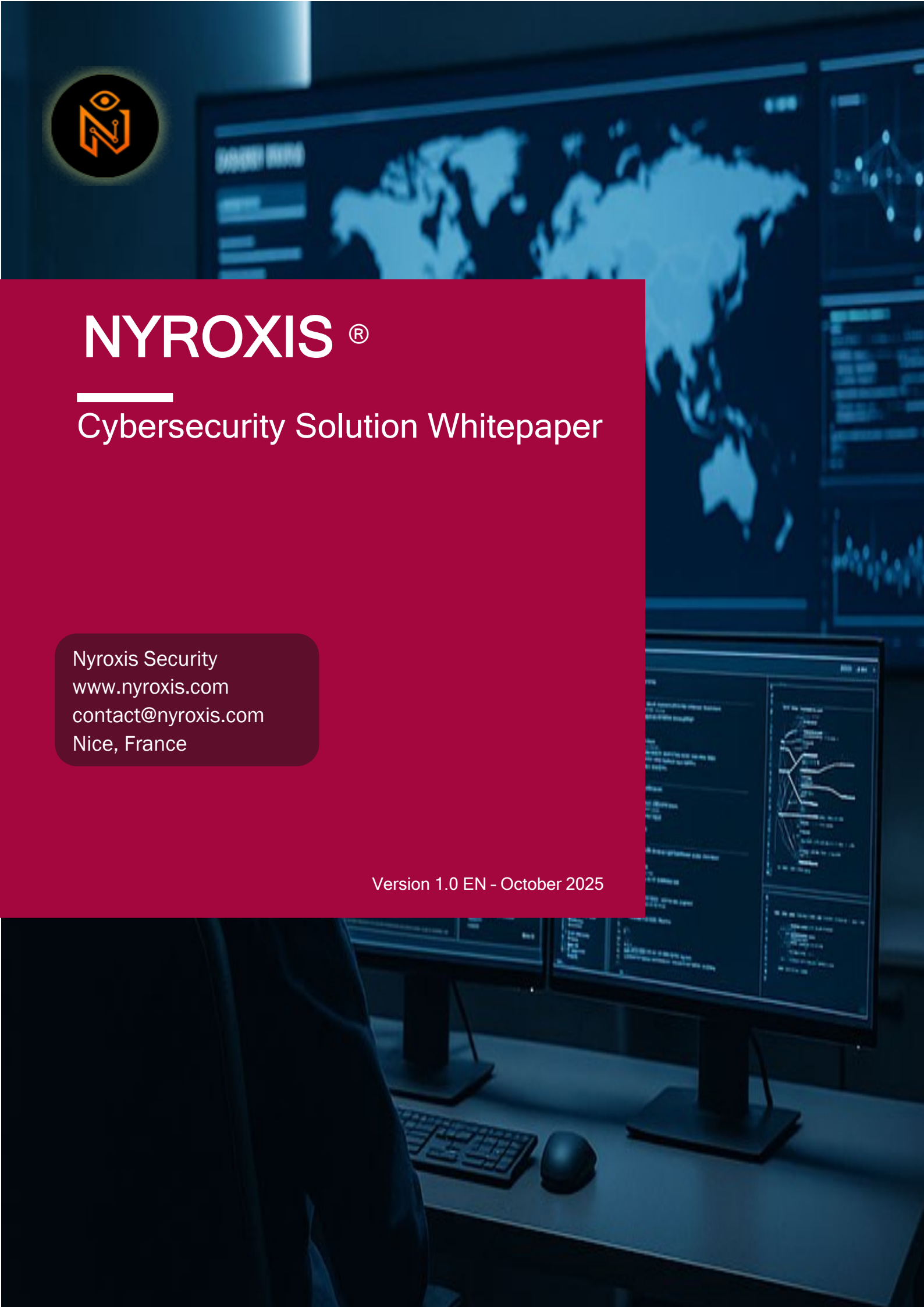


NYROXIS ®

Cybersecurity Solution Whitepaper

Nyroxis Security
www.nyroxis.com
contact@nyroxis.com
Nice, France

Version 1.0 EN - October 2025

Table of Contents

The New Cybersecurity Reality

Cyber threats today extend beyond corporate firewalls. Attackers increasingly target the personal devices of executives, administrators, judges, doctors, and other professionals whose decisions carry weight. A single compromised laptop at home, a shared tablet, or an unsecured family device can become the silent doorway into critical infrastructures.

The Blind Spot

Organizations invest heavily in enterprise security — firewalls, SOCs, and advanced monitoring platforms — yet these controls often stop at the office. The personal digital lives of key individuals remain exposed, creating a blind spot that attackers exploit. This imbalance leads to financial loss, regulatory exposure, and reputational damage.

The Nyroxis Solution

Nyroxis closes this gap with a lightweight, stealth, and offline-capable security agent paired with an intelligent dashboard. It silently monitors endpoints, preserves forensic-grade evidence, and correlates suspicious activity without relying on constant connectivity. The solution is designed to complement, not replace, existing enterprise defenses — extending protection to where it matters most.

Key Advantages

- **Executive & VIP Protection:** Safeguards decision-makers and their families from targeted intrusions.
- **Compliance & Assurance:** Aligned with global standards and directives, including GDPR, NIS2, and ISO 27001.
- **Forensic Readiness:** Provides tamper-resistant logs and reliable evidence for faster investigations.
- **Operational Simplicity:** Seamlessly integrates into existing security operations with minimal overhead.
- **Business Impact:** Reduces breach costs, shortens incident response time, and extends Zero Trust principles to the human perimeter.

