citrix

Centralized desktops vs. managed PCs: A smarter model for control and cost

As organizations contend with remote work, heightened cybersecurity risks, global instability, and increasing financial pressures, business resilience is top of mind.

Against this backdrop, IT leaders face a pivotal choice — either maintain the status quo with distributed, device-centric models, or embrace the transformative power of centralized computing infrastructure.

Organizations are moving away from capital-intensive, on-premises desktop platforms toward cloud-delivered Desktop as a Service (DaaS), where infrastructure is consumed as a service and costs scale with demand. This e-book provides a comprehensive analysis of the Total Cost of Ownership (TCO) for distributed architectures using managed PCs compared to a modern, centralized approach built on DaaS.

The scenario: A modern enterprise at a crossroads

Imagine an organization with 3,000 users utilizing laptops to deliver, collaborate, and innovate. The IT team faces a fundamental decision to either continue with the familiar model of distributed, device-centric management, or embrace a centralized approach, consolidating control and resources in the cloud. While DaaS is well known to deliver secure access to applications, there's a misconception that this model is expensive.

Centralized costs are easy to see, while the true costs of distributed environments remain hidden. In customer discussions and practitioner forums, IT teams frequently cite platform or licensing costs as proof that centralized infrastructure costs more. In practice, much of the real expense of managing thousands of PCs is driven by:

- Multiple security agents per device (EDR, DLP, ZTNA, MFA, email security)
- Frequent hardware refresh cycles and shipping logistics
- Break/fix inconsistencies across aging devices
- Patch testing, orchestration, and rollback across thousands of endpoints
- Ongoing helpdesk and support overhead

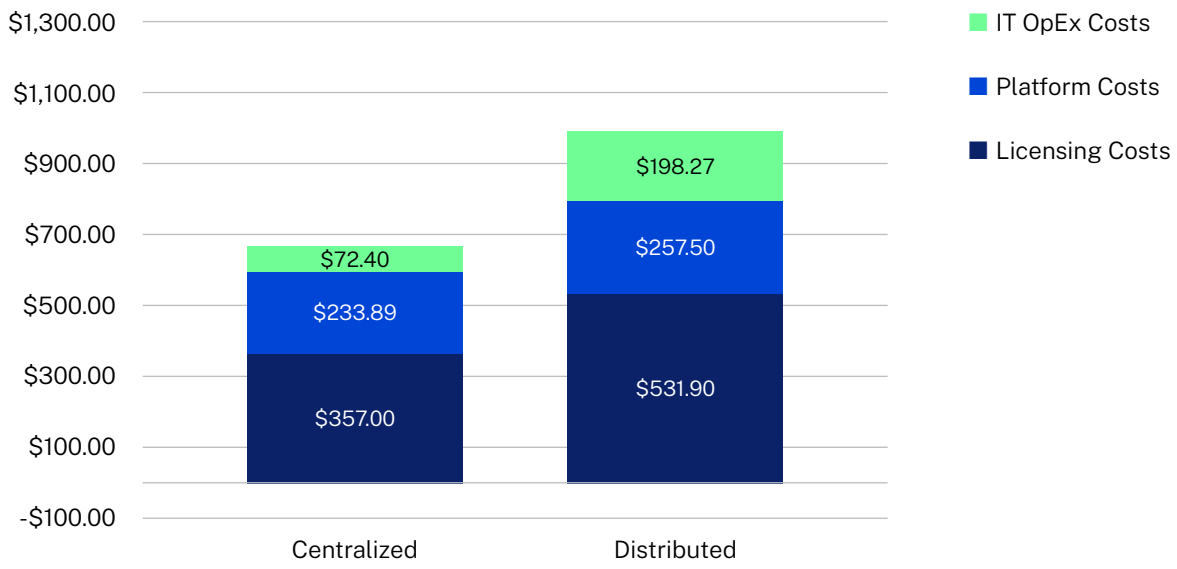
When viewed through a Zero Trust lens, distributed endpoints become the single largest driver of security tooling cost and operational overhead. Centralizing compute, data, and controls flip that model by reducing the attack surface, consolidating toolsets, and enabling platform-level efficiency in a way that simply isn't achievable in distributed architectures.

The cost of ownership: Where the money goes

Methodology: The most pressing question for any IT leader tends to be cost. Our cost model calculates the annual cost of both architectures based on three cost buckets — licensing, platform (compute + hardware), and IT operational expenses. Details on how we arrived at the figures for each category are highlighted at the end of this e-book.

