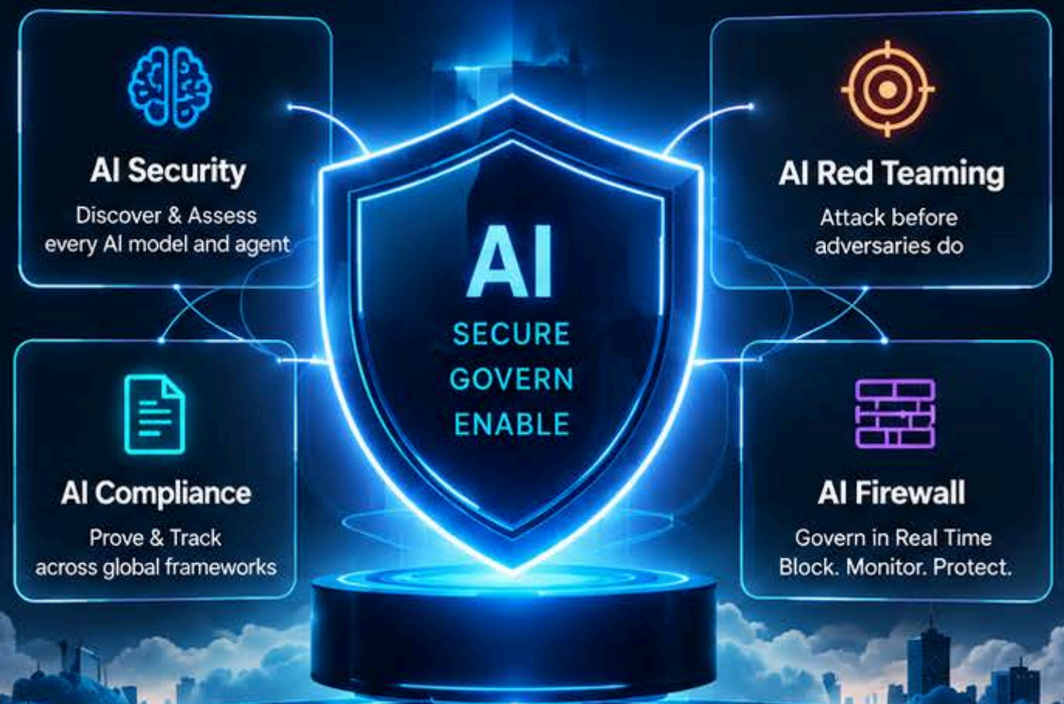
suroNEX®

Intelligent. Integrated. Compliant.

AI SECURITY | AI COMPLIANCE | AI RED TEAMING | AI FIREWALL

The AI Security Company for the Cloud-Native Enterprise.

Suronex discovers, red-teams, governs and protects every AI model and agent an enterprise runs — on one platform that also secures the cloud, SaaS and code around it. **One console. One data spine. One contract.**



4 AI-security pillars at our core

10 Integrated modules, one console

50+ Global compliance frameworks

30 min Agentless time-to-value

CLOUD & AI GROWING AT LIGHT SPEED

Market Landscape

Cloud keeps compounding- AI is already 3x its size



BIGGER CLOUD. BOLDER AI. GREATER OPPORTUNITY.

$1 Trillion → $1.7T
Public cloud spend by 2030 (~19% CAGR)