Conclusion

Nyroxis transforms the weakest link into a controlled surface. By protecting personal endpoints and bridging the gap between home and enterprise, it delivers both compliance confidence and measurable business value. It is not just a product, but a strategic layer of defense for organizations that cannot afford blind spots.

Introduction & Context

Cybersecurity at a Crossroads

Every week brings new headlines of massive data breaches, ransomware campaigns, or sophisticated nation-state attacks. Despite billions invested in advanced firewalls, SIEM platforms, and SOC operations, attackers continue to succeed. The question is no longer *if* a breach will occur, but *when* and *where*.

The Hidden Entry Point

While enterprise infrastructures are heavily defended, attacks often start where security policies end: at home. A personal laptop of a CEO, a family tablet connected to the same Wi-Fi as an administrator, or the late-night browsing of a judge or lawyer can all become attack vectors. These devices are rarely monitored at the same level as corporate assets, creating a vulnerability window.

The Human Impact

Behind every statistic lies a personal story — families waking up to drained accounts, professionals exposed to blackmail, or public servants whose credibility is undermined by a single compromised device. Cybersecurity is not just about protecting data; it is about safeguarding trust, dignity, and the continuity of critical decisions.

Why a New Approach Is Needed

Traditional antivirus and enterprise SIEM systems were not designed for this reality. They are optimized for corporate environments, but they fail to cover the personal sphere where high-value individuals live and work. Closing this gap requires a solution that is lightweight, discreet, and capable of functioning reliably even when offline — a solution that brings enterprise-grade defense into the personal digital space.

Our Commitment

Nyroxis was created to address this challenge directly. By extending protection beyond the office and into the personal lives of high-value individuals, it provides organizations with the missing layer they need to prevent breaches, reduce risk, and maintain trust in an increasingly hostile digital world.

Problem Statement

The Expanding Threat Surface

Cybersecurity investments have strengthened corporate infrastructures, yet attackers are not deterred. Instead, they adapt by seeking the weakest entry point: the personal digital lives of executives, administrators, and professionals. Home networks, family devices, and unmanaged personal endpoints have become the new attack surface.

Why Existing Tools Fall Short

Traditional security solutions — antivirus, EDR, and enterprise SIEMs — are designed for controlled office environments. They lack visibility into personal devices and cannot reliably monitor activity outside corporate perimeters. This blind spot leaves organizations vulnerable to breaches that begin far from the office but end inside the network.

Consequences of Inaction

- **Financial Losses:** A single compromised device can lead to multi-million-dollar breaches.
- **Reputational Damage:** Incidents involving executives or public servants quickly erode trust and credibility.
- **Regulatory Exposure:** Data protection laws and security directives require organizations to demonstrate due diligence across their ecosystems — including endpoints that attackers exploit.
- **Human Cost:** Beyond numbers, breaches impact families, careers, and the safety of those in critical roles.

The Core Problem

There is a critical security gap between enterprise-grade defenses and the everyday digital lives of the people who lead, decide, and protect. Attackers know this gap exists — and they exploit it. Organizations currently lack an effective, lightweight, and privacy-respecting solution to close it.

Our Solution – Nyroxis

Closing the Gap

Nyroxis was designed to address the most overlooked vulnerability in modern cybersecurity: the personal devices and home networks of high-value individuals. By combining a lightweight agent with an intelligent dashboard, Nyroxis extends enterprise-grade defense into the personal sphere — where attackers often begin.

Core Principles

- **Lightweight & Stealth:** Runs silently in the background with minimal resource usage, making it invisible to attackers while non-disruptive for users.
- **Offline-Capable:** Functions reliably without constant connectivity, ensuring evidence is preserved even when devices are isolated.
- **Forensic-Grade Monitoring:** Captures and encrypts security events to provide tamper-resistant, court-admissible evidence.
- **Complementary Design:** Works alongside existing enterprise defenses (AV, EDR, SIEM), adding an essential extra layer instead of replacing current tools.

How It Works

1. **Nyroxis Agent** – Deployed on personal devices, it continuously observes processes, connections, and system changes.
2. **Nyroxis Dashboard** – Provides real-time insights, correlation of suspicious events, and simplified reporting for decision-makers and security teams.
3. **License & Security Framework** – Ensures authenticity, integrity, and trust through hardware-based binding and cryptographic validation.

Unique Value

- Protects **executives, administrators, and professionals** from targeted attacks at home.
- Reduces **breach risk and regulatory liability** by closing the weakest security gap.
- Enhances **incident response** with reliable, forensic-ready data.
- Offers a **privacy-conscious design** aligned with global data protection principles.

In One Line

Nyroxis is not another corporate tool — it is the **strategic missing layer** that protects people where traditional cybersecurity ends.

Architecture & Technology

Overview

Nyroxis is built as a **modular, lightweight security platform** that combines endpoint monitoring with a central dashboard. Its architecture is designed to be simple to deploy, discreet in operation, and strong in forensic integrity.

