NYROXIS®

Whitepaper — Cybersicherheitslösung

Nyroxis Security

www.nyroxis.com | contact@nyroxis.com

Nizza, Frankreich

Version 1.0 DE — Januar 2026

Inhaltsverzeichnis

1. Zusammenfassung

Die neue Realität der Cybersicherheit

Trotz Milliarden an Investitionen in Unternehmens-Firewalls, SOC-Betrieb und fortschrittliche SIEM-Plattformen gelingen Cyberangriffe weiterhin. Der Grund ist einfach: Angreifer zielen nicht mehr auf die gesicherte Haustür — sie dringen durch die Hintetrttür ein, über die persönlichen Geräte von Führungskräften, Administratoren, Richtern und Fachleuten, deren Entscheidungen echtes Gewicht haben.

Die Nyroxis-Philosophie

Cybersicherheit muss im Zuhause von Entscheidungsträgern beginnen — nicht in Unternehmenshauptsitzen.

Die ausgefeilteste Unternehmensinfrastruktur nützt wenig, wenn der persönliche Laptop eines CEO oder das Heimnetzwerk eines leitenden Administrators unbeaufsichtigt und exponiert bleibt.

Die Lösung

Nyroxis bietet eine leichtgewichtige, offline-fähige Sicherheitsplattform, die SOC-grade Überwachung auf persönliche Endgeräte bringt. Sie kombiniert vier Kernkomponenten — Nyroxis Agent, Nyroxis Intelligence, Nyroxis System Guardian und das Dashboard — mit einer vollständig lokalen KI/ML-Engine und gewährleistet, dass keine Daten das Gerät des Benutzers jemals verlassen.

Wichtigste Highlights

- Echtzeit-Erkennung über 27 Erkennungsregeln, 12 Korrelationsregeln und 2 Kettenregeln
- Vollständig lokales Machine Learning — keine Cloud, keine Datenübertragung
- Forensisch-grade verschlüsselter Speicher (AES-256)
- HWID-basierte Lizenzierung mit kryptografischer Validierung
- Konform mit DSGVO, NIS2 und ISO/IEC 27001
- Verfügbar in Englisch, Französisch und Deutsch
- Windows (v1.0) — macOS & Linux bald verfügbar
- Ein Monat kostenlose Testversion

2. Einleitung & Kontext

Cybersicherheit an einem Wendepunkt

Jede Woche bringt neue Schlagzeilen — Ransomware-Kampagnen, Datenschutzverletzungen, Angriffe von Nationalstaaten. Doch das Muster ist immer dasselbe: Organisationen investieren stark in Unternehmensabwehr, und Angreifer umgehen diese einfach. Die Frage ist nicht mehr ob eine Verletzung auftreten wird, sondern wo sie beginnen wird.

Der verborgene Einstiegspunkt

Die Antwort lautet zunehmend: zu Hause.

Der persönliche Laptop eines CEO. Ein Familien-Tablet, das dasselbe WLAN wie ein leitender Administrator teilt. Die spätnächtliche Browsing-Sitzung eines Richters oder Anwalts. Diese Geräte existieren außerhalb der Unternehmenssicherheitsperimeter — unüberwacht, ungeschützt und für Unternehmens-SIEM-Plattformen unsichtbar. Angreifer wissen das. Sie nutzen es gezielt aus.

Warum bestehende Tools unzureichend sind

Herkömmliche Antivirensoftware und Unternehmens-EDR-Lösungen wurden für kontrollierte Büroumgebungen konzipiert. Sie haben keine Sichtbarkeit auf persönliche Geräte, keine Möglichkeit, Aktivitäten außerhalb des Unternehmensnetzwerks zu überwachen, und keinen Mechanismus zur Aufbewahrung forensischer Beweise auf nicht verwalteten Endgeräten. Dies schafft einen strukturellen blinden Fleck.

Die menschliche Dimension

Hinter jeder Verletzungsstatistik steht ein echter Mensch: eine Führungskraft, deren strategische Kommunikation kompromittiert wird, ein öffentlicher Bediensteter, dessen Glaubwürdigkeit untergraben wird, eine Familie, deren Privatsphäre verletzt wird. Cybersicherheit geht nicht nur um den Schutz von Daten — es geht darum, die Menschen zu schützen, die kritische Entscheidungen treffen.

Unsere Antwort

Nyroxis wurde speziell für diese Realität entwickelt. Durch die Erweiterung der SOC-grade Überwachung auf persönliche Endgeräte — still laufend, offline arbeitend, alles lokal speichernd — schließt es die Lücke, die Unternehmenstools nicht erreichen können.

3. Problembeschreibung

Die Lücke, die niemand schließt

Unternehmens-Cybersicherheit war noch nie so stark. Firewalls, Intrusion-Detection-Systeme, SIEM-Plattformen und dedizierte SOC-Teams repräsentieren enorme Investitionen in den Schutz. Dennoch gehen Verletzungen weiter — nicht weil Unternehmensabwehr versagt hat, sondern weil Angreifer woanders hingewandert sind.

