PRODUCT GUIDE

SnapOS

Secure, Purpose-Built Endpoint OS for Modern Workspaces

Modern IT environments are more distributed, complex, and exposed than ever. Endpoints running traditional operating systems carry large attack surfaces, demand constant patching, and accumulate licensing costs that compound over time. If you've already moved to a dedicated endpoint OS, industry consolidation among vendors has often meant rising renewal pricing and tighter lock-in instead of relief. SnapOS solves all of that on most x86-64 (64-bit); UEFI or Legacy BIOS devices you already own, or inside a virtual machine without replacing hardware, multiplying management tools, or accepting your current vendor's pricing as the ceiling.

01 - OVERVIEW

What Is SnapOS?

SnapOS is a secure, immutable Linux-based endpoint operating system purpose-built for modern virtual, cloud, SaaS, and browser-based workspaces. It installs bare metal on most x86-64 (64-bit); UEFI or Legacy BIOS compatible devices, including laptops, thin clients, desktop PCs, legacy PCs, and mini form factor devices, or runs inside virtual machine environments when physical hardware is not in scope. It combines endpoint OS, deployment, policy, diagnostics, and management in one platform.

Once deployed, endpoints boot directly into a controlled workspace where users access virtual desktops, remote applications, SaaS tools, and browser-based resources. Dual-Boot Deployment lets IT managers install SnapOS alongside Windows or an existing thin client OS on the same device, supporting phased migration without forcing an immediate cutover. SnapOS is designed for the direction enterprise computing is already moving: hybrid work, cloud-first applications, browser-based workflows, VDI/DaaS, Zero Trust security, and distributed operations.

Every endpoint is centrally managed through AmZetta zMAN Director, giving IT teams one console to provision, configure, update, and support the full fleet without touching each physical device. SnapOS reduces endpoint complexity by removing Windows licensing overhead, antivirus subscriptions, routine OS patching, and the larger attack surface of a general-purpose operating system.

Immutable
Read-only OS, no local data stored

Most x86
Bare metal or virtual machine

One Console
Centrally Managed via zMAN Director

02 - WHO IT'S FOR

Who SnapOS is For

IT Managers & Sysadmins
Centrally manage distributed endpoint fleets without adding headcount. Provisioning, policy enforcement, firmware updates, and remote support all happen from zMAN Director, reducing on-site visits and manual patching work.

Budget-Conscious IT Teams
Reduce Windows licensing, antivirus, patching, power, and hardware refresh costs while extending the useful life of existing PCs. SnapOS can also support lower-cost endpoint hardware with modest RAM and storage requirements.

Remote & Distributed Workforces
Deliver a consistent, secure endpoint experience across offices, branches, remote workers, conference rooms, signage, and public-facing kiosks, all from one management plane with the same immutable OS and security posture.

Organizations Running VDI or DaaS
Connect users to Citrix, Omnissa Horizon, Microsoft AVD, Amazon WorkSpaces, Parallels RAS, Leostream, RDS, and browser-based SaaS applications without a Windows OS at the endpoint.

Teams Outgrowing Current Vendor
Move from a dedicated endpoint OS that has become more expensive or restrictive after vendor consolidation. SnapOS provides a direct replacement path with enterprise control, hardware flexibility, and broad VDI compatibility.

Security & Compliance-Driven Organizations
Use an immutable, read-only OS with no local data storage to reduce endpoint risk. Certificate-based access, 802.1X authentication, and SCEP enrollment support secure deployment requirements.

Compatible VDI, DaaS, and Cloud Workspace Platforms

SnapOS is vendor-neutral by design. It works with your existing VDI and DaaS infrastructure no rip-and-replace required.

PLATFORM	SUPPORTED ACCESS METHOD
Citrix Virtual Apps and Desktops	Citrix Workspace app, ICA/HDX protocol
Omnissa Horizon (formerly VMware)	Horizon Client, Blast Extreme and PCoIP
Microsoft Azure Virtual Desktop	RDP, native AVD client support
Amazon WorkSpaces	WorkSpaces client, PCoIP and DCV protocols
Microsoft Remote Desktop Services	Citrix Workspace app, ICA/HDX protocol
SaaS Applications	Integrated lightweight browser, direct web app access

Vendor-Neutral by Design

Users connect to their virtual workspace with a single click from the SnapOS launcher across Citrix, Omnissa Horizon, Microsoft AVD, Amazon WorkSpaces, RDS, and any browser-based SaaS application.

