SYSTAL_SAM

Applying Agentic AIOps to Regulatory Compliance

Regulatory & Compliance Demands Intensify

Every compliance framework, regardless of scope or geography, depends on one foundational capability: a clear and current understanding of the IT estate.

New regulations are emerging while existing directives expand in reach and enforcement. Organisations operating across regions require continuous adjustment to align to the minimum security standard recommendations across multiple vendor baselines frameworks, including:

- DORA
- NIS2
- GDPR
- PCI Compliance
- EU AI Act

Despite the margin for error narrowing, only **43%** of IT professionals believe their organisation has full visibility across its IT estate.

SYSTAL_SAM

Why Compliance Readiness Falls Short

Many of the causes are largely structural. Manual approaches struggle to keep pace with complexity. Compliance becomes reactive, consuming time without reducing risk. Common issues:

Legacy tools and fragmented vendor-specific platforms

Siloed operational models prevent consistent oversight

Assets added and changed without clear ownership

Adversaries using AI to exploit weaknesses at speed

Organisations need compliance processes that operate continuously and adapt as quickly as the environments they are designed to protect. They need Agentic AIOps...

SYSTAL_SAM

Applying Agentic AIOps to Regulatory Compliance

Agentic AIOps offers a practical way to address regulatory challenges by embedding compliance into day-to-day operations.

Systal's [Secure AI Manager (SAM)](#), is a new agentic AI-powered platform designed to transform how enterprises manage complex IT environments.

It continuously monitors for vulnerabilities and misconfigurations, automates compliance checks against key industry frameworks, adds continuous policy drift detection and uses AI and machine learning to predict and resolve issues before they disrupt your operations.
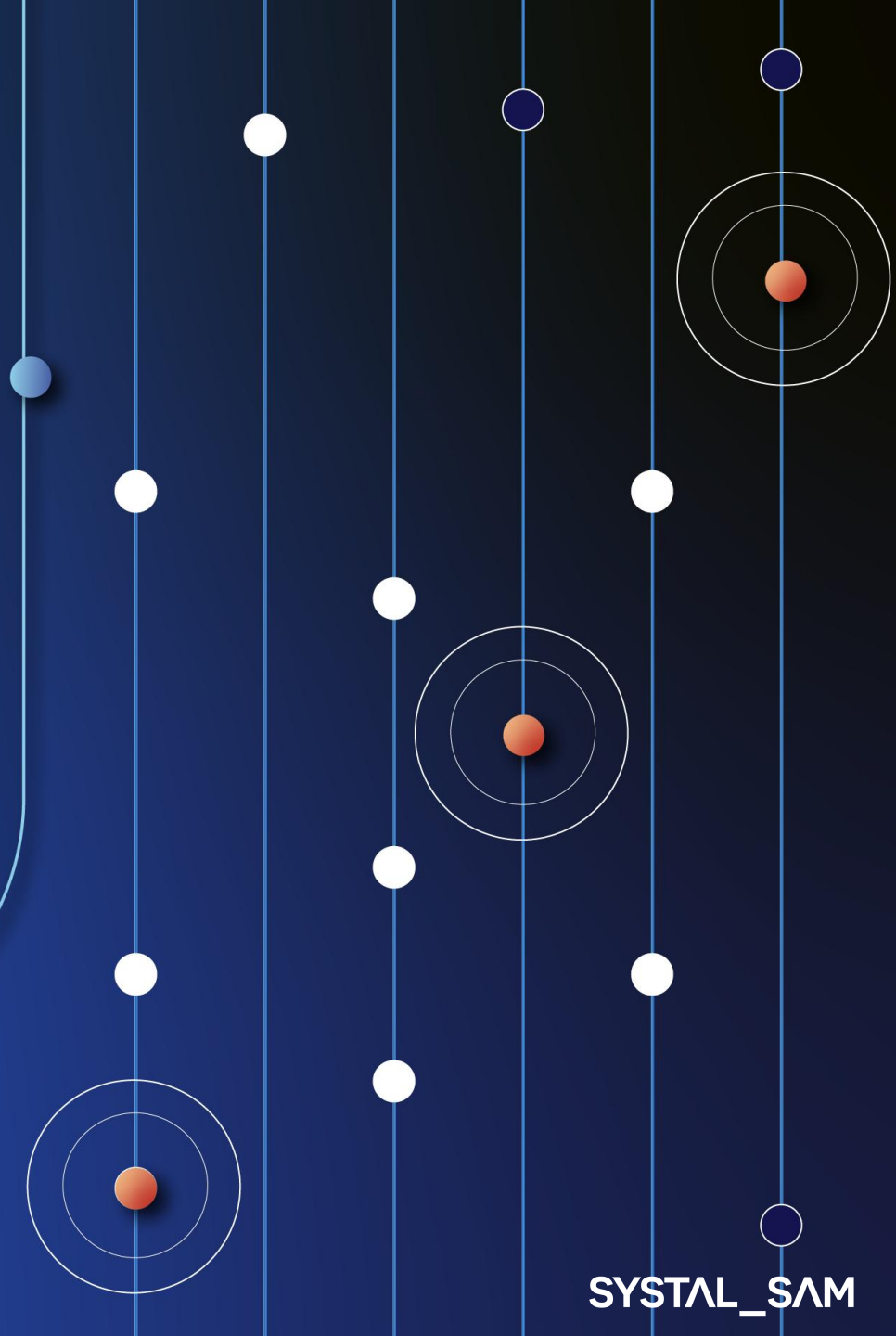
Discover how SAM delivers visibility while strengthening security, resilience, and compliance at scale...