Key Components

1. **Nyroxis Agent**
   - Installed on personal endpoints (Windows, Linux; future macOS).
   - Collects telemetry: processes, connections, system events.
   - Stores logs in encrypted format, resistant to tampering.
   - Operates with minimal resource consumption, invisible to attackers.
2. **Nyroxis Dashboard**
   - A modern Windows-based interface (WPF) for security teams and VIP users.
   - Displays real-time insights, correlation results, and forensic data.
   - Supports log search, severity filtering, visualization, and export (PDF/CSV).
   - Integrated alerting system for critical events.
3. **Correlation Engine**
   - Identifies suspicious patterns across events.
   - Supports rule-based and scenario-based detection.
   - Designed for future AI/ML integration.
4. **License & Security Framework**
   - Hardware-bound licensing (HWID).
   - Strong cryptography (Ed25519 signatures, AES-encrypted logs).
   - Offline validation for tamper resistance.

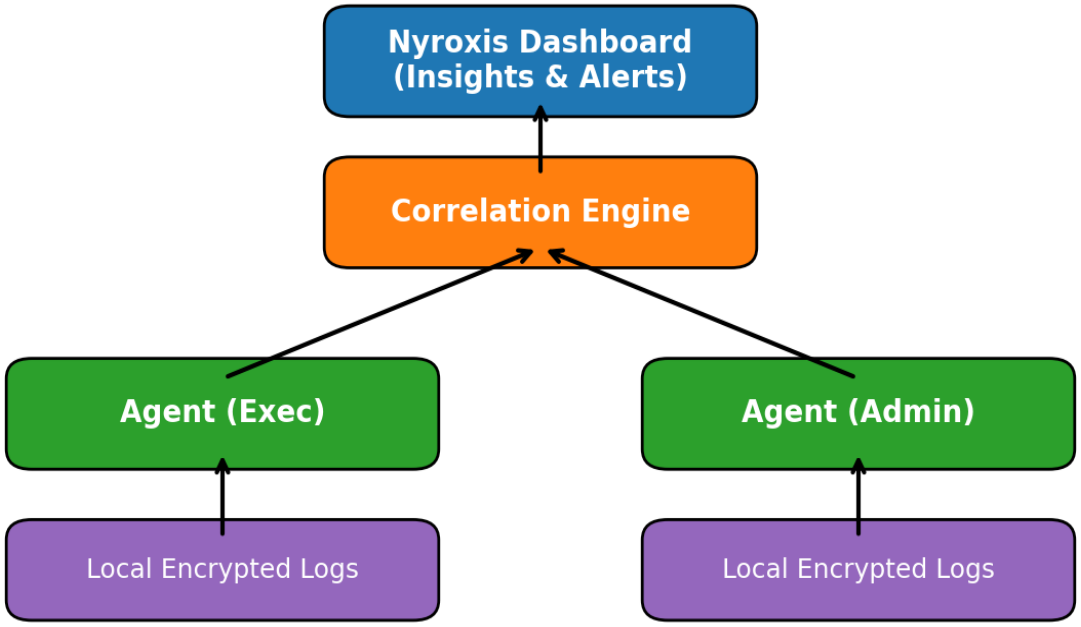
Technology Stack

- **Agent:** C# (.NET 8), Python (for open-source edition).
- **Dashboard:** WPF, LiveCharts/SkiaSharp for visualization, SQLite for local storage.
- **Crypto:** SHA-256 hashing, Ed25519 for signatures, AES-256 for encryption.
- **Cross-Platform Vision:** Windows (current), macOS/Linux (roadmap).

Design Principles

- **Simplicity:** Easy deployment, minimal maintenance.
- **Stealth:** Invisible to attackers, non-intrusive for users.
- **Forensic Integrity:** Logs remain reliable and admissible.
- **Complementarity:** Works with, not against, existing AV/EDR/SIEM investments.

Architecture Diagram



* Forensic-Grade Storage (Tamper Resistant)

* Offline-Capable Operation

Summary

The Nyroxis architecture ensures **continuous visibility**, **forensic readiness**, and **privacy by design**. Its modular structure allows enterprises to scale from a few protected VIP endpoints to entire holding networks — without sacrificing simplicity or performance.

Where Nyroxis Delivers Real Value

Cyber threats evolve by exploiting blind spots. Nyroxis was designed to address the most critical gaps where traditional cybersecurity tools cannot reach. The following scenarios illustrate where the solution creates immediate impact:

1. Executive & Family Protection

Executives, administrators, and public figures are high-value targets. Their family members, often less security-aware, become indirect entry points for attackers. Nyroxis ensures that personal laptops, tablets, and shared home devices are silently monitored, reducing the chance of a single personal compromise escalating into a corporate breach.

2. Sensitive Professions

Judges, police officers, lawyers, and SOC administrators hold sensitive information and influence over critical operations. A compromise of their personal digital life can lead to blackmail, reputational damage, or even manipulation of justice. Nyroxis protects these individuals with discreet, forensic-ready monitoring that safeguards both their privacy and professional credibility.

3. Multinational Holdings

Large corporations with globally distributed leadership face additional risks: inconsistent personal device security across borders. Attackers know that targeting a regional executive's personal laptop may unlock access to global infrastructure. Nyroxis provides a unified protective layer that scales seamlessly across countries and subsidiaries, closing the weakest links.

4. Organizational Deployments

Nyroxis is not limited to VIPs. Enterprises can deploy it for **internal red-team simulations, awareness projects, and insider risk monitoring.** Its lightweight design allows security leaders to extend visibility into environments where traditional SIEMs or EDRs cannot reach, creating a holistic view of enterprise risk.

Summary

From boardrooms to courtrooms, from multinational holdings to family homes, Nyroxis extends protection beyond the corporate perimeter. By following people wherever they live and work, it transforms the most vulnerable spaces into controlled, monitored environments — without disrupting daily life.

