orcharhino | LinuxGuard
Visibility. Confidence. Control.

JOINT WEBINAR 7 JULY 2026

LINUX LIFECYCLE × IDENTITY SECURITY × SOVEREIGNTY

Zero Blind Spots.

Linux lifecycle automation, identity security & digital sovereignty for European enterprises.

See how orcharhino & LinuxGuard work together to deliver compliance-ready, sovereign Linux infrastructure — simply and at scale.

- **Dr. Jonas Trüstedt**
  Product Manager orcharhino, ATIX
- **Peter Cummings**
  Founder & CEO, LinuxGuard

BEFORE WE BEGIN

Housekeeping

orcharhino | LinuxGuard
Visibility. Confidence. Control.

This session is being recorded

You'll receive the recording after the webinar.

All participants are muted

Microphones stay off for the duration of the session.

Use the Q&A or chat for questions

We'll answer them during the Q&A at the end.

Ask at any time

Submit questions throughout the presentation.

Slides will be shared

You'll get the deck after the webinar too.

orcharhino | LinuxGuard
Visibility. Confidence. Control.

Why you want Zero Blind Spots

Linux carries some of the workloads that matter most — the gaps in how it is run and governed are exactly where risk accumulates.

01
Critical infrastructure
Essential systems depend on Linux at their core.

02
Fragmented estates
Distributions sprawl, each managed its own way.

03
No clear overview
Of every system and its state.

04
Tooling dependence
Reliance on tools controlled outside Europe.

05
Regulation tightening
Raising the bar on control and evidence.

orcharhino | LinuxGuard
Visibility. Confidence. Control.

Lifecycle of a Linux-server

A server is never “done.” It moves continuously through six stages — and every stage is a place where a blind spot can open.

- Every stage must be actively managed
- Manual configuration is error-prone
- Management has to scale with the fleet
- Automation and control are non-negotiable