SYSTAL_SAM

Enhanced Compliance

Systal's SAM (Secure AI Manager) automates the assessment of IT infrastructure against relevant regulatory and organisational standards in near real time. Rather than relying on periodic reviews, compliance is continuously measured and maintained.

SAM maps infrastructure to applicable policy frameworks, providing clear visibility and targeted remediation guidance. It supports a broad range of standards, including DORA, HIPAA, PCI Compliance, NIS2, and ICO requirements, alongside organisation-specific policies. This allows compliance to be managed consistently across regions and multivendor environments.
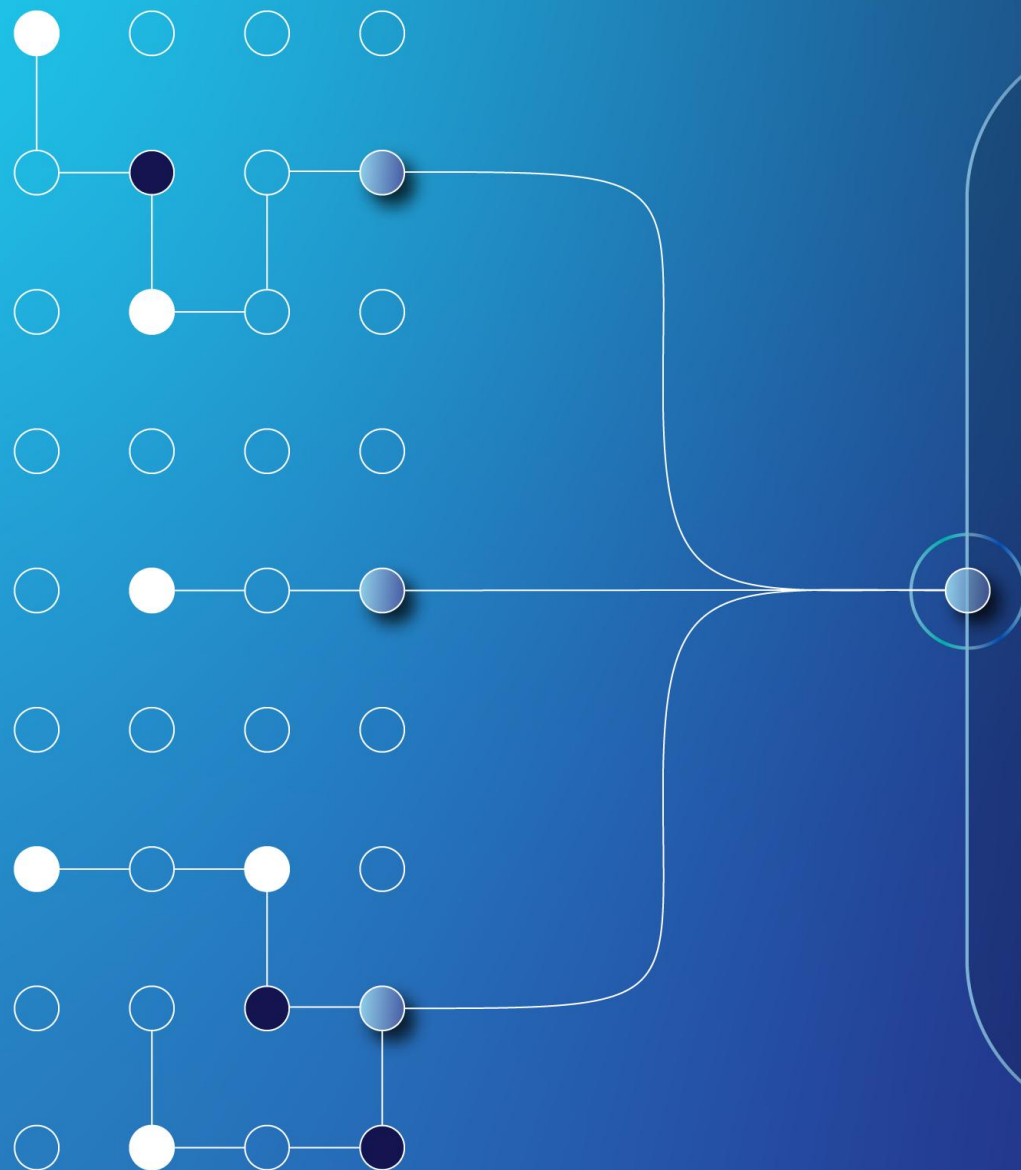
SYSTAL_SAM

Proactive Security

SAM continuously monitors your infrastructure for vulnerabilities. Identifying potential concerns before they become problems, SAM highlights red flags such as vulnerabilities and misconfigurations, keeping you ahead of threats.

SAM integrates up-to-date global vulnerability threat and analyses with live device configurations automatically. It applies rule recertification for automated lifecycle and cleanup workflows. The system also identifies, prioritises, and correlates vulnerabilities across the estate, highlighting severity and exposure.
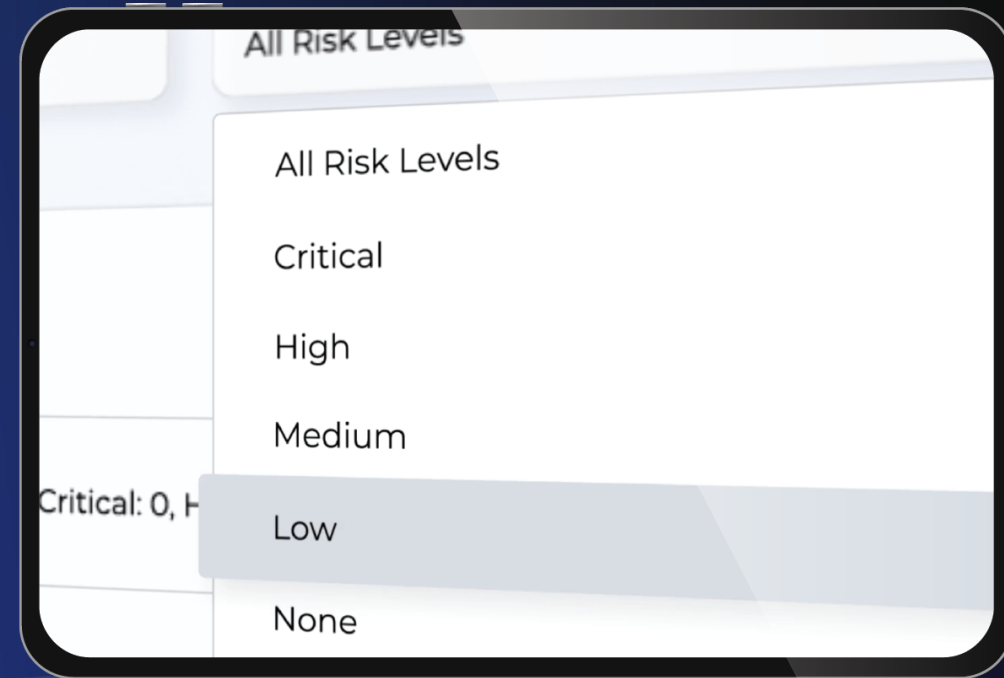
SYSTAL_SAM

