

# Uniting technology with education to secure your data and your people

Enterprise-grade protection, consumer-grade experience.



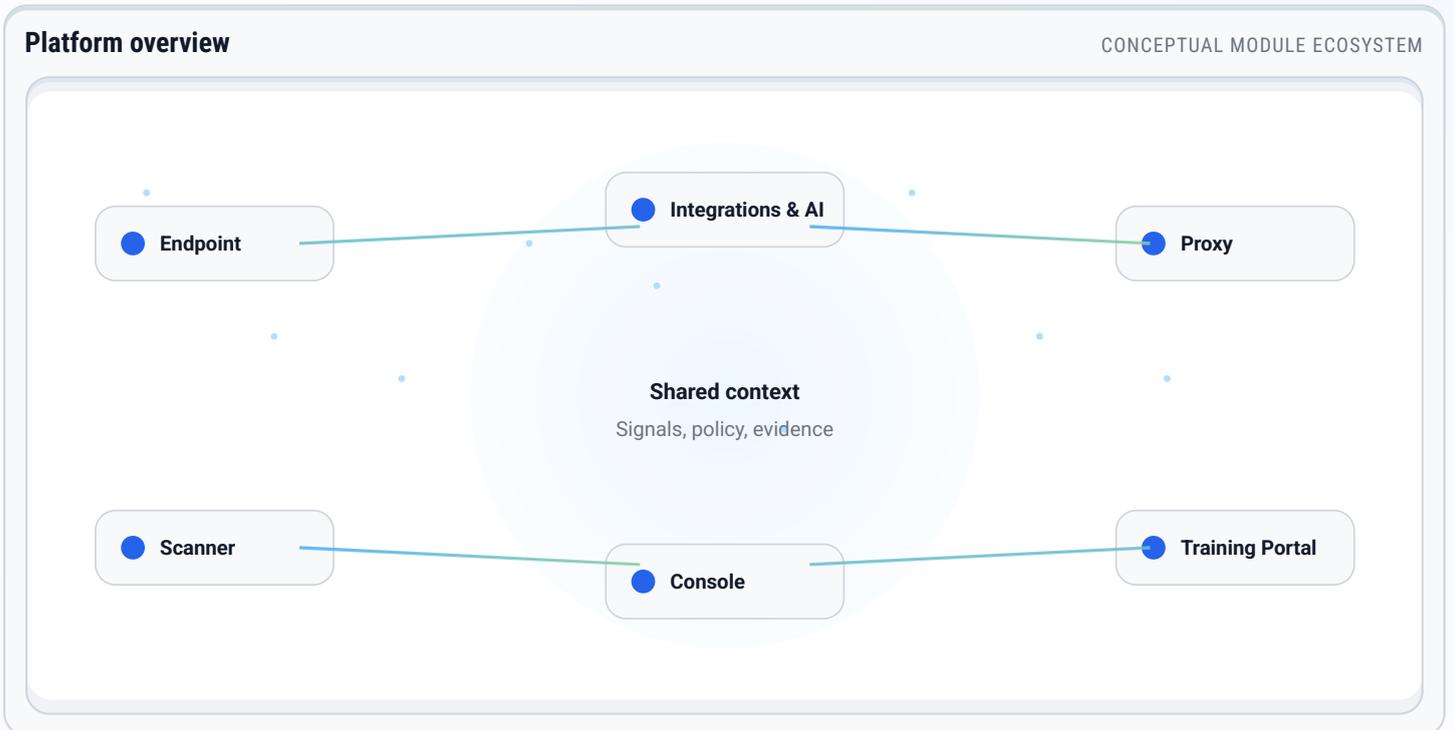
Security as Enablement



Education as Interface



Technology Serves Humanity



**AT A GLANCE**

- Platform security + education in one system
- Integrated governance & policy across modules
- Designed for SMB → enterprise + partners

**MODULES**

Console	Endpoint
Scanner	Proxy
Training Portal	Integrations & AI

3SN is a cybersecurity platform built to protect organizations and individuals without sacrificing usability. We blend enterprise-grade protection with an experience that people actually use — and learn from.

Our approach combines proactive technical security, integrated education, and pragmatic governance. The result is a security posture that improves continuously — technologically and culturally.

