Syteca

Compliance in Action: Privileged Access & User Monitoring for NIS2/DORA

created by
Syteca

The role of PAM in compliance

> Privileged access management (PAM) plays a key role in enabling zero trust and defense-in-depth strategies that extend beyond mere compliance requirements.

Gartner

Core Syteca PAM capabilities for establishing NIS2 & DORA compliance

Identity and access management

- Promote zero trust with multi-factor authentication (MFA)
- Implement granular privileged access management (PAM)
- Enable secure remote access to your infrastructure
- Conduct regular user access reviews
- Implement just-in-time access

Requirements supported

NIS2 | Article 21, req. 2. c, d, i, j

DORA | Chapters II, IV

Password management

- Securely store and deliver secrets to users
- Implement automated password rotation
- Encrypt user passwords and secrets
- Grant access without revealing the password
- Provide one-time passwords for remote third-party users

Requirements supported

NIS2 | Article 21, req. 2. d, h, i

DORA | Chapters II, V

Just-in-time access

- Provide access on demand / upon request
- Revoke access automatically upon task completion
- Enable granular role-based permissions
- Implement time-based access restrictions

Requirements supported

NIS2 | Article 21, req. 2. d, i

DORA | Chapters II, IV

Incident response and investigation

- Leverage user activity monitoring (UAM) for context about security threats
- Implement real-time security alerts
- Enable automatic response to threats
- Facilitate incident investigation with user session recordings and session export

Requirements supported

NIS2 | Article 21, req. 2. a, b, d
Article 16

DORA | Chapters II, III, V

Auditing and reporting

- Monitor privileged users in real time
- Record user sessions to enhance accountability and support incident reporting
- Track third-party user actions with your data
- Leverage behavioral analytics to detect anomalies in user activity

Requirements supported

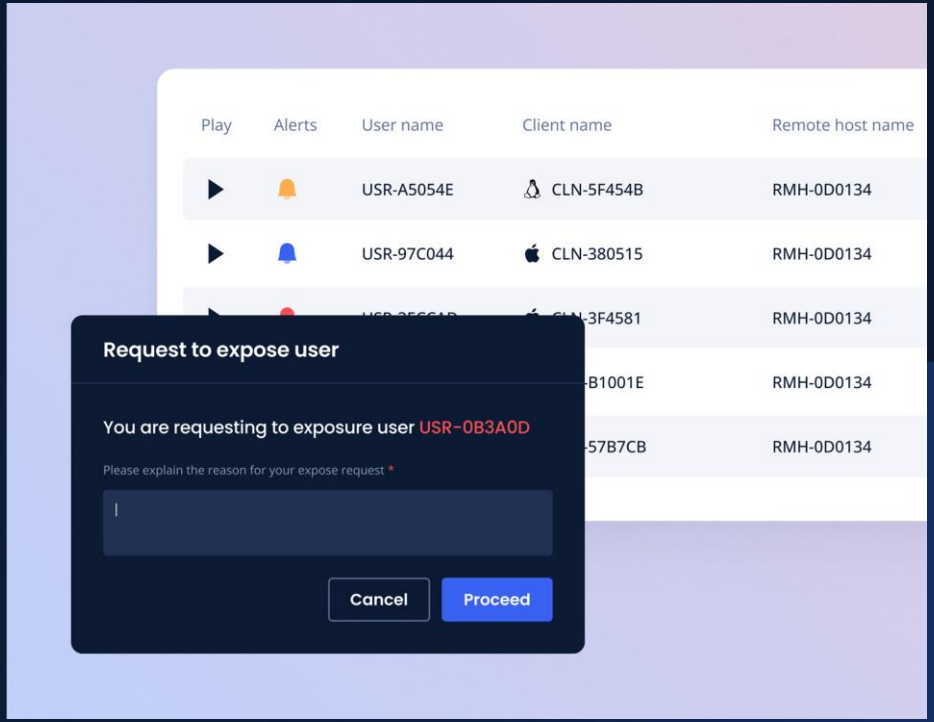
NIS2 | Article 21, req. 2. a, b, d, f, i; Article 23

DORA | Chapters II, III, V

User data pseudonymization

Replace personal data with aliases to comply with GDPR, CCPA, and other data privacy requirements.

Pseudonymization can be reversed for investigation purposes by authorized personnel.



