THINSCALE

Securing endpoints for any scenario

DATASHEET

Secure BYOD & Software-defined Thin Clients

Secure Remote Worker and ThinKiosk deliver software-defined secure workspaces that enable existing Windows devices to be repurposed. They also allow employees or agents to securely access their remote environments.

Both solutions were built primarily as security solutions for the endpoint. Secure Remote Worker and ThinKiosk provide unmatched levels of security and have been vetted by two independent assessment agencies: Coalfire Systems and Schellman & Company, meeting the QSAs standards for PCI DSS, HIPAA, and GDPR compliance on the endpoint.

Key Benefits of Secure Remote Worker and ThinKiosk

- Full Device Lockdown
- Prevent Unauthorized Applications & Services from Being Launched
- Secure the Employee's Browsing Experience
- Prevent USB Mass Storage Devices from Being Accessed
- Secure Virtual Machines with Contextual Endpoint Information
- Prevent USB Mass Storage Devices from Being Accessed
- Physical and Contextual Device Security
- Ensure Devices are Protected, Updated, and Monitored
- Centralized Management

Key Benefits

Full device lockdown

Secure Remote Worker and ThinKiosk run on **any Windows device** and **denies employees access to the underlying Windows operating system**, effectively rendering it disabled. Employees can **only access a secure, and IT approved, workspace environment**, ensuring secure connection to corporate resources. Secure Remote Worker and ThinKiosk can even **pass through standard keystrokes** to connected virtual/remote desktops. This ensures components, such as the task manager, cannot be used to get outside of the secure UI. Both products also support **single sign-on**, meaning employees have no opportunity to try and break out of their workspace.

Prevent unauthorized applications & services from being launched

Secure Remote Worker and ThinKiosk's Application Execution Prevention (AEP) and Service Execution Prevention (SEP) add an additional layer of security by **preventing the execution of unauthorized applications and services**. IT admins, employing a **rules-based system**, can configure explicitly which apps and services can run on their endpoint device. These rules allow IT admins to create **white/blacklists** for applications and services.

© Copyright ThinScale 2022, All Rights Reserved. Visit ThinScale.com

Securing the employee's browsing experience

Secure Remote Worker and ThinKiosk both come with an **integrated web browser**. This browser supports a fully customizable user interface that allows agents to securely browse internet sites or access virtual resources via HTML based on policy set by the IT department; all with the full support **of URL white/blacklisting**. The browser is fully compatible with all websites as it uses the browser rendering engines of **Chrome and Microsoft's Internet Explorer**.

Prevent USB mass storage devices from being accessed

USB devices are often seen as one of the **leading causes of security breaches** and data leakage within an organization. Employees can plug in their own USB memory sticks and other write-enabled media devices to copy sensitive data and remove them from the corporate environment. Secure Remote Worker and ThinKiosk's USB Device Blocking feature can **prevent these devices from being used** while **maintaining compatibility with USB hardware** (e.g., headsets) with its USB Device Blocking feature.

Physical and contextual device security

Secure Remote Worker and ThinKiosk can also **prevent the access of virtual/remote resources from unsecured endpoints** using the Virtual Desktop Agent's (VDA) **contextual access rules**. The VDA installs onto any virtual machine/RDSH and performs checks on any machine attempting to access the VM/RDSH. The VDA can be configured to take several actions based on the results of these checks, including **denying access from the VM/RDSH outright if it detects an employee trying to connect from outside a Secure Remote Worker or ThinKiosk session**. The VDA enables full security and control over virtual/remote resources across your entire endpoint environment.

Ensure devices are protected, updated, and monitored

Secure Remote Worker and ThinKiosk proactively check and monitor the security components of the device OS. Vital components, such as **Firewall Protection, Anti-Virus, and Anti Spyware protection can all be monitored and controlled**. If one of these components is not compliant or configured correctly, Secure Remote Worker and ThinKiosk **can take automatic action for remediation**, ensuring that issues are both quickly identified and resolved. **Windows patching can also be carried out** through Secure Remote Worker and ThinKiosk; the solutions can scan all relevant devices connected to the ThinScale Management Platform to detect their update status, and push new patches based on preferences set by IT.