Benefits & Value Proposition

Turning Security Into Strategic Value

Cybersecurity is not just a technical concern — it is a matter of business continuity, reputation, and trust. Nyroxis delivers value across every level of the organization, from the security operations center to the boardroom and down to the individual executive.

1. For Security Leaders (CISO & SOC Teams)

- **Reduced Attack Surface:** Extends visibility into the personal devices of executives and high-value staff, eliminating a common blind spot.
- **Forensic-Grade Evidence:** Secure, tamper-resistant logs support faster incident response and legal proceedings.
- **Operational Fit:** Designed to integrate with existing SOC workflows without adding unnecessary complexity.

2. For Senior Management (CEO & Board)

- **Protection of Intangible Assets:** Safeguards brand reputation, investor trust, and strategic decision-making.
- **Reduced Risk Exposure:** Limits the potential of high-cost breaches originating from personal endpoints.
- **Demonstrated Due Diligence:** Shows regulators, shareholders, and partners that leadership is proactively secured.

3. For VIP Users (Executives, Judges, Public Servants)

- **Seamless Protection:** Lightweight, invisible, and non-intrusive security that requires no technical expertise.
- **Privacy-Respecting Design:** Built with encryption and minimal data collection to ensure personal confidentiality.
- **Peace of Mind:** Confidence that personal devices and family environments are shielded from sophisticated threats.

The Strategic Advantage

Nyroxis transforms personal security into **organizational resilience**. By protecting the people who matter most, it prevents breaches, accelerates investigations, and reduces costs — all while strengthening trust at every level of the enterprise.

Compliance & Standards

Security That Aligns With Global Regulations

In today's regulatory environment, cybersecurity is not only about protection — it is about compliance and accountability. Organizations must demonstrate that they are actively managing risks across every layer of their digital ecosystem, including personal endpoints that attackers exploit. Nyroxis has been developed with these requirements in mind, ensuring that enterprises can both strengthen defenses and prove compliance.

European Frameworks

- **GDPR (General Data Protection Regulation):** Nyroxis respects data minimization principles, encrypts all collected telemetry, and ensures personal information is never exposed unnecessarily.
- **NIS2 Directive:** Provides continuous visibility and incident-readiness on personal endpoints, helping organizations meet new EU cybersecurity obligations.
- **ENISA Guidelines:** Aligns with European best practices for resilience, monitoring, and incident reporting.

International Standards

- **ISO/IEC 27001:** Nyroxis supports alignment with the global benchmark for information security management systems.
- **Forensic Readiness:** Tamper-resistant log storage ensures that evidence is reliable, auditable, and admissible for legal or regulatory review.

US & Global Best Practices

- **NIST Cybersecurity Framework:** Complements Identify–Protect–Detect–Respond–Recover functions by covering personal endpoints often excluded from corporate scope.
- **Zero Trust Principles:** Extends the "never trust, always verify" model into the personal space of executives and VIPs.

Summary

By embedding compliance and audit-readiness into its design, Nyroxis helps organizations not only **reduce risk** but also **demonstrate due diligence** to regulators, auditors, and stakeholders worldwide. It is a solution built for resilience in both technical and regulatory dimensions.

Roadmap

From Vision to Full-Scale Deployment

Nyroxis was created to address a clear security gap, but its ambition goes far beyond the initial release. The project is structured with a phased roadmap that ensures immediate value today while laying the foundation for continuous innovation tomorrow.

Phase 1 – Community Edition (Open Source)

- Initial lightweight agent and dashboard released on GitHub.
- Focus on transparency, awareness, and education.
- Enables early adopters, researchers, and security enthusiasts to test the core vision.
- Serves as the “first brick” of the larger Nyroxis ecosystem.

Phase 2 – Pro Edition (Commercial)

- Advanced agent with HWID-bound licensing and tamper resistance.
- Full-featured dashboard with correlation engine, forensic export, and compliance-ready reporting.
- Tailored for **VIP customers, professionals, and organizations** that cannot afford blind spots.
- Offers both subscription and perpetual licensing models.

Phase 3 – Enterprise Integration

- Support for large-scale deployments in multinational holdings.
- Custom configurations for compliance (GDPR, NIS2, ISO/IEC 27001).
- Seamless integration with existing SOC/CSIRT workflows.
- Enterprise support and premium service-level agreements.

Future Development

- **macOS Agent:** Expanding protection to Apple environments used by executives.
- **AI/ML Correlation:** Automated anomaly detection for faster, smarter insights.
- **Cloud Integration:** Optional cloud-based analytics for large-scale organizations requiring centralized oversight.

