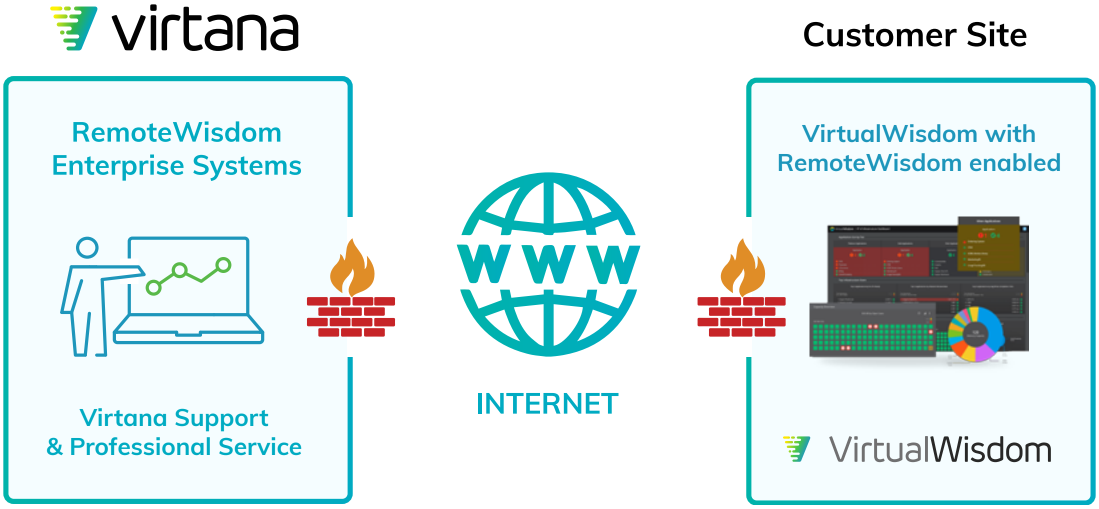
virtana

White Paper

RemoteWisdom Access Platform Security

Benefits of RemoteWisdom

RemoteWisdom enables Virtana Service and Support staff to securely access your VirtualWisdom Server remotely. This connection allows Virtana to monitor your devices and provide you with fast and efficient service.


virtana
Customer Site
RemoteWisdom Enterprise Systems
Virtana Support & Professional Service
WWW
INTERNET
VirtualWisdom with RemoteWisdom enabled
VirtualWisdom

Overview

The Virtana RemoteWisdom Access Platform includes a suite of products that allows our highly trained Service and Support staff to exclusively and securely access your VirtualWisdom Server remotely. This connection allows us to monitor your VirtualWisdom infrastructure and provide you with fast and efficient service, without the need to schedule an on-site visit, thus maximizing your uptime and operational continuity.

The RemoteWisdom Access Platform uses the same technology found today in highly secure environments such as government, banking, health care, data centers, and manufacturing environments.

The RemoteWisdom Access Platform consists of the following components, which address the strictest of security and privacy requirements.

- RemoteWisdom Gateway
- RemoteWisdom Enterprise System

RemoteWisdom Gateway

The RemoteWisdom Gateway resides on the VirtualWisdom Server installed at your site and is built on patented Firewall-Friendly™ communication technology that allows it to exchange information securely with our Enterprise servers, even when protected behind firewalls and proxy servers.

The RemoteWisdom Gateway achieves this secure exchange by initiating all communications with enterprise servers. This method of communication:

- **Leverages existing security infrastructure at the VirtualWisdom Server location.** The Gateway receives the same network security coverage as all other computers within your facility.
- **Secures the Gateway from attack.** Because the Gateway initiates all communication, and only with our Enterprise servers, it does not have a public IP address and is therefore not publicly accessible or subject to exploitation.

The RemoteWisdom Gateway encrypts all communications between your VirtualWisdom Servers and our secure Enterprise System by using Transport Layer Security (TLS).

The RemoteWisdom Enterprise System

The RemoteWisdom Enterprise System encompasses the full set of tools that our Service and Support staff uses to monitor and maintain your devices for maximum uptime and operational availability. These tools reside in a highly secure environment and are accessible only to our employees, following industry standard security measures.

Access to RemoteWisdom Enterprise System applications is limited exclusively to our highly trained Service and Support staff and requires username and password authentication. User access security is addressed in two ways:

- Activity-based access control
- Device-based access control

Activity-based access control limits our staff to accessing only the application functions that are required to complete their specific roles. Device-based access control limits our staff to accessing only the customers and devices that they are required to support. This combination of access controls provides a maximum level of security and auditing.

The RemoteWisdom Enterprise System encrypts all communications between its servers and our Service and Support staff by using TLS technology to provide secure transmission of data. Data is encrypted in transit using HTTPS/TLS (Transport Layer Security).

For most of our connections, the content of the messages is further secured using Advanced Encryption Standard (AES) 128 algorithm, and the RSA 2048 algorithm is used for key exchanges. Data uploads are also encrypted through SSH tunnels or VPN. These security measures protect all operational device data from being susceptible to unauthorized access while it is in transit and creates a complete end-to-end secure communication path.

The RemoteWisdom Enterprise System requires our Service and Support staff to log in again after ten minutes of inactivity. This inactivity period logout ensures greater confidentiality of secure device information.

The RemoteWisdom Enterprise System maintains extensive audit logs of all user access requests and all application functions performed on your devices. These audit logs provide extensive reporting capabilities and allow us to ensure complete accountability for staff activities. Examples of audited functions include:

- User logins
- Remote access sessions
- Trigger creation or modification

Certifications from our provider PTC

- PTC has the following security certifications:
- Federal Risk and Authorization Management Program (FedRAMP): U.S. government program to assure standardized approach to security for cloud products and services
- DOD Information Assurance Certification and Accreditation Process (DIACAP): Formal management process to assure security for all DOD information systems
- SSAE-16 (SOC 2 Type 2): Standard annual reporting for U.S. publicly traded companies to ensure physical and environmental security for data centers
- Conform to International Organization for Standardization (ISO) 27001:2013 standards
- ITAR compliant

The RemoteWisdom Access Platform system has been designed to leverage the power of the Internet while ensuring that the data handled by the system is protected. As new security standards and practices continue to evolve, we will assess them for possible incorporation into the RemoteWisdom Access Platform.

Learn more about VirtualWisdom

Contact a Virtana Expert

View more Resources

Virtana
2331 Zanker Road
San Jose, CA 95131
Phone: +1.408.579.4000