Sie sind in das persönliche digitale Leben der Menschen innerhalb dieser Unternehmen gewandert.

Der strukturelle blinde Fleck

Heimnetzwerke werden nicht überwacht. Persönliche Laptops sind nicht in Unternehmens-EDR-Systeme eingeschrieben. Familiengeräte teilen WLAN mit sensiblen professionellen Kommunikationen. Diese Umgebungen befinden sich vollständig außerhalb des Geltungsbereichs von Unternehmenssicherheitsrichtlinien — und vollständig in Reichweite von ausgeklügelten Angreifern.

Ein einziges kompromittiertes persönliches Gerät kann zum stillen Einstiegspunkt in kritische Infrastruktur, Führungskommunikation oder sensible Gerichtsverfahren werden.

Wer ist gefährdet

- **Führungskräfte & leitende Manager** — deren strategische Entscheidungen und Kommunikationen finanzielles und reputationsbezogenes Gewicht haben
- **Öffentliche Bedienstete & Rechtsfachleute** — Richter, Anwälte, Polizeibeamte, deren persönliche Kompromittierung die Integrität von Institutionen beeinträchtigen kann
- **SOC-Administratoren & IT-Leiter** — deren persönliche Anmeldedaten, wenn gestohlen, Unternehmensinfrastruktur direkt entsperren können
- **Ihre Familien** — die Netzwerke und Geräte teilen, oft ohne jegliches Sicherheitsbewusstsein

Die Kosten der Unterlassung

- Finanzielle Verluste durch Verletzungen, die außerhalb des Unternehmensperimeters entstehen
- Reputationsschäden, wenn Führungskräfte oder öffentliche Personen kompromittiert werden
- Regulatorische Exposition unter DSGVO, NIS2 und verwandten Rahmenwerken
- Persönlicher Schaden — Erpressung, Datenschutzverletzungen, Manipulation — gegen Personen in kritischen Rollen

Das Kernproblem

Es gibt keine leichtgewichtige, datenschutzfreundliche, offline-fähige Lösung, die speziell zum Schutz persönlicher Endgeräte von hochrangigen Personen entwickelt wurde. Unternehmenstools sind zu schwer, zu aufdringlich und zu abhängig von Unternehmensinfrastruktur. Consumer-Antivirus ist zu oberflächlich.

Nyroxis existiert, um diese Lücke zu schließen.

4. Unsere Lösung – Nyroxis

Eine andere Art von Sicherheit

Nyroxis ist kein weiteres Unternehmenstool, das für den persönlichen Gebrauch verkleinert wurde. Es wurde von Grund auf mit einem einzigen Zweck entwickelt: SOC-grade Schutz auf persönliche Endgeräte von hochrangigen Personen zu bringen — still, lokal und ohne Kompromisse.

Die Grundphilosophie

Wo herkömmliche Cybersicherheit an der Bürotür aufhört, beginnt Nyroxis. Es operiert auf der Überzeugung, dass die kritischste Sicherheitslücke nicht technischer — sondern geografischer Natur ist. Das persönliche Gerät eines Entscheidungsträgers ist strategisch genauso wertvoll wie jeder Unternehmensserver.

Wie Nyroxis funktioniert

Die Plattform ist um vier Kernkomponenten aufgebaut, die zusammenarbeiten:

Nyroxis Agent

Sammelt kontinuierlich Protokolle aus mehreren Systemkanälen — Prozesse, Netzwerkaktivität, Dienste, Skripte und Systemereignisse. Er normalisiert diese Daten in Echtzeit, verschlüsselt die Nutzlast und speichert alles in einer lokalen verschlüsselten Datenbank. Nichts verlässt das Gerät.

Nyroxis Intelligence

Wendet eine intelligente Regel-Engine über drei Erkennungsschichten an: Erkennung (27 Regeln zur Identifizierung bekannter Bedrohungsmuster), Korrelation (12 Regeln zur Verknüpfung verwandter Ereignisse über Zeit und Quellen) und Kette (2 Regeln zur Erkennung mehrstufiger Angriffssequenzen). Die Regel-Engine ist für Sicherheitsexperten erweiterbar.

Nyroxis System Guardian

Läuft still in der Windows-Systemleiste und fungiert als Wächter der Plattform. Er überwacht alle 3 Sekunden den Betriebsstatus aller Dienste, verwaltet Datenbank-Backups, validiert die Lizenz in Echtzeit, prüft auf Updates und stoppt automatisch Dienste, wenn die Lizenz abläuft.

Nyroxis Dashboard

Eine klare, intuitive Oberfläche für Sicherheitsexperten und nicht-technische Benutzer. Sie bietet Echtzeit-Sichtbarkeit über Ereignisse, Erkennungen, Korrelationen und Ketten, mit integrierter Berichterstattung, forensischer Suche und KI/ML-Analyse-Engine — alles lokal ausgeführt.

