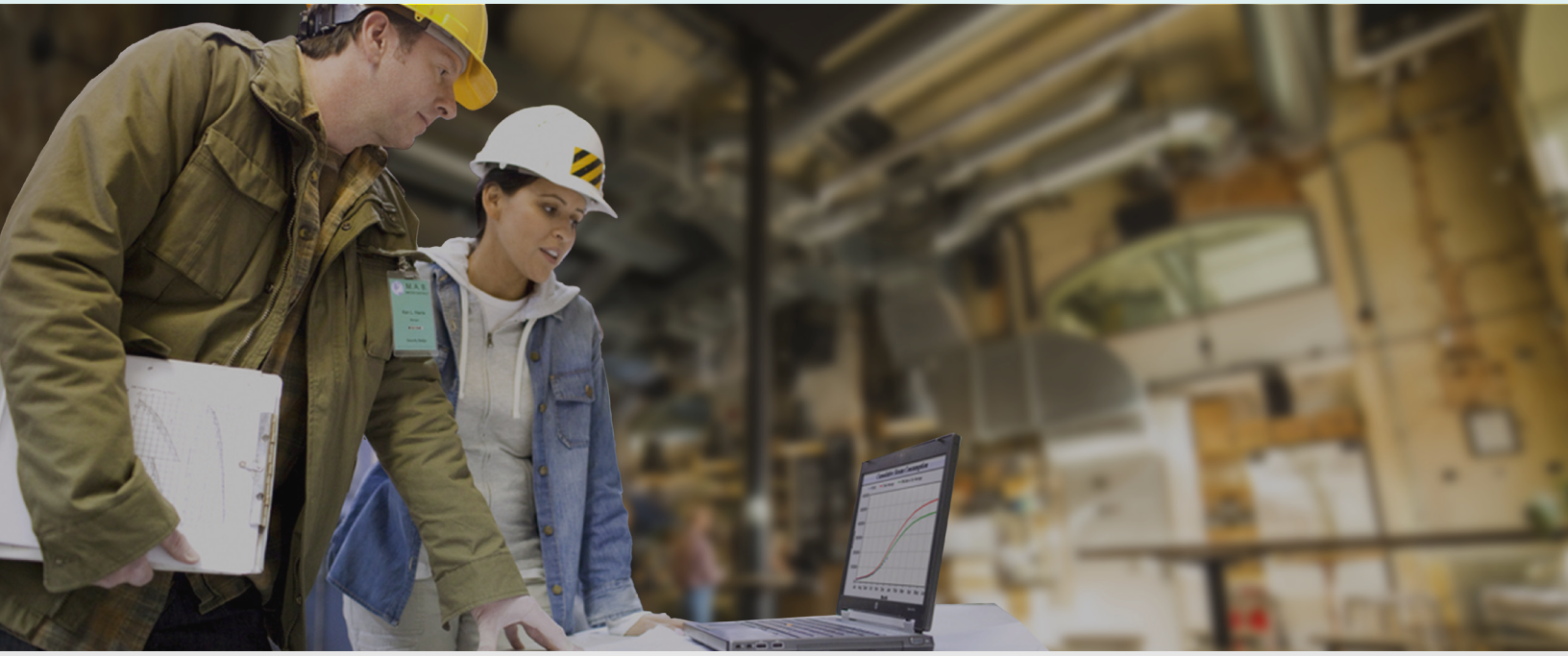
Securing OT Remote Access

Sure Access Enterprise for OT Risk Remediation



Background – The OT Remote Access Cybersecurity Risk

Operational Technology (OT) is critical to the safety and availability of mission critical processes in industries such as manufacturing, utilities and oil & gas. OT and ICS control elements such as HMI and SCADA terminals often have Internet connectivity to administer remote maintenance functions. Although these connections help companies enable third party support and increase the efficiency of their field technicians, they are the perfect entry point for attackers attempting to access the OT domain.

