3 Reasons Why You Need to Rethink Your Endpoints

Are you just fixing today's endpoint problems when you should be rethinking them?

Does your endpoint architecture give IT greater control, or does it create more work, increase cyber risk, and demand higher costs?

IGEL



Table of Contents

Reason #1: Too Much Time Spent Managing Endpoints 3

Reason #2: Reactive Security Leaves Endpoint Security Gaps 4

Reason #3: Your Hardware Lifecycle Is Being Decided for You 5

Solution #1: Simplify Endpoint Management and Reclaim Valuable Resources 7

Solution #2: Stop Waiting for Patches, Start With a Secure OS 9

Solution #3: Take Control of Your Hardware Lifecycle 10

Your Journey Starts Here 11

About IGEL 12

REASON #1

Too Much Time Spent Managing Endpoints

Does your endpoint work for you or do you work for your endpoints?

IT Managers are hired to transform IT. Too often, time and budgets get consumed by legacy, patch dependent endpoint architecture that forces them to just maintain it.

Your team is talented, but burnout is high when they are tasked with monotonous admin work. What if there was a way to streamline:

- Provisioning and onboarding PCs, laptops, thin clients, etc.
- Patching and routine maintenance on current devices
- Customizing the tools and applications needed for each team or user
- Securing each endpoint to meet compliance and organizational standards

And give your team time back to do their more advanced and strategic work?

On average

53%

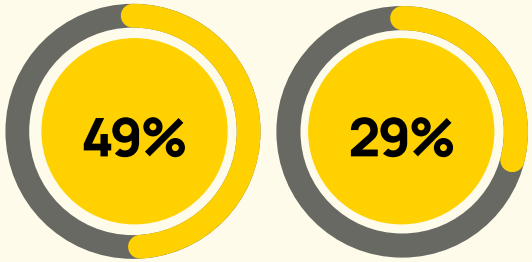
of an IT team's time is spent managing the needs of the endpoint.[1]



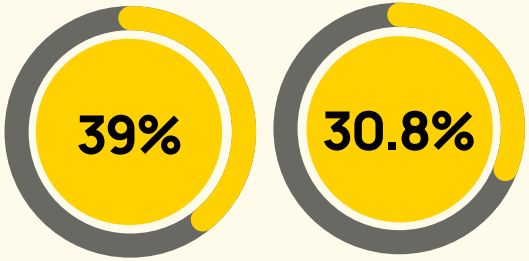
REASON #2

Reactive Security Leaves Endpoint Security Gaps

The reality of your endpoint security is that there are often critical gaps between when known security alerts are issued and when your team applies the patch. Not to mention the potential pre-existing vulnerabilities that your team and tools may be unaware of. Windows accounted for approximately **29%—22 of 75—of the zero-days GTIG originally reported as exploited in 2024.**[2] Waiting for the next security patch is no longer a sufficient endpoint security strategy. Enterprises are shifting toward preventative architectures designed to reduce risk before remediation is required.



49% of organizations use between 5 and 15 endpoint security tools, while another 29% use 16 or more.[3]



In 2025, 39% of vulnerabilities addressed through Microsoft Patch Tuesday were classified as elevation-of-privilege flaws, while 30.8% were classified as remote-code-execution vulnerabilities.[4]



Microsoft saw a 275% increase in ransomware activity over an 18-month period.[5]

REASON #3

Your Hardware Lifecycle Is Being Decided for You

A device can work perfectly well and still be headed for replacement.

Operating system requirements, application changes and support policies can force organizations into hardware refresh cycles before the underlying device has reached the end of its useful life. Across hundreds or thousands of endpoints, that turns a technology decision into a recurring capital expense.

External factors such as chip shortages and supply chain changes can increase the cost of hardware, while organizational budgets set aside for new devices remains the same.

Are you replacing endpoints because the hardware has reached the end of its useful life, or because your software says it has?

However, the problem is not simply the cost of buying new devices. Every refresh brings additional work for IT:

- Evaluating and procuring replacement hardware
- Configuring and deploying new devices
- Migrating users, applications, and settings
- Securely retiring or repurposing existing equipment
- Supporting multiple generations of hardware during the transition

When the endpoint operating model dictates the hardware lifecycle, IT has less control over when and why devices are replaced.

It’s Time for a Secure, Easy-to-Manage, Cost-efficient Endpoint Strategy



SOLUTION #1

Simplify Endpoint Management and Reclaim Valuable Resources

Endpoint management becomes expensive when every device carries its own combination of applications, settings, security controls and maintenance requirements.

A simpler endpoint strategy reduces the amount of work IT has to perform on each individual device. Instead of treating every endpoint like a separate project, organizations can standardize how devices are configured, secured, updated and connected to the applications users need.

The goal is not simply to manage endpoints faster. It is to remove unnecessary work from the endpoint operating model altogether.

Put skilled IT resources back on higher-value work

Reduce the work behind every endpoint

Simplify provisioning and onboarding
Standardize device configurations so new endpoints can be prepared and deployed with less hands-on effort.

Centralize configuration and policy
Manage common settings, security requirements and user access consistently across the environment rather than maintaining devices individually.

Reduce routine maintenance
Minimize the number of local components, applications and dependencies that require continual patching, troubleshooting and remediation.

