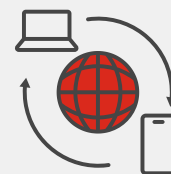**FORTINET**

Secure Remote Access for OT Systems with Fortinet FortiSRA

Executive Summary

Operational technology (OT) organizations across many industries are using technology to transform their business activities and processes. To increase operational productivity and efficiency, traditionally siloed systems are now connecting to untrusted networks like the internet and cloud. But these benefits can lead to increased risks as well. Providing remote access to third-party contractors and remote employees also presents a unique challenge because granting privileged access to OT systems that are unable to have security endpoint agents deployed leaves the network vulnerable to misuse and other insider threats.

Fortinet FortiSRA helps OT organizations implement secure remote access (SRA), mitigating the risk associated with maintaining external access to critical OT resources. It manages user access and privileges and monitors, logs, and records user activity during remote sessions. FortiSRA also helps ensure uptime for SRA services through high availability (HA) and active/standby HA capabilities. It supports privileged access management features that control user accounts with elevated privileges and manages access and permissions for remote users, accounts, processes, systems, and sensitive data across the OT infrastructure. FortiSRA also provides gated access to sensitive OT resources within an organization with end-to-end management of remote accounts, control of privileged user access, and visibility into account usage with monitoring and audit capabilities.

According to a Fortinet global survey, 54% of more than 560 OT professionals use secure remote access.[1]

The Need for Secure Access to Critical Systems

OT enables factories, power generation, and transmission facilities, public transportation networks, oil and gas facilities, and utilities to function. These critical products and services operate using technologies such as industrial automation and control systems (IACS), including distributed control systems and supervisory control and data acquisition systems (DCS/SCADA). It's important for OT organizations to have a business continuity plan in place, and FortiSRA can help securely support remote work and maintain business continuity.

Remote users in OT organizations, such as third-party contractors and remote employees, are often granted access to critical systems. This access includes elevated privileges and credentials to manage site operations, machinery, network infrastructure, SCADA, and human-machine interface (HMI) systems. Having a flexible way to grant and revoke remote access, as well as rotate privileged credentials, can help OT organizations implement secure policies of least privilege and reduce their organizational risk and overall attack surface.

Complicating the need to secure remote users, OT organizations often include devices that are too resource-constrained for an endpoint security software agent. Or company policies may not allow vendor agents to be installed. In either case, OT admins are not able to secure remote access with agent-based solutions.

Protect OT Networks with FortiSRA

FortiSRA helps protect OT networks against remote access threats with advanced management and security capabilities that provide enhanced network visibility and control. FortiSRA uses a web browser extension deployed on remote user clients to provide secure remote access.

Secure remote access

Privileged accounts demand careful management due to their access to critical OT resources. FortiSRA addresses this need by ensuring that end-users, including third-party contractors, are granted access to essential resources based on assigned roles, such as standard user or administrator, while consistently adhering to the principle of least privilege. FortiSRA provides full control over resource secrets through centrally defined policies, including the option for automatic password changes upon check-in. OT organizations can also use FortiSRA to implement a hierarchical approval system and regulate potentially risky commands.

