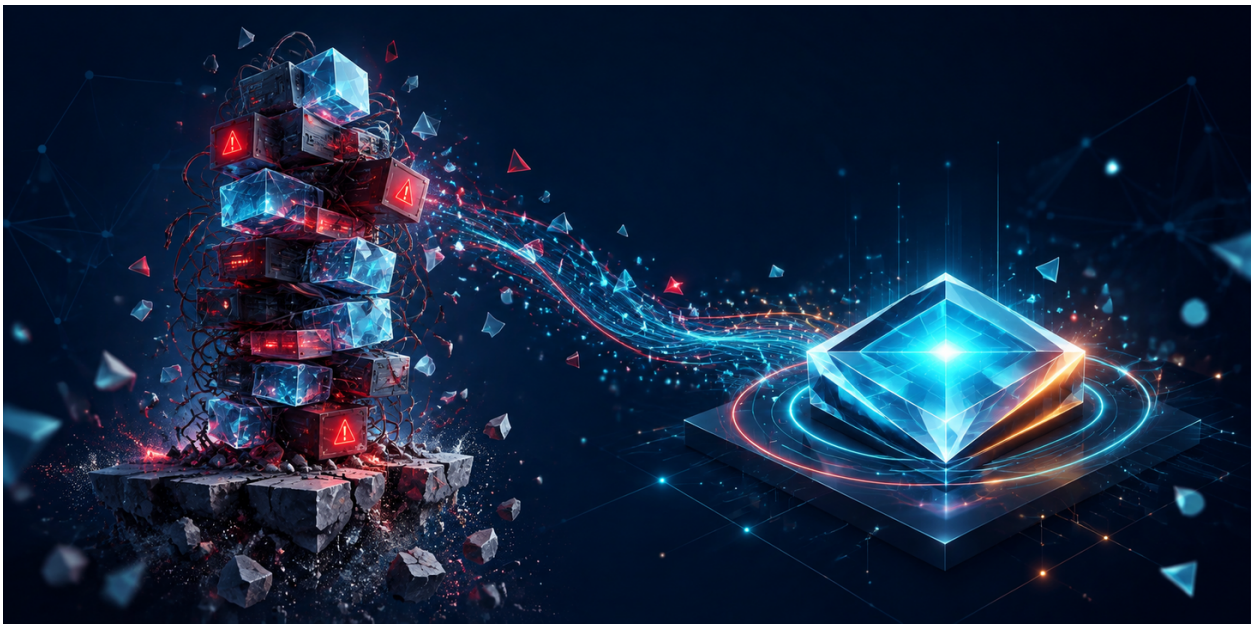

WHITEPAPER

The Hidden Cost of the General-Purpose Edge

Total Cost of Ownership for Securing and Operating Edge Fleets

October 2026

nova8 Technologies

nova8.io

© 2026 nova8 Technologies, LLC. All rights reserved.

Table of Contents

1. Executive Summary
2. How the Edge Tool Stack Accumulates
3. Why the Attack Surface Drives the Spend
4. The Update-Outage Risk
5. The Cost of a Site Visit
6. A Total Cost Model You Can Fill In
7. What Changes with the Container Foundation Platform
8. Questions to Ask Any Edge Platform Vendor
9. How nova8 Technologies Approaches This
10. References

© 2026 nova8 Technologies, LLC. All rights reserved.

1. Executive Summary

> **nova8OS takes cost out of the edge: fewer tools to license, less to defend, no trips to the field.**

Most edge fleets are built the way servers were built twenty years ago: start with a general-purpose operating system, then buy the tools needed to make it safe and manageable. An endpoint security agent. Patch management. Vulnerability scanning. Configuration management. Remote access. Device management. Each one is licensed per device, installed as its own agent, updated on its own schedule, and integrated by someone on your team.

That stack exists to compensate for the base it runs on. A general-purpose operating system ships thousands of components the edge workload never uses, and every one of them is something to patch, scan, watch, and defend. The result is a cost structure that grows with every device and every tool, and a risk structure in which the tools themselves become part of the attack surface and the outage surface.

This paper gives leadership and procurement teams a way to see that cost clearly. It breaks down where the money goes, explains why the attack surface drives the spend, examines the risk that a single tool update can take down a fleet, and provides a total-cost model you can fill in with your own numbers. It closes with the questions to ask any edge platform vendor.

