

NURPSUITE

Cyber Executive Decision Support & Operational Resilience Platform

Most platforms tell security teams what happened.

NurpSuite helps organizations understand what it means, what is at risk, and what to do next.

NurpSuite transforms telemetry from existing security investments into a shared operational picture for analysts, IT teams, incident responders, and executives.

By combining AI agents, Digital Twin modeling, threat intelligence, MITRE ATT&CK, MITRE ATLAS, and operational context, NurpSuite enables organizations to make faster, more informed decisions during cyber events.

THE PROBLEM

Organizations have invested heavily in cybersecurity tools.

CrowdStrike

Microsoft Defender

Sentinel

Splunk

Elastic

Tenable

Corelight

Recorded Future

The challenge is no longer collecting data. The challenge is understanding:

- Which business services are affected?
- Which operational functions are at risk?
- What decisions should leadership make?
- Which actions should be prioritized?
- How resilient is the organization today?
- Are we prepared for tomorrow's threats?

Most organizations do not have a visibility problem.

They have a decision problem.

THE NURPSUITE APPROACH

The operational layer above existing security investments.

Rather than replacing SIEMs, EDRs, threat intelligence platforms, ticketing systems, or cloud security tools, NurpSuite connects them into a common operating picture.

THE PLATFORM CONTINUOUSLY COMBINES

- Security telemetry
- Operational dependencies
- ATT&CK coverage
- Executive reporting
- Business services
- Threat intelligence
- AI threat analysis
- Digital Twin context

to create actionable decision support.

CORE PLATFORM CAPABILITIES

Built for decisions, not just detections.

Executive Lens

Purpose-built for executives, CISOs, CIOs, and operational leadership.

PROVIDES

- Current business risk
- Services affected
- Operational impact
- Recovery readiness
- Recommended decisions
- Executive briefings
- Organizational resilience metrics

Instead of technical alerts, leadership receives business context.

Digital Twin

The Digital Twin is the foundation of NurpSuite.

IT MODELS

- Business services
- Identity systems
- Infrastructure
- Operational dependencies
- Applications
- Cloud environments
- Security controls
- Mission-critical functions

THE DIGITAL TWIN ANSWERS

If this attack succeeds, what happens next?

DIGITAL TWIN OUTPUTS

- Service dependency mapping
- Impact analysis
- Recovery readiness assessment
- Business risk modeling
- Attack path visualization
- Operational resilience measurement

AI-Assisted Twin Creation

Organizations can rapidly create Digital Twins by importing:

Architecture diagrams

Visio exports

PDFs

Whiteboard designs

Cloud diagrams

AI extracts systems, relationships, and dependencies and presents them for review before building the model.

AI Orchestrator

The NurpSuite Orchestrator coordinates specialized AI agents working across the platform.

Rather than a single copilot, NurpSuite deploys purpose-built agents focused on resilience, detection effectiveness, investigation acceleration, and executive awareness.

SPECIALIZED AI AGENTS

Purpose-built agents, coordinated by the Orchestrator.

Detection Agent

CONTINUOUSLY EVALUATES

- Detection quality
- Rule performance
- False positives
- Coverage gaps

PROVIDES

- Tuning recommendations
- Optimization opportunities
- Detection effectiveness scoring

Detection Validation Agent

Validates defensive controls against known adversary behaviors.

CAPABILITIES INCLUDE

- Atomic Red Team execution
- ATT&CK validation
- Detection testing
- Coverage measurement
- Control validation

Threat Hunter Agent

Performs proactive analysis across telemetry sources.

IDENTIFIES

- Emerging threats
- Suspicious activity
- Behavioral anomalies
- Potential adversary activity

Coverage Agent

Measures defensive readiness.

TRACKS

- ATT&CK coverage
- ATLAS coverage
- Telemetry health
- Detection gaps
- Visibility deficiencies

Provides actionable recommendations.

Executive Agent

Transforms technical findings into executive understanding.

GENERATES

- Incident briefings
- Daily SITREPs
- Executive summaries
- Operational impact assessments
- Board-level reporting

ATT&CK & ATLAS COVERAGE

Traditional cyber threats and emerging AI attack surfaces.

MITRE ATT&CK

For adversary behavior, detection coverage, and defensive effectiveness.

MITRE ATLAS

For AI and machine-learning attack techniques.

This allows organizations to understand both traditional cyber threats and emerging AI-related attack surfaces.

BUSINESS IMPACT & OPERATIONAL RESILIENCE

Focused on outcomes, not alert counts.

Unlike traditional security platforms that focus on alerts and incidents, NurpSuite focuses on outcomes.

MEASURES INCLUDE

- Operational risk
- Critical service protection
- Business continuity
- Decision velocity
- Recovery readiness
- Exposure reduction
- Mission impact
- Agent-assisted time savings

INTEGRATIONS

Designed to work with existing security investments.

Supported and planned integrations include:

Microsoft Sentinel

Microsoft Defender

CrowdStrike

Splunk Enterprise Security

Elastic Security

Trellix

Tenable

Corelight

Recorded Future

Zeek

Suricata

ServiceNow

The platform enriches existing investments rather than replacing them.

TARGET MARKETS

Where operational resilience matters most.

Healthcare

Understand cyber events in terms of clinical and operational impact.

Education

Protect learning environments and critical student services.

MSSPs

Provide operational resilience as a service.

Federal Government

Support mission assurance and cyber-informed decision making.

Critical Infrastructure

Protect essential services and operational technology environments.

Financial Services

Improve resilience and executive visibility.

WHY NURPSUITE?**MOST PLATFORMS ANSWER**

What happened?

NURPSUITE ANSWERS

What does it mean, what is at risk, and what should we do next?