incident management, as well as to comply with reporting obligations as required under ART. 23?

# Incident handling & Reporting obligations

## Netwrix StealthINTERCEPT



| | | | | |
|---|---|---|---|---|
| Brute Force Attacks | 2 attacks for last 24 hours | Enabled | ⚙ | ⓘ |
| User Account Hacking | 1 attacks for last 24 hours | Enabled | ⚙ | ⓘ |
| Horizontal Movement Attacks | 0 attacks for last 24 hours | Enabled | ⚙ | ⓘ |
| Bad User ID (by user) | 5 attacks for last 24 hours | Enabled | ⚙ | ⓘ |
| Breached Password | 2 attacks for last 24 hours | Enabled | ⚙ | ⓘ |
| Impersonation Logins | 5 attacks for last 24 hours | Enabled | ⚙ | ⓘ |
| Golden Tickets | 1 attacks for last 24 hours | Enabled | ⚙ | ⓘ |



Get Top 1000 Events □ For each policy ● Production ○ Archive

Event: Policy Name · Agent: Domain · Agent: Computer · Event: Raw Name

| Event: Time Logged | Affected Object: Path | Affected Object: Class | Event: Type | Event: Success | Event: Blocked |
|---|---|---|---|---|---|
| Event: Policy Name: StealthDEFEND Authentication [997] | | | | | |
| Agent: Domain: Production [557] | | | | | |
| Agent: Domain: Production [420] | | | | | |
| Agent: Computer: PRODUCTION\MDDC01 [408] | | | | | |
| Event: Raw Name: Kerberos Login failed [202] | | | | | |
| Event: Raw Name: Kerberos Login succeed [204] | | | | | |
| Event: Raw Name: NTLM Login succeed [2] | | | | | |
| Agent: Computer: PRODUCTION\HALD02 [12] | | | | | |
| Event: Raw Name: Kerberos Login failed [5] | | | | | |
| 12/13/2021... | CN=Defend-Sync, OU=Se... | user | Authentication | ☑ | □ |
| 12/13/2021... | CN=Defend-Sync, OU=Se... | user | Authentication | ☑ | □ |
| 12/13/2021... | CN=Defend-Sync, OU=Se... | user | Authentication | ☑ | □ |
| 12/13/2021... | CN=Defend-Sync, OU=Se... | user | Authentication | ☑ | □ |
| 12/13/2021... | CN=Defend-Sync, OU=Se... | user | Authentication | ☑ | □ |
| Event: Raw Name: Kerberos Login succeed [5] | | | | | |
| Event: Raw Name: NTLM Login succeed [5] | | | | | |
| Event: Policy Name: Kerberos Authentication Auditing [3] | | | | | |

Netwrix StealthINTERCEPT alerts you in real-time about changes, authentications, and other suspicious or risky events within your infrastructure so you can prevent them from turning into breaches.

StealthINTERCEPT combines an enriched and optimized audit activity stream with relevant contextual data to effectively build organizational behavioral profiles using unsupervised machine learning algorithms.
Slash the time spent on audit preparation with a wide variety of compliance reports aligned with common standards.

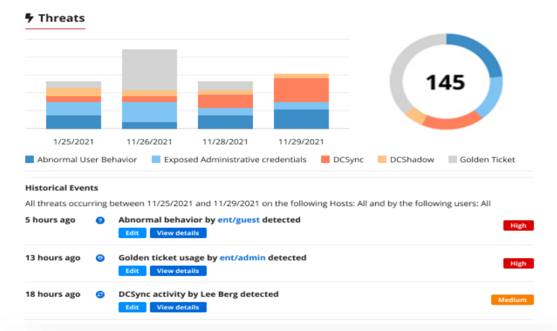
It also allows you to prevent critical events from happening.

## Netwrix Threat Manager

Netwrix Threat Manager is a real-time threat detection and response solution that enable you to respond immediately to threat detection by leveraging the comprehensive catalog of pre-configured response actions or by integrating Netwrix Threat Manager into your business processes, using PowerShell or webhook frameworks.

The result is the ability to detect, correlate, and respond to anomalous behavior and advanced attacks with unprecedented accuracy and speed.