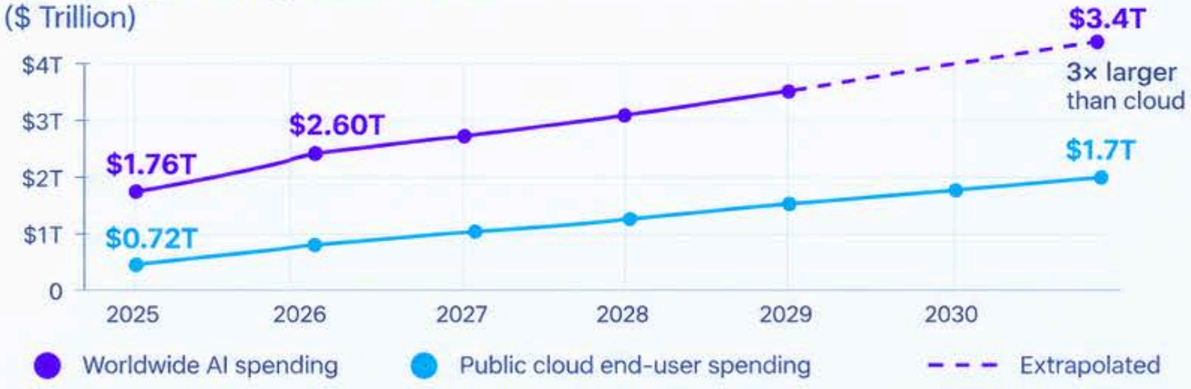
$2.6T
Worldwide AI spending in 2026 (+47% YoY)

55%
Infrastructure is 55% of AI spend

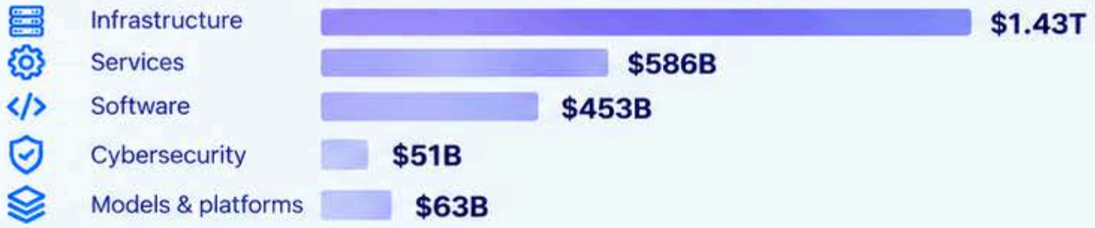
41%
of total IT spending is now AI (32% in 2025)

Global Spending 2025–2030

($ Trillion)



Where the 2026 AI Spend Goes — $2.6T, by category



Artificial Intelligence — the faster curve

$2.6 Trillion
Worldwide AI spending in 2026 (+47% YoY)

$1.43 Trillion
AI infrastructure in 2026 (55% of all AI spend)

41%
of total IT spending is now AI (32% in 2025)

$1.21 Trillion
AI infrastructure alone by 2030 (~30% CAGR)

Public Cloud — the larger base

$723.4 Billion
Spent on public cloud services in 2025

$1.7 Trillion
Public cloud spending by 2030 (~19% CAGR)

>$1 Trillion
Public cloud services in 2026 (+21% YoY)

+37%
PaaS growth — fastest segment, driven by AI platforms

Asia & India — the fastest-growing market

$17.5 Billion
India public cloud in 2026, up from $13.7B (+28.1%, IaaS +40%)

$4.4 Trillion
Asia/Pacific cumulative AI economic value, 2025–31

$647 Billion
Asia/Pacific ICT spend in 2026 → $758B by 2029

By 2027, AI spending alone **will exceed $3.4 trillion** — more than three times the entire public cloud market.

A SAFER TOMORROW BUILDS ON SECURE AI.

PROBLEM

AI is evolving faster than enterprise security can keep up



NEW CAPABILITIES.
NEW RISKS.
A MORE COMPLEX TOMORROW.

01

Shadow AI Is Creating an Invisible Attack Surface

Employees are adopting AI tools, copilots and agents without visibility or governance.



Key gaps:

- AI discovery
- Shadow AI detection
- SaaS visibility
- Ownership
- Risk classification

02

AI Identity & Excessive Agency Create New Attack Paths

AI agents get identities, credentials and access to data, APIs and tools—creating new attack paths.