Seamless Multi-Vendor Integration

SAM integrates effortlessly with your existing systems and suppliers, preventing the cost and complications of forced transformation. It eliminates blind spots created by vendor silos, ensuring strategy is driven by business needs, not supplier limitations.

Supporting major ITSM platforms, SAM prevents vendor lock-in and scales easily across multi-vendor environments.

SYSTAL_SAM

Augmented Network Security Insights

SAM provides both current and historical insight into network security posture. It equips your teams with actionable intelligence and the tools they need to stay ahead of evolving cybersecurity threats, drastically cutting the time and cost of incident response.

All Risk Levels

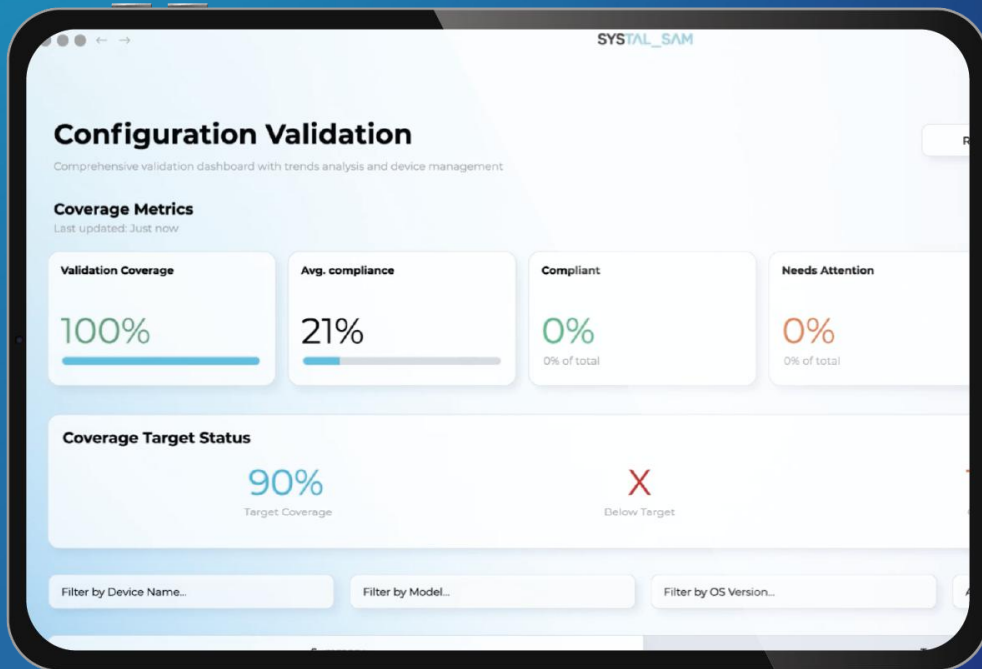All Risk Levels

Critical

High

Medium

Critical: 0, H

Low

None

SYSTAL_SAM

AI-Enhanced Efficiency

Automating operations, SAM reduces overheads, manual effort and downtime. Resolving issues in seconds instead of weeks, SAM frees your teams to focus on innovation, not administration.

