NØNOS

Target Markets & One-Page Use Case Briefs

Investor edition - concise market sizing, problem fit, and target accounts for demos.

Date: 25 February 2026

Note: Market sizing figures are directional and sourced from publicly available material. Where noted, counts are derived from cited rates.

Product snapshot

NØNOS is a zero-trust operating system designed for 'zero-trace' sessions: it runs from RAM, isolates apps, and minimizes the ways data and malware can persist on a host machine.

Core design points

- Pure Rust microkernel and isolation-first architecture (smaller trusted core; reduced blast radius).
- Runs entirely in RAM by default (no disk writes unless encrypted storage is explicitly enabled).
- Signed 'capsule' apps with predefined permissions; untrusted code is constrained.
- No telemetry by default; privacy is the starting point.
- Encrypted onion-routed networking / mesh options for privacy-resilient connectivity.

Primary investor narrative

- NØNOS turns any commodity laptop/desktop into a clean, disposable workstation for high-risk tasks (admin, provisioning, support, incident response).
- The same core approach applies across device-heavy industries: routers, TVs, appliances, vehicles, OT/utility infrastructure, payments, kiosks, and security systems.

Use case 01

Privileged Admin & Support Workstations Disposable High-Risk Sessions (PAM/IAM)

Privileged admin and support workstations are the keys to the kingdom. They access IAM/PAM consoles, cloud dashboards, remote access tools, and production systems across many environments. The risk is persistence: browser sessions, cached tokens, temp files, and tooling artifacts accumulate on long-lived laptops, and a single compromise becomes a repeatable bridge for lateral movement.

NØNOS turns the admin laptop into a resettable least-privilege tool. Operators can boot a clean session per task, run only required utilities as signed capsule apps, and shut down to eliminate residue. Because sessions run from RAM and avoid disk writes by default, credentials and sensitive artifacts do not quietly accumulate on the host. This reduces blast radius and makes privileged workflows repeatable without relying on perfect user discipline.

Market size ($)

~ $3.29B (PAM market, 2024).

Buyer / entry point

CISO, IAM lead, IT security engineering, MSSP/IR lead

Why NØNOS fits

- Boots clean, stateless sessions from RAM, reducing persistence risk on admin machines.
- Microkernel isolation + signed “capsule” apps limit blast radius from a compromised tool.
- No telemetry by default; fewer background processes and less data exhaust.

Direct faults fixed

- Credential theft from cached sessions, temp files, and browser artifacts.
- Malware persistence (disk implants, scheduled tasks, startup items).
- Lateral movement via compromised admin laptops used across environments.

Targets to approach (demo-ready)

- Microsoft
- Okta
- CyberArk
- BeyondTrust
- Palo Alto Networks
- CrowdStrike
- Accenture
- Deloitte
- Kyndryl
- Wipro
- HCLTech
- NTT DATA

Demo to showcase

- Boot NØNOS on an admin laptop; open an "Admin Access" capsule.
- Log into a demo IAM/PAM portal; perform a privileged workflow (rotate creds / approve access / SSH).
- Shutdown and show no residue on the host machine.

Sources: Grand View Research - Privileged Access Management (PAM) market size (2024).

Use case 02

Incident Response, Malware Triage & “Clean-Room” Digital Forensics

Incident response teams constantly handle hostile artifacts, such as suspicious attachments, disk images, USB media, logs from compromised hosts, and unknown executables that can detonate the moment they are opened. The core problem is cross contamination, where analysts use long-lived workstations or VMs that still depend on a large host OS. Investigation work also leaves traces, including tool caches, extracted payloads, and case notes, that can leak or become reinfection sources later.

NØNOS supports clean room computing by booting into a sterile environment that runs in RAM, allowing analysis and detonation, then wiping the session on shutdown. Because it minimizes persistence by design and isolates applications, it reduces the risk that malware can implant itself for later, or that sensitive case data remains on an analyst machine. Signed capsule apps also allow teams to constrain tools to strict permissions, limiting blast radius while working with hostile content.

Market size ($)

~ $10.46B DFIR solutions market (2025).

Buyer / entry point

IR director, DFIR lead, SOC manager, MSSP

Why NØNOS fits

- Disposable, repeatable analysis environment (fresh boot per case).
- Reduces contamination of evidence and analyst tooling across incidents.
- Isolated capsules support controlled toolchains for analysis and reporting.

Direct faults fixed

- Cross-case contamination (tools, indicators, samples persisting between cases).
- Analyst workstation compromise from detonating/handling malware artifacts.
- Forensic integrity risk from OS background writes and uncontrolled telemetry.

Targets to approach (demo-ready)

- Mandiant (Google)
- CrowdStrike
- Palo Alto Networks Unit 42
- Microsoft DART
- IBM Security
- Secureworks
- SentinelOne
- Rapid7
- Trellix
- Cisco Talos
- Kroll
- Stroz Friedberg

Demo to showcase

- Boot NØNOS; open a “Triage” capsule with tooling + write-blocked media access.
- Analyze a sample; export report to encrypted removable storage only.
- Reboot to prove the environment resets with no residue.