Key gaps:

- AI identity visibility
- Least privilege
- Agent permissions
- Tool authorization
- Identity lifecycle

03

AI Behavior Can Be Manipulated

Prompt injection, jailbreaks, poisoning and malicious tool use can compromise AI without traditional vulnerabilities.



Key gaps:

- AI red teaming
- Adversarial testing
- Behavioral testing
- Attack simulation
- AI-specific vulnerability discovery

04

AI Interactions Need Real-Time Protection

Traditional security controls cannot understand or inspect every prompt, response, agent action or tool call.



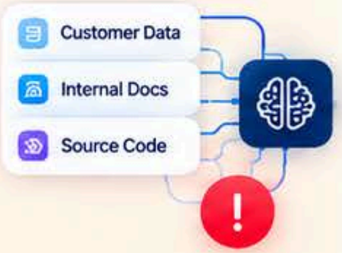
Key gaps:

- AI firewall
- Prompt inspection
- Response monitoring
- Policy enforcement
- Real-time blocking

05

AI Data Exposure & Behavioral Risk Are Difficult to See

Prompts, RAG pipelines, vector stores and agents can expose sensitive data or behave outside intended boundaries.



Key gaps:

- Data-flow visibility
- Sensitive-data detection
- RAG monitoring
- Agent behavior analytics
- AI interaction monitoring

06

AI Security & Compliance Cannot Be Proven Continuously

Organizations must demonstrate AI governance, risk management and controls across frameworks like ISO 42001, NIST AI RMF and OWASP LLM Top 10.



Key gaps:

- Continuous compliance
- Control mapping
- AI risk assessment
- Red-team evidence
- Audit trails
- Continuous assurance

What Could Happen
If AI Deployment is not Secured?

Six real-world AI security incidents show the potential impact on your data, systems, customers and compliance.



01 SHADOW AI

Employees use unapproved AI tools



Real incident:
DeepSeek database exposure
January 2025

IMPACT
1M+ log lines with chat histories and API keys publicly queryable.

What this shows
Sensitive data shared in unvetted AI tools can be exposed to anyone.

02 AI IDENTITY & EXCESSIVE AGENCY

Stolen or over-privileged AI agent tokens



Real incident:
Salesloft Drift OAuth token theft
August 2025

IMPACT
Stolen tokens used to export numerous Salesforce instances and hunt for secrets.

What this shows
AI agents with excessive permissions can access critical systems and data without human oversight.

03 AI BEHAVIOR MANIPULATED

Malicious prompts change agent behavior



Real incident:
Amazon Q extension wipe prompt
July 2025

IMPACT
Poisoned instructions to delete files and cloud resources shipped in a public release.

What this shows
AI behavior can be manipulated through prompts, leading to destructive actions.

04 REAL-TIME PROTECTION

Hidden prompts can steal your data



Real incident:
EchoLeak in Microsoft 365 Copilot
June 2025

IMPACT
Zero-click email could exfiltrate anything Copilot can read.

What this shows
Hidden prompts can steal sensitive data without any user action or click.

05 DATA EXPOSURE & BEHAVIORAL RISK

AI agents can delete or expose sensitive data



Real incident:
Replit agent deletes production DB
July 2025

IMPACT
Records for 1,200+ executives deleted during a code freeze.

What this shows
AI agents can perform destructive actions and cause irreversible data loss.

06 COMPLIANCE NOT PROVEN

Lack of governance leads to regulatory action



Real incident:
Italy fines OpenAI €15M
December 2024
(overturned March 2026)

IMPACT
Regulatory fine, mandated public campaign, over a year of legal challenge.

What this shows
Without proper AI governance and compliance, organizations face significant legal, financial and reputational risk.

SOLUTION

Suronex: The Security Platform
Built for the AI-Powered Enterprise



DISCOVER.
TEST.
PROTECT.
GOVERN.
THE AI ERA.

Four Pillars. One Continuous AI Security Lifecycle.

