

Act on exposure before attackers do

Continuous Threat Exposure Management

Highlights

Exposure management spanning Zero Trust, AI Trust, and Quantum Trust

Continuous identification and exposure assessment across cyber, quantum, and AI

Asset, identity, cloud, network, application, cryptographic, and agentic risk visibility

Exposure prioritization based on business context and quantified risk

Validation of attack paths and exploitable weaknesses

Trusted AI acceleration powered by the Unisys Intelligence Accelerator

AI-driven, focused remediation paths

Executive reporting and exposure management metrics

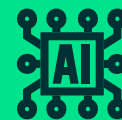
Integration with existing security operations and governance

In a typical enterprise, multiple attack vectors can expose critical assets, yet traditional vulnerability management alone can't address the full breadth of the modern attack surface. Reactive, periodic scanning can't keep pace with cloud sprawl, hybrid work, IoT/OT growth, surging AI adoption, agentic systems, and the coming quantum threat to cryptography.

The Unisys Continuous Threat Exposure Management solution continuously identifies, assesses, prioritizes, validates, and remediates exposures across digital infrastructure, cloud, identities, applications, AI estate, and cryptographic posture. Using business context, threat intelligence, and telemetry, it drives continuous risk-based decisions, validating exposure states, simulating attacks, and guiding remediation by criticality and compliance.

Our Trusted AI security framework applies AI to speed up triage, prioritization, and remediation guidance and execution, with guardrails keeping decisions human-governed and auditable.

Trusted AI meets business context



Prioritize real risk instead of raw severity scores, with business context added by the Unisys Intelligence Accelerator.

One foundation. Three dimensions of trust.

Continuous Threat Exposure Management extends exposure management across dimensions: assets and identities under Zero Trust; the AI and agentic estate under AI Trust; and cryptographic posture under Quantum Trust. Together, they bring every dimension of enterprise trust into a single business-aligned view.

How you benefit

- **Business-aligned risk prioritization:** Move beyond raw Common Vulnerability Scoring System scores. Unisys enriches exposures with asset context, exploit intelligence, threat intel, and crown-jewel classification to focus remediation on business-critical risk.
- **Comprehensive exposure visibility:** Gain a consolidated view across internal, external, cloud, identity, and IoT/OT surfaces through integrated attack surface discovery, vulnerability management, and threat intelligence by reducing blind spots.
- **Validated exposures, not just findings:** Validate exploitable exposures through breach and attack simulation, continuous automated red teaming, and penetration testing, reducing noise and rework.
- **Trusted AI acceleration:** Speed up triage, prioritization, evidence collection, and remediation with Trusted AI acceleration. Powered by the Intelligence Accelerator, the solution applies AI with human oversight, guardrails, and auditability built in so you maintain control.
- **Faster, smarter remediation:** Match the response path to the risk from autonomous handling of low-risk exposures to guided analyst workflows and emergency containment of critical, actively exploited exposures, reducing mean time to remediate.
- **Continuous maturity progression:** Progress along a structured maturity path from ad-hoc vulnerability management to continuous, business-driven exposure management, with measurable maturity at each stage.

- **Operational efficiency and cost reduction:** Reduce tooling sprawl and manual effort through tool convergence and Cyber Defense Center-led vulnerability operations, improving governance outcomes and cost efficiency.
- **Stronger security posture:** Continuously identify and reduce attack paths, misconfigurations, vulnerabilities, and identity weaknesses before they can be exploited, strengthening overall cyber resilience.

Why Unisys?

As a recognized cybersecurity leader, Unisys takes a holistic approach to business cyber threats and exposure, delivered globally through Unisys Cyber Defense Centers with centralized governance. We combine best-of-breed tooling with proprietary methodology, including our unified vulnerability management framework, business-context risk quantification, risk-based remediation, and continuous threat exposure management maturity model. This results in the delivery of an outcome-driven exposure management program rather than a tool stack.



Get ahead of
exposure

Swap fragmented, periodic vulnerability scanning for continuous exposure management, remediating exposures before attackers can exploit them

To explore how the Continuous Threat Exposure Management solution can help you continuously reduce cyber risk, [visit us](#) online or [contact us](#) today.



unisys.com

© 2026 Unisys Corporation. All rights reserved.

Unisys and other Unisys product and service names mentioned herein, as well as their respective logos, are trademarks or registered trademarks of Unisys Corporation. All other trademarks referenced herein are the property of their respective owners.