Sources: Mordor Intelligence - DFIR solutions market size (2025).

Use case 03

Government and Defense Secure Travel and Field Workstations

Field work and travel create a perfect storm of hostile networks, increased device loss or seizure risk, and time pressure. Traditional laptops accumulate operational residue, such as documents, chat artifacts, cached authentication tokens, and Wi-Fi credentials, that can be extracted if a device is inspected, stolen, or compromised during travel.

NØNOS addresses the travel threat model by enabling zero-trace sessions that run from RAM and leave no disk trail by default. When persistence is needed, it can be explicitly enabled using encrypted storage rather than silently accumulating data over months. Application isolation and capsule apps allow the workstation to run only approved communications, document, and access tools with narrowly scoped permissions, making the device disposable by default while still usable on commodity hardware.

Market size ($)

~ $100.6B defense IT spending (2024).
Context: ~ $2.63T global defense spending (2025).

Buyer / entry point

CIO/CISO (public sector), security operations, defense primes

Why NØNOS fits

- Zero-trace sessions mitigate hotel/airport/ foreign network risk and device seizure scenarios.
- Onion-routed networking can reduce metadata exposure in hostile environments.
- Signed capsules standardize approved apps (browser, comms, wallet) across agencies.

Direct faults fixed

- Sensitive artifacts left behind on travel laptops (docs, caches, logs).
- Long-lived endpoint compromise from phishing/malvertising during travel.
- Policy drift from unmanaged app installs and inconsistent hardening.

Targets to approach (demo-ready)

- DHS (US)
- DoD (US)
- NCSC (UK)
- GCHQ ecosystem (UK)
- Australian Defence
- NATO agencies
- Thales
- BAE Systems
- Raytheon
- Lockheed Martin
- Northrop Grumman
- Leonardo

Demo to showcase

- Travel laptop boots NØNOS from an official USB; launches approved comms capsule.
- Show encrypted networking mode; demonstrate no disk residue after shutdown.
- Optional: show encrypted storage enablement for approved cases.

Sources: IMARC Group - Defense IT spending market (2024). IISS - global defense spending (2025).

Use case 04

ISPs and Field Technicians Router and Home Gateway Provisioning Kits

Provisioning and servicing routers and home gateways is high volume work performed in uncontrolled environments. Technician laptops touch customer networks, removable tooling, and vendor utilities, then move to the next site. The operational risk is that these laptops become compromise vectors, picking up malware from one location and carrying it to others, while also storing customer credentials, configs, and network identifiers in logs and tool caches.

NØNOS turns the provisioning laptop into a resettable least-privilege tool. Technicians can boot a clean session for each job, run the required provisioning utilities as signed capsule apps, and shut down to eliminate job residue. Since it runs from RAM and avoids disk writes by default, customer credentials and configuration artifacts do not accumulate on the tech machine. This clean per visit model reduces cross-customer contamination and shrinks the attack surface of field workflows without relying on perfect user discipline.

Market size ($)

~ $15.05B Wi-Fi router market (2025).

Buyer / entry point

ISP security, field ops, CPE engineering, managed services

Why NØNOS fits

- Technician laptops are common infection vectors; NØNOS provides a clean boot for provisioning.
- Ephemeral sessions reduce leakage of customer Wi-Fi credentials and ISP admin creds.
- Capsules can bundle vendor-specific onboarding tools in a controlled permission model.

Direct faults fixed

- Credential sprawl: saved passwords, cached config files, screenshots.
- Field laptop compromise leading to fleet-wide credential reuse attacks.
- Uncontrolled tool installs and “driver packs” that broaden attack surface.

Targets to approach (demo-ready)

- Comcast
- Charter (Spectrum)
- BT
- Vodafone
- Orange
- Deutsche Telekom
- Telstra
- Optus
- NBN Co
- Cisco
- Juniper Networks
- Ubiquiti

Demo to showcase

- Boot NØNOS on a field laptop; open an “ISP Provisioning” capsule.
- Provision a router, rotate credentials, generate a customer handover QR.
- Shutdown and show no residue on the host machine.

Sources: Mordor Intelligence - Wi-Fi router market size (2025).

Use case 05

Smart TVs and Connected Entertainment Secure Content and Support Workstations

Smart TV ecosystems combine high scale with high value assets. They include DRM materials, firmware signing, content pipelines, and vendor support channels where untrusted files and crash dumps arrive constantly. Support and release workstations often become repositories of sensitive material, including tokens, keys, debug builds, and customer logs, while remaining connected to broad corporate networks. This creates a high value target for theft and persistent compromise.

NØNOS fits because it treats these tasks as high-risk sessions that should not persist by default. Running from RAM and minimizing disk residue reduces the likelihood that keys, tokens, and proprietary artifacts are left behind in caches and temporary directories. Capsule apps allow a vendor to lock a support desktop to only the required tools and endpoints, reducing both secrets exposure and long-lived workstation compromise by changing the session model rather than just hardening a stateful OS.

Market size ($)

~ $246.96B smart TV market (2025).

Buyer / entry point

OEM security, content security, customer support operations

Why NØNOS fits

- Supports high-trust operations (content keys, DRM workflows, support tooling) in clean sessions.
- Capsule apps can lock support tools to approved binaries and permissions.