Core Capabilities

Secure, Immutable Endpoint OS
Linux-based, read-only OS with no local data storage. Eliminates the Windows attack surface entirely, reduces persistent malware risk, and supports faster recovery. No antivirus, no patch management, no OS licensing on converted endpoints.

Virtual Desktop & Remote App Access
Native client support for Citrix, Omnissa Horizon, Microsoft AVD, Amazon WorkSpaces, and RDS. Users connect to their virtual workspace with a single click from the SnapOS launcher.

Dual-Boot Deployment
Install SnapOS alongside Windows or existing thin client OS on the same device and boot either OS at startup. Supports a phased migration timeline, or gives users occasional access to native Windows applications without a second device.

Network & Wi-Fi Configuration
Supports wired Ethernet and 802.11 wireless. Configurable for office, branch, remote, and public network environments through centralized policy profiles.

Display & Peripheral Management
Manage multi-monitor configurations, audio output, USB peripheral access, and input device behavior from zMAN Director without touching the physical device.

Firmware & OS Updates
Push SnapOS updates to any number of endpoints simultaneously from zMAN Director. No on-site visits required. Scheduled maintenance windows supported.

Remote Diagnostics & Support
IT teams investigate and resolve endpoint issues remotely via integrated diagnostic tools, reducing help desk workload, on-site service calls, and resolution time.

Hardware Agnostic
Runs on most x86-64 (64-bit); UEFI or Legacy BIOS compatible laptops, thin clients, desktops, legacy PCs, mini form factor devices or inside a virtual machine. If it runs a 64-bit x86 OS today, it runs SnapOS.

Browser & SaaS Access
Built-in lightweight browser delivers direct access to web applications and SaaS tools without requiring a full Windows OS or additional software installation on the endpoint.

Live Boot for Contractors & BYOD
Run SnapOS as a secure live session from a USB drive with no install required. It gives contractors, BYOD users, testing labs, and training environments a locked-down, fully managed workspace that can be provisioned quickly and reset cleanly after each session.

Certificate & 802.1X Support
Certificate-based network access with 802.1X authentication and SCEP enrollment, enabling trusted endpoint access in security-conscious and compliance-driven environments.

Policy & Profile Controls
Apply configuration profiles, security policies, certificates, and compliance controls across individual devices, groups, or the full fleet. Changes propagate automatically on next connection or reboot.

Power & Session Management
Configure power schedules, auto-lock behavior, session timeouts, and reboot workflows to support operational consistency across all deployment environments.

05 - **DEPLOYMENT**

Enterprise Deployment Methods

SnapOS supports multiple enterprise deployment paths, giving IT teams the flexibility to roll out at any scale without disrupting existing workflows.

Display & Peripheral Management
Manage multi-monitor configurations, audio output, USB peripheral access, and input device behavior from zMAN Director without touching the physical device.

USB Install or Live Boot
Install SnapOS directly from a USB drive on individual devices, or run it as a live boot session with zero install footprint ideal for contractors, BYOD users, lab testing, and evaluations.

PXE Boot Mass Imaging
Roll out SnapOS across hundreds or thousands of devices simultaneously using PXE network boot. Devices image automatically on startup with no manual intervention required at each endpoint.

Dual-Boot Deployment
Install SnapOS alongside Windows or an existing thin client OS, preserving the ability to boot into either environment. Supports phased migration, automated Windows-to-SnapOS transition planning, and low-risk cutover timelines.

06 - **VIRTUAL MACHINES**

Virtual Machine Deployments

SnapOS is not limited to physical hardware. It runs inside virtual machine environments, giving organizations the flexibility to deploy SnapOS-powered endpoints where physical devices are not in scope including VDI test environments, virtual lab setups, and hosted workspace deployments.

The same centralized management through zMAN Director applies to virtual SnapOS instances as it does to bare metal deployments. Provisioning, policy enforcement, firmware updates, and remote diagnostics all function identically regardless of whether the endpoint is physical or virtual.

01 - THE COST ADVANTAGE

Lower Total Cost of Ownership, By Design

Extend What You Have. Invest Where It Matters.

Most endpoint solutions reduce one cost while quietly raising another. Windows endpoints carry licensing, antivirus, patch management, and hardware refresh cycles that add up year over year. Dedicated endpoint OS platforms have offered some relief from that, but vendor consolidation in this category has often turned into a different problem: renewal pricing that keeps climbing and platform lock-in that makes switching painful.