Summary

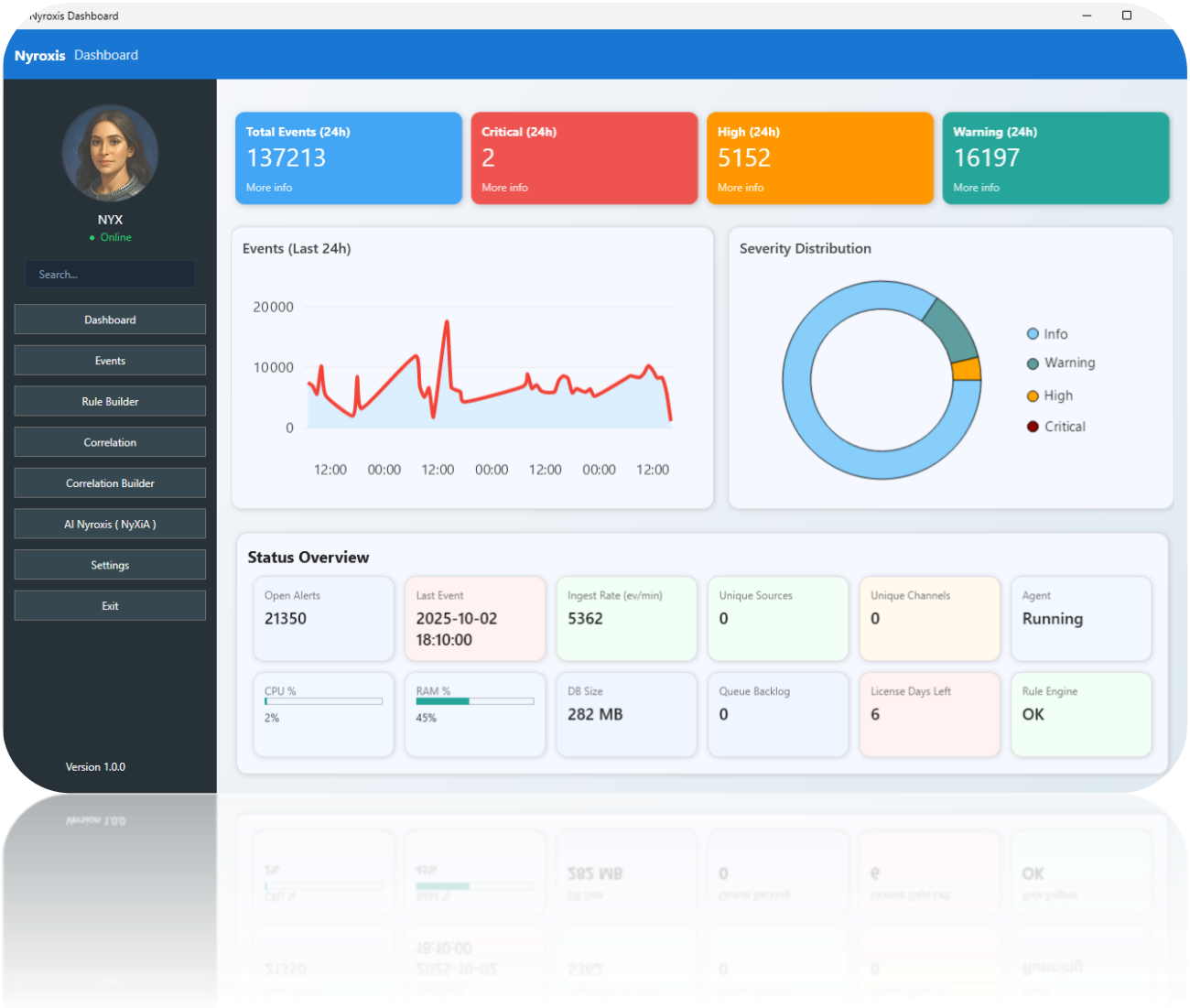
The Nyroxis roadmap reflects a balance between **immediate practicality** and **long-term innovation**. From open-source transparency to enterprise-grade deployments, every phase is designed to close the personal security gap and strengthen resilience for individuals and organizations alike.

Dashboard Demonstration

Nyroxis comes with a modern and intuitive dashboard designed to provide real-time visibility, correlation, and forensic insights. Below are selected screenshots illustrating the main features:

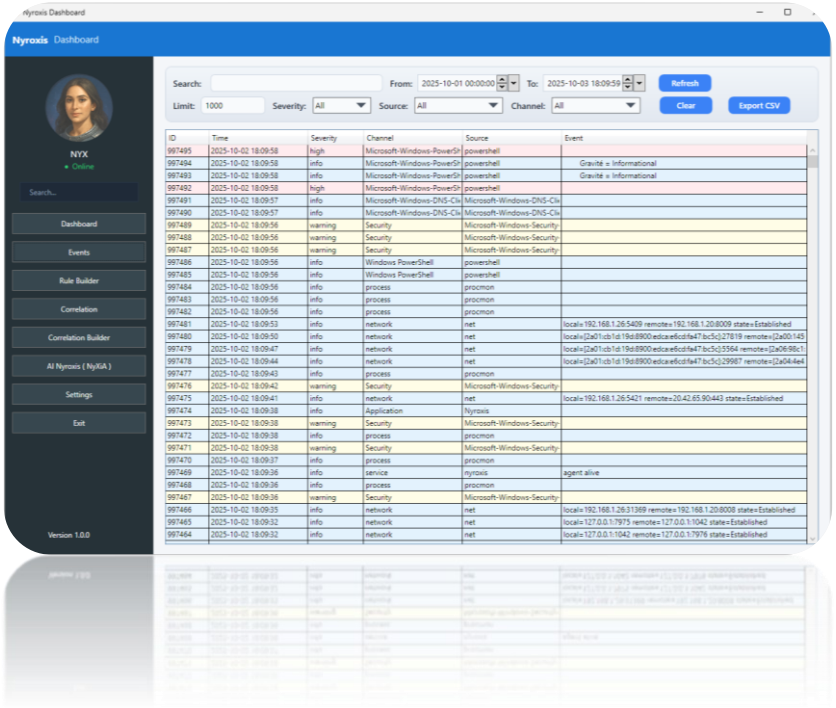
1. Main Dashboard

Provides an overview of total events, severity distribution, and system status.