By combining automation, continuous monitoring, and historical context, SAM evaluates environments continuously, reducing manual effort and supporting more reliable compliance outcomes as regulatory requirements evolve.

SYSTAL_SAM

Rapid Issue Resolution

Every second counts when risk can cost millions. SAM's automation capabilities delivers workflows and recommendations that reduce errors and accelerate response. Quickly assessing and prioritising potential concerns, SAM resolves incidents before they escalate.
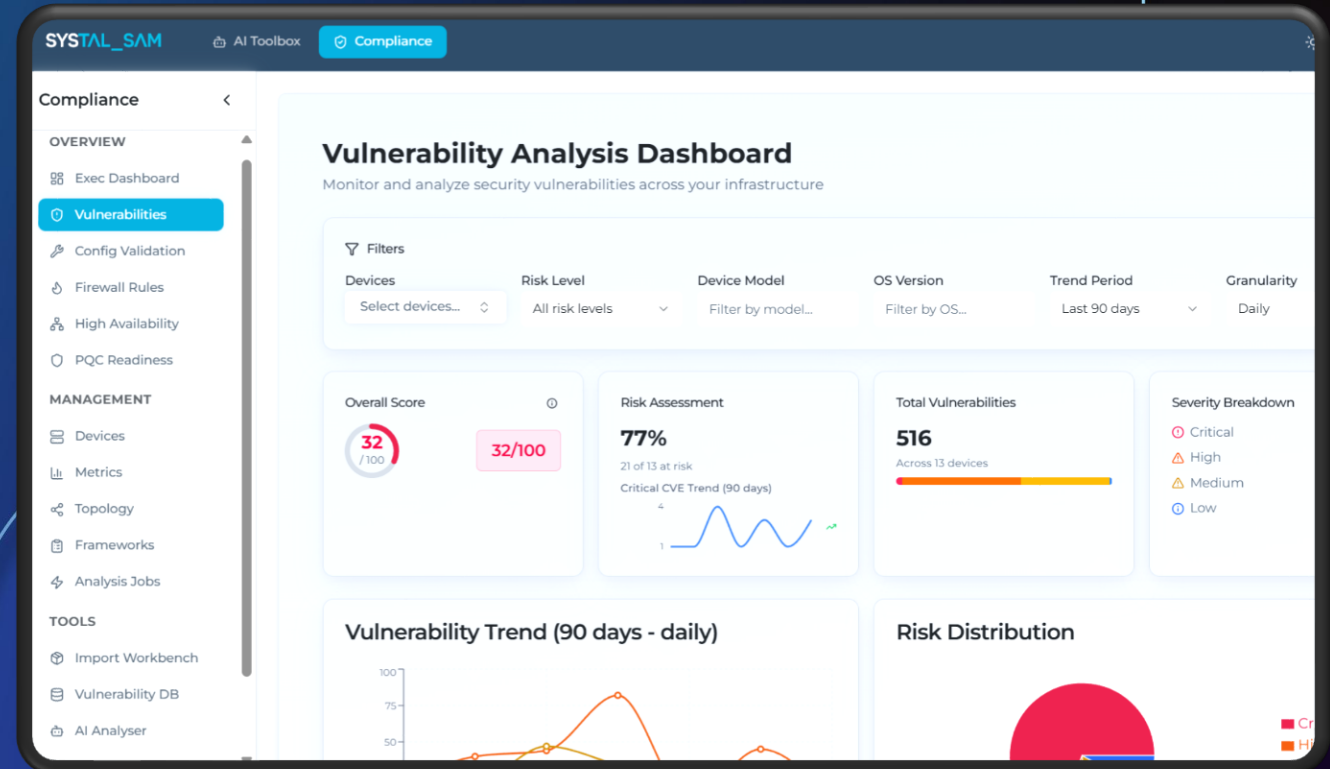

SYSTAL_SAM

Configuration Validation

Comprehensive validation dashboard with trends analysis and device management

Coverage Metrics
Last updated: Just now

Validation Coverage	Avg. compliance	Compliant	Needs Attention
100%	21%	0%	0%
		0% of total	0% of total

Coverage Target Status

90%
Target Coverage

X
Below Target

Filter by Device Name...   Filter by Model...   Filter by OS Version...