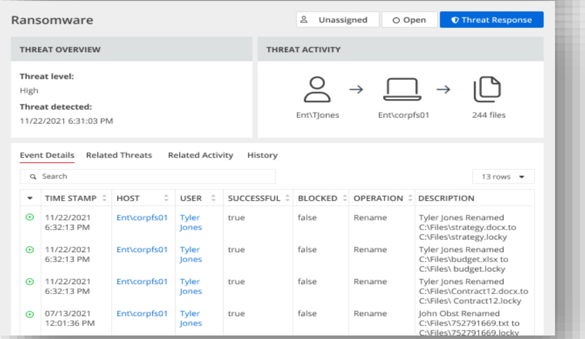
Easily gather the entire timeline of related events that comprised an attack to simplify investigation, threat analysis and recovery



Historical Events

All threats occurring between 11/25/2021 and 11/29/2021 on the following Hosts: All and by the following users: All

| | | |
|---|---|---|
| 5 hours ago | Abnormal behavior by ent/guest detected<br>Edit View details | High |
| 13 hours ago | Golden ticket usage by ent/admin detected<br>Edit View details | High |
| 18 hours ago | DCSync activity by Lee Berg detected<br>Edit View details | Medium |



Ransomware

THREAT OVERVIEW

Threat level:
High

Threat detected:
11/22/2021 6:31:03 PM

THREAT ACTIVITY

| TIME STAMP | HOST | USER | SUCCESSFUL | BLOCKED | OPERATION | DESCRIPTION |
|---|---|---|---|---|---|---|
| 11/22/2021 6:32:13 PM | Ent\corpfs01 | Tyler Jones | true | false | Rename | Tyler Jones Renamed C:\Files\strategy.docx.to C:\Files\strategy.locky |
| 11/22/2021 6:32:13 PM | Ent\corpfs01 | Tyler Jones | true | false | Rename | Tyler Jones Renamed C:\Files\budget.xlsx to C:\Files\ budget.locky |
| 11/22/2021 6:32:13 PM | Ent\corpfs01 | Tyler Jones | true | false | Rename | Tyler Jones Renamed C:\Files\Contract12.docx.to C:\Files\ Contract12.locky |
| 07/13/2021 12:01:36 PM | Ent\corpfs01 | Tyler Jones | true | false | Rename | John Obst Renamed C:\Files\752791669.txt to C:\Files\752791669.locky |