Was Nyroxis unterscheidet

- Vollständig offline-fähig — keine Abhängigkeit von Cloud-Infrastruktur, keine Datenübertragung
- Forensisch-grade Speicher — AES-256-verschlüsselt, manipulationssicher, gerichtsverwertbar
- Leichtgewichtig & still — minimaler Ressourcenverbrauch, für Angreifer unsichtbar
- Erweiterbar — Sicherheitsteams können benutzerdefinierte Erkennungsregeln erstellen und einsetzen
- Mehrsprachig — Oberfläche auf Englisch, Französisch und Deutsch
- Privacy by Design — persönliche Daten verlassen nie das Gerät

Nyroxis ist die fehlende Schicht — der Schutz, der dort beginnt, wo Unternehmenssicherheit endet.

5. Architektur & Technologie

Übersicht

Nyroxis ist als modulare, leichtgewichtige Sicherheitsplattform aufgebaut, die Endgeräteüberwachung, Echtzeit-Erkennung und lokale KI-Analyse kombiniert. Die Architektur basiert auf drei Prinzipien: Einfachheit der Bereitstellung, Integrität der Beweise und absolute Datenlokalität.

Kernkomponenten

Komponente	Rolle	Schlüsseltechnologie
Nyroxis Agent	Protokollsammlung, Normalisierung, verschlüsselter Speicher	Rust, SQLite, AES-256
Nyroxis Intelligence	Erkennung, Korrelation, Regel-Engine	Rust, JSON-Regel-Engine
Nyroxis System Guardian	Überwachung, Backup, Lizenz, Updates	Rust, Systemleiste
Nyroxis Dashboard	UI, Forensik, KI/ML, Berichterstattung	Tauri + WebView

Erkennungsschichten

Schicht	Regeln	Zweck
nyroxis_detection	27	Bekannte Bedrohungsmuster in einzelnen Ereignissen identifizieren
nyroxis_correlations	12	Verwandte verdächtige Ereignisse über Zeit und Quellen verknüpfen
nyroxis_chains	2	Mehrstufige Angriffssequenzen erkennen

Technologie-Stack

Komponente	Technologie
Kerndienste	Rust
Dashboard	Tauri + WebView
Lokale Datenbank	SQLite
Verschlüsselung	AES-256 (Protokolle), Ed25519 (Signaturen), SHA-256 (Hashing)

Komponente	Technologie
ML-Engine	Isolation Forest — reines Rust, keine externe ML-Bibliothek
Statistische Analyse	Z-Score, IQR, Gleitender Durchschnitt — lokale Berechnung
Plattform	Windows (v1.0) — macOS & Linux: Bald verfügbar

Designprinzipien

- **Datenlokalität** — alle Verarbeitung, Speicherung und Analyse erfolgt auf dem Gerät des Benutzers. Keine Cloud, keine Telemetrie, keine externe Übertragung
- **Forensische Integrität** — verschlüsselte, manipulationssichere Protokolle geeignet für rechtliche und regulatorische Verfahren
- **Diskretion** — für Angreifer unsichtbar, für Benutzer nicht intrusiv
- **Erweiterbarkeit** — Regel-Engine für Expertenanpassung ohne Systemmodifikation konzipiert
- **Komplementärität** — arbeitet neben bestehenden AV-, EDR- und SIEM-Investitionen

6. Kernkomponenten

Nyroxis Agent — Die Sammel-Engine

Nyroxis Agent ist das Fundament der gesamten Plattform. Als stiller Windows-Dienst betrieben, arbeitet er kontinuierlich im Hintergrund und nimmt sicherheitsrelevante Daten aus mehreren Systemkanälen gleichzeitig auf:

- Windows-Ereignisprotokolle (Sicherheit, System, Anwendung)
- Netzwerkverbindungen und Datenverkehr-Metadaten
- Laufende Prozesse und Dienstaktivität
- PowerShell- und Skriptausführung
- Änderungen am Dateisystem und der Registrierung

Jedes gesammelte Ereignis durchläuft eine Normalisierungspipeline, die Format standardisiert und Kontext anreichert. Die normalisierte Nutzlast wird dann mit AES-256 verschlüsselt und in eine lokale SQLite-Datenbank geschrieben — auf dem Gerät des Benutzers, unter seiner Kontrolle.

Ressourcenverbrauch: ca. 57 MB RAM, 0,1% CPU — geeignet für den kontinuierlichen Betrieb auf persönlichen Laptops ohne Beeinträchtigung der Produktivität.

Nyroxis Intelligence — Die Erkennungs-Engine

Nyroxis Intelligence ist der analytische Kern der Plattform. Es arbeitet mit hoher Geschwindigkeit über drei sequentielle Erkennungsschichten:

Schicht 1 — Erkennung (27 Regeln)

Identifiziert bekannte Bedrohungsmuster innerhalb einzelner Ereignisse: verdächtige Prozessausführung, nicht autorisierte Dienstinstallation, abnormales Netzwerkverhalten, Anmeldedaten-Zugriffsversuche und mehr.