TAKEAWAY

Without automation and control, gaps open at **every stage of the loop.**

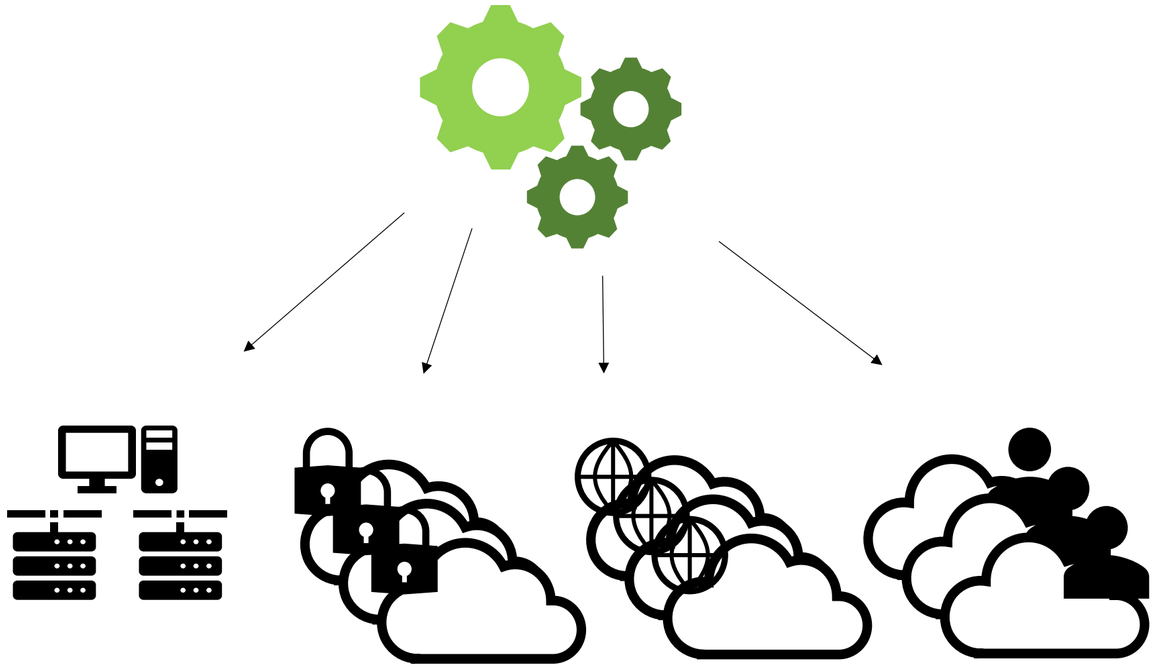
Orchestration with orcharhino

- Centralized automation to control
- Provisioning
- Configuration
- Content (Release management)
- Patching & Security Updates
- Compliance & Subscriptions

orcharhino

Powered by ATIX

Vendor independence



debian CentOS Red Hat ORACLE LINUX SUSE

Rocky Linux AlmaLinux ubuntu Amazon Linux

orcharhino

OpenVox puppet ANSIBLE SALT PROJECT

vmware vSphere KVM ORACLE Linux Virtualization Manager PROXMOX

amazon web services EC2 Microsoft Azure Google Cloud Platform

more to come... NUTANIX

ATIX & orcharhino – Well established.

- 30+ years Linux, Open Source and Consulting
- ISO/IEC 27001 certified

- 10 years of orcharhino
- Global customers: Europe/US/Australia
- Global Partnerships & ECO-System