DISCOVER & ASSESS
KNOW WHAT EXISTS

Discover every AI model, agent, API, MCP server, dataset and Shadow AI application. Assess posture, identity, data exposure and misconfigurations.

Complete AI visibility >

AI RED TEAMING
ATTACK BEFORE ADVERSARIES

Continuously challenge models and agents with adversarial testing — including prompt injection, jailbreaks, data leakage and agent abuse.

Find and fix weaknesses >

AI PROXY & FIREWALL
PROTECT IN REAL TIME

Inspect AI interactions in real time. Detect and block prompt injection, sensitive-data leakage, malicious responses and unauthorized tool activity.

Stop threats in real time >

AI COMPLIANCE
PROVE & GOVERN

Map AI risks and controls to ISO/IEC 42001, NIST AI RMF, EU AI Act, OWASP LLM Top 10 and MITRE ATLAS. Generate continuous evidence for audit and governance.

Continuous assurance >

From AI Discovery to Continuous Protection

A connected AI asset and risk layer links models, agents, identities, prompts, data, APIs and applications — so you know what is risky, why, and what to do.

DISCOVER Find everything >>> **ASSESS** Understand risk >>> **ATTACK** Test continuously >>> **ENFORCE** Protect in real time >>> **GOVERN** Prove & improve

ONE PLATFORM.
A SAFER AI FUTURE.

200+ AI Security Posture Checks

10,000+ Adversarial AI Probes

300+ AI Compliance Clauses Mapped

50+ Security & Compliance Standards

DEEP DIVE

AI Firewall

One secure gateway for all AI traffic — inspect, protect and govern.

Governed — Policy-driven control

Protected — Block threats in real time

Visible — Full audit trail

Compliant — Enterprise ready

Users, Applications and Agents

- **Employees** — Web and mobile apps
- **Enterprise copilots** — Microsoft 365, Slack, etc.
- **Developers** — IDEs and coding agents
- **AI agents** — MCP clients and tools
- **Third-party apps** — Browser extensions

AI Requests (Prompts, files, API calls)

Safe Responses (Filtered, monitored)

Suronex AI Firewall

- **Inspect** — Scan prompts, files and context
- **Detect** — Identify threats and risky behavior
- **Enforce** — Apply policies in real time
- **Log** — Audit and retain evidence

AI FIREWALL — Suronex

- **Policy Engine** — Custom & regulatory policies
- **AI Threat Intelligence** — LLM & agent specific
- **Real-time Enforcement** — Block, sanitize, route

Sanitized Requests (Safe, policy-compliant)

Model Responses (Monitored, logged)

AI Models and Providers

- OpenAI
- Anthropic Claude
- Google Gemini
- Meta Llama
- Mistral
- Cohere
- aws
- Azure

And more... NVIDIA, Oracle, Databricks, Self-hosted models and others

What AI Firewall Stops

- **Prompt Injection & Jailbreaks** — Block malicious prompts and intent manipulation
- **Sensitive Data Leakage** — Prevent PII, secrets and confidential data exposure
- **Unauthorized Tool Use** — Control agent actions, tool calls and external access
- **Malicious Content** — Detect and block harmful responses and data exfiltration

SAFER AI. STRONGER BUSINESS.