Schicht 2 — Korrelation (12 Regeln)

Verknüpft verwandte Ereignisse über Zeit und Quellen, um Bedrohungsmuster zu identifizieren, die kein einzelnes Ereignis allein offenbaren würde. Eine fehlgeschlagene Anmeldung gefolgt von einer erfolgreichen von einem anderen Ort. Ein neuer Prozess, der unmittelbar nach dem Anschließen eines USB-Geräts startet.

Schicht 3 — Kette (2 Regeln)

Erkennt mehrstufige Angriffssequenzen — die Art koordinierter, progressiver Eindringung, die fortgeschrittene anhaltende Bedrohungen charakterisiert.

Erweiterbar von Anbeginn

Sicherheitsexperten können neue Erkennungs-, Korrelations- oder Kettenregeln erstellen und direkt in das System einsetzen, ohne Kernkomponenten zu modifizieren. Regeln folgen einem strukturierten JSON-basierten Format.

Ressourcenverbrauch: ca. 87 MB RAM, 1,8% CPU.

Nyroxis System Guardian — Der Plattform-Wächter

Nyroxis System Guardian läuft still als Systemleisten-Anwendung (6,5 MB RAM, 0,1% CPU) und bietet kontinuierliche Aufsicht über die gesamte Plattform:

Dienstüberwachung

Alle 3 Sekunden überprüft System Guardian, ob Nyroxis Agent und Nyroxis Intelligence laufen. Wenn ein Dienst unerwartet stoppt, erkennt Guardian die Störung sofort.

Lizenzvalidierung

Guardian überwacht kontinuierlich das HWID-basierte Lizenzrahmenwerk. Wenn eine Lizenz abläuft oder ungültig wird, stoppt Guardian automatisch beide Dienste. Die Validierung erfolgt vollständig offline über AES-GCM-Verschlüsselung und HMAC-Verifizierung.

Backup-Verwaltung

Alle Nyroxis-Datenbanken sind kritische forensische Vermögenswerte. Guardian verwaltet geplante und bedarfsgesteuerte Backups und überwacht Dateigröße, Zeitstempel und Integrität.

Update-Prüfung

Guardian prüft automatisch in konfigurierbaren Intervallen auf neue Versionen und benachrichtigt Benutzer, wenn Updates verfügbar sind. Kritische Updates werden sofort markiert.

Zusammen bilden diese vier Komponenten ein selbständiges, widerstandsfähiges Sicherheitsgefüge — das sich selbst überwacht, erkennt und schützt, sodass der Benutzer dies nie tun muss.

7. Künstliche Intelligenz & Machine Learning

Ein anderer Ansatz zur KI

Die meisten KI-gestützten Sicherheitslösungen verlassen sich auf Cloud-Infrastruktur. Nyroxis verfolgt den entgegengesetzten Ansatz. Jeder Aspekt der Nyroxis KI-Engine läuft lokal auf dem Gerät des Benutzers. Es werden keine Daten übertragen. Kein Verhaltensprofile verlässt jemals die Maschine.

Isolation Forest — Anomalieerkennung

Im Kern der Nyroxis ML-Engine befindet sich eine benutzerdefinierte Implementierung des Isolation-Forest-Algorithmus, vollständig in Rust ohne Abhängigkeit von einer externen Machine-Learning-Bibliothek erstellt.

Isolation Forest arbeitet durch den Aufbau eines Waldes aus zufälligen Entscheidungsbäumen. Anomale Ereignisse — solche, die statistisch selten oder strukturell ungewöhnlich sind — benötigen weniger Splits zur Isolierung und erhalten daher einen höheren Anomalie-Score.

Die Nyroxis-Implementierung arbeitet mit 100 Isolationsbäumen pro Zyklus, maximal 256 Stichproben pro Baum und 8 Verhaltensmerkmalen pro Analysefenster:

Merkmal	Beschreibung
Ereignisanzahl	Gesamtereignisse im Analysefenster
Eindeutige Quellen	Anzahl der unterschiedlichen Ereignisquellen
Eindeutige Ziele	Anzahl der unterschiedlichen Netzwerkziele
Tageszeit	Zeitlicher Kontext für die Verhaltensbasis
Wochentag	Wöchentliche Mustererkennung
Ereignisse pro Stunde	Aktivitätsraten-Normalisierung
Neue-Quellen-Verhältnis	Anteil zuvor ungesehener Quellen
Neue-Ziele-Verhältnis	Anteil zuvor ungesehener Ziele

Statistische Analyse-Engine

Z-Score-Klassifikation

Z-Score	Schweregrad	Konfidenz
> 3,0	Kritisch	99,7%
> 2,0	Hoch	95%
> 1,5	Mittel	86%

Z-Score	Schweregrad	Konfidenz
> 1,0	Niedrig	68%

Zusätzliche statistische Methoden

- **IQR-Ausreißererkennung** — identifiziert Werte außerhalb des Interquartilbereichs
- **Gleitender Durchschnitt** — verfolgt Verhaltenstrends über konfigurierbare Zeitfenster
- **Exponentieller gleitender Durchschnitt** — gewichtet aktuelle Aktivität stärker für schnellere Reaktion
- **Spitzenerkennung** — markiert plötzliche Abweichungen von historischen Normen
- **Korrelationsanalyse** — misst statistische Beziehungen zwischen unabhängigen Verhaltenssignalen

Warum lokales ML wichtig ist

Für die Personen, die Nyroxis schützt — Führungskräfte, Rechtsfachleute, öffentliche Bedienstete — ist die Sensibilität ihrer Verhaltensdaten selbst ein Sicherheitsanliegen. Eine lokale ML-Engine eliminiert dieses Risiko vollständig und liefert die analytische Tiefe von cloud-basierter Verhaltensintelligenz ohne den Datenschutzkompromiss.