30 ATIX YEARS OF INNOVATION

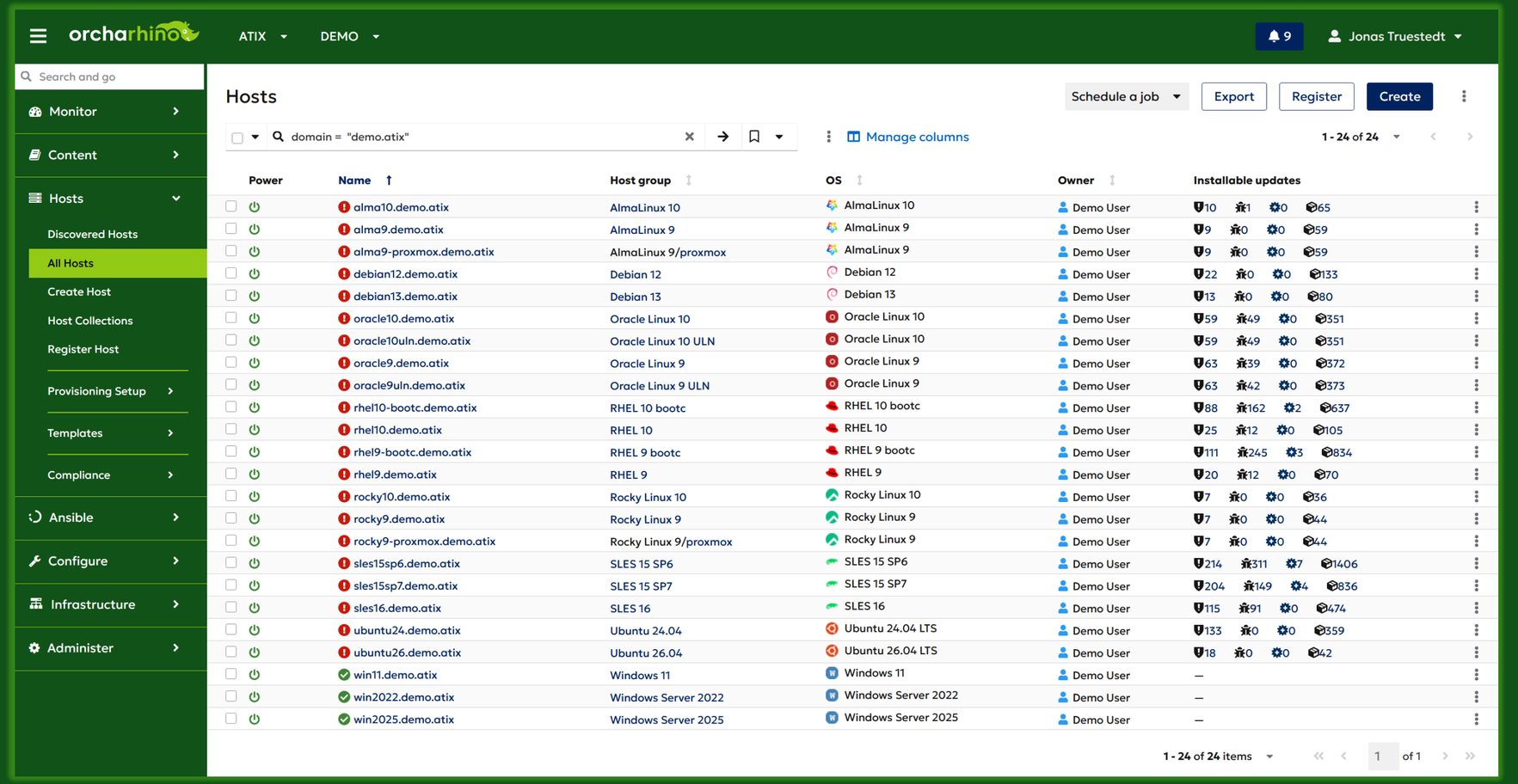
10 years orcharhino

orcharhino

Powered by ATIX

Live-Demo

- Provisioning of new hosts
- Patching of hosts
- Configuration change
- OpenSCAP Report



orcharhino | LinuxGuard
Visibility. Confidence. Control.

orcharhino covers the lifecycle

orcharhino Not yet covered

Orchestration with orcharhino

- Lifecycle automation & Provisioning
- Standardized base configuration
- Staged patching cycles
- Patch management and Security Errata
- OpenSCAP Compliance reports

→ **One box stays dark — who can act on it?**

LinuxGuard
Visibility. Confidence. Control.

LINUXGUARD HANDLES IDENTITY & PRIVILEGE

The identity blind spot

The operating system is provisioned, standardised and patched. But access to it drifts quietly — and no patch cycle ever closes that gap.

Shadow privilege

Accounts accrue sudo rights over months. No one can say who can actually become root, on which host.

Unmanaged SSH keys

Orphaned keys, weak algorithms and cross-server sprawl — invisible without fleet-wide analysis.

Uncontrolled service accounts

Databases, pipelines and app runners holding stale credentials and standing access nobody owns.

WHAT LINUXGUARD IS

LinuxGuard
Visibility. Confidence. Control.

Identity-first Linux security

Real-time monitoring, identity-aware detection, and continuous compliance for Linux servers — without kernel modules or persistent root access.

eBPF-native

Kernel-level visibility with none of the kernel-module risk, in a 50–100 MB footprint.

Identity-first

Every event tied back to the original logged-in user — even through sudo escalation chains.

SaaS, no infrastructure

A single-line installer with Ansible, Chef, Puppet and major cloud automation built in.

CAPABILITY · VISIBILITY

LinuxGuard
Visibility. Confidence. Control.

Central identity control

One place to see every human and machine identity, understand the privilege behind it, and act before it becomes exposure.

See

Every identity, mapped

Cross-server profiles for every human and service account, each with a composite risk score and dormancy detection.

Understand

Every privilege, explained

SSH-key posture and sudo policy analysed fleet-wide — weak algorithms, sprawl and escalation paths surfaced automatically.

Control

Every access, owned

Service accounts classified and attributed to an owner, so standing access can be questioned and reduced.

LinuxGuard
Visibility. Confidence. Control.