Centralized management

With Secure Remote Worker and ThinKiosk, **IT admins can manage their secure devices remotely** through the ThinScale Management Platform. IT can fully **control their employee's devices, update security policies, and push third-party applications** on the fly, with no need for a deskside visit or dealing with logistics. Through the ThinScale Management Platform, IT can also **pull reports and perform in-depth auditing on all devices within their environment**. IT has both full visibility and control over its employee's machines.

© Copyright ThinScale 2022, All Rights Reserved. Visit ThinScale.com

ThinKiosk and Secure Remote Worker

Both Secure Remote Worker and ThinKiosk are software-defined endpoint solutions designed to secure endpoint devices, ease device management for IT, and to speed up deployment and onboarding. Secure Remote Worker and ThinKiosk were tailor-made for specific use cases such as:

Secure BYOD

Secure Remote Worker

LOG ON/OFF FUNCTIONALITY

Built to provide secure BYOD by allowing the use of personal devices. Installs as a lightweight application that, when launched, will log the employee out of their personal session into a secure "worker" session where they can access corporate resources in a controlled and locked down UI. Once the employee is finished working they simply log out of Secure Remote Worker and return to their personal machine.

DEVICE READINESS AND VALIDATION

With Secure Remote Worker's Validation tool and Access Policy, IT can vet employee's personal devices before Secure Remote Worker is installed to ensure that hardware, software and network security is all up to date and meets company policy.

COMPLETE ACCESS AND APPLICATION CONTROL

Ensure employees are not accessing locally installed corporate resources with Secure Remote Worker you can deny access to any application even when Secure Remote Worker is not running. Ensuring employees can only access corperate resources within their secure workspace. With Secure Remote Worker's Virtual Desktop Agent, users will be unable to access remote/virtual resources from devices not running Secure Remote Worker.

COMPLETE DATA LEAKAGE CONTROL

With Secure Remote Worker's Write Filter you can prevent employees from saving any information while in the secure "worker" session. IT can also apply corporate watermarking as a deterrent.

COMPLIANT PERSONAL MACHINES

Assessed by Coalfire Systems, an independent Cyber security assessor (who also provide assessments for Microsoft, Amazon AWS and VMWare). While active, Secure Remote Worker meets compliance standards at the endpoint level for PCI DSS, HIPAA and GDPR.

Secure Corporate Machines

ThinKiosk

FULL DEVICE LOCKDOWN

The ThinKiosk client on an end user's PC denies them access to the underlying Windows operating system, effectively rendering it disabled. Employees are immediately launched into the ThinKiosk shell from where they can securely access their resources on their corporate machines. Employees are unable to leave the ThinKiosk UI.

DEDICATED SOFTWARE-DEFINED THIN CLIENTS

With ThinKiosk installed, employee's machines are transformed into dedicated thin clients. Securely connecting users to their virtual/remote desktops & applications as well as local resources.

SIMPLIFIED RESOURCE ACCESS

ThinKiosk integrates seamlessly into remote desktop and application environments enabling employees to quickly connect and launch their virtual and published desktops or remote applications. With polices configured centrally, and delivered directly to the end user's software-defined ThinKiosk thin client

FAMILIAR END-USER EXPERIENCE

As part of the overall end user experience, a unique feature of ThinKiosk is Magic Filter. Magic Filter is a dynamic key press pass-through feature that traps the local Ctrl + Alt + Del and Windows + L keystrokes and passes them directly through to the remote environment, just as if the user was working locally on their device.

COMPLIANT CORPORATE MACHINES

Assessed by Coalfire Systems, an independent Cyber security assessor (who also provide assessments for Microsoft, Amazon AWS and VMWare). While active, ThinKiosk meets compliance standards at the endpoint level for PCI DSS, HIPAA and GDPR.

© Copyright ThinScale 2022, All Rights Reserved. Visit ThinScale.com

hello@thinscale.com