Direct faults fixed

- Support workstation compromise leading to credential theft and account takeover.
- Persistent malware on media ops machines handling valuable content pipelines.
- Shadow IT tooling installed to “debug” devices and capture streams.

Targets to approach (demo-ready)

- Samsung
- LG
- Sony
- TCL
- Hisense
- Roku
- Amazon (Fire TV)
- Google TV
- Netflix
- Disney
- Comcast
- Sky

Demo to showcase

- Boot NØNOS; launch a “TV OEM Support” capsule (diagnostics + key management).
- Show secure remote session into a test device; export logs to encrypted storage.
- Reboot to demonstrate clean state.

Sources: Grand View Research - Smart TV market size (2025).

Use case 06

Connected Home Appliances Service and Warranty Tech Workstations

Appliance service workflows routinely connect laptops to embedded systems for diagnostics, calibration, and firmware updates. This often happens via USB, serial adapters, or local network links in customer environments. The risks are that tech workstations can pick up malware from uncontrolled networks or devices, and they can retain customer data or device identifiers in logs, backups, and support folders across thousands of visits.

NØNOS enables a disposable service session. Technicians boot into a known clean RAM-resident environment, run signed service tooling with constrained permissions, complete the job, and shut down to wipe traces. This breaks the pattern of field laptops acting as long-lived state containers that cause cross-customer exposure and persistent compromise. Every service call starts from a clean baseline, reducing security risk and operational variability caused by drift and accumulated software changes.

Market size ($)

~ $503.03B home appliances market (2024).

Buyer / entry point

OEM service operations, warranty networks, field service IT

Why NØNOS fits

- Service laptops touch customer networks and devices daily; a stateless OS reduces contamination.
- Prevents storage of customer credentials, diagnostics dumps, and personal data by default.
- Capsules can package OEM diagnostic tools with minimal permissions.

Direct faults fixed

- Tech laptop malware spreading across home networks via service visits.
- Customer data exposure from logs, photos, and diagnostic exports left on devices.
- Unpatched Windows toolkits used long past vendor support windows.

Targets to approach (demo-ready)

- Whirlpool
- Electrolux
- GE Appliances
- LG
- Samsung
- Bosch
- Haier
- Midea
- Carrier
- Trane
- Daikin
- Lennox

Demo to showcase

- Boot NØNOS and run an “Appliance Diagnostics” capsule (OEM tool).
- Pull diagnostics, generate a signed service report, store to encrypted media only.
- Shutdown to show session clean-up.

Sources: Grand View Research - Home appliances market size (2024).

Use case 07

Mobile Devices Repair Warranty Refurbishment and Secure Trade In

Repair and refurbishment centers handle massive volumes of personal devices. Privacy risk is inherent because customer data, authentication tokens, synced accounts, and backups can accidentally persist on technician PCs through diagnostic and migration tools. Devices may also be compromised or contain malicious software that attempts to exploit the connected workstation as soon as debugging bridges or file transfers are enabled.

NØNOS reduces this risk by making the technician environment non accumulative. Sessions run from RAM and nothing is written to disk unless explicitly enabled, limiting data retention and reducing privacy liability. Diagnostic and transfer utilities can run as signed capsule apps with fixed permissions so the workstation only accesses what it must. This combination reduces both data leakage and persistent infection pathways in high throughput device handling.

Market size ($)

~ $42.33B refurbished/used smartphones (2025)
Alt (broader): ~ $63.5B (2025).

Buyer / entry point

Repair operations, warranty partners, OEM channel security

Why NØNOS fits

- Repair/refurb sites handle sensitive customer data and high volumes of devices.
- Bootable, disposable workstations reduce data leakage during diagnostics and wiping.
- Capsules can standardize device wipe/QA tooling and enforce logging to controlled storage.

Direct faults fixed

- Residual customer data in repair logs, screenshots, or copied backups.
- Malware persistence on shared shop PCs used for unlocking/flashing.
- Credential theft from OEM portals and MDM dashboards used by technicians.

Targets to approach (demo-ready)

- Apple
- Samsung
- Google
- AT&T
- Verizon
- Vodafone
- Telstra
- Asurion (uBreakiFix)
- Assurant
- Foxconn
- Flex
- Ingram Micro

Demo to showcase

- Boot NØNOS on a bench PC; run a “Device Intake” capsule.
- Perform identity-verified wipe workflow; export audit record to encrypted storage.
- Reboot to reset the station for the next device.

Sources: Custom Market Insights - Refurbished & used mobile phones market (2025). Dimension Market Research (alt).

Use case 08

IoT Fleet Provisioning and Device Operations

IoT provisioning is a supply chain hotspot. Factories and integrators inject credentials, certificates, firmware, and configuration into devices at scale. The weak link is often the provisioning station itself. If the workstation is compromised, attackers can steal keys, silently alter firmware, or poison configuration in a way that propagates to thousands or millions of deployed devices.