CAPABILITY · ZERO TRUST

Least privilege, continuously enforced

- ✓ Findings mapped to MITRE ATT&CK — you see *what* happened **and who did it**.
- ✓ Identity survives sudo escalation through LoginUID attribution.
- ✓ Behaviour baselined: observation → shadow → active enforcement.

97

MITRE ATT&CK-mapped signal types, enriched with identity context

4

Targeted containment actions, each behind a triple opt-in safety model

7

Component types tracked for configuration drift across the fleet

CAPABILITY · COMPLIANCE

Continuous compliance evidence

LinuxGuard
Visibility. Confidence. Control.

Evidence that is generated continuously, not assembled the week before an audit — mapped to the frameworks that European and UK enterprises answer to.

NIS2 | DORA | GDPR | ISO 27001 | SOC 2 | NIST CSF 2.0 | CIS v8.1 | PCI-DSS v4 | HIPAA

Per-control scoring

Every control scored and trended over time, with on-demand PDF evidence packages for auditors.

Chain-hashed audit trail

Every response action recorded in a tamper-evident trail, with suppression tracking and expiry.

Mapped to the mandate

NIS2 requires identity governance; DORA requires access-control evidence. Capabilities map to the articles.

LinuxGuard
Visibility. Confidence. Control.

CAPABILITY · RESPONSE

Automated, reversible response

Contain a threat the moment it's detected — with the safety nets that let an enterprise actually leave automation switched on.

Targeted containment

Lock an account, end a session, disable a key or revoke sudo — scoped to exactly the host that needs it.

Triple opt-in safety

Playbook, server-group scope and agent flag must all agree. Rate limits and a circuit breaker prevent runaway action.

Reversible by design

Pre-action state is captured and restored, so containment never costs you forensic integrity.

LIVE DEMO

LinuxGuard, in action

LinuxGuard
Visibility. Confidence. Control.

LIVE PRODUCT WALKTHROUGH

- Identity risk scores across the fleet
- MITRE ATT&CK-mapped detections
- SSH-key posture & sudo escalation paths
- One-click, reversible containment

Zero blind spots across the lifecycle

orcharhino | LinuxGuard
Visibility. Confidence. Control.

orcharhino LinuxGuard Both tools

Orchestration with orcharhino

- Lifecycle automation & Provisioning
- Standardized base configuration
- Staged patching cycles
- Patch management and Security Errata
- OpenSCAP Compliance reports

Assurance by LinuxGuard
Visibility. Confidence. Control.

- Identities and Privileged Access (SSH-keys, sudo, PAM)
- Security configuration drift
- Zero Trust enablement
- Automated remediation
- Continuous compliance evidence

DIGITAL SOVEREIGNTY

Two European tools, one sovereign stack

orcharhino

LinuxGuard
Visibility. Confidence. Control.

From OS provisioning to identity governance, the entire Linux lifecycle stays under European, transparent, verifiable control.

European vendors

Both products built in Europe, with no US cloud dependency in the control path.*

Full transparency

See and verify exactly what each tool does on your servers.

Regulation-ready

Designed for NIS2, DORA and GDPR articles.

*subject to terms and conditions

IN SUMMARY

Key takeaways

orcharhino | LinuxGuard
Visibility. Confidence. Control.

1 **Patching closes the OS gap. Identity closes the access gap.**

orcharhino keeps the system current and standardised; LinuxGuard governs who can act on it. Neither gap stays open.

2 **Continuous evidence, not point-in-time audits.**

Identity, privilege and compliance are observed continuously and mapped to the NIS2 and DORA articles that require them.

3 **A sovereign Linux lifecycle, end to end for the first time.**

Two transparent European tools give you control of the full lifecycle with no hidden dependencies.

QUESTIONS & NEXT STEPS

Thank You! We're happy to answer your questions...

LinuxGuard
Visibility. Confidence. Control.

@LinuxGuard

linuxguard.io

orcharhino
Automate your infrastructure • Free your business

orcharhino.com/en/start-now/

@orcharhino

orcharhino.com

Let’s close the blind spots.