8. Anwendungsfälle & Szenarien

Wo Nyroxis echte Wirkung erzielt

Nyroxis wurde für Umgebungen entwickelt, in die herkömmliche Sicherheitstools nicht vordringen können. Die folgenden Szenarien veranschaulichen die realen Kontexte, in denen die Plattform sofortigen und messbaren Wert schafft.

Szenario 1 — Die Führungskraft zu Hause

Ein CFO arbeitet drei Tage pro Woche von zu Hause. Sein persönlicher Laptop wurde nie in das EDR-System des Unternehmens eingeschrieben. Eines Abends installiert eine Phishing-E-Mail eine stille Hintetrttür. Die Unternehmens-Firewall sieht sie nie.

Mit installiertem Nyroxis erfasst Nyroxis Agent die anomale Prozessausführung in dem Moment, in dem sie auftritt. Nyroxis Intelligence korreliert sie mit einem verdächtigen ausgehenden Verbindungsversuch Minuten später. Eine Warnung wird ausgegeben, bevor Daten das Gerät verlassen.

Szenario 2 — Der Rechtsfachmann

Ein leitender Richter verwendet einen persönlichen Laptop zur Überprüfung von Falldokumenten außerhalb des Gerichtsgebäudes. Ein Angreifer injiziert über einen kompromittierten Router bösartige Skripte in Browser-Sitzungen.

Nyroxis erkennt das anomale Skript-Ausführungsmuster und markiert das ungewöhnliche Netzwerkverhalten durch Korrelation. Der Richter wird gewarnt. Der Versuch wird mit forensisch-grade Beweisen dokumentiert.

Szenario 3 — Der SOC-Administrator

Ein SOC-Teamleiter greift nachts von einem persönlichen Gerät aus remote auf interne Systeme zu. Angreifer zielen speziell auf dieses Gerät, wissend, dass seine Kompromittierung direkten Zugang zur Unternehmensumgebung verschaffen könnte.

Nyroxis überwacht das Gerät kontinuierlich, erkennt Anmeldedaten-Zugriffsversuche über seine Kettenerkennung und gibt eine kritische Warnung aus. Der Unternehmensperimeter wird nie erreicht.

Szenario 4 — Die multinationale Organisation

Ein Konzern mit Operationen in mehreren Ländern steht vor einer inkonsistenten Sicherheitslandschaft für persönliche Geräte. Nyroxis bietet eine einheitliche Schutzschicht, die unabhängig von der Geografie auf allen Endgeräten eingesetzt werden kann, wobei jede Installation unabhängig ohne zentralisierte Infrastruktur betrieben wird.

Szenario 5 — Die sicherheitsbewusste Organisation

Ein fortschrittliches Unternehmen setzt Nyroxis als Teil eines umfassenderen internen Sicherheitssensibilisierungs- und Überwachungsprogramms ein. Die erweiterbare Regel-Engine ermöglicht es dem Sicherheitsteam, benutzerdefinierte Erkennungsregeln zu verfassen, die auf ihr spezifisches Bedrohungsmodell zugeschnitten sind.

9. Vorteile & Wertversprechen

Sicherheit, die strategischen Wert schafft

Cybersicherheit ist nicht nur eine technische Disziplin — es ist eine Frage der Geschäftskontinuität, des institutionellen Vertrauens und der persönlichen Sicherheit. Nyroxis liefert Mehrwert auf jeder Ebene der Organisation.

Für Sicherheitsverantwortliche — CISO & SOC-Teams

- **Sichtbarkeit, wo sie nicht existierte** — erweitert die Überwachung auf persönliche Endgeräte, die Unternehmenstools nicht abdecken
- **Forensisch-grade Beweise** — verschlüsselte, zeitgestempelte, manipulationssichere Protokolle beschleunigen die Reaktion und unterstützen rechtliche Verfahren
- **Nahtlose Integration** — ergänzt bestehende AV-, EDR- und SIEM-Einsätze ohne Komplexität hinzuzufügen
- **Erweiterbare Erkennung** — Teams können benutzerdefinierte Regeln erstellen und einsetzen, die auf ihre Umgebung zugeschnitten sind