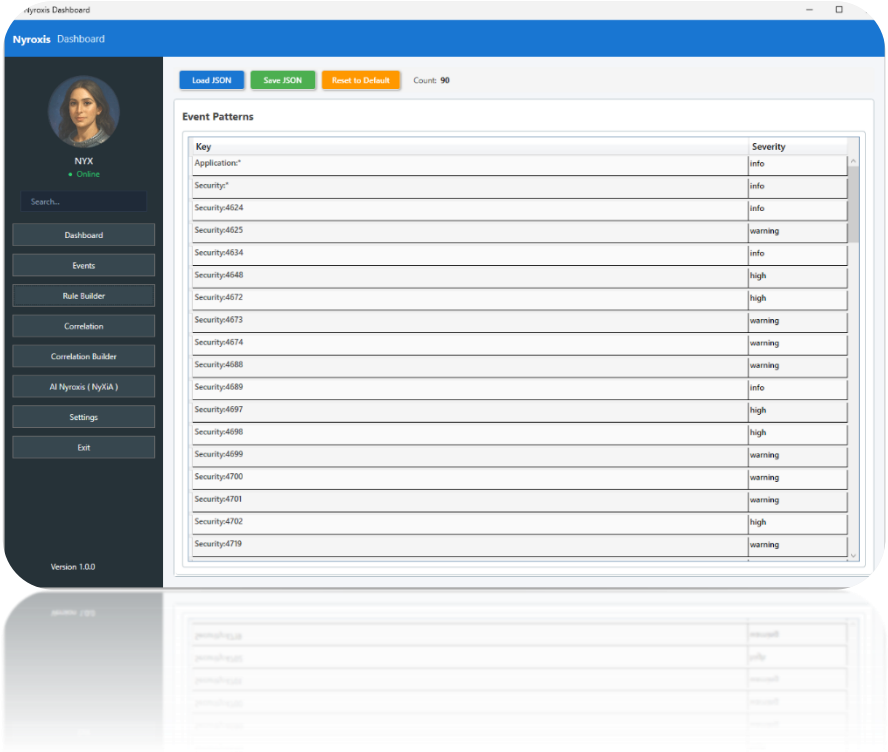
2. Events View

Displays detailed event logs with filtering by severity, source, and channel.



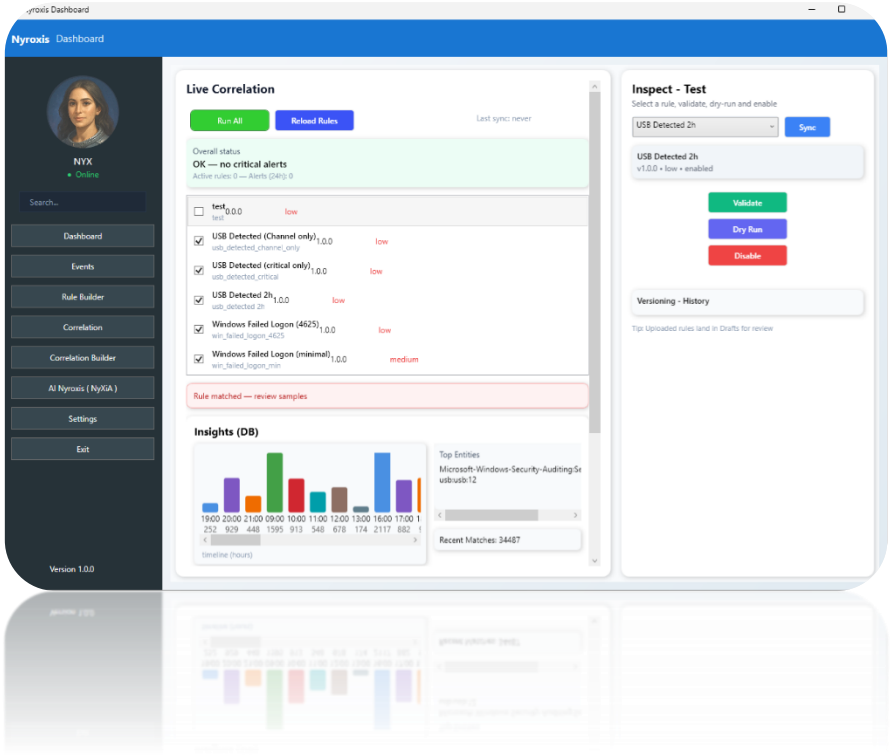
3. Rule Builder

Allows security teams to define and customize detection rules using JSON patterns.