### Outcomes you can communicate

- Reduce social engineering exposure through continuous reinforcement
- Improve visibility and response coordination across teams
- Strengthen governance with policies aligned to standards and industry needs
- Show progress with clear reporting suitable for leadership and stakeholders
- Correlate signals across modules to reduce noise and improve prioritization

### The journey we enable

- Immediate protection (day one)
- Progressive understanding (through use)
- Behavioral change (habits shift naturally)
- Cultural transformation (security becomes reflex)

### How modules reinforce outcomes

CONCEPTUAL ROLLOUT PHASES



### Ideal for

- SMB to enterprise teams who need real protection without complexity
- Organizations reducing social engineering risk through ongoing awareness
- Partners seeking white-label cybersecurity + education capabilities

### Delivery model

- Modular platform that scales with your maturity
- Built-in education + governance, not bolt-ons
- Designed for adoption: secure because it's usable

### Governance & standards

- Policy guidance embedded across modules
- Evidence and reporting that support audits and renewals
- Industry-aware alignment (healthcare, finance, legal, education, retail)



## Enterprise security

Powerful but complex  
Adoption fails at the human layer  
Training is separate from tools

## Consumer security

Simple but shallow  
Limited visibility and control  
Hard to prove progress

## 3SN approach

Enterprise-grade capability  
Consumer-grade experience  
Education + governance built in

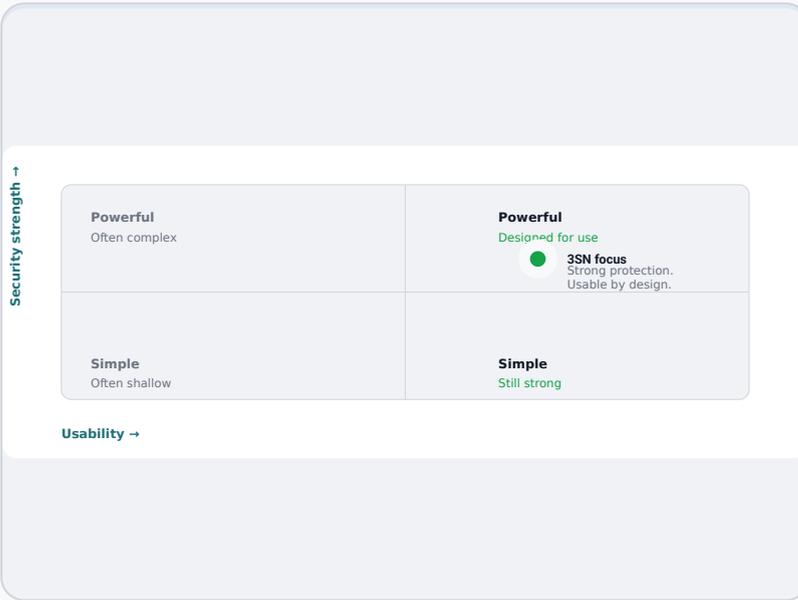


## Why this matters

Many incidents start with social engineering and workflow gaps. We design security that fits how people actually work — so protection is used consistently.

## Security + usability framing

CONCEPTUAL VIEW



## Signals by module

DESCRIPTIVE VIEW

<b>Endpoint</b>	Posture + endpoint activity
<b>Proxy</b>	Web/DNS access + enforcement
<b>Scanner</b>	Discovery + vuln findings
<b>Training Portal</b>	Awareness progress + reinforcement
<b>Integrations &amp; AI</b>	Normalize + correlate context
<b>Console</b>	Policies/workflows + reporting

## Built for regulated environments

Governance and policy guidance aligned to standards and industry expectations  
Controls that reinforce correct behavior, not just enforcement  
Reporting that supports audits, renewals, and executive visibility





## Security as Enablement

Protection that increases freedom – not friction. Powerful defaults. Clear controls. Confidence without complexity.



## Education as Interface

Every interaction teaches. We strengthen the human layer of defense through contextual learning, not lectures.