Für die Geschäftsleitung — CEO & Vorstand

- **Schutz immaterieller Vermögenswerte** — schützt Markenreputation, Anlegervertrauen und strategische Entscheidungskapazität
- **Nachgewiesene Sorgfaltspflicht** — liefert dokumentierte, nachprüfbare Beweise für aktives Risikomanagement für Regulatoren
- **Reduzierte Verletzungskosten** — erkennt Bedrohungen am persönlichen Endgerät, bevor sie die Unternehmensinfrastruktur erreichen

Für die geschützte Person — Führungskraft, Fachmann, Bediensteter

- **Stiller, nahtloser Schutz** — läuft unsichtbar im Hintergrund, kein technisches Fachwissen erforderlich
- **Absolute Privatsphäre** — keine Verhaltensdaten werden jemals außerhalb des Geräts übertragen
- **Seelenfrieden** — Vertrauen, dass persönliche Geräte und Familienumgebungen überwacht und geschützt sind

Der strategische Vorteil

Dimension	Ohne Nyroxis	Mit Nyroxis
Sichtbarkeit pers. Endgerät	Keine	Vollständig, Echtzeit
Bedrohungserkennung zu Hause	Keine	27+12+2 Regelschichten
Forensische Beweise	Nicht verfügbar	Verschlüsselt, gerichtsverwertbar
KI-Anomalieerkennung	Keine	Lokaler Isolation Forest
Datenschutz	Gefährdet	Garantiert — vollständig lokal
Compliance-Haltung	Unvollständig	DSGVO, NIS2, ISO 27001 konform
Benutzerstörung	N/A	Null

10. Compliance & Standards

Sicherheit, die Regulatoren überzeugt

Im heutigen regulatorischen Umfeld wird Cybersicherheit durch nachweisbare Rechenschaftspflicht bewertet. Organisationen müssen nachweisen, dass sie Risiken aktiv über ihr gesamtes digitales Ökosystem verwalten, einschließlich persönlicher Endgeräte des Schlüsselpersonals. Nyroxis wurde mit dieser Anforderung als Kern entwickelt.

Europäische Rahmenwerke

DSGVO — Datenschutz-Grundverordnung

Nyroxis ist um Datenminimierung und Privacy by Design aufgebaut. Alle gesammelten Telemetrie wird im Ruhezustand mit AES-256 verschlüsselt. Es werden keine persönlichen Daten extern übertragen. Der Benutzer behält jederzeit vollständige Souveränität über seine eigenen Daten.

NIS2-Richtlinie

NIS2 verlangt von Organisationen, kontinuierliche Überwachungskapazität, Incident-Bereitschaft und aktives Risikomanagement nachzuweisen. Nyroxis erweitert diese Fähigkeit auf persönliche Endgeräte — genau die Umgebungen, die am wahrscheinlichsten angegriffen werden.

ENISA-Leitlinien

Nyroxis richtet sich nach den besten Praktiken der Agentur der Europäischen Union für Cybersicherheit für Endgeräte-Resilienz, Verhaltensüberwachung und Incident-Dokumentation.

Internationale Standards

ISO/IEC 27001

Nyroxis unterstützt die Ausrichtung an der globalen Benchmark für Informationssicherheits-Managementsysteme. Seine forensisch-grade Protokollierung und strukturiertes Erkennungsrahmenwerk erweitern die ISMS-Abdeckung auf persönliche Endgeräte.

Forensische Bereitschaft

Jedes von Nyroxis erfasste Ereignis wird verschlüsselt, zeitgestempelt und in einer manipulationssicheren lokalen Datenbank gespeichert — was forensische Bereitschaftsanforderungen in allen Rechtsordnungen erfüllt.

NIST Cybersicherheits-Framework

NIST-Funktion	Nyroxis-Beitrag
Identifizieren	Kontinuierliche Sichtbarkeit auf persönliche Endgeräteaktivität und Asset-Verhalten
Schützen	Verschlüsselter Speicher, HWID-basierte Lizenzierung, manipulationssichere Architektur
Erkennen	27 Erkennungsregeln, 12 Korrelationsregeln, 2 Kettenregeln, lokale ML-Anomalieerkennung
Reagieren	Echtzeit-Warnungen, forensische Beweise, erweiterbare Regel-Engine

Compliance-Übersicht

Rahmenwerk	Nyroxis-Ausrichtung
DSGVO	Privacy by Design, Datenminimierung, ausschließlich lokaler Speicher
NIS2	Kontinuierliche Überwachung, Incident-Bereitschaft, Abdeckung persönlicher Endgeräte
ENISA-Leitlinien	Endgeräte-Resilienz, Verhaltensüberwachung, Incident-Dokumentation
ISO/IEC 27001	Forensische Protokollierung, strukturierte Erkennung, ISMS-Erweiterung
NIST CSF	Funktionen Identifizieren, Schützen, Erkennen, Reagieren abgedeckt
Zero Trust	Kontinuierliche Verifizierung auf Ebene des persönlichen Endgeräts

11. Fahrplan

Von der Grundlage zum vollständigen Ökosystem

Nyroxis 1.0 repräsentiert eine vollständig funktionale, produktionsreife Plattform. Der Fahrplan erweitert das, was bereits funktioniert, in neue Umgebungen, neue Fähigkeiten und neue Gemeinschaften.