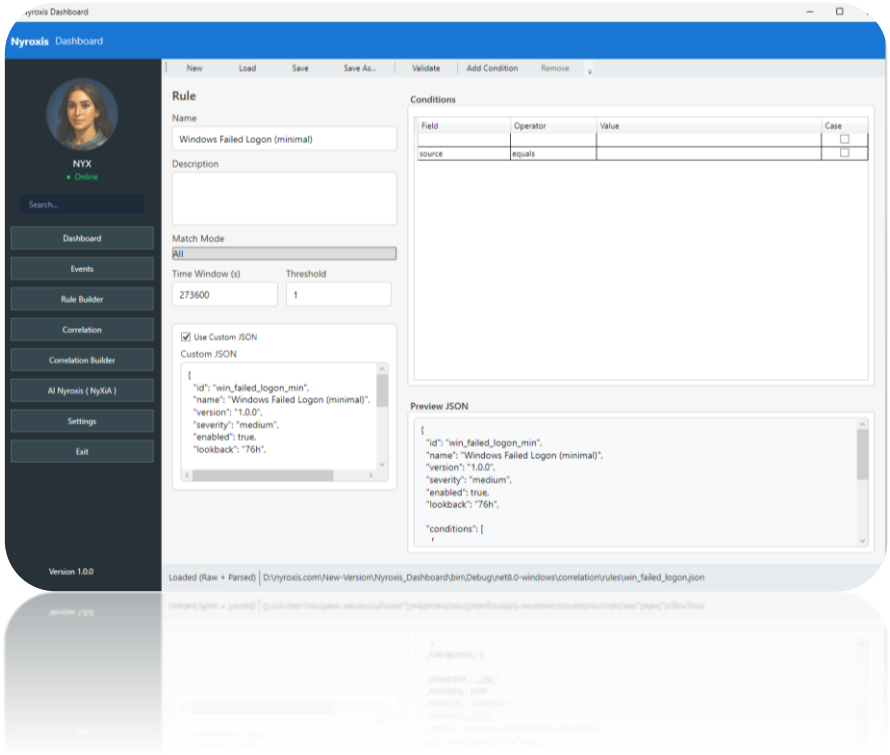
4. Live Correlation

Shows active correlation rules, matches, and insights with severity levels.



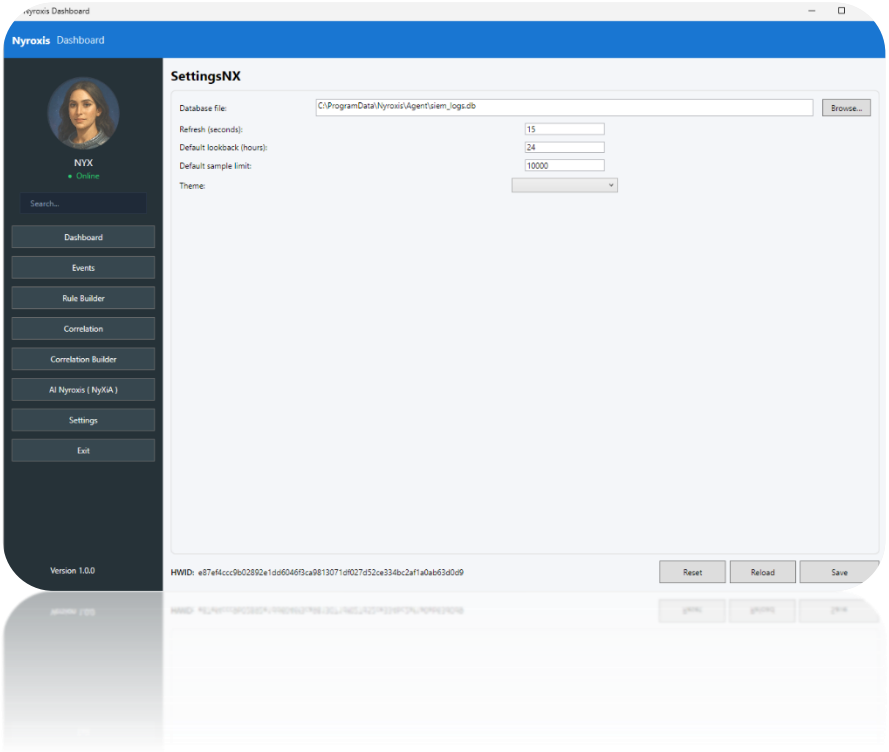
5. Rule Editing

Advanced rule editor supporting conditions, thresholds, and versioning.



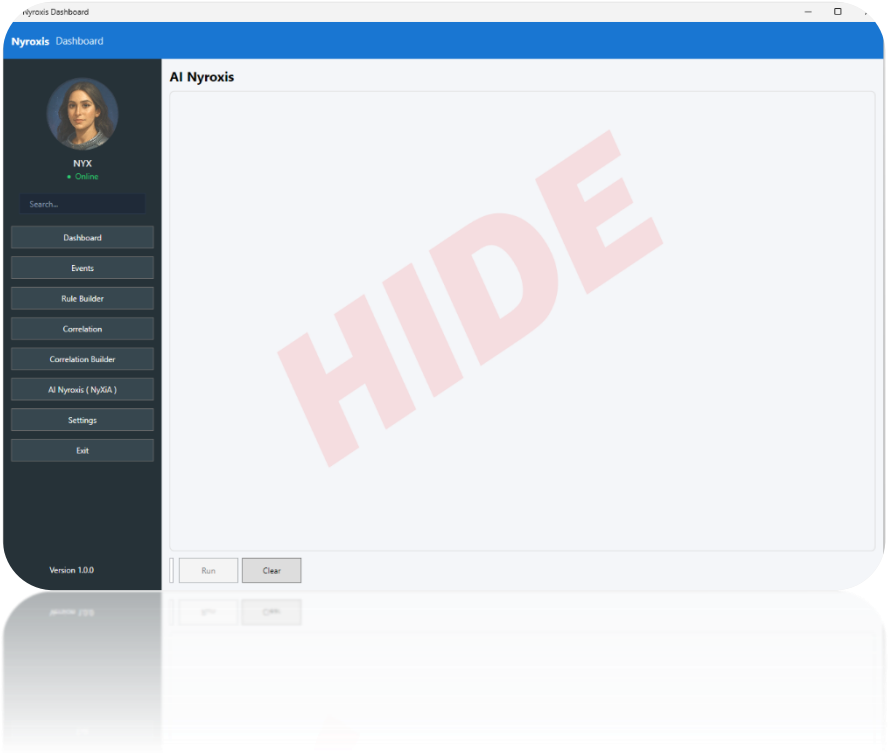
6. Settings

Configuration of database paths, refresh intervals, and lookback options.