COMPETITIORS

Competitive Landscape

Capability Focus area for AI security	suroNEX® AI Security Company	WIZ	CROWDSTRIKE	CHECK POINT	Orca Security	Cisco AI Defense
1. AI Asset Discovery and Posture Management Discover and assess AI models, agents, data and risks	Full AI asset discovery Risk & posture management	Full AI/ML asset discovery Visibility & risk analysis	Partial Model visibility Threat detection	Partial AI asset visibility Risk analysis for AI apps	Partial AI/GenAI workload discovery Cloud posture for AI/ML	Partial AI application visibility Model telemetry
2. Automated AI Red Teaming Test for jailbreaks, prompt injection, data leakage and agent abuse	Full Automated red teaming Prompt & data testing	Partial Red teaming (preview) Attack-path testing	Partial AI red teaming (paid) Model integrity focus	Partial Research & testing Limited details	Limited No dedicated AI red teaming Limited research	Partial Model testing and validation Limited details
3. Agentic AI & MCP Security Discover, control and secure AI agents, tools and MCP interactions	Full Agent & MCP discovery Security & tool controls	Partial Basic agent visibility Limited controls	Partial Agentic AI protection Limited details	Partial AI agent security Limited details	Limited No dedicated agentic AI Limited coverage	Partial Runtime security Limited details
4. Real-Time AI Firewall & Enforcement Inline inspection, policy enforcement and blocking	Full Real-time AI gateway Block and enforce policies	Limited No inline gateway Posture and risk focus	Partial Runtime protection Limited AI gateway	Partial Application protection Partial controls	Limited No dedicated AI firewall Focus on detection	Full Runtime protection Threat blocking
5. AI Compliance, Governance & Audit Evidence Framework mapping, evidence collection and reporting	Full 50+ frameworks (incl. NIST, ISO, OWASP) Automated evidence & reporting	Partial General compliance coverage Limited AI-specific mapping	Partial Standard frameworks Limited AI governance	Partial Major frameworks Limited AI-specific features	Partial Standard coverage Limited AI-specific mapping	Partial Compliance requirements Limited AI governance

Based on publicly available information as of October 2026. "Partial" indicates incomplete capabilities; "Limited" indicates no clear public evidence of dedicated capability.
Product names are trademarks of their respective owners.

BUSINESS MODEL

GTM and Business Model



SAME SECURITY CHALLENGES. A SMARTER GROWTH ENGINE.

Business Model

Recurring revenue, built to expand.

SaaS Subscription
Annual & monthly recurring fees

Enterprise Licensing
Large deployments + custom modules

Managed Compliance
Monitoring & advisory services

Channel / MSP
Revenue share & white-label

HOW A CUSTOMER BECOMES RECURRING REVENUE

LAND
Annual SaaS subscription — priced per cloud account + modules

→

ONBOARD
Live in under 30 minutes — immediate value

→

EXPAND
Add modules & cloud accounts — usage scales up

→

RENEW
Annual renewals — predictable, compounding ARR

Illustrative ACV:
a mid-market customer lands at ~$6–8 L ARR (posture + compliance + security), then expands to ~$15–20 L by Year 2 as modules and cloud accounts grow.

Go-To-Market Strategy

A focused wedge, then compounding channels.

1 · WEDGE

Regulated mid-market, India first

- BFSI, healthcare, government & ICT
- RBI/SEBI/IRDAI/DPDP pressure is acute
- Decision makers: CISO, CIO, Head of InfoSec, AI Lead

2 · CHANNELS

Partner-led distribution

- Hyperscaler co-sell (ESDS, AWS, NVIDIA ecosystem)
- MSP white-label for reach into hundreds of mid-market accounts
- Plus founder-led direct sales for lighthouse logos

3 · EXPANSION

US / UK / APAC / ME Market

- Same regulatory playbook in global markets
- On-prem & air-gapped offering unlocks government and defence segments
- SaaS-only rivals create adjacent opportunities

CHANNEL ECOSYSTEM

Hyperscaler
ESDS

›

MSP Partners
White-label

›

Direct Sales
Lighthouse accounts

›

Regional Expansion
US / UK / APAC / ME

Retention by design: 30-minute onboarding converts free pilots fast; land-and-expand grows accounts; MSP white-label compounds reach without headcount.