**Netwrix StealthINTERCEPT**

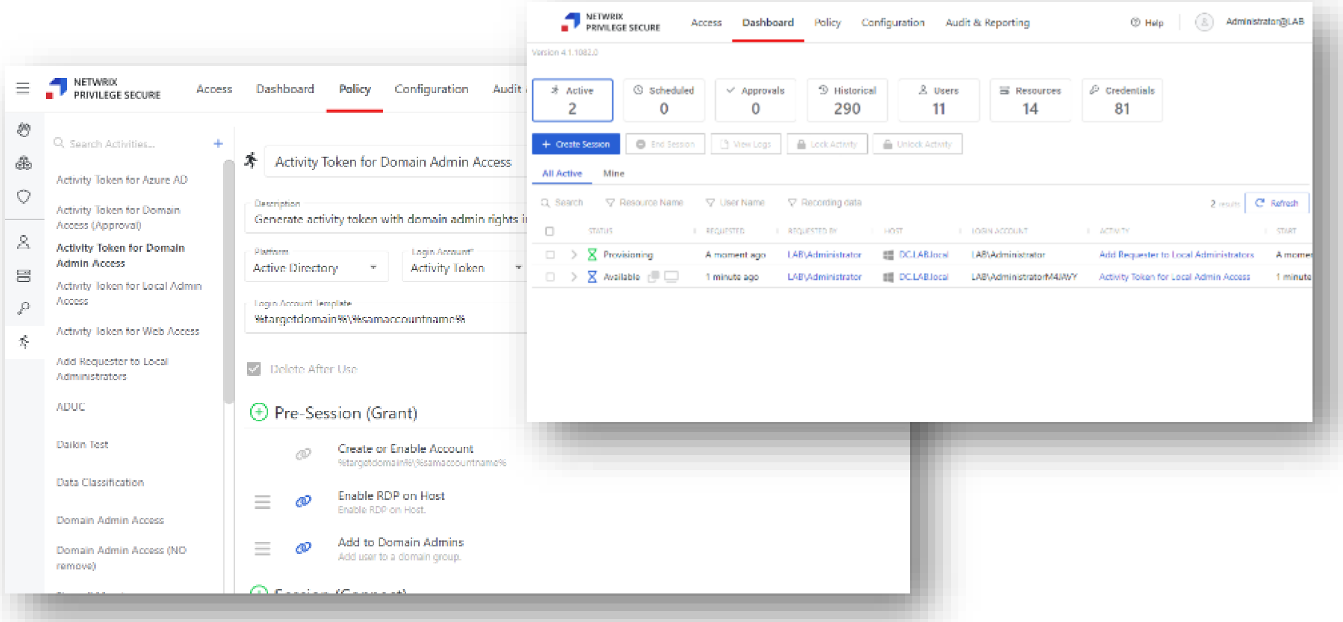
**Netwrix Threat Manager**

Another key point is art. §21.2.d supply chain security, and ART. §21.2.i which requires you to implement access control and asset management strategies; How Netwrix can help?

# Access control policies & supply chain security

### Privilege Access Management

- Remove standing privileges to reduce risk
- Grant the right access to the right users with just-in-time access
- Closely monitor the activity of third-party user accounts and applications that connect remotely to your systems and applications, even if their activity doesn’t produce any logs, to ensure full accountability. Get notified anytime a vendor does something outside of their approved scope, since their unauthorized actions could put your data at risk.



Activity Token for Azure AD
Activity Token for Domain Access (Approval)
**Activity Token for Domain Admin Access**
Activity Token for Local Admin Access
Activity Token for Web Access
Add Requester to Local Administrators
ADUC
Daikin Test
Data Classification
Domain Admin Access
Domain Admin Access (NO remove)

Activity Token for Domain Admin Access

Description: Generate activity token with domain admin rights i

Platform: Active Directory

Login Account*: Activity Token

Login Account Template: %targetdomain%\%samaccountname%

☑ Delete After Use

Pre-Session (Grant)

- Create or Enable Account — %targetdomain%\%samaccountname%
- Enable RDP on Host — Enable RDP on Host.
- Add to Domain Admins — Add user to a domain group.

Session (Connect)

| Active | Scheduled | Approvals | Historical | Users | Resources | Credentials |
|---|---|---|---|---|---|---|
| 2 | 0 | 0 | 290 | 11 | 14 | 81 |

| STATUS | REQUESTED | REQUESTED BY | HOST | LOGIN ACCOUNT | ACTIVITY | START |
|---|---|---|---|---|---|---|
| Provisioning | A moment ago | LAB\Administrator | DC.LAB.local | LAB\Administrator | Add Requester to Local Administrators | A mome |
| Available | 1 minute ago | LAB\Administrator | DC.LAB.local | LAB\AdministratorM4JWY | Activity Token for Local Admin Access | 1 minute |

## Just-in-Time Orchestration

Creare ciò che serve per svolgere un'attività specifica nel momento in cui serve, e rimuovere la superficie di attacco quando non la si utilizza.

### Identity

- Create / Remove Accounts
- Enable / Disable Accounts

### Privilege

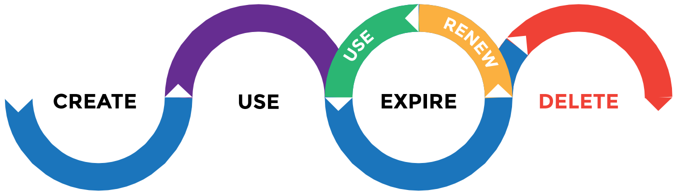
- Add / Remove Permissions
- Enforce Group Membership

### Endpoint

- Enable/Disable RDP
- Purge Kerberos Tickets
- Pre/Post File Comparison
- Dynamic SMB Shares
- Custom PowerShell
- Dynamic sudoers