Aktuell — Version 1.0 (Jetzt verfügbar)

- Nyroxis Agent — Multi-Kanal-Protokollsammlung, Normalisierung, AES-256-verschlüsselter lokaler Speicher
- Nyroxis Intelligence — Drei-Schichten-Erkennungs-Engine (27 Erkennung, 12 Korrelation, 2 Kette)
- Nyroxis System Guardian — Dienstüberwachung, Backup-Verwaltung, Lizenzvalidierung, Update-Prüfung
- Nyroxis Dashboard — Echtzeit-Sichtbarkeit, forensische Suche, Erkennungsvisualisierung, Berichterstattung
- Lokale KI/ML-Engine — Isolation-Forest-Anomalieerkennung, statistische Analyse, vollständig offline
- Mehrsprachige Oberfläche — Englisch, Französisch, Deutsch
- Ein Monat kostenlose Testversion

Phase 2 — Plattformerweiterung

macOS & Linux-Unterstützung

Der Nyroxis-Agent und das Dashboard werden auf macOS- und Linux-Umgebungen ausgeweitet — und bringen dasselbe Schutzniveau auf die gesamte Bandbreite persönlicher Geräte.

Erweiterte Erkennungsbibliothek

Neue Erkennungs-, Korrelations- und Kettenregeln werden veröffentlicht, um aufkommende Bedrohungsmuster zu bewältigen, mit Beiträgen der Sicherheitsexperten-Gemeinschaft.

Verbesserte ML-Fähigkeiten

Die lokale KI-Engine wird mit zusätzlichen Verhaltensmodellen, längeren Basislinienfenstern und granularerer Merkmalsanalyse vertieft — ohne Cloud-Abhängigkeit einzuführen.

Phase 3 — Bildung & Gemeinschaft

Nyroxis Sicherheitsbildungsprogramm

Nyroxis wird eine strukturierte Sicherheitsbildungsinitiative starten, die mit Schulen beginnt — und die nächste Generation durch kurze, fokussierte und zugängliche Schulungsinhalte in praktisches Cybersicherheitsdenken einführt.

Gemeinschaft der Sicherheitsexperten

Die erweiterbare Regel-Engine schafft eine natürliche Grundlage für eine Praktiker-Gemeinschaft — einen strukturierten Kanal, über den Sicherheitsexperten beitragen, teilen und die kollektive Erkennungsfähigkeit der Plattform ausbauen können.

Phase 4 — Unternehmensintegration

Für Unternehmen, die den Nyroxis-Schutz auf ihre gesamte Führung und operative Mitarbeiter ausweiten möchten, wird ein strukturiertes organisatorisches Bereitstellungsmodell zentralisierte Aufsicht bieten, während die Datenlokalitätsgarantien erhalten bleiben.

Fahrplan-Übersicht

Phase	Schwerpunkt	Status
v1.0	Vollständige Windows-Plattform	✓ Jetzt verfügbar
Phase 2	macOS & Linux, erweitertes ML	In Entwicklung
Phase 3	Bildungsprogramm, Gemeinschaft	Start 2026
Phase 4	Unternehmensintegration, SOC/CSIRT	Geplant

12. Lizenzmodell

Einfach, transparent, datenschutzfreundlich

Das Nyroxis-Lizenzmodell spiegelt dieselben Prinzipien wie die Plattform selbst wider: Einfachheit, Integrität und Respekt für den Benutzer. Es gibt keine Abonnementfallen, keine versteckte Datenerfassung im Zusammenhang mit der Lizenzvalidierung und keine Abhängigkeit von externen Servern.

Wie die Lizenzierung funktioniert

Jede Nyroxis-Lizenz ist an die Hardware des Benutzers gebunden, über einen eindeutigen Bezeichner, der aus den physischen Merkmalen des Geräts (HWID) abgeleitet wird. Ein kryptografischer Schlüssel wird aus demselben Hardwareprofil generiert und erstellt eine Lizenz, die:

- **Nicht übertragbar** — an das spezifische Gerät gebunden, für das sie ausgegeben wurde
- **Manipulationssicher** — jede Änderung der Lizenz wird sofort von Nyroxis System Guardian erkannt
- **Vollständig offline** — die Validierung erfordert keine Internetverbindung, keinen externen Server

Testzeitraum

Jede neue Nyroxis-Installation enthält einen kostenlosen Monat Testversion — mit vollem Zugriff auf alle Plattformfunktionen ohne Einschränkungen. Es ist keine Kreditkarte erforderlich.