Summary of results: For 3,000 users, the annual cost of supporting managed PCs totals around $3 million. In contrast, a centralized DaaS environment can bring this down to approximately $2 million per year. Over 3 years, the cumulative savings reach around $3 million, resulting in a **33% reduction in the total cost of ownership.**

Centralized vs Distributed - Per user per year



Breaking down the numbers

Licensing

Licensing remains a significant cost driver in both models, but the way those costs accumulate differs fundamentally between distributed managed PCs and a centralized DaaS environment.

In a managed PC model, each device requires its own stack of security and management tools to compensate for a broad, inconsistent attack surface. Application management, extended detection and response, data loss prevention, secure access services, identity controls, and email security are all licensed and maintained per device. While each tool may seem reasonable in isolation, at scale this layered approach becomes a substantial recurring expense — modeled here at approximately **$531.90 per user per year**.

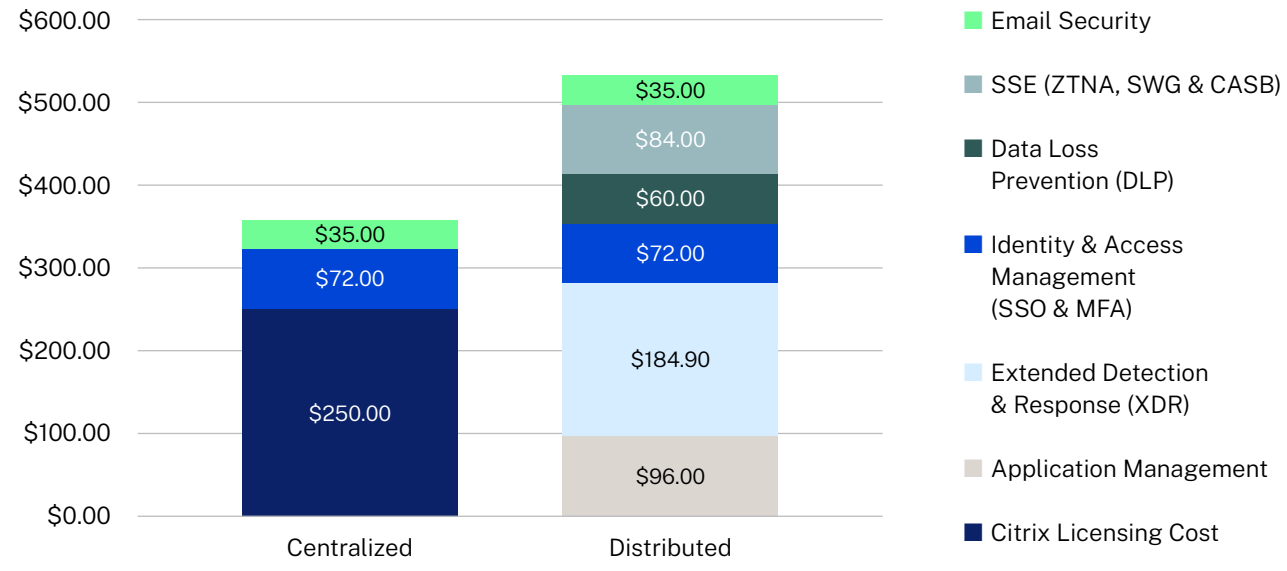
DaaS consolidates much of this functionality into the cloud platform itself. Security, monitoring, and policy enforcement are applied once at the platform level rather than replicated across thousands of endpoints. As a result, endpoints function primarily as access points, reducing the need for multiple device-resident agents and lowering annual licensing costs to approximately **$357 per user**.

> **Gartner has declared hosted PCs are now often cheaper to operate than on-prem laptops, and two years away from being cost-effective for 95 percent of workers.**

Desktop-as-a-service now often cheaper to run than laptops, theregister.com, Aug, 2025

The **$174.90 difference per user** compounds quickly at scale, but the impact goes beyond direct savings. Centralization reduces licensing sprawl, simplifies renewals, and eliminates variability caused by inconsistent configurations and agent conflicts. In practice, DaaS lowers both the licensing bill and the ongoing administrative effort created by device-centric software stacks.

Centralized vs Distributed Licensing - Per user per year



Platform: Compute + Hardware

Platform costs are often the most visible difference between distributed and centralized architectures, and the most frequently misunderstood. The key distinction is not simply where compute runs, but what role the endpoint plays.

In a distributed model, platform cost is embedded in every device. Each laptop is purchased, shipped, configured, maintained, and refreshed on a fixed cycle, creating thousands of independently managed assets that run applications locally, store data, and enforce security controls on the device itself. In this scenario, devices are refreshed every four years at an average cost of $1,000 per unit, resulting in an annualized cost of approximately **$257.50 per user**. While familiar and predictable, this approach scales linearly and locks organizations into perpetual endpoint refresh cycles.