## Netwrix Privilege Secure

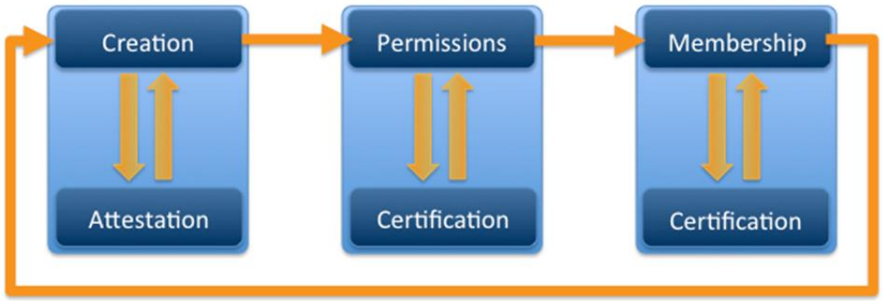
# Access control policies & supply chain security



- Provisioning User Objects from an Authoritative Source
- Viewing Users, Groups, Memberships, and Attributes
- Link objects across identity stores
- Establish a clear managerial hierarchy, including dotted line management
- Deprovision user accounts at the right time
- Evaluate on-premises and cloud resource permissions
- Transfer and terminate accounts with one click
- Enable managers to manage their direct reports, groups, and permissions
- Unlock accounts and reset passwords