Lizenzstufen

Stufe	Zielgruppe	Funktionen
Testversion	Alle Benutzer	Vollständiger Plattformzugang — 1 Monat, keine Einschränkungen
Persönlich	Führungskräfte, Fachleute, Einzelpersonen	Vollständige Plattform, ein Gerät, HWID-gebunden
Professionell	Sicherheitspraktiker, Berater	Vollständige Plattform, Regelbereitstellung, Prioritäts-Support
Unternehmen	Organisationen, Holdings, Institutionen	Multi-Geräte-Bereitstellung, organisatorische Aufsicht, dedizierter Support

Immer enthalten

- Nyroxis Agent, Nyroxis Intelligence, Nyroxis System Guardian — vollständige Plattform
- Lokale KI/ML-Engine — vollständig offline, keine Cloud-Abhängigkeit
- Vollständige Erkennungs-, Korrelations- und Kettenregel-Bibliothek
- Mehrsprachiges Dashboard — Englisch, Französisch, Deutsch
- Forensisch-grade verschlüsselter lokaler Speicher
- Datenbank-Backup-Verwaltung
- Offline-Lizenzvalidierung

Niemals enthalten

- Keine Telemetrie an Nyroxis oder Dritte gesendet
- Keine Verhaltensdaten für Lizenzierungszwecke erfasst
- Keine Abhängigkeit von Internetkonnektivität für den Plattformbetrieb
- Keine versteckten Kosten im Zusammenhang mit Datenvolumen oder Ereignisanzahl

Kontakt

Nyroxis Security

www.nyroxis.com | contact@nyroxis.com

Nizza, Frankreich

13. Dashboard-Demonstration

Sichtbarkeit durch Design

Das Nyroxis-Dashboard ist die operative Schnittstelle der gesamten Plattform. Es wurde mit zwei Benutzern gleichzeitig im Sinn entwickelt: dem Sicherheitsexperten, der Präzision, Tiefe und forensische Fähigkeit benötigt — und dem nicht-technischen Führungskraft, die Klarheit, Einfachheit und sofortiges Situationsbewusstsein braucht.

1. Hauptübersicht

Der Einstiegspunkt des Dashboards bietet ein Bild der aktuellen Sicherheitslage: Gesamtereignisse in den letzten 24 Stunden, aktive Warnungen nach Schweregrad (Kritisch, Hoch, Warnung, Info), Echtzeit-Ereigniszeitlinie, Schweregrad-Verteilung und Systemstatus.

2. Ereignisansicht

Die Ereignisansicht ist der forensische Kern des Dashboards. Sie bietet vollständigen Zugriff auf die rohe Ereignisdatenbank mit vollständiger Such-, Filter- und Exportfähigkeit — einschließlich forensischer Inspektion einzelner Ereignisse und Export in CSV für rechtliche Dokumentation.

3. Erkennungsansicht

Die Erkennungsansicht präsentiert alle von der Nyroxis Intelligence Erkennungsregelschicht generierten Ergebnisse. Jedes Ergebnis enthält die ausgelöste Regel, die übereinstimmenden Ereignisse, die Schweregrad-Klassifikation und einen direkten Link zu den zugrunde liegenden rohen Ereignissen.

4. Korrelationsansicht

Die Korrelationsansicht zeigt Ergebnisse der 12-Regel-Korrelations-Engine — die Muster, die nicht aus einzelnen Ereignissen, sondern aus den Beziehungen zwischen ihnen entstehen. Hier werden isolierte Signale zu verwertbarer Intelligenz.

5. Kettenansicht

Die Kettenansicht präsentiert Ergebnisse der anspruchsvollsten Erkennungsschicht — die Erkennung mehrstufiger Angriffssequenzen. Kettenergebnisse repräsentieren die höchstprioritären Warnungen im System.

6. Berichte

Der Berichtsbereich bietet strukturierte, exportierbare Dokumentation der Plattformaktivität und Ergebnisse. Berichte können über konfigurierbare Zeitfenster generiert und in PDF oder CSV exportiert werden — geeignet für interne Überprüfung, regulatorische Einreichung oder rechtliche Verfahren.

7. KI / ML-Analyse

Das KI-Modul bietet Zugriff auf die lokale Machine-Learning-Engine. Analysten können Anomalieerkennung-Ergebnisse mit Merkmalszerlegung überprüfen, Z-Score-Klassifikationen inspizieren und statistische Ausreißer identifizieren. Alle Analysen werden lokal durchgeführt.

8. Einstellungen

Die Einstellungsansicht bietet vollständige Plattformkonfiguration: Datenbankdateipfad, Dashboard-Aktualisierungsintervall, Standard-Rückblickfenster, Standard-Stichprobenlimit, Oberflächensprachauswahl (Englisch, Französisch, Deutsch) und Designkonfiguration.

9. Backup

Der Backup-Bereich bietet direkte Verwaltung von Datenbank-Backup-Operationen — Planung, bedarfsgesteuerte Ausführung und Backup-Verlauf. Alle Backup-Dateien sind verschlüsselt und lokal gespeichert.

Für jeden konzipiert

Das Nyroxis-Dashboard bittet seine Benutzer nicht, zwischen Leistung und Einfachheit zu wählen. Sicherheitsexperten haben die Tiefe, die sie benötigen. Nicht-technische Benutzer haben die Klarheit, die sie brauchen.

Dies ist das Nyroxis-Designprinzip sichtbar gemacht: Unternehmens-grade Schutz, zugänglich für jeden, den es schützt.