DaaS shifts the execution into a shared, cloud-delivered platform. Compute, storage, and security are no longer duplicated across endpoints but delivered as a centralized service optimized to support hundreds of users per system. The endpoints function primarily as secure access devices. Instead of relying on expensive and fully featured PCs, organizations can standardize on thin clients (TC) that are purpose-built for centralized delivery. In our model, thin clients are refreshed on a seven-year cycle, significantly reducing endpoint churn. When combined with the annualized cost of shared cloud infrastructure, the total cost averages approximately **$233.89 per user per year**.

The result is a platform that appears comparable on paper but enables savings elsewhere. Centralized platforms **reduce operational overhead and hardware dependency, extend endpoint lifespans, and eliminate many of the hidden costs** associated with distributed architectures. In practice, platform costs in a centralized model are the foundation that enables **lower IT operational expenses, improved user experience, and stronger security posture** across the organization.

IT operational efficiency

Platform costs only tell part of the story. The real financial impact of centralization emerges in day-to-day operations. In a distributed managed PC environment, IT operations scale linearly with the number of devices. IT operations must contend with:

- Device-by-device patching and validation
- Testing across countless hardware and OS combinations
- Configuration drift over time
- Failed updates and inconsistent remediation
- Agent conflicts that degrade performance and reliability

The result is IT spends more time maintaining the status quo than improving services or enabling new capabilities. DaaS changes this by centralizing execution into a small set of standardized images and shared services. Updates are deployed once and applied consistently, eliminating repetitive work and reducing operational variability.

The impact is clear in core operational activities. Testing and rollout preparation, which must account for countless device states in a managed PC model, become far more predictable when changes are applied centrally. A centralized cost model realizes a 20% improvement in testing efficiency and a 60% improvement in rollout preparation, reducing both the time and risk associated with application and OS updates.

Centralized operational gains

- **20% improvement in testing efficiency**
- **60% faster rollout preparation**
- **45% reduction in helpdesk tickets**
- **~80% reduction in Mean Time to Patch (MTTP)**

Helpdesk follows the same pattern. Distributed environments generate higher ticket volumes because failures manifest differently across devices and are harder to remediate consistently. Centralized infrastructure reduces these tickets by eliminating endpoint-specific issues and enabling faster, more uniform remediation. Centralized architecture reflects a 45% reduction in helpdesk tickets, freeing IT staff from reactive support work and lowering the cost of ongoing operations.

Patching is another major driver of operational cost. In a distributed model, patching requires coordination across thousands of devices. IT teams spend an average of 40 to 60 hours a week on patch management. Centralization reduces this to a fraction as patching is no longer applied on individual devices but through a single console. **Mean time to patch (MTTP) is slashed by approximately 80%, shrinking both labor cost and operational risk.**

When these efficiencies are combined, IT operational costs fall from approximately **$198.27 per user per year** in a managed PC environment to **$72.40 per user per year** with DaaS — a **reduction of more than 60%**. This is where platform cost discussions come full circle. The centralized DaaS platform is consumed as an ongoing cloud service, enabling IT to operate at a fundamentally different efficiency level and lowering the total cost of ownership.

Operational consistency, security, productivity loss, and business resiliency

Beyond measurable costs, distributed infrastructure increases financial risk by amplifying security exposure, downtime impact, and operational inconsistency — each of which can translate directly into unplanned spend and business disruption.

Operational consistency and compliance

Centralization enhances operational consistency. Instead of navigating a patchwork of device configurations, tool versions, and hardware states, IT manages a uniform platform where updates, policies, and security measures are applied predictably and reliably. This reduces the "unknowns" tied to distributed endpoint fleets and creates a more resilient, tightly controlled environment — one that supports not only lower costs but a stronger overall security and compliance posture.

Security

In distributed environments, every device becomes a potential point of compromise. Applications and data are stored locally, expanding the attack surface and forcing organizations to layer security controls onto each endpoint. This approach can become costly, complex, and disruptive at scale. With DaaS, applications and data are found within a controlled, cloud-based platform and are delivered to endpoints only as a secure display stream. Endpoints no longer store or process corporate data, eliminating entire classes of risk associated with device loss, compromise, or tampering.

Because controls are enforced centrally, policies are applied once and reflected everywhere. Patching, remediation, and rollbacks occur at the platform level, shrinking vulnerability windows and removing the need for many endpoint-resident agents and compensating controls that are required to approximate Zero Trust in a distributed model. The result is a stronger security posture with fewer tools, lower operational overhead, and reduced data leakage risk. Increasingly, this is why organizations are adopting DaaS not only as an end-user computing strategy, but as a foundational component of their Zero Trust security architecture.