TRACTION

Early Product, Real Momentum

From Early Wins to a Bigger Tomorrow

CUSTOMERS
PARTNERS
PIPELINE
GLOBAL REACH

5 Paid Customers

15+ Active POCs / Pilots

20+ Pipeline Opportunities

15+ Team & Advisors

PIPELINE-TO-REVENUE JOURNEY

50+ Pipeline Opportunities → **~30%** Advance → **15+** Active POCs → **~33%** Convert → **5** Paid Customers

OUR CUSTOMERS

Trusted by innovative and forward-looking organizations

CLOUDVERSE · MLRS TRANSFORMING LIVES · ZERO FORG INTELLIGENCE LAYER FOR PHYSICAL SYSTEMS · PIVOT Detect. Defend. Disrupt. · ACYi

PARTNER ECOSYSTEM 4 INDIA · 2 INTERNATIONAL · AND GROWING

esds enabling futurability · SecMyIT Infosec Solutions Pvt Ltd · Kalky Trusted IT Distribution Network · VERDANT CYBERZ · RISK GUARD ENTERPRISE SOLUTIONS

INTERNALTIONAL PARTNERS

Under Review

KMG KMG US · MOORE Kingston Smith

RECOGNITION & PROGRAMS

- NVIDIA Inception Program
- Anthropic Startup Program
- AWS Startup Program
- Google Cloud Startup Program
- Microsoft for Startups
- NASSCOM AI Centre of Excellence
- National CoE Incubation (DSCI)
- DPIIT Recognized Startup
- PDEU Incubation & Innovation Centre

15+ POCS IN PROGRESS CLOSING SOON

Working with leading organizations across India and globally

TROJAN HUNT · Finnulate · EffiGO · Capovex · DALOOPA · +11 more advancing

3 GLOBAL FOOTPRINT
India · USA · UK



TEAM

Built by security pioneers. Back us to scale.

A focused team with deep domain expertise. A clear roadmap. A upto $1M pre-seed round to build the AI security category.

PEOPLE
PRODUCT
POSSIBILITY.

Our Team

A focused team of 15+ builders and advisors with depth in cloud security, compliance and applied AI.

FOUNDING MEMBERS



Manish K Saini
CEO & Founder

25+ YOE, CEO, CISO,
Internal Audit
Ex – IBM, HCLTech, Sunlife



Prashant Mavinkurve
CTO & Co-Founder

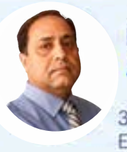
25+ YOE, Technology
Entrepreneur, Engineering Leader
Ex – Oracle, EMC,
Societe Generale



Maulshri Dube
Chief Growth Officer

25+ YOE, Sales, Marketing,
Tech consulting &
Entrepreneurship
Ex – Gartner, Oracle Mindfire
Solutions, eBiz Solutions

ADVISORY BOARD



Dr. Nakul Parashar
Advisor

35+ YOE
Ex – GEO – Vigyan Prasar,
Ex – Exela
Launched & Mentor 4+ Startups



T R Rajesh
Advisor

28+ YOE
Director – Cyber Security
Ex – Kyndryl, Ex – IBM



Abhijit Sanzgiri
Advisor

35+ YOE
Co Chair – MACCIA
Partner at AP Sanzgiri Co
Ex – CFO

Our Priorities

Four key focus areas to accelerate our next phase of growth.

Scale Go-to-Market
Expand sales, marketing and channel partnerships

Grow the Team
Hire top engineering, research and GTM talent

Deepen Compliance
Add regional frameworks and on-prem / air-gapped editions

Accelerate Innovation
Enhance AI Firewall, Red Teaming and Agent Security

Our Roadmap

From product maturity to market leadership.

Build the global AI security leader

FY26
Go-to-Market
- Ship AI Proxy & Firewall to GA
- Expand enterprise deployments
- Build strategic partnerships

50+ Customers

FY27
Scale
- Scale across BFSI, healthcare, government (India first, then APAC/ Middle East)
- Expand platform adoption
- Grow partner ecosystem

200+ Customers

FY28
Market Leadership
- Reach ₹100 Cr revenue
- 500+ customers
- Expand globally
- Continuous innovation in AI security & compliance

500+ Customers

Our Ask

Upto $1 Million Pre-Seed funding to accelerate the next stage.

