unosecur

Defend your enterprise infrastructure from identity and access threats

Unosecur is a comprehensive identity security platform that addresses identity-related threats in multi-cloud and on-premise environments, providing end-to-end protection and identity management for human and non-human identities

---

The Unified Indentity Fabric by Unosecur integrates automated least-privilege implementation, Mitre Att&ck framework-based threat detection, AI-powered policy creation, and more. We seamlessly manage your organization's human and non-human identities: from discovery and analysis to monitoring, control, remediation, and governance

support@unosecur.com unosecur.com

unosecur

DATASHEET

Table of contents

unosecur

DATASHEET

Securing identities: Unosecur's approach

80% of data breaches in 2023 involved misuse of credentials, according to the 2024 Verizon Data Breach Investigations report

Today, human and non-human identities are the most preferred attack vector by the bad actors. Securing identities is the highest ROI investment to make for protecting your cloud and data. Your digital fortress is as strong as your weakest link - a compromised identity.

Safeguard your cloud identities with Unosecur's Real-Time ISPM + ITDR + NHI platform

Unified Identity Fabric

Provides a comprehensive, contextual inventory of human and non-human identities, keys, secrets, and their interconnections, with detailed risk mapping.

Real-time identity monitoring

Monitors identity activities in real-time, quantifying risks and enforcing strict least-privilege policies.

Active threat detection & response

Detects privilege escalation, credential theft, and lateral movement, with immediate response capabilities to stop attacks as they happen.

No-code IAM workflow management

Detects privilege escalation, Streamlines identity posture management with no-code workflows for Just-in-Time access requests, policy building, and more redential theft, and lateral movement, with immediate response capabilities to stop attacks as they happen.

Granular compliance & reporting

Ensures compliance with regulatory frameworks like SOC2, ISO27001, and PCI DSS 4.0, with IAM risk tracking and detailed reporting within 15 minutes of onboarding.

unosecur

DATASHEET

Key features and benefits

Continuous least privilege implementation	Unosecur ruthlessly implements least privileges for human and non-human identities in real-time. The activity based automated approach ensures the right balance between productivity and security
Credential theft detection	Unosecur advanced threat detection engine effectively finds the indicators of credential theft with zero noise.
Privilege escalation detection	Unosecur's ITDR(identity threat detection and remediation) capability detects unauthorized activities that point towards privilege escalation.
Lateral movement detection	Unosecur locates lateral movement and kills attack chain to stop the attack as it happens.
User behavior analytics	Discover unusual login patterns - unexpected locations and time.
Compliance	Unosecur helps you comply with ISO 27001 and SOC2 while fixing a bunch of misconfigurations.
Privilege access management	Use no-code workflows to create JIT access requests to ensure business continuity without risking security.
Auditing and reporting	Detailed audit logs and reports to help you with audits and compliance needs.

unosecur

DATASHEET

How Unosecur works

1 Discover & analyze

Discover your complete inventory of human and machine identities, enabling you to efficiently identify rogue identities and take decisive actions based on prioritized identity risks. With our powerful graph database visualizations, you can trace the pathways of identity threats and effectively resolve them at their source.

2 Monitor & control

Gain real-time visibility into identity activities to quickly detect anomalous behavior, giving you immediate control over your identities. Easily manage the identity access lifecycle and optimize user permissions by enforcing a least privilege access policy with automated no-code workflows.

3 Audit & govern

Create policies with simple prompt and access reviews to meet cybersecurity benchmarks and other governance requirements. Easily search audit logs, generate one-click downloadable reports, and quickly implement corrective actions directly from the platform, saving time and effort.

4 Compliance

Check your cloud environment against various ISO27001 and SOC2 controls to comply with industry's best practices.

5 Respond & remediate

Disrupt malicious activities while it is happening (Yes, at runtime). Terminate attack chains and quarantine suspicious actors using ATT&CK model and machine learning to detect potential threats. It includes tools for in- depth forensic analysis, providing real-time alerts and notifications for any suspicious activities.

Use cases

Identity Threat Detection and Response

Leverage MITRE ATT&K model-based real-time threat detection and response capability to swiftly identify bad actors and kill attack chains.

Identity Security Posture Management

Monitor access controls, permissions, and activities of human and non-human identities. Fix gaps using simplified yet granular no-code workflows.

Identity Least Privileges Implementation

Dynamically adjust permissions in real-time to implement the least privilege at scale powered by GenAI across multiple cloud providers.

Identity Privilege Access Management

Manage privileged access by granting or revoking permissions based on roles and security policies. Utilize Slack and email communication to ensure business continuity.

Identity Audit and Compliance

Maintain regulatory compliance with Unosecur's comprehensive visibility into identity activities and access controls, addressing gaps directly from the platform.

FAQs

Is Unosecur compliant with industry standards and regulations?

Unosecur meets major compliance standards SOC 2 and ISO 27001, confirming that our security, risk management, and data protection controls are robust and globally recognized. Compliance with GDPR and HIPAA standards ensure that we rigorously protect sensitive personal and healthcare data. Additionally, our Trusted Cloud Provider badge from the Cloud Security Alliance validates our best practices in cloud security, underscoring our commitment to maintaining a secure environment for our clients.

Does Unosecur provide a SaaS deployment option?

Yes, Unosecur is available as a SaaS solution, allowing you to benefit from quick setup, scalability, and seamless updates without managing hardware or infrastructure.

Where is my data stored while using Unosecur?

With Unosecur, data can be stored in your own environment (on-premises or in the cloud) or in our secure cloud infrastructure. All data is encrypted in transit and at rest, ensuring security at every level.

Does Unosecur offer data retention policies?

Yes, Unosecur allows you to configure data retention policies based on your organization’s requirements. You can set timeframes for audit logs, user activity data, and more.

How do I set up an integration with a third-party tool?

Setting up integrations is simple through the Unosecur dashboard. Just navigate to the "Integrations" tab, select the tool you want to integrate, and follow the guided setup instructions. You can also refer to our detailed documentation for API-based integrations.

unosecur

DATASHEET

For identity security, they trust us

Rakuten

INNOVAPPTIVE

axel springer

ZEOTAP

Universität Bremen

Ready to secure your enterprise identities?

Take a free risk assessment!

AICPA SOC

ISO 27001 Certified

GDPR

Cloud Security Alliance Trusted Cloud Provider CSA

HIPAA COMPLIANT

The ITDR + ISPM + NHI Solution