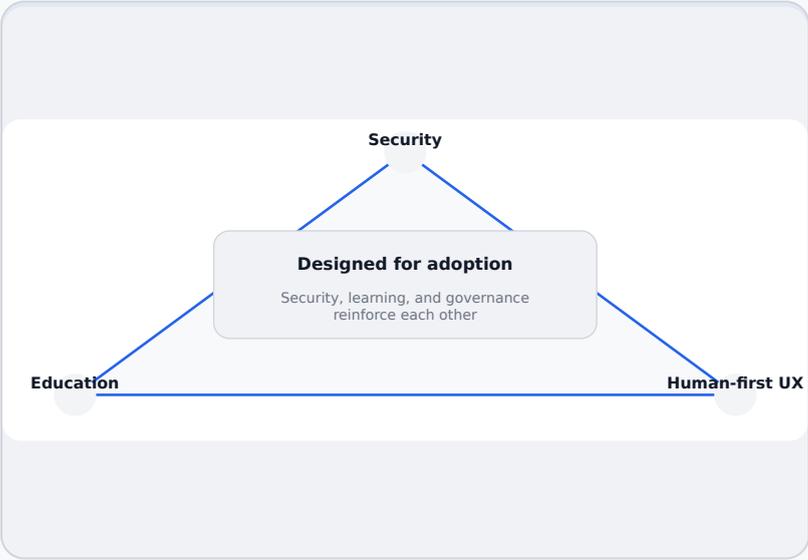


## Technology Serves Humanity

Tools fit hands – not the other way around. Enterprise capability with consumer-grade clarity.

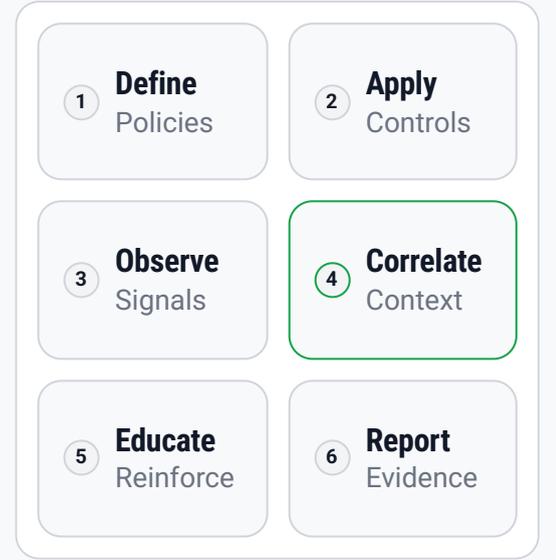
### Pillars working together

CONCEPTUAL MODEL



### Policy lifecycle

GOVERNANCE EMBEDDED



### How this shows up in the platform

- Default-secure configurations that reduce operational overhead
- Contextual education that reinforces the right actions at the right time
- Governance and policy support embedded across modules
- A shared data layer that enables correlation, prioritization, and reporting





## Console

Central management and orchestration

Unified visibility across your environment  
Policy management and response workflows  
Actionable reporting for leadership and teams



## Training Portal

Continuous education & awareness

Phishing simulation and reinforcement  
Role-based learning journeys  
Measurable progress and accountability



## Endpoint Client

Lightweight endpoint protection

Behavior-focused detection  
Minimal performance impact  
Cross-platform coverage



## Scanner

Asset discovery & vulnerability insight

Find unknown devices and exposures  
Prioritize remediation by risk  
Track trends over time



## Proxy Platform

Secure web traffic and routing

Block phishing and malicious destinations  
Improve control over outbound traffic  
Visibility and analytics



## Integrations & AI Correlation

Connect signals, align governance, accelerate response

Unify signals across modules and environments  
AI-assisted correlation to surface actionable risk  
Support governance/policy adherence with standards-aware guidance

### Works better together

Each module is valuable alone – together they create shared context for faster decisions.  
Correlation and governance signals reduce noise and improve prioritization.  
Reporting becomes stakeholder-ready when data is unified and explainable.



## Connect

Deploy endpoint + connect assets  
Bring modules online quickly  
Establish shared context

## Detect

Monitor, scan, and identify risk  
Visibility into exposure and behavior  
Prioritize what matters

## Respond

Act from a unified console  
Coordinate workflows  
Improve time-to-action

## Improve

Train and harden continuously  
Reinforce secure behavior  
Turn lessons into policy

## Governance & Policy

Standards-aligned guidance across modules  
Industry-aware controls and documentation  
Audit-friendly reporting and evidence

## Outcome

Immediate protection with progressive understanding.  
Correlation + governance reduces noise and improves prioritization.  
Behavior change becomes measurable – suitable for leadership and stakeholders.

## Next Steps

We invite you to explore the platform and discuss your security roadmap.

### Choose your next step

Book a demo: see the platform and a recommended rollout plan  
Partner inquiry: white-label and integration opportunities  
Security roadmap: align governance/policy with your industry and risk profile

Contact

[contact@3sn.com](mailto:contact@3sn.com)

Website

[3sn.com](https://3sn.com)

Contact

Email us to schedule a demo or roadmap review

### What you'll get

A clear overview of modules and how they work together  
A governance/policy alignment conversation tailored to your industry  
Next steps and a suggested implementation path

### Education

Reinforce the right habits  
Included throughout the platform experience – protection that teaches through use.