NØNOS strengthens provisioning by enabling a cryptographically controlled stateless station. Each session starts clean from RAM, tooling runs as signed capsule apps with predefined permissions, and secrets do not need to live on a long-lived desktop where they can be harvested over time. This reduces quiet persistence and operator drift, which are common root causes of supply chain compromise, and it provides leverage because securing the provisioning point secures the downstream fleet identity and firmware lineage.

Market size ($)

~ $805.7B worldwide IoT spending (2023).
Forecast: > $1T by 2026 (IDC).

Buyer / entry point

OEM security, manufacturing engineering, IoT platform teams

Why NØNOS fits

- Provisioning stations are a root-of-trust bottleneck; NØNOS provides clean, repeatable build/provision sessions
- Capsules can contain signing/provisioning tools with locked-down permissions.
- RAM-only operation helps protect secrets (tokens, certificates) from persisting on shared stations.

Direct faults fixed

- Secret leakage from build machines (API keys, certs, manufacturing tokens).
- Supply-chain compromise via infected engineering laptops or USB tooling.
- Cross-project contamination from shared environments.

Targets to approach (demo-ready)

- AWS IoT
- Microsoft Azure IoT
- Siemens
- Schneider Electric
- Honeywell
- Bosch IoT
- Arm
- STMicroelectronics
- Texas Instruments
- NXP
- Jabil
- Flex

Demo to showcase

- Boot NØNOS; run a “Provisioning” capsule to generate and inject device credentials.
- Show secret material stored only in-memory unless explicitly exported.
- Shutdown to reset station state between batches.

Sources: IDC Worldwide IoT Spending Guide (reported in trade press, 2023/2026).

Use case 09

Smart Cars and Dealership Service Bays Diagnostic and ECU Flashing Stations

Dealership diagnostics and ECU flashing blend safety-critical operations with messy realities. Shared service laptops, removable media, vendor utilities, and high turnover are common. Compromised or misconfigured service workstations can become mechanisms for pushing corrupted firmware, leaking vehicle and customer data, or enabling repeatable exploitation across many vehicles serviced by the same shop.

NØNOS supports high integrity servicing through clean diagnostic and flashing sessions that can be restarted between vehicles. Running from RAM minimizes residue and reduces the chance malware persists between jobs. Capsule apps can constrain diagnostic tooling to required device interfaces and approved OEM endpoints rather than allowing a general-purpose PC on an open network. This improves hygiene without depending on perfect patching and perfect operator behavior on a long-lived OS.

Market size ($)

~ $43.99B automotive diagnostics scan tools (2025).

Buyer / entry point

OEM service security, dealership IT, automotive cybersecurity

Why NØNOS fits

- Service bay laptops interface directly with vehicles; a clean boot reduces risk of malicious tooling
- Prevents VIN data, customer PII, and firmware artifacts persisting on shared diagnostics PCs.
- Capsules can package OEM diagnostics and limit network exposure.

Direct faults fixed

- Compromised diagnostic laptops pushing tampered firmware or extracting data.
- Credential leakage for OEM service portals and tooling licenses.
- Persistent malware from USB tools used across bays.

Targets to approach (demo-ready)

- Bosch Mobility Aftermarket
- Snap-on
- Autel
- Launch Tech
- Aptiv
- Continental
- Tesla
- Ford
- General Motors
- Toyota
- Volkswagen Group
- Stellantis

Demo to showcase

- Boot NØNOS at the service bench; launch an “Auto Diagnostics” capsule.
- Run diagnostics and produce a signed service record; export to encrypted storage.
- Shutdown and reset between vehicles.

Sources: Precedence Research - Automotive diagnostics scan tool market size (2025).

Use case 10

Medical Implant and Critical Device Programmer Stations

Clinical programmer workflows are uniquely sensitive because integrity failures can become patient safety incidents, and downtime from ransomware or instability disrupts urgent care. Many ecosystems still depend on general-purpose computing environments for programming, support, or maintenance. Patch constraints, third party drivers, and long-lived system state increase the chance of exploitable flaws and persistent compromise.

NØNOS provides a high integrity known clean workstation model. It uses RAM resident sessions that minimize persistent state, isolates applications, and constrains programmer support tooling to predefined permissions. This reduces the surface for persistence and reduces residue of sensitive artifacts on the workstation. Instead of relying on a stateful OS to remain clean indefinitely, NØNOS makes clean by default the operating mode, which aligns with safety critical requirements for repeatable trust.

Market size ($)

~ $5.7B pacemakers market (2024).
Alt: ~ $5.91B (2025).

Buyer / entry point

Medical device security, clinical engineering, hospital IT

Why NØNOS fits

- Programmer laptops and clinic stations are high-trust endpoints; NØNOS reduces persistence risk.
- Stateless sessions lower the chance of patient data lingering in logs and caches.
- Signed capsules enforce only approved programming software and permissions.

Direct faults fixed

- Patient data exposure through residual files, logs, and screenshots on clinic PCs.
- Persistent malware on shared medical programming stations.
- Uncontrolled software installs on legacy clinic endpoints.