Benefits of using Syteca for NIS2 & DORA compliance

Manage privileged accounts and sessions with lightweight PAM solution

Secure and control access to sensitive data for third-party vendors

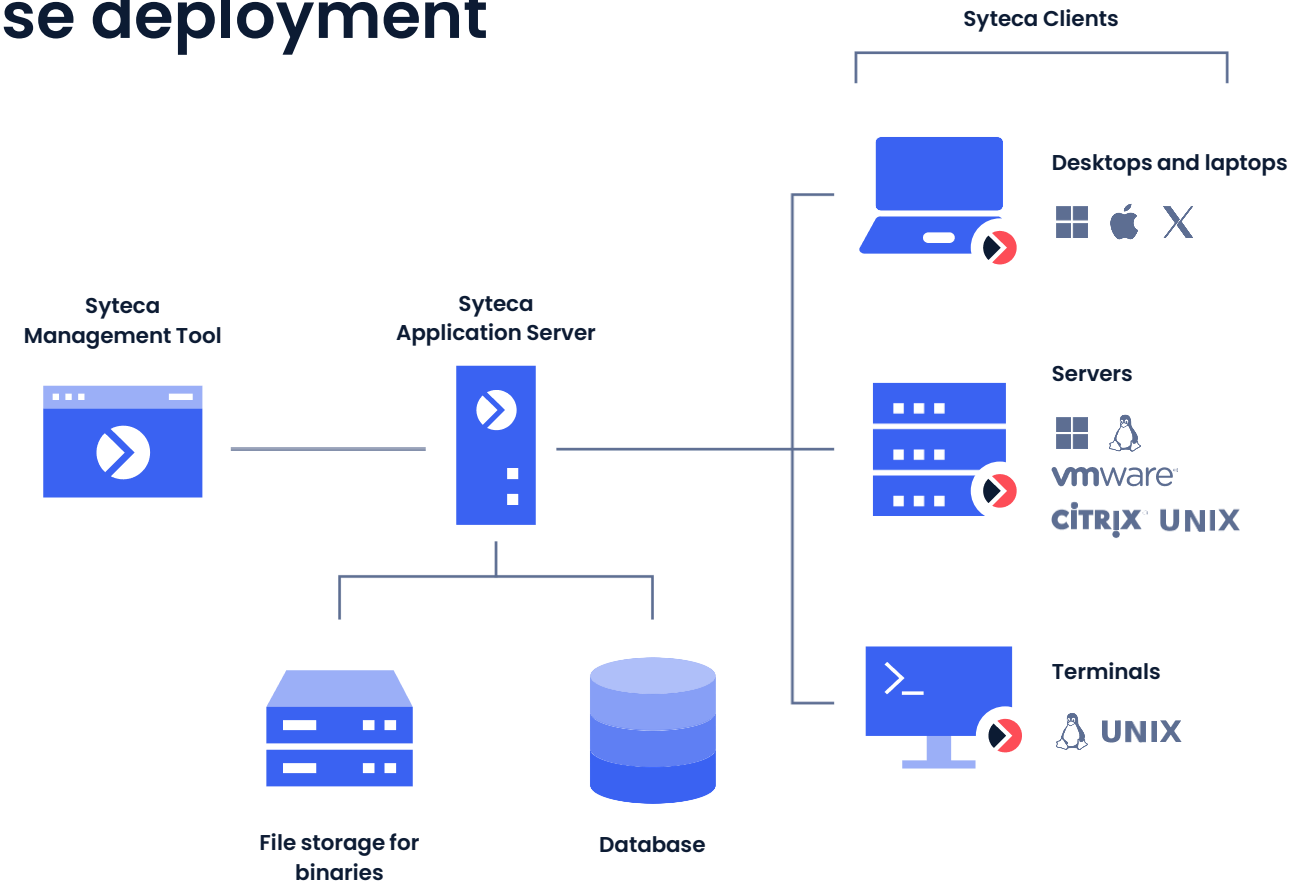
Detect and disrupt insider threats

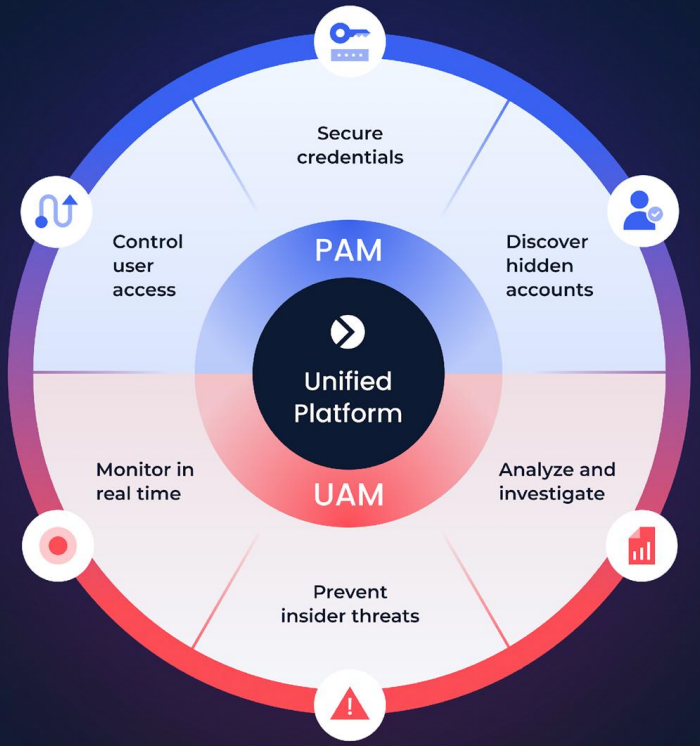
Promptly respond to incidents

Avoid fines and lawsuits

Get full network visibility by tracking user actions

On-premise deployment





One platform to secure your inside perimeter

- Privileged Access Management (PAM)
- User Activity Monitoring (UAM)

Fast to deploy

Easy to scale

Founded
in 2013

More than
1,500 customers

Offices in
4 countries

300 partners
in 56 countries

About Syteca

Syteca is recognized by cybersecurity experts

aws PARTNER

Gartner

Included in the Gartner 2025 Market Guide for Insider Risk Management Solutions

Microsoft Azure

Value Add Partner

NIST

Mentioned in NIST Special Publication 1800-18

kuppingercole ANALYSTS

Included in 2024 Kuppingercole Leadership Compass for PAM

ISO accelerator Registered ISO27001 USAS Management Systems 0269

ISO accelerator Registered ISO9001 USAS Management Systems 0269

CYBER ESSENTIALS CERTIFIED

Compliant with ISO 9001, ISO 27001, and Cyber Essentials

Our customers

VISA

SAMSUNG

ups

Panasonic

accenture

Finat

cecabank

KOICA

TURKISH AIRLINES

Payoneer

CBCG
CENTRAL BANK OF MONTENEGRO

CENTRAL BANK OF CYPRUS
EUROSYSTEM