Remote access comprises two of the seven MITRE ATT&CK most common lateral movement techniques in industrial control systems, including Exploitation of Remote Services and other remote services methods.[2]
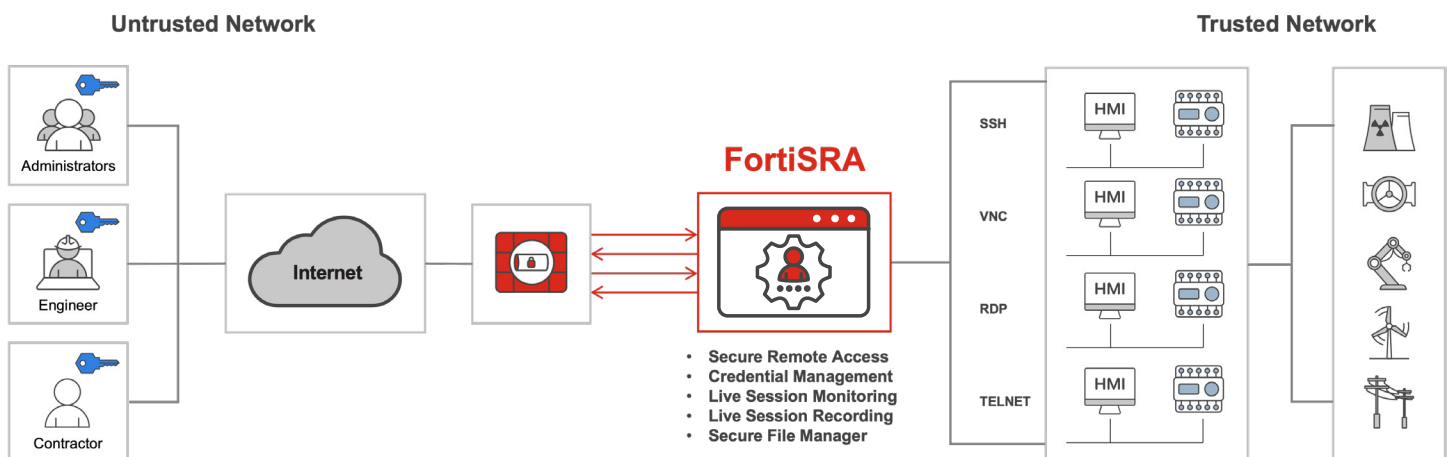
Privileged account management

Maintaining security and operational resilience in OT environments requires effective management of privileged accounts for both users and third-party contractors. FortiSRA offers a comprehensive solution that goes beyond just credential storage. It automates the entire life cycle of privileged accounts. It facilitates automatic password changes based on predefined policies, reducing the risk of unauthorized access and addressing the challenge of orphaned accounts or outdated credential policies for both internal users and external contractors. FortiSRA also assumes control of the privileged credential vault for specific resources, eliminating the need for users and contractors to directly interact with sensitive credentials and mitigating the potential for credential exposure. By ensuring that sensitive, privileged account information is not transmitted to end-user devices, FortiSRA strengthens the organization's overall security posture. It helps effectively maintain operational continuity and safeguard critical infrastructure systems.

Remote session monitoring and recording

It's crucial for OT organizations to provide monitoring capabilities for users, especially third-party contractors who need to access highly sensitive resources remotely. FortiSRA offers reporting of privileged account usage in the event of a security incident. It also provides full-session video recordings to capture user activity on critical OT systems, including keystrokes and mouse events. FortiSRA also offers comprehensive tracking of privileged accounts and target system usage when required for audit purposes.

Untrusted Network

Administrators

Engineer

Contractor

Internet

FortiSRA

- Secure Remote Access
- Credential Management
- Live Session Monitoring
- Live Session Recording
- Secure File Manager

SSH

VNC

RDP

TELNET

HMI
HMI
HMI
HMI

Trusted Network

Protect Against Remote Access Threats

Because OT organizations provide critical products and services, it's particularly important for them to be protected against remote access threats and to have a business continuity plan in place. FortiSRA can enable these organizations to:

- Securely support hybrid and remote work for employees
- Securely leverage the expertise of remote third-party contractors
- Maintain business continuity
- Enhance file security
- Protect remote users against content-based malware

Fortinet FortiSRA provides advanced secure remote access for OT organizations to securely support remote and hybrid work for employees and remote third parties. FortiSRA requires no endpoint software agent to operate, simplifying deployment and providing the necessary secure remote access solution for organizations working to transform their OT networks.

[1] Fortinet 2024 State of Operational Technology and Cybersecurity Report

[2] MITRE ATT&CK tactics, Lateral Movement

F⊟RTINET

www.fortinet.com