Targets to approach (demo-ready)

- GE HealthCare
- Siemens Healthineers
- Mayo Clinic
- HCA Healthcare
- Kaiser Permanente
- Cleveland Clinic
- Medtronic
- Abbott
- Boston Scientific
- Biotronik
- MicroPort
- Philips

Demo to showcase

- Boot NØNOS; run a “Medical Programmer” capsule (simulator/demo environment).
- Show audit logging to approved encrypted storage only.
- Shutdown and demonstrate session reset.

Sources: Global Market Insights - Pacemakers market (2024). Fortune Business Insights (alt 2025).

Use case 11

Physical Security CCTV NVR VMS Admin Consoles and Installer Toolkits

Physical security deployments are administered through powerful consoles that can view, export, and reconfigure fleets of cameras and recorders across multiple sites. Installer laptops and admin machines regularly touch insecure networks and unpatched devices, yet they retain credentials and configuration data that can be used to compromise the entire surveillance environment and sometimes pivot into corporate IT networks.

NØNOS makes admin and installer operations safer by making the workstation disposable and tightly permissioned. A clean RAM-only session prevents credentials and sensitive exports from lingering in caches, while capsule apps restrict tools to required camera subnets, management servers, and device interfaces. This limits persistence and lateral movement. Even if a security device network is hostile, the workstation is engineered to minimize what can be retained and how far incidents can spread.

Market size ($)

~ $73.75B video surveillance market (2024).

Buyer / entry point

Physical security, integrators, enterprise security operations

Why NØNOS fits

- Security installers and control-room operators use high-privilege consoles; NØNOS reduces persistence and credential leakage.
- Capsules can bundle VMS tooling (camera discovery, configuration) safely.
- RAM-only operation limits storage of site maps, access codes, and footage exports.

Direct faults fixed

- Default passwords and credential reuse across-sites stored on technician laptops.
- Malware persistence on NVR/admin PCs connected to sensitive physical security networks.
- Unpatched Windows boxes running VMS software for years.

Targets to approach (demo-ready)

- Avigilon (Motorola Solutions)
- Bosch Security Systems
- Honeywell
- Verkada
- Cisco
- Johnson Controls
- Axis Communications
- Hikvision
- Dahua Technology
- Hanwha Vision
- Genetec
- Milestone Systems

Demo to showcase

- Boot NØNOS; run a “VMS Admin” capsule to discover and configure demo cameras.
- Demonstrate enforced credential rotation and secure export controls.
- Shutdown to reset operator workstation.

Sources: Grand View Research - Video surveillance market size (2024).

Use case 12

Retail Payments POS Terminals Store Back Office and Payment Operations

Retail payments are heavily targeted because the payoff is immediate. The weak point is often the management layer. Back office PCs used for POS administration, remote support, and exception handling are credential rich and connected to store networks. Over time they accumulate tools, tokens, and remote access utilities, making them attractive as persistent footholds into payment environments.

NØNOS provides a secure admin workstation pattern. POS management and support sessions run from RAM so tokens and credentials do not persist. Application isolation and capsule permissions restrict tools to only required endpoints and interfaces.

This directly addresses the persistent foothold problem that often precedes widespread POS compromise and reduces both the probability and the dwell time of payment incidents.

Market size ($)

~ $113.38B POS terminal market (2024).
~ $123.15B (2025).

Buyer / entry point

Retail CIO/CISO, payments security, store operations

Why NØNOS fits

- Reduces risk of payment admin credentials persisting on store/back-office PCs.
- Clean boot can lower infection rates from USB, phishing, and “shared PC” usage in stores.
- Capsules can harden back-office portals and remote support tooling.

Direct faults fixed

- Credential theft leading to remote takeover of payment admin dashboards.
- Malware persistence on store PCs used for refunds, reconciliation, and updates.
- Poor patch hygiene on low-cost back-office endpoints.

Targets to approach (demo-ready)

- Block (Square)
- Toast
- Shopify
- Adyen
- Stripe
- Fiserv (Clover)
- Verifone
- Ingenico
- Worldpay
- Global Payments
- NCR Voyix
- PayPal

Demo to showcase

- Boot NØNOS; run a “Retail Ops” capsule with least-privilege support tools.
- Show secure remote support session and controlled export of reports.
- Shutdown to clear session.

Sources: Grand View Research - POS terminal market size (2024/2025).

Use case 13

ATMs and Banking Kiosks Secure Maintenance and Update Stations

ATM and kiosk fleets are serviced using maintenance workflows that may involve removable media, field laptops, and vendor utilities applied repeatedly across devices. A compromised service workstation can become an infection amplifier by spreading malicious updates or leaking administrative credentials across an entire fleet.

NØNOS breaks the amplification path by making the maintenance environment clean session by default. RAM resident operation reduces credential residue and makes it harder for malware to persist between service calls. With signed capsule apps, banks and vendors can enforce which utilities run and what they can access, reducing operator error and attacker opportunity. This controls statefulness itself rather than hoping a long-lived OS remains clean across hundreds of field interactions.

Market size ($)

~ $25.29B ATM market (2024).

Buyer / entry point

Bank security, ATM operations, field service providers

Why NØNOS fits

- ATM service endpoints are high-risk: they touch cash networks and privileged update channels.
- NØNOS can provide a standard clean boot image for field updates and diagnostics.
- Capsules can package vendor maintenance tools with locked-down permissions.