SnapOS takes a different approach. There is no Windows licensing on converted endpoints, no antivirus subscription, no routine OS patching, lower endpoint power demand, and no pressure to replace hardware that still works. Because SnapOS is lightweight, organizations can also use modestly configured devices instead of overbuying RAM, storage, and processing power for endpoint access use cases. SnapOS runs on most x86 devices already in your environment, extending their useful life by years. For organizations moving off a legacy endpoint OS, the savings go further still. You get comparable enterprise control at a fraction of what established thin client OS platforms charge at renewal, and the pricing stays predictable as your fleet grows.

That cost efficiency shows up across the industries where SnapOS gets deployed most, including healthcare, education, financial services, manufacturing, retail, hospitality, call centers, and government.

02 - INDUSTRY USE CASES

Where SnapOS Gets Deployed

Healthcare

Patient rooms, nurse stations, and clinical workstations are shared across staff throughout the day. SnapOS delivers a secure, read-only endpoint that keeps patient data off the device, resets cleanly between users, and supports the access controls that compliance-driven environments require. IT manages the entire clinical fleet from zMAN Director without on-site visits or per-device configuration.

Financial Services

Branch banking, trading floors, and back-office operations need secure, consistent access to financial applications with full auditability. SnapOS provides an immutable endpoint with certificate-based authentication, 802.1X network access, and centralized policy enforcement. Sensitive data stays off the device, and IT maintains control across every location from one console.

Education

Schools, universities, and training facilities run shared devices across classrooms, labs, and libraries where students and faculty rotate constantly. SnapOS extends the life of existing hardware, eliminates per-seat Windows licensing, and gives IT a single console to manage every endpoint across every campus location. Students get a consistent, locked-down workspace every time they sit down.

Manufacturing & Logistics

Shop floors, warehouse stations, and inventory tracking environments need endpoints that stay operational across shifts without requiring local IT support, including industrial HMI terminals tied to production systems. SnapOS runs on most x86 hardware including older and ruggedized devices, boots directly into the tools workers need, and stores nothing locally. Firmware updates and policy changes push silently from zMAN Director without interrupting operations.

Retail

Point-of-sale terminals, inventory lookup stations, and back-office workstations all need to be fast, secure, and easy to manage across dozens or hundreds of store locations. SnapOS delivers a locked-down endpoint that protects payment data and customer information while giving IT a single console to push updates and policy changes across every store without a truck roll. Hardware can be repurposed or replaced store by store without disrupting operations.

Hospitality

Hotels and resorts run shared computing across front desks, business centers, and back-office operations where staff and guests both need reliable, secure access. SnapOS keeps guest data off the endpoint, resets business center terminals automatically between users, and lets IT manage devices across multiple properties from one console. The same platform that secures a front desk workstation also runs the back-office systems that keep a property operating.

Call Centers and Contact Centers

High-turnover environments with shift workers and shared workstations benefit from an endpoint that resets cleanly between users and delivers a consistent experience every time. SnapOS provisions automatically, applies the right profile on connection, and requires no local configuration. IT overhead drops significantly and the security risks of shared Windows sessions are eliminated entirely.

Government and Public Sector

Federal, state, and local agencies face strict security mandates, zero-trust requirements, and budget accountability that Windows endpoints struggle to satisfy. SnapOS provides an immutable, air-gappable endpoint with no local data storage, certificate-based access controls, and centralized management across distributed locations. The cost per managed endpoint stays predictable and scales without penalty as fleet size grows.

The Hardware Repurposing Advantage

Extend What You Have. Invest Where It Matters.

Hardware refresh cycles are expensive, disruptive, and often unnecessary. SnapOS installs on most x86-64 (64-bit); UEFI or Legacy BIOS compatible devices in minutes, including laptops, desktop PCs, thin clients, legacy PCs, and mini form factor devices, converting them into secure, centrally managed endpoints.

For budget-conscious organizations, that means existing hardware can stay in service longer while Windows licensing, antivirus subscriptions, and patch management overhead are reduced or removed from the endpoint.

For organizations already using a dedicated endpoint OS, vendor acquisitions often lead to higher renewal costs, reduced flexibility, and greater platform lock-in, making the cost of staying higher than the cost of moving to SnapOS.

500

EXISTING PCS CONVERTED

What This Means for IT Budgets
Converting 500 existing PCs to SnapOS instead of replacing them eliminates the cost of 500 new endpoints while simultaneously removing Windows OS licensing, antivirus subscriptions, and ongoing patch management overhead for those devices.