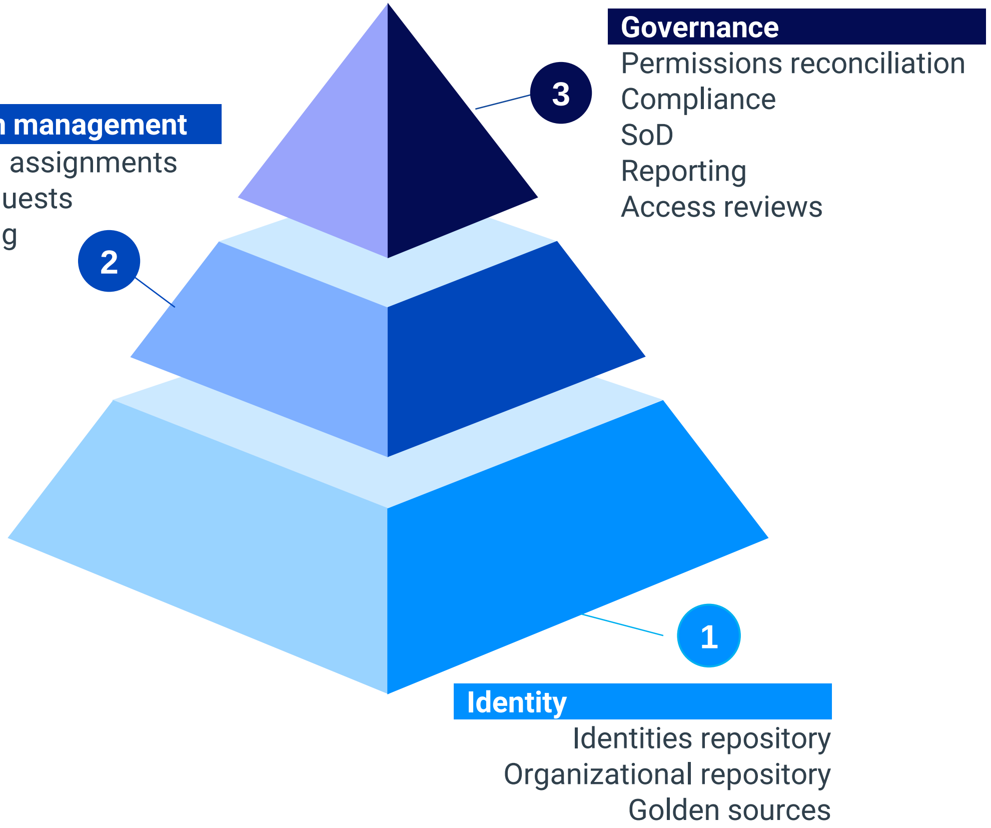
**Identity Management**

**Group Management**



**Netwrix GroupID**

# Access control policies & supply chain security



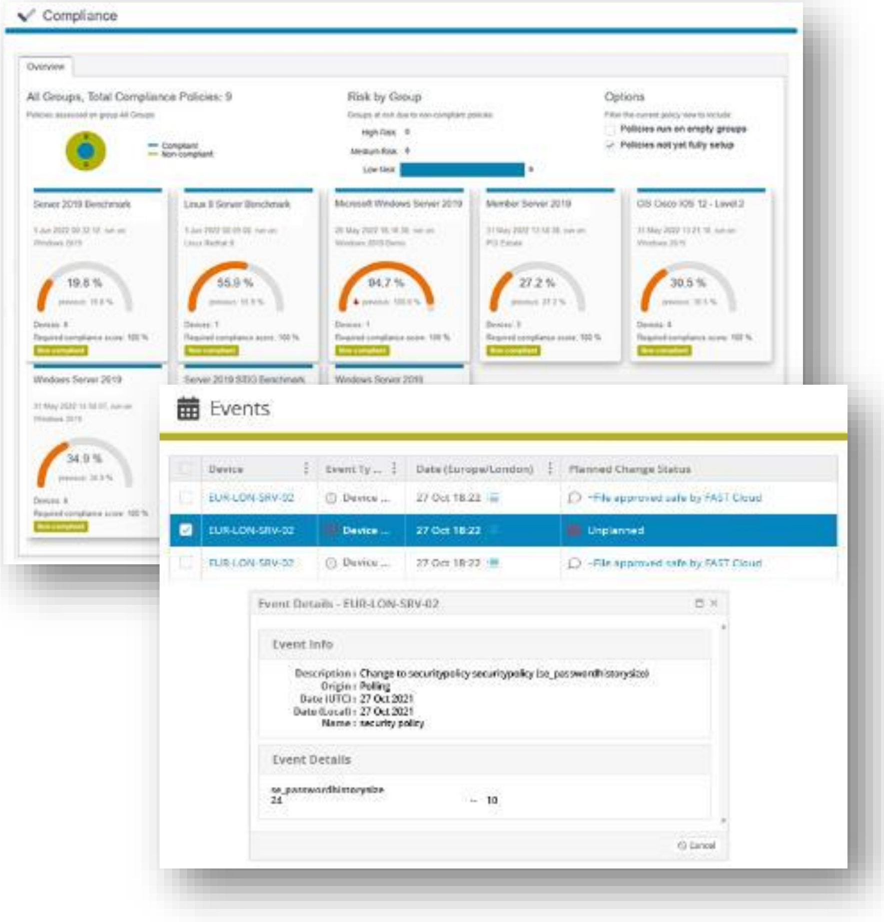
**Ensure users have the right access to the right things at the right time**

- Usercube builds a repository of organizations, sites, users and resources, from different sources, to become the centralized location for reliable and exhaustive information.
- Each user can make a request to obtain, modify or revoke access rights or equipment for the users in their scope. Workflows enable you to push the request to the appropriate people in order to obtain approval and/or start processing the request as soon as possible.
- Usercube enables compliance verification of access rights granted based on rules in place for your organization
- IGA brings together all of your organization’s processes to enable each identified individual to have the correct access rights at the right time for the right reasons.

Netwrix Usercube

# No less important is ART. §21.2.e Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure; What solutions Netwrix offer?

# Configuration management & vulnerability handling



| | Device | Event Ty ... | Date (Europe/London) | Planned Change Status |
|---|---|---|---|---|
| □ | EUR-LON-SRV-02 | Device ... | 27 Oct 18:22 | ~File approved safe by FAST Cloud |
| ☑ | EUR-LON-SRV-02 | Device ... | 27 Oct 18:22 | Unplanned |
| □ | EUR-LON-SRV-02 | Device ... | 27 Oct 18:22 | ~File approved safe by FAST Cloud |

Event Details - EUR-LON-SRV-02

Event Info

Description : Change to securitypolicy securitypolicy (se_passwordhistorysize)
Origin : Polling
Date (UTC) : 27 Oct 2021
Date (Local) : 27 Oct 2021
Name : security policy

Event Details

se_passwordhistorysize
24 ← 10

System Hardening-File Integrity Monitoring-Compliance & Forensic Analysis

- Netwrix Change Tracker reduces "change noise" and false positives by more than 90% by creating a set of scheduled change rules. Enables automatic approval of legitimate files based on reputation with the Netwrix FAST Threat Intelligence service. Verify that your most important system files are genuine by cross-checking against a database of over 10 billion file reputations.
- Change Tracker has a machine learning capability to quickly extend existing scheduled change rules to capture relevant unplanned events, or even to create new intelligent scheduled change rules on the fly.
- Identifies vulnerabilities in software and server configurations and close these gaps before they are exploited

Automated CIS Controls - Continuous Compliance

Reduce the work required to demonstrate compliance by automating repetitive tasks and using over **250 CIS-certified reports** including NIST, PCI DSS, CMMC, STIG, and NERC CIP.