- Fewer tools to license: a platform that combines the operating system, fleet management, remote access, and updates removes several per-device line items at once.
- Less to defend: when the device ships without a shell, a package manager, or a writable root, security spending can shift from detection to prevention.
- Updates that can't take down the fleet: atomic updates with automatic rollback, and no third-party kernel agents, shrink the blast radius of any single change.
- No trips to the field: remote recovery and support remove the most expensive line item in edge operations, the site visit.

© 2026 nova8 Technologies, LLC. All rights reserved.

2. How the Edge Tool Stack Accumulates

A typical edge deployment on a general-purpose operating system accumulates tools in a predictable order. The operating system arrives first. Security asks for an endpoint agent. Operations asks for patch management and a way to reach devices remotely. Compliance asks for vulnerability scanning and configuration baselines. Each request is reasonable on its own. Together, they create a stack that can cost more than the operating system it protects.

Every tool in that stack carries more than its license fee. It needs an agent on every device, compute and memory on hardware that is often small, bandwidth on links that are often expensive, a console that someone must watch, an update cadence that someone must manage, and an integration with every other tool. When the tools disagree, someone has to reconcile them.

For a fleet of a few hundred devices this is an annoyance. For a fleet of thousands, spread across remote sites, it becomes one of the largest recurring costs in the program.

- Endpoint security agent, licensed per device
- Patch management and software distribution
- Vulnerability scanning, run per device
- Configuration management and drift detection
- Remote access and remote support tools
- Device and fleet management
- Disk imaging and recovery tooling

© 2026 nova8 Technologies, LLC. All rights reserved.

3. Why the Attack Surface Drives the Spend

Security tools exist in proportion to what they have to watch. A general-purpose distribution ships an interactive shell, a package manager, broad driver support, debug utilities, and a writable root filesystem, because it was designed for an administrator who installs and changes software over time. On an unattended edge device, each of those is a way in, a place to persist, or a component that will need a patch.

Detection-based security accepts that surface and watches it: agents monitor processes, scanners inventory packages, and analysts triage alerts. Prevention-based design removes the surface instead. A component that was never shipped cannot be exploited, cannot drift, and does not need to be scanned on every device.

The nova8 Container Foundation Platform takes the prevention approach. The host is a single signed, read-only image that runs from memory, with no shell and no package manager. Applications run as containers, isolated from the host. The device returns to a known-good state on every boot. There is far less for an agent to watch, and far less for an attacker to use.

- No interactive shell on production images
- No package manager or in-place software installation
- A single signed image, verified at boot
- A read-only, RAM-resident root that resets on reboot
- Workloads isolated as containers, never installed on the host

© 2026 nova8 Technologies, LLC. All rights reserved.

4. The Update-Outage Risk

In July 2024, a faulty update to a widely deployed, kernel-level security agent caused about 8.5 million Windows devices to crash, by Microsoft's estimate. Many required hands-on recovery, one machine at a time. Airlines, hospitals, banks, and broadcasters were affected. No attacker was involved. The outage came from a tool that was installed to protect those systems.

The lesson for edge programs is not about one vendor. It is about architecture. Any agent that runs inside the kernel runs with the highest privilege on the device, and any update to it can stop the device from booting. On a server in a data center, recovery is painful. On a device in a field cabinet, on a wellhead, or on a vessel, recovery can mean a site visit to every location.

The Container Foundation Platform reduces that risk in two ways. First, there is no third-party kernel agent: if policy still requires a security tool, it runs as a container, outside the kernel. Second, every update is atomic: the new image is written beside the current one and promoted only after it boots and passes health checks, and the device rolls back automatically if it does not.

- No third-party code in the kernel by default
- Updates rolled out in stages across the fleet, not everywhere at once
- Atomic image replacement with automatic rollback
- Recovery that does not depend on someone standing next to the device

© 2026 nova8 Technologies, LLC. All rights reserved.

5. The Cost of a Site Visit

The most expensive minute in edge operations is the one spent driving to a device. A site visit carries labor, travel, downtime for the equipment the device supports, and often safety and access requirements at industrial sites. When the device has no keyboard or screen, the technician may also need to bring their own.

General-purpose systems generate site visits through failed updates, configuration drift that cannot be diagnosed remotely, and recovery procedures that require console access. A platform that is managed from the first boot changes that. Devices are claimed into the Cloud Platform during onboarding, from a phone or a browser. From then on, remote terminal, remote desktop, updates, and health are available over the internet, for one device or the whole fleet.