And for organizations already on a dedicated endpoint OS, moving to SnapOS removes the renewal pricing increases and platform lock-in that often follow vendor consolidation in this category. The endpoint OS cost per device is a fraction of either a traditional Windows or existing thin client OS replacement cycle or a locked-in endpoint OS renewal freeing budget for higher-priority IT initiatives.

Installs in Minutes
On most x86 devices, with no new hardware required

$0
Windows licensing on converted endpoints

No CapEx
On new endpoint hardware required

Managed by zMAN Director

Every SnapOS endpoint, physical or virtual, is managed through AmZetta zMAN Director from the moment of first boot. Available for cloud or on-premises management, zMAN Director gives IT teams complete visibility and control over the endpoint fleet, including provisioning, policy enforcement, reporting, diagnostics, and hardware inventory.

Zero-Touch Provisioning

Endpoints auto-discover the zDM management relay via DHCP, DNS, or mDNS at first boot. Remote and public network devices can be manually provisioned. No IT staff required on-site for either path.

Centralized Policy Management

Profiles, settings, certificates, and firmware updates deploy from zMAN Director to any connected device. Apply policies to individuals, device groups, or the full fleet with a single operation.

WebSSH & NoVNC Remote Access

IT teams access any endpoint remotely via WebSSH

and NoVNC without VPN or physical access from any browser, from any location.

Remote Diagnostics via zDiag

Integrated diagnostic tools let IT teams investigate endpoint issues, review logs, and resolve problems without dispatching field technicians or interrupting users.

Why Organizations Choose SnapOS

IT teams choose SnapOS because it combines stronger endpoint security, simpler management, lower cost, and greater deployment flexibility in one platform. It is not simply another endpoint operating system. It is a new model for enterprise endpoint computing.

SnapOS uses an immutable, read-only OS with no local data storage, reducing persistent malware risk and keeping sensitive data off the endpoint. Utilize Dual-Boot Deployment to install SnapOS automatically alongside Windows or an existing thin client OS, giving users or administrators the ability to boot into either environment. Security is built into the endpoint design, not left to user behavior.

Security Built Into the Endpoint
SnapOS uses an immutable, read-only OS with no local data storage, reducing persistent malware risk and keeping sensitive data off the endpoint. Security is built into the endpoint design, not left to user behavior.

Operational Control at Any Scale
Every physical or virtual SnapOS endpoint is managed through AmZetta zMAN Director. IT teams can provision devices, apply policies, push updates, run diagnostics, and provide remote support from one console.

Hardware and Platform Freedom
SnapOS runs on most x86-64 (64-bit); UEFI or Legacy BIOS compatible devices and connects to major VDI, DaaS, RDS, and browser-based SaaS environments. Organizations keep control of their hardware, workspace platform, and migration timeline.

A Migration Path That Moves at Your Pace
Organizations can fully cut over to SnapOS, run it in a virtual machine, live boot from USB, or install it alongside Windows or existing thin client OS using Dual-Boot Deployment. This gives IT a practical path to migrate gradually without forcing an immediate cutover.

Cost Reduction That Compounds Over Time
SnapOS helps reduce Windows licensing, antivirus, patch management, endpoint replacement, and locked-in renewal costs. The savings grow as more devices move into the managed SnapOS fleet.

Enterprise-Grade Control Without the Complexity
Zero-touch provisioning, centralized policy control, WebSSH, NoVNC, certificate-based access, diagnostics, and firmware updates are managed from one platform. SnapOS delivers enterprise endpoint control without the weight, lock-in, or cost structure of traditional endpoint OS solutions.

System Requirements

CPU ARCHITECTURE	x86-64 (64-bit); UEFI or Legacy BIOS supported
MEMORY	4 GB RAM minimum
STORAGE	8 GB minimum (HDD, SSD, or eMMC)
NETWORK	Wired Ethernet or 802.11 wireless
DISPLAY	Standard VGA, HDMI, or DisplayPort output
DEPLOYMENT	USB installation, PXE network boot, MSI via SCCM/Intune, live boot from USB key, or dual boot alongside Windows or existing thin client OS
VIRTUAL MACHINE	Runs inside VM environments same minimum requirements apply

GET STARTED

See SnapOS Running in Your Environment

Connect with an AmZetta Solutions Engineer for a free 30-day evaluation. No obligation. No pressure. Expert setup guidance included. AmZetta can help your organization evaluate SnapOS on the hardware you already own, in your own environment, with no disruption to existing workflows.

amzetta.com/eval | **Call 1-877-991-1809**

Visit **amzetta.com/eval** or call **1-877-991-1809** to learn more or connect with an AmZetta Solutions Engineer.