




FyrSoft Helps a Government Organization Better Secure and Manage their Remote Work Environment with a Solution Comprising Microsoft Azure and Microsoft Surface Devices

As its technology partner, FyrSoft helped the government organization assess its current security policies and design a solution to configure, secure, and manage its remote work environment. FyrSoft developed a comprehensive solution built on Microsoft Azure's full suite of capabilities and Microsoft Surface devices for its remote employees to enable better device management and monitoring.

Customer Challenges:

Like any government organization, the Georgia OST was looking at several challenges that were only amplified by the COVID-19 situation. At a high level, the business challenges were:








-  Employees going remote and operating from outside their on-premises network
-  Rising budget cuts
-  A need for heightened security posture owing to the nature of sensitivity and confidentiality of business operations

Engagement Scope:

The principal objective of the engagement for FyrSoft was to:

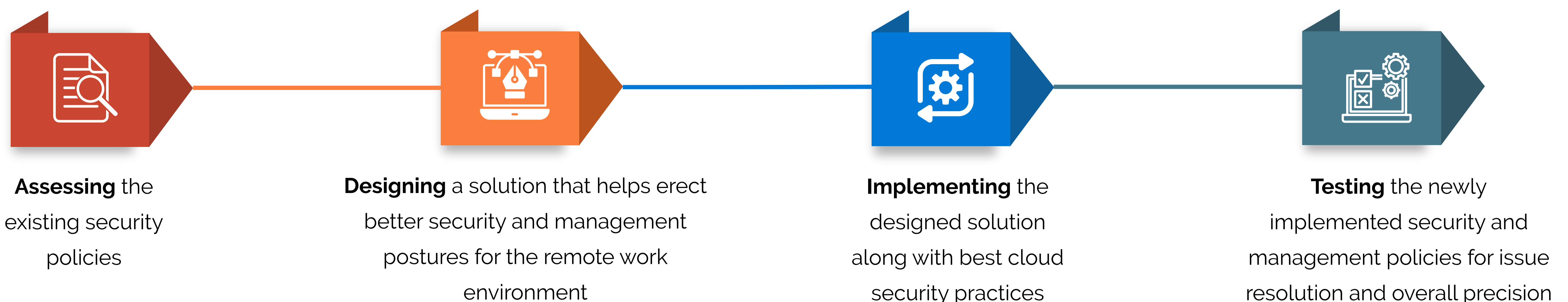
- ✓ Assess and analyze the security posture of customer's current Azure environment
- ✓ Configure features that enable better management and enhanced security of the customer's remote work environment

As part of the scope, FyrSoft leveraged:

-  **Microsoft Surface devices** – as modern endpoint devices to facilitate better device management & monitoring
-  **Azure AD** – for identity management
-  **Multifactor Authentication (MFA)** – with conditional access – to enable user login contingent on predefined conditions
-  **Windows Hello for Business** – for strong, two-factor authentication
-  **Microsoft Intune** – for device compliance policies and secure access to data
-  **Device configuration profiles** – to enable automatic device configurations through Microsoft Autopilot feature
-  **Azure Sentinel** – for reporting that in turn contributes to better decision-making

Solution Approach:

FyrSoft devised a schematic approach to help the customer that goes as:



Customer Overview

Industry:

Government

About:

The Office of the State Treasurer is responsible for the disbursement of state funds, and the management of the state's cash resources. OST generates monthly cash flow for the Governor's Office of Planning and Budget.

Objective:

To assess the current security policies & posture of the customer to develop a solution that would help configure, secure, and manage remote work environment directly from the cloud to enable a secure and productive remote work experience for its users

Solution:

The solution involved assessing current management policies in Azure Active Directory and Microsoft Intune. This also included enabling FIDO2 security key login for Windows Hello for Business. Microsoft Surface devices were leveraged for remote employees to allow direct shipment, configuration, security, and management from the cloud without IT intervention; to support the 'remote work' environment the customer wanted to establish.

Results:







Our solution allowed the customer's remote users to securely access business applications and data through their Microsoft Surface devices that can be remotely managed and monitored. The environment was secured by Azure's full suite of compliances and policies.

“For us, security is everything. We oversee some \$20B USD for the State of Georgia annually, so we have to be secure,”

- Craig Cannon, an Infrastructure Security Engineer at the Georgia OST

Our Solution:

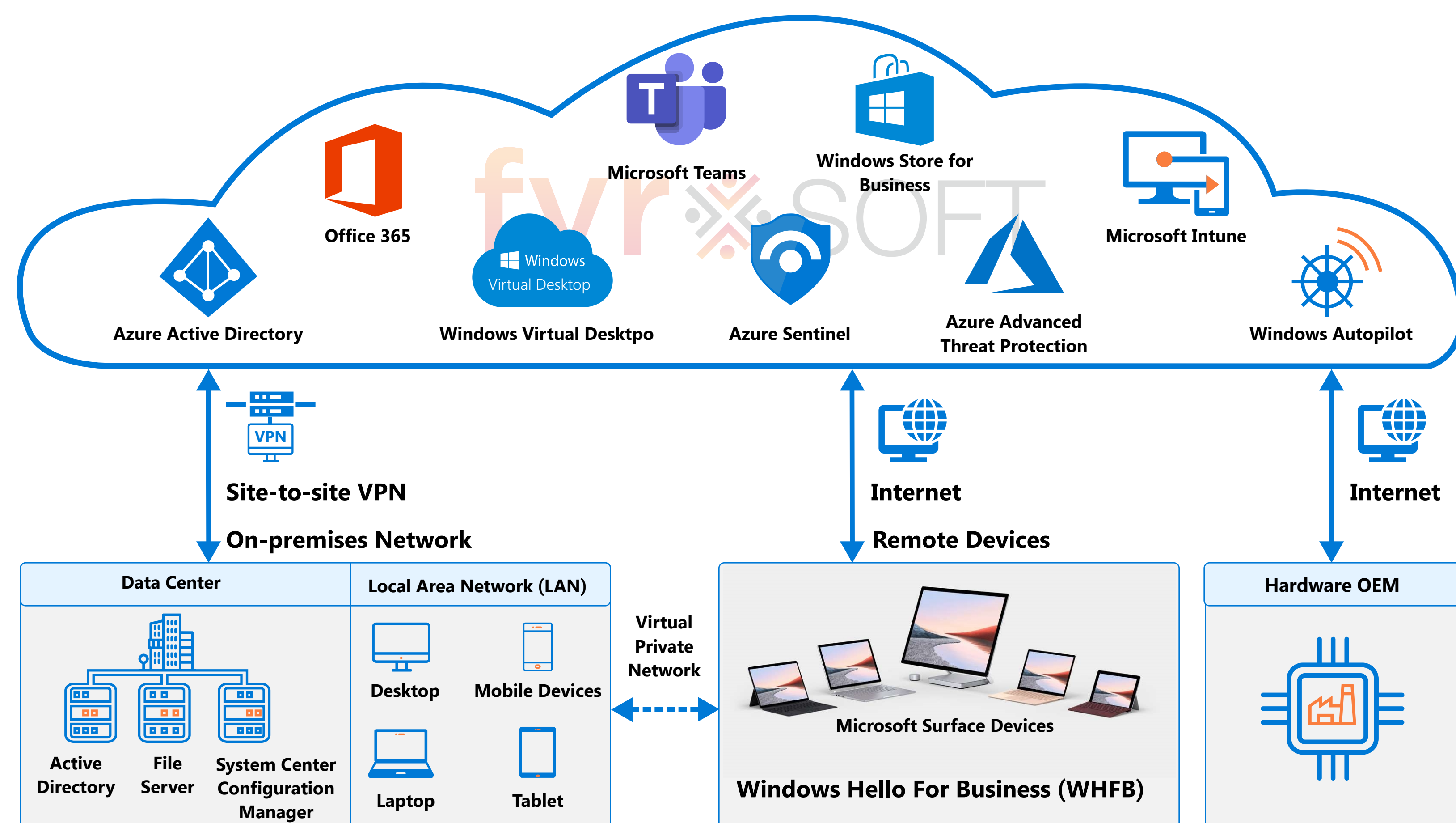
FyrSoft's solution involved:

-  Commissioning Microsoft Surface devices as endpoint devices for remote employees for better modern device management practices
-  Assessing customer's existing security policies, configurations, and settings on Azure such as Multifactor Authentication, Microsoft Intune Device Compliance, etc.
-  Designing a solution by juxtaposing customer's existing policies with Microsoft recommended practices and settings
-  Implementing the designed solution by closely working with the customer
-  Testing the implemented solution by creating test groups to verify the new policies for Microsoft Intune, Multifactor Authentication, while enabling FIDO2 security key login access with Windows Hello for Business
-  Configuring Autopilot for newly procured Microsoft Surface devices to ensure that users need little to zero assistance in enrolling their devices on Microsoft Intune

“With Microsoft being at the forefront of what we were doing, we wanted to continue to work with them to take advantage of their tools and technology to simplify our operations and ideally lower costs.”

- Bill Wyatt, CISO and CIO at the Georgia OST

Architecture Overview of the Solution:



Business Takeaways:

- ✓ Customer enabled to procure and directly ship Microsoft Surface devices to end users without having their IT intervene to configure security and device management policies
- ✓ Multifactor Authentication helped enhance security for remote users' devices
- ✓ Enrolled MS Surface devices were configured to automatically register with Azure Active Directory to enable Hybrid Management
- ✓ The solution allowed the customer carry out rapid provisioning and de-provisioning of users
- ✓ Direct management of MS Surface devices made possible from the cloud without the need for a VPN

fyrSOFT – Highlights

Microsoft Gold Certified Partner

Customers from Fortune 1000 Quadrant

300+ Man Years of Consulting Experience

150+ Man Years of Microsoft Systems Management Expertise

“The trusted chip, the fact that Windows Hello uses biometrics and facial recognition every day I log in. I am totally sold on the Surface.”

- Craig Cannon, Infrastructure Security Engineer at the Georgia OST

To know more about FyrSoft's offerings, please visit:

<https://fyrsoft.com>