$1M | **Pre-Seed Funding**
To scale product, team and go-to-market and establish category leadership.

Use of Funds

40% Product & Engineering
Build and enhance platform capabilities

30% Go-to-Market
Sales, marketing and strategic partnerships

20% Team Expansion
Hire across product, research and GTM

10% Compliance & Infra
Regional frameworks, on-prem and scale

THE SURONEX SUITE

One Platform, 10 Integrated Modules.



APPENDIX

ADDITIONAL CAPABILITIES

suroNEX®

Intelligent. Integrated. Compliant.

SURONEX

suroNEX®

Intelligent. Integrated. Compliant.

One Platform. Complete Cloud-Native Security.

Discover, assess and secure your Cloud, Containers, Code, SaaS, AI and more — all in one platform.

And 100+ Integrations

AssetGraph

- Discover all cloud assets across environments
- Visualize asset relationships



CloudPosture

- Real-time monitoring across multi-cloud
- Detect misconfigurations and security risks



KubePosture

- Real-time monitoring for EKS, AKS, GKE & Kubernetes
- Detect misconfigurations and risky permissions



CodeShield

- Scan code and secrets in CI/CD pipelines
- Detect vulnerabilities and risky dependencies



VulSense

- Find vulnerabilities across cloud, containers and IaC
- Scan and prioritize risks



SupplyTrust

- Monitor open source risk (SBOM, licenses)
- Detect malicious and risky packages



SaaSPosture

- Discover and monitor SaaS apps (100+ integrations supported)
- Detect shadow SaaS and risky usage



AccessGraph

- Manage cloud identities and entitlements
- Detect excessive access and risky permissions



suroNEX®

Unified Cloud-Native Security Platform

DISCOVER | ASSESS | PRIORITIZE | REMEDIATE | MONITOR

AISentinel

- Real-time monitoring and blocking of AI traffic
- AI security, red teaming and compliance

Business Outcomes

- Stronger Security Posture
- Complete Visibility
- Faster Remediation
- Lower Business Risk
- Simpler Operations
- Reduced Tool Costs

suroNEX®

Intelligent. Integrated. Compliant.

Global Compliance. Built for Today. Ready for What's Next.

Automate compliance, map controls, collect evidence and monitor continuously across 50+ global standards, regulatory requirements and 30+ industry best practices.

One Platform. All Standards. Continuous Compliance.

Global Standards

Comply with leading global frameworks

- ISO 27001
- ISO 42001
- SOC 2
- PCI DSS
- NIST
- CYBER ESSENTIALS (UK)
- CCM (CSA)
- HIPAA
- FedRAMP
- and more

Regulatory Requirements

Stay aligned with regional and industry regulations

- DORA
- DPDP 2025
- RBI CSF
- IRDAI
- SEBI
- MAS
- APRA
- UK
- PDPA Singapore
- and more

Industry Best Practices

Leverage trusted frameworks and benchmarks

- CIS Benchmarks
- NIST CSF
- NIST AI RMF
- OWASP Top 10
- MITRE ATT&CK
- NCSC UK
- AWS Well Architected Framework
- AI Verify
- Essential Eight Maturity Model
- and more

Bring Your Own Compliance

Import and map custom frameworks

Policy Management

Create and manage policies

Automated Evidence Collection

Collect evidence from 100+ tools



Dashboards & Reporting

Audit-ready reports

Risk Management

Track and prioritise risks

Portfolio View

Compliance across business units

Full GRC Capabilities (Coming Dec 2026)

- Risk Management
- Third-Party Risk Management
- Policy Management
- Audit Management
- Exception Management
- Issue Management

THANK YOU!

suroNEX®

Intelligent. Integrated. Compliant.

contact@suronex.ai

www.suronex.ai

SURONEX