Direct faults fixed

- Field laptop compromise leading to malicious software updates.
- Credential leakage for bank maintenance portals and vendor VPNs.
- Persistent malware and untracked tool installs on service PCs.

Targets to approach (demo-ready)

- NCR Voyix
- Diebold Nixdorf
- Hyosung
- GRG Banking
- Fiserv
- Euronet
- FIS
- JPMorgan Chase
- Bank of America
- HSBC
- Wells Fargo
- Westpac

Demo to showcase

- Boot NØNOS from an official USB; launch an “ATM Service” capsule.
- Demonstrate authenticated update workflow and logging to encrypted media.
- Reboot to reset the service station.

Sources: Grand View Research - ATM market size (2024).

Use case 14

Utilities Smart Meter and AMI Operations and OT Jump Hosts

Utilities rely on jump hosts and operational tooling that bridge IT and OT environments. These systems are long-lived, heavily used, and rich in credentials and remote access tooling. Once compromised, they provide durable footholds for lateral movement into operational environments that are difficult to patch and monitor, with high consequences for availability and safety.

NØNOS turns jump access into a disposable trust boundary. Each access session can start from a RAM resident no-trace baseline with only required OT access tools and network paths. Application isolation and capsule permissions reduce the chance that a compromised tool expands access, while low persistence reduces credential residue that attackers typically harvest. This yields safer access by preventing the jump workflow from accumulating compromise over time.

Market size ($)

Smart meters: ~ $30.92B (2025). Smart grid cybersecurity: ~ $7.5B (2024) / $8.3B (2025).

Buyer / entry point

CISO (utilities), OT security, grid operations

Why NØNOS fits

- Utility OT networks require strict separation; NØNOS enables disposable jump hosts for admin access.
- Capsules can control which tools are allowed onto OT segments.
- RAM-only sessions reduce persistence of credentials and network artifacts.

Direct faults fixed

- Credential leakage from OT jump hosts and engineering laptops.
- Malware persistence bridging IT/OT via shared admin workstations.
- Uncontrolled software on long-lived OT admin PCs.

Targets to approach (demo-ready)

- Itron
- Landis+Gyr
- Sensus (Xylem)
- Honeywell
- Siemens
- Schneider Electric
- Enel
- National Grid
- Duke Energy
- AEMO (AU)
- Ausgrid
- EDF

Demo to showcase

- Boot NØNOS; run an “OT Jump Host” capsule with restricted networking.
- Access a demo AMI/SCADA environment; export audit logs to encrypted media.
- Shutdown to reset state.

Sources: Grand View Research - Smart meter market size (2025). Global Market Insights - Smart grid cybersecurity (2024/2025).

Use case 15

Public EV Charging Operator and Maintenance Toolkits

Public EV charging networks have thousands of endpoints, remote management stacks, firmware updates, and billing integrations. Field service and operator consoles are high leverage attack points. If the maintenance workstation or operator environment is compromised, it can become the mechanism for pushing malicious updates, stealing credentials, or disrupting availability across wide footprints.

NØNOS enables clean and constrained maintenance sessions that do not accumulate secrets or malware over time. A RAM-only session reduces the likelihood that credentials, API tokens, and firmware packages remain on technician machines. Signed capsule apps can lock maintenance tooling to approved update servers and required interfaces, reducing the risk that compromised software or human error turns the workstation into a fleet-wide compromise vector.

Market size ($)

~ $40.22B EV charging infrastructure (2025).
~ $50.20B (2026).

Buyer / entry point

CPO security, field operations, infrastructure security

Why NØNOS fits

- Charge networks rely on distributed operations; secure technician workstations reduce compromise risk.
- Capsules can package firmware update tools and site access workflows.
- Stateless boot reduces credential persistence and cross-site infection.

Direct faults fixed

- Compromised service laptops pushing malicious firmware or configs.
- Credential leakage for charger management platforms and site VPNs.
- Persistent malware acquired from public networks during field work.

Targets to approach (demo-ready)

- ChargePoint
- Electrify America
- EVgo
- Shell Recharge
- Bp pulse
- Tesla (Supercharger)
- Ionity
- ABB
- Siemens
- Tritium
- Schneider Electric
- Enel X Way

Demo to showcase

- Boot NØNOS; run an “EVSE Service” capsule to update a demo charger controller.
- Show secure credential handling and controlled export of service logs.
- Shutdown to reset between sites.

Sources: Grand View Research - EV charging infrastructure market size (2025/2026).

Use case 16

Industrial Automation OT Engineering Laptops Robotics and Factory Floor Administration

OT engineering laptops connect to PLCs, robots, HMIs, and controllers using legacy protocols and drivers. They are used across lines and plants and often cannot follow normal patch cycles. The engineering workstation becomes a universal adapter. If it is compromised, it can introduce malware into environments that prioritize uptime and can lead to sabotage, safety incidents, or prolonged outages.