SYSTAL_SAM

SAM in Action: Vulnerability Management

SAM integrates up-to-date global vulnerability threat and analyses with live device configurations automatically. The system identifies, prioritises, and correlates vulnerabilities across the estate, highlighting severity and exposure.

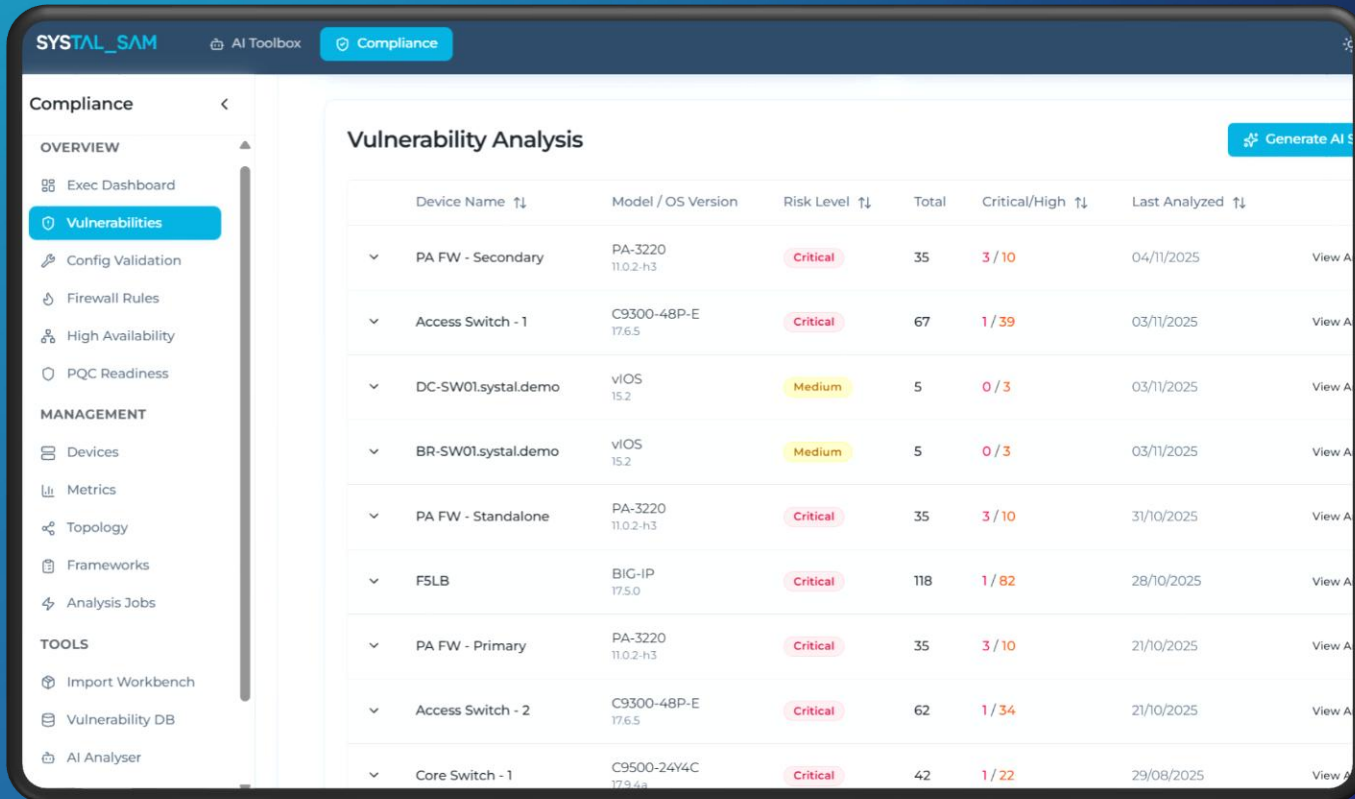SYSTAL_SAM

SAM in Action: Executive-level Visibility

Insights are available through an interactive dashboard, enabling:

> Executive-level visibility of the organisation's risk profile.