7. AI Nyroxis Module (NyxIA)

Reserved for AI-driven analytics and anomaly detection, enabling future integration.



Summary

The dashboard demonstrates that **Nyroxis is not just a concept but a fully functional product**. Its interface has been built to provide **clarity for executives** and **precision for SOC analysts**, making it suitable for both technical experts and non-technical users.

- **For security professionals**, it offers advanced event search, live correlation, and rule customization, enabling detailed investigations and rapid incident response.
- **For non-technical users**, Nyroxis provides pre-configured, ready-to-use JSON rule sets. With a single click, these rules can be loaded and applied, eliminating the need for complex configuration. This ensures that even individuals with limited technical knowledge can benefit from enterprise-grade protection without effort.
- **For organizations**, the system bridges the gap between technical monitoring and executive oversight, turning raw event data into actionable insights while remaining lightweight and scalable.

In essence, the Nyroxis dashboard transforms raw telemetry into **clear, actionable intelligence**. It proves that Nyroxis is not only a vision but a **ready-to-deploy solution** designed to close the most overlooked security gaps — from complex SOC operations down to the simplest end-user experience.

Nyroxis Agent – Core Security Service

The Heart of Nyroxis

While the dashboard provides visibility and control, the foundation of Nyroxis is its **Agent** — a lightweight background service that continuously monitors, records, and protects endpoint activity where traditional solutions fail.

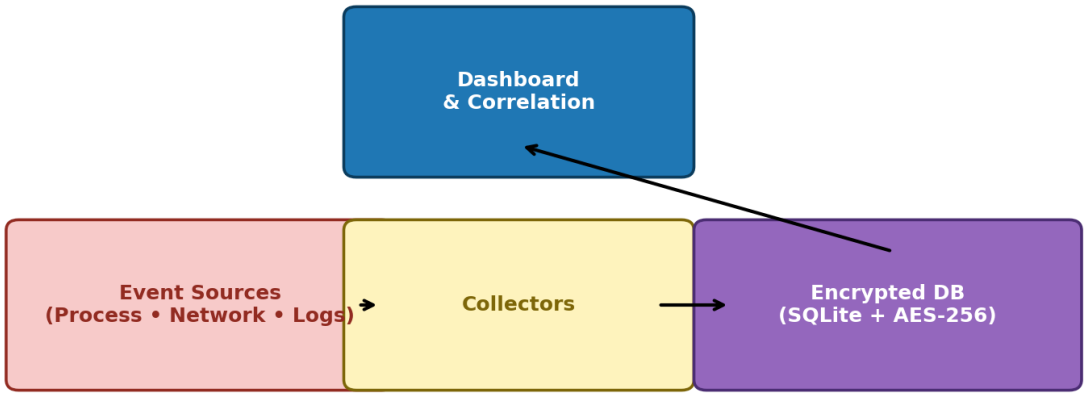
Key Capabilities

- **Event Collection:** Observes processes, services, network activity, scripts, and system events in real time.
- **Encrypted Storage:** All telemetry is written into a tamper-resistant local database (SQLite, AES-256 encryption).
- **Offline Operation:** Works reliably even without network connectivity, ensuring no loss of evidence.
- **License & Security Layer:** Each deployment is bound to the hardware (HWID) and validated with cryptographic signatures (Ed25519, SHA-256).
- **Stealth & Efficiency:** Runs silently as a Windows service with minimal CPU and memory usage, invisible to attackers and transparent for users.

Architectural Role

1. **Collection Layer** → Gathers raw data from the operating system.
2. **Normalization Layer** → Enriches and standardizes events for correlation.
3. **Protection Layer** → Encrypts and secures logs against tampering.
4. **Integration Layer** → Feeds data into the Nyroxis Dashboard and Correlation Engine.

Nyroxis Agent Flow



Nyroxis Agent Flow: Sources → Collectors → Encrypted DB → Dashboard & Correlation

Why It Matters

The Agent ensures that:

- No activity on critical endpoints goes unnoticed.
- Evidence is preserved in a format suitable for forensic and legal use.
- Security coverage extends beyond the corporate perimeter into the personal and unmanaged environments attackers exploit.

Summary

The Nyroxis Agent represents the **core of trust and resilience** within the entire platform. Unlike traditional collectors or antivirus services, it is engineered to provide **continuous, verifiable, and tamper-resistant security** on devices that were previously outside the scope of enterprise defenses.

- For **security teams**, the Agent guarantees a reliable data stream that feeds correlation engines and dashboards with high-quality, normalized events. This means faster investigations, stronger incident response, and court-admissible forensic material.
- For **organizations**, it extends the perimeter of defense beyond the office, transforming unmanaged personal endpoints into **controlled security nodes** without requiring complex deployment or maintenance.
- For **end-users**, it delivers seamless protection: the Agent runs silently in the background, does not interfere with daily tasks, and ensures that their devices remain under constant, invisible watch.

By combining **offline capability**, **cryptographic validation**, and **low-footprint operation**, the Nyroxis Agent closes one of the most critical gaps in modern cybersecurity. It ensures that **no event is lost, no evidence is altered, and no compromise goes unnoticed**.

In essence, the Nyroxis Agent is not just another endpoint service — it is the **strategic anchor of the Nyroxis ecosystem**, turning vulnerable personal environments into secure extensions of the organizational defense fabric.