Standardize application delivery
Give users access to the applications and workspaces they need without requiring every application to be installed and maintained locally on every device.

Reduce overlapping endpoint tools
Simplify the endpoint stack where possible and reduce the operational burden created by multiple management, security and access products performing overlapping functions.

Improve consistency across the fleet
A more standardized endpoint architecture can reduce configuration drift, improve security, simplify troubleshooting and make endpoint behavior more predictable for IT.

Simplify your endpoint architecture to reduce costs and management burden



Reduce costs associated with legacy hardware management and new hardware procurement

Better utilize IT resources

Lower dependence on local software and security tools

SOLUTION #2

Stop Waiting for Patches, Start With a Secure OS

A traditional endpoint is designed to do many things at once. All of which create potential attack paths that must be continually monitored, patched, and maintained. It is complex, always changing, and expensive to secure.

Get better endpoint security by design

The endpoint does not have to be the most vulnerable or difficult to manage point on your network. A preventative security approach rethinks its role in modern IT architecture. An endpoint that carries less software, less local data and fewer moving parts offers less for attackers to exploit, less for IT to patch, and better alignment to Zero Trust.

Does your OS reduce risk across your environment, or does it need excessive time, budget and resources to achieve that?

Preventative Security Principles:

- Reduce the attack surface with an immutable, read-only, endpoint OS
- Minimize local data exposure through SaaS, browser, VDI or DaaS
- Enforce access based on trusted context and Zero Trust principles
- Maintain a known-good endpoint state and prevent persistence and drift with centrally managed configuration and policy



SOLUTION #3

Take Control of Your Hardware Lifecycle

A hardware refresh should happen because a device can no longer meet the needs of the user or the business, not simply because the endpoint software demands it.

Rethinking the role of the endpoint can give IT more flexibility over how long existing hardware remains useful. Instead of requiring every device to run a complex local workspace, applications and desktops can increasingly be delivered through the browser, SaaS, VDI or DaaS, allowing the endpoint itself to perform a simpler role.

Your endpoint strategy should help you decide when hardware needs replacing, not make that decision for you.

Make the workload drive the device decision

Extend the useful life of existing hardware
Continue using capable devices when they can still securely deliver the applications and experiences employees need.

Reduce unnecessary refresh cycles
Avoid automatically tying hardware replacement to every operating system or application lifecycle change.

Match devices to workloads
Give users the endpoint capabilities their work actually requires instead of applying the same hardware standard to every employee.

Repurpose devices instead of replacing them
Give existing PCs and laptops a useful second life when they no longer make sense for their original workload.

Create more flexibility in hardware procurement
Make endpoint purchases based on business requirements, user needs and lifecycle economics rather than software dependency alone.

Your Journey Starts Here

Management complexity, rising device costs, Windows lifecycle pressure, ransomware, cyber-attacks, and modern secure access models are all exposing the same issue: **endpoint strategies that are built around a legacy full feature OS cannot support business resilience in today's disrupted world.**

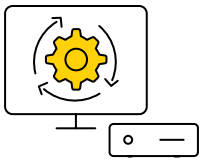
Organizations that rethink the endpoint can provide a better and more secure endpoint user experience for their employees, extend the life of their endpoints and spend less time on device management.



Lower
Management Costs



Better Security
and Lower Risk



Greater Control
of Device Lifecycles

Built on a Preventative Security Model, the IGEL Adaptive Secure Endpoint Platform™ can improve endpoint security, extend the life of existing devices and reduce endpoint management costs by 62%.[6]

- → Reduce the attack surface
- → Prevent persistence and drift
- → Maintain a known-good endpoint state
- → Minimize local data exposure
- → Enforce access based on trusted context

Take back control of your endpoints, your time, and your budgets with IGEL.

Visit IGEL.com to learn more

About IGEL

IGEL is a global software company delivering the Adaptive Secure Endpoint Platform™ for modern digital workspaces and secure access. Through its secure endpoint OS, Universal Management Suite (UMS), and IGEL App Portal®, IGEL enables a Preventative Security Model that helps organizations strengthen security, improve resilience, and centrally govern endpoint access across distributed environments.

The platform delivers the IGEL Adaptive Secure Desktop®, providing secure, reliable access to SaaS, DaaS, VDI, and enterprise applications across distributed environments. Backed by more than 130 validated technology partners, IGEL extends Zero Trust and SASE frameworks to the endpoint. Founded in 2001, IGEL is headquartered in Germany and has operations in the United States.

Learn more at **IGEL.com**

SOURCES

1. Splashtop. IT Teams Spend 53% of Time on Endpoint Maintenance.
2. Google Threat Intelligence Group. 2024 Zero-Day Trends.
3. Enterprise Strategy Group. Endpoint Management Report.
4. 451 Research. Transition from Isolation to Exposure: Evolving Threats to IoT and OT Systems.
5. Microsoft. How Microsoft Defender for Endpoint Is Redefining Endpoint Security.
6. IGEL. How Enterprises Cut Enterprise IT Costs by 62%.

Do you have control of your endpoints or do they have control over you?

→ Contact Us

IGEL is a registered trademark of IGEL Technology GmbH. All hardware and software names are registered trademarks of the respective manufacturers. Errors and omissions excepted. Subject to change without notice. © 10/2026