THINSCALE

C-Suite's Guide to Scalable, Secure Hybrid & Remote Work

DATASHEET

Hybrid & Remote Working

Hybrid working and remote working have become mainstays for modern workplaces. Its adaptive and scalable nature makes it a perfect fit for almost any business continuity scenario, allowing organizations to truly work from anywhere. This datasheet is intended to highlight the benefits and risks of hybrid and remote environments, and how ThinScale can provide scalable and cost-effective secure endpoints that resolve these risks and enhance the hybrid work offering.

The Benefits

Fast Hiring & Scalability

One of the key benefits of remote working is the ability to quickly hire people from any location. Hybrid working maintains this benefit but allows the option of premises for some employees if required. This method of work allows companies to quickly find the exact employee they require from any location, rather than being tied to on singular region.

Reduce Costs

One of the most measurable benefits of adopting a hybrid workforce is the ability to downsize or outright eliminate many of the costs associated with a traditional workforce. Office rent, maintenance, utilities, are all things that are drastically reduced when a company embraces remote or hybrid working.

Increased Productivity

Employee efficiencies while working remotely have been shown to improve substantially. As opposed to working in an office environment. ConnectSolutions' 2022 survey showed that employees working remotely are 77% more productive.

Streamlined Communication

Employees substantially benefit from having their work routines made simple. This is especially the case with many devices they need to use. Limiting the number of devices required to work simplifies their work and promotes productivity.

The Risks

Low Security

In some cases hybrid working can introduce security risks to a corporate network. Malware, outdated applications, or simple employee negligence on their own machines can result in some serious security issues. A hybrid working environment should not be in place without some checks and balances to prevent security pitfalls.

Low IT Visibility & Control

IT has very little control when it comes to work from home devices, often these solutions have little to no management tools involved. The auditing and monitoring of employees' activity on their devices can also be difficult in these scenarios.

Inconsistent Device environments

Corporate devices deployed to remote locations often require re-imaging in order to remain up to date, and for any major changes to occur. Re-imaging, even if a company is able to do it remotely, can take upwards of an hour per machine, which at scale is simply not efficient, compared to how quickly IT departments can update their on-premises machines.

Streamlined Communication

Remote employees should be operating in a similar environment to that of on-premises employees. This is difficult as remote environments are normally managed with different technologies, sometimes the user experience is completely different than those found in corporate environments, leading to a dissonance between on-prem and remote workers.

How ThinScale makes hybrid working possible

ThinScale creates secure workspaces on both company-owned and BYOD machines, on-prem and remote. All with the same, IT curated UI and workspaces, managed by the same management platform. ThinScale allows devices to maintain consistent security standards regardless of who owns the device or where it is accessing corporate resources from. IT have full control over their endpoint environment where they can easily deploy updates, policy changes and troubleshoot remotely.

ThinScale

ThinScale solutions have been built from the ground up to provide security, control, and increased productivity. All while reducing management time and associated costs.

ThinScale allows true work from anywhere by allowing companies to provide secure and compliant endpoints to their employees regardless of location. All easily controlled and managed, making IT's life easier while maintaining stringent compliance standards on the endpoint.

Why ThinScale?

Secure Devices

Provide a locked-down environment for access to corporate resources. ThinScale solutions meet PCI, GDPR, and HIPAA compliance standards at the endpoint. ThinScale also implements advanced security features and policies to ensure a Zero-Trust environment where customer data is secure.

Total IT Control & Visibility

ThinScale solutions are completely monitored and controlled by IT. They can perform no action outside of their IT designated role. IT can also perform in-depth auditing on all devices running ThinScale solutions. ThinScale also allows IT to automate many tedious tasks.

Device checks & uniformity

With ThinScale, IT can be 100% confident of device security, specification, and compatibility. Through initial and ongoing access policy checks & validation – vastly reducing IT workload.

Unified Endpoint Security & Employee Experience

ThinScale provides the same experience and security for remote workers as that of on-premises employees. It does this by enforcing industry-leading endpoint security on any Windows device and providing a pre-set workspace configured by the employer.

Productivity control

ThinScale enforces strict lockdown rules on employees. They are unable to access non-work related applications, websites, or materials while inside the secure workspace. Further, IT can view when and if specific work applications are launched to ensure productivity standards are met.

THINSCALE

Got a question?

hello@thinscale.com