NØNOS reduces engineering laptop risk by making it a clean per task tool. Engineers boot from RAM into a known baseline, run only required engineering utilities as signed capsule apps, and shut down to eliminate persistence and cross-site contamination. This removes the long-lived state attackers exploit for durable footholds and reduces configuration drift that accumulates on shared engineering machines over years.

Market size ($)

~ $274.99B industrial automation market (2025).

Buyer / entry point

OT security, plant engineering, industrial IT

Why NØNOS fits

- Factory engineering laptops are a top infection vector; NØNOS offers clean boots for OT access.
- Capsules can lock down PLC programming tools and vendor utilities.
- RAM-only operation reduces persistence of credentials and proprietary project files.

Direct faults fixed

- Malware persistence on engineering laptops used across lines and sites.
- Unauthorized tool installs and legacy drivers expanding attack surface.
- Credential reuse and weak separation between IT and OT environments.

Targets to approach (demo-ready)

- Siemens
- Schneider Electric
- Rockwell Automation
- Mitsubishi Electric
- Omron
- ABB
- FANUC
- KUKA
- Yaskawa
- Emerson
- Bosch Rexroth
- Honeywell

Demo to showcase

- Boot NØNOS; open a “PLC/Robot Engineering” capsule.
- Connect to a demo PLC/robot controller; show least-privilege tooling.
- Shutdown to reset state.

Sources: MarketsandMarkets - Industrial control & factory automation market size (2025).

Use case 17

Digital Signage Content Operations Media Players and Fleet Maintenance Consoles

Digital signage is a visible target where defacement damages brand trust quickly. Signage fleets often share centralized content credentials and update pipelines. The content operations workstation or CMS admin environment can become a single point of failure. Once compromised, attackers can push malicious media, steal fleet credentials, or manipulate update workflows across many sites.

NØNOS secures the control plane by providing a disposable least-privilege content operations workstation. RAM resident sessions reduce persistent credential and token residue. Capsule apps restrict content tools to approved upload endpoints and repositories. Because the environment minimizes persistence, compromise is less likely to stick long enough to quietly manipulate fleet content over time.

Market size ($)

~ $28.83B digital signage market (2024).

Buyer / entry point

Digital signage operators, AV integrators, retail media networks

Why NØNOS fits

- Signage fleets are often managed via low-cost PCs and remote tools; NØNOS reduces persistence and credential leakage.
- Capsules can package CMS admin tools and remote support securely.
- Stateless sessions reduce risk of long-lived compromise in NOC environments.

Direct faults fixed

- Credential theft for CMS platforms and remote access tools.
- Malware persistence on signage operations workstations.
- Uncontrolled downloads and plug-ins used to “fix” playback issues.

Targets to approach (demo-ready)

- Cisco Meraki
- Scala
- Broadsign
- Clear Channel Outdoor
- JCDecaux
- Daktronics
- BrightSign
- Samsung
- LG
- Sony
- Sharp/NEC
- Panasonic Connect

Demo to showcase

- Boot NØNOS; launch a “Signage Ops” capsule and manage a demo signage player.
- Show controlled deployment of content updates and audit logging.
- Shutdown to reset operator station.

Sources: Grand View Research - Digital signage market size (2024).

Use case 18

Self Ordering and Self Service Kiosks Secure Operator Workstations

Kiosk environments mix payments, customer data, and physical exposure in public locations. Kiosk fleets are managed through operator consoles and service workflows spanning many vendors and locations. If the operator workstation is compromised, attackers can gain a durable control path to push malware, exfiltrate secrets, or disrupt availability across an entire kiosk network.

NØNOS reduces control plane risk by turning the operator console into a clean session management station. RAM-only sessions and no default disk writes prevent administrative residue from accumulating. Signed capsule apps constrain management tooling to required interfaces and destinations. This delivers repeatable trust without defending a long-lived OS that grows more complex and vulnerable over time.

Market size ($)

~ $34.36B self-service kiosk market (2024).
~ $37.21B (2025).

Buyer / entry point

QSR IT, kiosk OEMs, managed services, payments security

Why NØNOS fits

- Kiosk fleets are maintained by field techs and vendors; NØNOS provides clean boot service stations.
- Capsules can bundle vendor kiosk admin utilities and payment integrations.
- Stateless sessions reduce credential persistence for remote management.

Direct faults fixed

- Compromised support laptops pushing malicious kiosk updates.
- Credential leakage for remote monitoring, payment, and CMS portals.
- Persistent malware on shared vendor workstations.

Targets to approach (demo-ready)

- McDonald's
- Yum! Brands (KFC/ Taco Bell)
- Starbucks
- Wendy's
- Domino's
- Woolworths
- NCR Voyix
- Acrelec
- Diebold Nixdorf
- Toshiba TEC
- Fujitsu
- Elo Touch Solutions

Demo to showcase

- Boot NØNOS; run a “Kiosk Support” capsule to update a demo kiosk image
- Show controlled export of logs and strict permissioning.
- Reboot to reset for the next service call.

Sources: Grand View Research - Self-service kiosk market size (2024/2025).