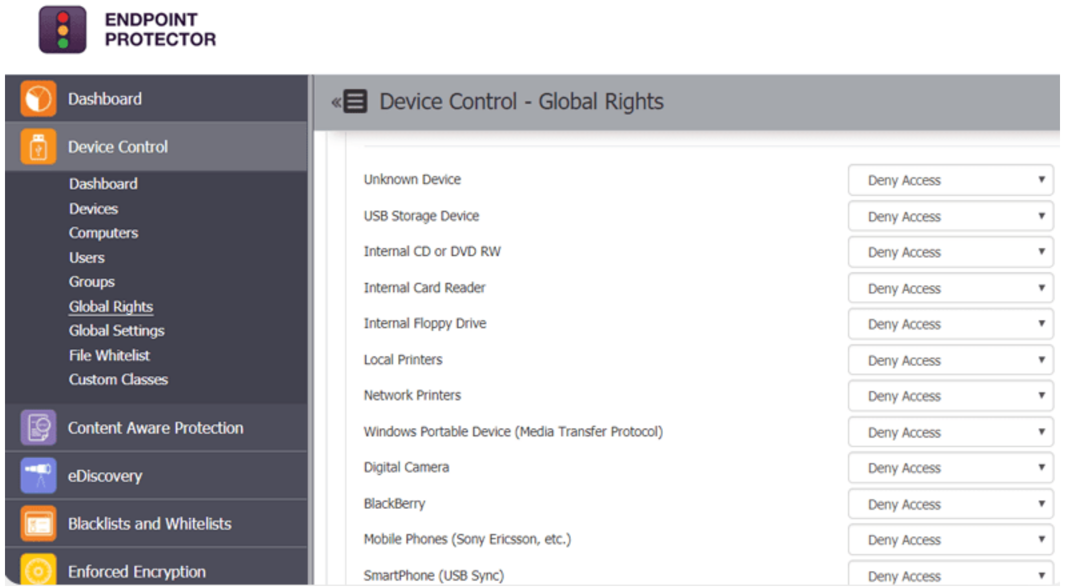
**Netwrix Change Tracker**

As reported by ART. §21.2 in points g, h and i regarding basic cyber hygiene practices, encryption and human resources security policies, access control, does Netwrix offer Data Loss Prevention solutions?

# Basic Hygiene, Training, Encryption and Controls

Discover, monitor, and protect sensitive data across employee endpoints

- Ensure endpoint data loss prevention across all your endpoints, regardless of the operating system they run on. Netwrix Endpoint Protector's real-time DLP engine actively monitors and safeguards your sensitive data, preventing breaches, unauthorized sharing and malicious exfiltration to achieve regulatory compliance.
- Insider Threats: Prevents information leaks by attackers, negligent, or compromised users
- Extend device control policies by encrypting data moved to removable storage. Safeguards data in transit and ensures that sensitive data is protected in the event that your USB device is lost or stolen
- Remote wipe capabilities
- Multi-OS support



Device Control - Global Rights

| | |
|---|---|
| Unknown Device | Deny Access |
| USB Storage Device | Deny Access |
| Internal CD or DVD RW | Deny Access |
| Internal Card Reader | Deny Access |
| Internal Floppy Drive | Deny Access |
| Local Printers | Deny Access |
| Network Printers | Deny Access |
| Windows Portable Device (Media Transfer Protocol) | Deny Access |
| Digital Camera | Deny Access |
| BlackBerry | Deny Access |
| Mobile Phones (Sony Ericsson, etc.) | Deny Access |
| SmartPhone (USB Sync) | Deny Access |

Device Control

Content-Aware Protection

Enforced Encryption

eDiscovery

# Visit our stand N1 to learn more about NIS2 solutions

# Thank you!

Visit us at netwrix.com