© 2026 nova8 Technologies, LLC. All rights reserved.

6. A Total Cost Model You Can Fill In

We do not publish industry averages, because the numbers vary widely by sector, site, and contract. Instead, the model below lets you calculate your own baseline in an afternoon. Gather the per-device license costs from your current contracts, the number of site visits from your field service records, and the hours your team spends operating each tool.

Annual cost of the edge stack = devices x (sum of per-device tool licenses + per-device operating effort) + site visits per year x cost per visit + cost of tool-caused outages + compliance and audit effort.

Then fill in the same model for the Container Foundation Platform. Some lines go to zero, some shrink, and one new line appears: the platform subscription itself. The difference is your business case.

- Devices in the fleet: N
- Endpoint security license, per device per year: $
- Patch management, per device per year: $
- Vulnerability scanning, per device per year: $
- Configuration management, per device per year: $
- Remote access, per device per year: $
- Device management, per device per year: $
- Team hours per year to operate the tools: hours x loaded rate
- Site visits per year: count
- Average cost per site visit, including labor, travel, and downtime: $
- Tool-caused outages per year, and their cost: $
- Audit preparation per year: hours x loaded rate

© 2026 nova8 Technologies, LLC. All rights reserved.

7. What Changes with the Container Foundation Platform

Each line of the traditional stack either disappears, shrinks, or moves into the platform itself.

A note on compliance. Frameworks such as NIST SP 800-171 require protection from malicious code (requirement 3.14.2). An immutable, signed host with no way to install software can address the intent of that requirement through prevention rather than a scanning agent. Confirm the approach with your assessor, and keep the option to run an approved security tool as a container where policy requires it.

Early feedback supports the model. In testing, an energy operator told us it expects to stop paying separately for the host security, remote access, and patch management services its current fleet requires.

- Endpoint security agent: prevention by design. Designed so most devices don't need a host security agent; if policy requires one, it runs as a container, not in the kernel.
- Patch management: atomic image updates with automatic rollback, delivered through the Cloud Platform.
- Per-device vulnerability scanning: scan the image once; every device on that version is identical.
- Configuration management: no drift to manage. The image defines the host, and fleet policy defines the rest.
- Remote access tools: remote terminal and remote desktop are built into the Cloud Platform.
- Device management: included from the first boot.
- Site visits: replaced by remote recovery, rollback, and support.

© 2026 nova8 Technologies, LLC. All rights reserved.

8. Questions to Ask Any Edge Platform Vendor

Use these questions to compare platforms on total cost, not just license price.

- How many separate tools and agents does a device need before it is production-ready?
- What runs in the kernel that you did not write, and how is it updated?
- What happens when an update fails on a device no one can reach?
- Can a device be recovered without a site visit or a local console?
- Is every device on the same version provably identical?
- Can vulnerability scanning be done once per image instead of once per device?
- What does the platform include, and what will we still have to buy?
- How does the platform support our compliance requirements without additional host agents?

© 2026 nova8 Technologies, LLC. All rights reserved.

9. How nova8 Technologies Approaches This

The nova8 Container Foundation Platform is nova8OS, an immutable operating system, and its Cloud Platform, managed from the first boot, from far edge to data centers. Customers run their containers, virtual machines, and choice of orchestrator on top.

nova8OS takes cost out of the edge: fewer tools to license, less to defend, no trips to the field.

nova8 Technologies is aligning infrastructure and development practices with CMMC Level 2 expectations. The company holds U.S. Provisional Patent Applications 63/897,352, 63/897,609, 63/903,132, 63/903,161, 63/903,164, and 63/903,168 related to edge computing, security architecture, and operational resilience innovations.

For more information, visit nova8.io or contact the team at contact@nova8.io.

© 2026 nova8 Technologies, LLC. All rights reserved.

10. References

[1] NIST, "SP 800-123: Guide to General Server Security," July 2008, csrc.nist.gov/pubs/sp/800/123/final

[2] NIST, "SP 800-190: Application Container Security Guide," September 2017, csrc.nist.gov/pubs/sp/800/190/final

[3] NIST, "SP 800-171 Rev. 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," requirement 3.14.2, csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

[4] Microsoft Official Blog, July 20, 2024, estimate of Windows devices affected by the July 2024 security agent update outage, blogs.microsoft.com

© 2026 nova8 Technologies, LLC. All rights reserved.