Use case 19

Printers and MFPs Secure Print Administration and Maintenance Workstations

Printers and MFPs touch directories, email, scan workflows, and internal networks, and require admin tooling for configuration and firmware updates. Print admin stations and service laptops can store credentials, configs, and scanned artifacts. They also interact with device ecosystems that can be vulnerable and may serve as stepping stones back into core IT networks.

NØNOS provides a safer print admin pattern by making management tasks non-persistent and permissioned. Running from RAM reduces leftover artifacts and cached credentials. Capsule apps restrict utilities to specific network segments and approved management endpoints. This reduces the chance print administration becomes a hidden long-lived foothold and makes each admin task a clean controlled operation.

Market size ($)

~ $32.09B multifunction printer market (2024).
~ $33.81B (2025).

Buyer / entry point

IT operations, print fleet managers, managed print services

Why NØNOS fits

- Printers and MFPs are frequent footholds; NØNOS secures the admin station used to manage firmware and credentials.
- Capsules can lock print admin tools and reduce exposure from browser-based management.
- Stateless sessions reduce leakage of directory creds, scan-to-email configs, and address books.

Direct faults fixed

- Admin credential theft and persistent sessions on print servers.
- Malware persistence on print admin PCs used across-sites.
- Ad-hoc tooling installed to “fix” printers, increasing attack surface.

Targets to approach (demo-ready)

- HP
- Canon
- Xerox
- Ricoh
- Konica Minolta
- Lexmark
- Epson
- Kyocera
- Brother
- PaperCut
- Kofax
- Sharp

Demo to showcase

- Boot NØNOS; run a “Print Admin” capsule and manage a demo printer fleet.
- Show firmware update workflow + credential rotation with minimal persistence.
- Shutdown to reset state.

Sources: Grand View Research - Multifunction printer market size (2024/2025).

Use case 20

Trading and Risk Terminals High Trust Financial Workstations

Trading terminals concentrate high value access to execution workflows, market data entitlements, research, and client information. Traditional desktops are stateful. Browser sessions linger, clipboard history persists, and background services accumulate. A single persistent compromise can silently siphon data, manipulate workflows, or capture credentials over extended periods.

NØNOS enables a high trust low residue trading session model. Sessions run from RAM, applications are isolated, and default disk persistence is prevented so sensitive artifacts do not accumulate. Signed capsule apps and predefined permissions constrain what the workstation can reach and what tools can do, shrinking attack surface without sacrificing usability. This reduces both credential residue and persistent compromise risk by changing the workstation trust model at the OS layer.

Market size ($)

Online trading platforms: ~ $10.82B (2025).
Financial risk management software: ~ $4.19B (2025).

Buyer / entry point

CISO (financial services), trading desk IT, risk and compliance

Why NØNOS fits

- High-value credentials and sensitive market data workflows benefit from a clean boot and reduced persistence.
- Capsules can harden access to trading platforms, internal chat, and risk systems.
- Built-in wallet/identity-less tooling aligns with crypto/DeFi adjacencies where relevant.

Direct faults fixed

- Credential theft from browser artifacts and session caches on trading desks.
- Persistent malware on high-privilege finance workstations.
- Shadow tooling and plug-ins installed under time pressure.

Targets to approach (demo-ready)

- Bloomberg
- LSEG (Refinitiv)
- FactSet
- Broadridge
- Intercontinental Exchange (ICE)
- Nasdaq
- CME Group
- JPMorgan Chase
- Goldman Sachs
- Citadel Securities
- Cboe
- Jane Street

Demo to showcase

- Boot NØNOS; open a “Trading Desk” capsule (market data + secure comms).
- Show controlled import/export and strict separation between sessions.
- Shutdown to reset workstation between users or shifts.

Sources: Fortune Business Insights - Online trading platform (2025) and financial risk management software (2025).

Source list (public)

The following public sources were used for the proxy market sizing figures in this document. Market size estimates vary by analyst methodology and scope; figures are included for directional context.

1. NØNOS - nonos.systems (Home) and /features (product positioning and capabilities).
2. Grand View Research - PAM (2024); Smart TV (2025); Home appliances (2024); Video surveillance (2024); POS terminals (2024/2025); ATM (2024); Smart meter (2025); EV charging infrastructure (2025/2026); Digital signage (2024); Self-service kiosk (2024/2025); Multifunction printer (2024/2025).
3. Mordor Intelligence - DFIR solutions (2025); Wi-Fi router market (2025).
4. IMARC Group - Defense IT spending market size (2024).
5. International Institute for Strategic Studies (IISS) - The Military Balance 2026 (global defense spending, 2025).
6. Custom Market Insights - Refurbished & used mobile phones market (2025).
7. Dimension Market Research - Refurbished smartphone market (broader estimate, 2025).
8. IDC Worldwide IoT Spending Guide (reported in trade press) - worldwide IoT spending (2023) and forecast to surpass $1T (2026).
9. Precedence Research - Automotive diagnostics scan tool market size (2025).
10. Global Market Insights - Pacemakers market size (2024); Smart grid cybersecurity market (2024/2025).
11. Fortune Business Insights - Online trading platform market size (2025); Financial risk management software market size (2025); Pacemaker market size (2025).
12. MarketsandMarkets - Industrial control & factory automation market size (2025).