Secure enterprise browsers extend this model to web and SaaS applications. Rather than securing the entire endpoint, policies, isolation, and data controls are enforced within the browser itself. This enables Zero Trust access for unmanaged or lightly managed devices while keeping corporate data centralized and protected. Together with DaaS, they allow organizations to apply the right level of centralized security to each workload without reintroducing endpoint sprawl.

Productivity loss: the human factor

Hard costs show up clearly on a balance sheet, productivity loss does not. Yet this is often where distributed architectures quietly create a drag on the business.

In a distributed model, each new hire requires device provisioning, configuration, policy enforcement, and troubleshooting often across multiple teams and systems. With DaaS, IT delivers a standardized and centrally managed workspace, making onboarding repeatable and significantly faster. At scale, faster onboarding reduces the time employees spend unproductive during role transitions and growth periods.

Downtime is another source of productivity loss. Distributed fleets produce device failures and configuration drifts that manifest as outages or degraded access. Centralized architectures reduce both the frequency and duration of outages by enabling remediation once at the platform level rather than across thousands of devices.

Business resiliency

When disaster strikes - be it a poor-quality software update, cyberattack, hardware failure, or natural event - the ability to recover quickly is critical. Centralized architectures simplify backup, replication, and restoration. Instead of orchestrating recovery across thousands of devices, IT can focus on a single, well-defined environment. Failover is rapid and reliable, minimizing downtime and ensuring that business can continue with minimal disruption.

The bottom line

The numbers are clear. Centralized infrastructure delivers up to a 33% cost advantage over distributed models, driven by **lower operational costs, fewer helpdesk tickets, and reduced number of security tools**.

The benefits extend beyond the balance sheet, enhancing security, resilience, and the user experience.

Centralization presents a strong and definitive argument for organizations aiming to maximize efficiency, safeguard data, and enhance employee productivity. In sum, it shifts spending away from distributed, repetitive endpoint work and end user disruption toward a more efficient shared platform.

Ready to quantify the impact?

Connect with your Citrix representative to model cost, security, and operational gains for your environment.

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Headquarters
851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States

citrix

Appendix I: How we arrived at these figures

1. **Licensing**: Licensing refers to the software stack needed to manage and secure users in each model. Managed PC licensing includes application management, extended detection and response (EDR), data loss prevention (DLP), security service edge (ZTNA, SWG, and CASB), multi-factor authentication, and email security. DaaS licensing would only require our subscription fee on top of multi-factor authentication and email security.

2. **Platform (compute + hardware)**: This includes endpoint device costs for both architectures, amortized over their respective refresh cycles. In the centralized model, platform costs also include the annualized cost of shared infrastructure — cloud consumption, storage, networking — allocated across the user population. While centralized platform costs appear higher on a per-user basis, it reflects a deliberate shift from thousands of underutilized endpoints to a shared platform designed for efficiency, resilience, and scale.

3. **IT operational efficiency**: IT operations aggregate the recurring labor and operational effort required to keep environments stable and up to date. In the model, it includes testing, rollout preparation, helpdesk, and patching efforts based on the following factors:

    - Testing and rollout preparation for 30 releases per year: 20% improvement in testing and 60% in rollout preparation with DaaS
    - Helpdesk ticket volume: the savings are mostly driven by a 45% reduction in the number of tickets under a centralized architecture
    - Patching efforts: Centralization significantly reduces patching efforts yielding $12.53 per user per year in patching cost. In the case of distributed architectures that adds up to $62.67 per user per year, assuming the hourly IT FTE cost is $100.

Appendix II: Key assumptions

Number of users	3,000
Cost of a PC	$1,000
PC refresh cycle	4 years
TC refresh cycle	7 years
Shipping	$30 per device
Hourly cost IT fully loaded FTE	$100
DaaS instance	D8s_v5
DaaS workload level	Medium
Monthly egress cost	$0.09 per month
Helpdesk ticket reduction	45% with DaaS (IDC)
Patch management efforts	40 hours spent weekly (Forrester)
TC OS management and deployment	Unicon

Appendix III: Sources

- CFO. Companies' employee turnover rate eased to 18%
- Citrix Blogs. Reduce the duration of your app deployments with Citrix
- Forrester. The Total Economic Impact of Citrix DaaS for Azure
- Gartner. Cost Analysis: Traditional Desktops Vs. Virtual Desktop Infrastructure
- IDC. The Business Value of Hybrid Citrix Infrastructure
- Research and Markets. Thin Client Market - Forecast from 2026 to 2031