> Operational insights for delivery and network teams.

> AI powered recommendations and patch configuration options.

SYSTAL_SAM

SAM in Action: Remediation Actions

SAM generates remediation actions - including updated configurations and patch recommendations that can be validated by a human Network Engineer

Changes can be managed transparently through existing ITSM tools and workflows, ensuring traceability, compliance, and minimal disruption.
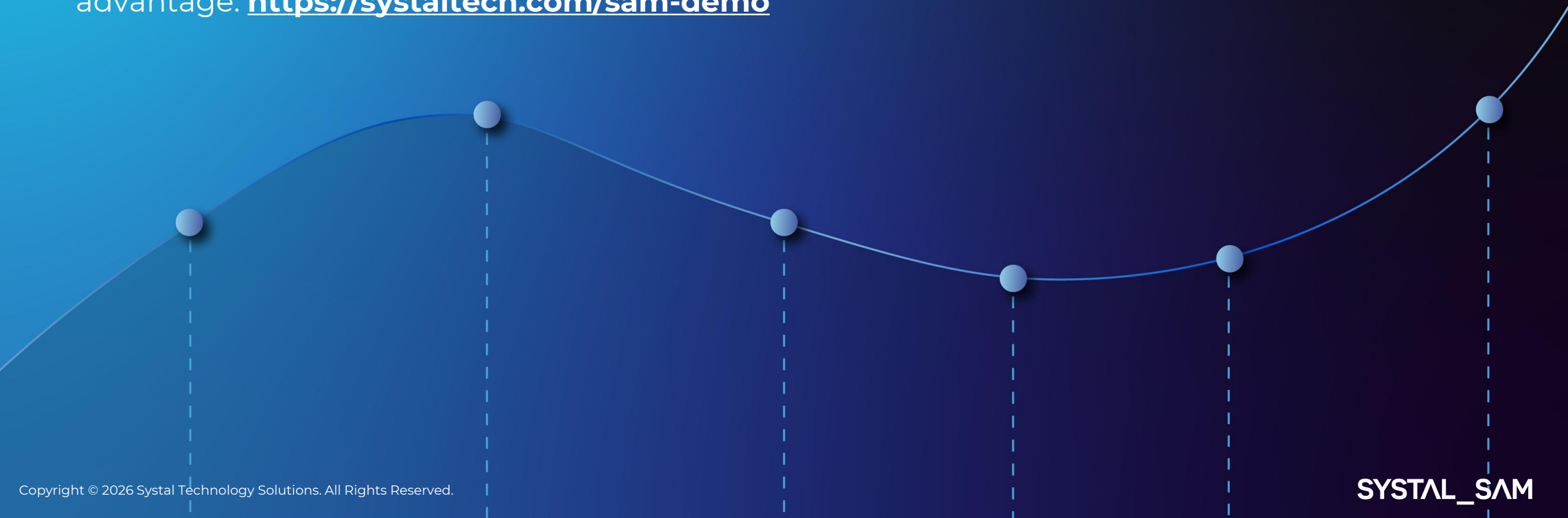
This human-in-the-loop approach combines AI-powered automation with expert oversight, delivering faster patching, fewer errors, and greater confidence in network security.

SYSTAL_SAM

Get Your SAM Demo

SYSTAL_SAM

Leading global enterprises trust Systal to manage their most complex IT estates.

Discover how SAM transforms visibility into competitive advantage: **https://systaltech.com/sam-demo**

SYSTAL_SAM