OT Internet remote access creates significant cyber-risk: the connections bypass security controls and allow an attacker direct access to the OT infrastructure. The risk is increased due to remote administration being performed by an OT support firm or equipment provider. This makes it difficult to assess the trustworthiness of the remote user or system.

The potential impact from a compromised remote access session is significant. For example, if the PC used for remote access has been infected by malware, the attacker can use the remote access session to infect the OT environment. From there, they can spread across the OT and IT networks, establish a persistent presence, modify OT system configurations, steal data, and worst of all, impact operational availability and safety.

In summary, OT remote access requires strong security controls to achieve a "secure-by-design" environment that reduces risk associated with compromise of HMI and SCADA systems.

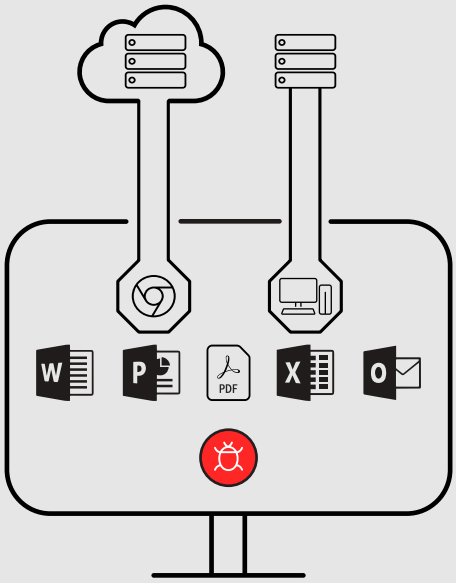
EXAMPLE OT REMOTE ACCESS ATTACK: FLORIDA WATER TREATMENT PLANT HIT BY CYBER ATTACK

In 2021, a hacker exploited a remote access connection to an ICS system at a water treatment plant in Florida, USA. They briefly increased the sodium hydroxide level in the water to 100 times the normal amount. The attack was only thwarted because a vigilant employee saw the attack in progress and was able to stop it. Because the ICS system wasn't configured to be secure-by-design, the attack was relatively easy to execute.[1]

HP Sure Access Enterprise – Remote Access Risk Mitigation

Sure Access Enterprise[2] (SAE) is a hardware-enforced software solution designed specifically to secure remote access activity, such as connecting to support OT infrastructure. SAE is installed on PCs used by remote technicians for OT remote access, and supports all common access protocols:

Web	RDP	Citrix ICA	SSH



SAE applies "zero-trust" principles to the remote PC. It assumes the worst: that PC might have been hacked and infected with malware. To keep an attacker from compromising the remote access session even in this case, SAE builds a tight "virtual wall" around each remote access application initiated from the technician's PC. The protected space is enforced by the PC's CPU hardware, so malware can't get around it. Even if the PC is infected, the attacker can't do any of the following:

- Intercept or inject keystrokes
- Capture display contents
- Access memory, execution or I/O state

With SAE's unique approach, the risk of a successful attack via an OT remote access session is greatly reduced.

SAE – Flexible Deployment Options and Integrations

Sure Access Enterprise is built for flexibility and ease of operations. A cloud or on-premises centralized management console handles policy definition and monitoring. Policies are created centrally and distributed securely to all workstations. The policy definitions for privileged activity can be customized on a per-app basis, and are locked down with strong encryption and authentication. Multiple privileged access sessions can be supported simultaneously on each technician's PC.

Integrations and interoperability are essential for any security architecture. SAE co-exists with multi-factor authentication used by OT systems. It's also compatible with Privileged Access Management (PAM) solutions that are often used for management of privileged credentials. Alerts can be sent to a SIEM for centralized event management.

FLEET-WIDE THREAT CONTAINMENT - SURE CLICK ENTERPRISE

HP offers Sure Click Enterprise[3] (SCE) to compliment SAE for broader threat containment. SCE is designed as a general-purpose endpoint security solution that provides protection above what's available from NGAV and EDR offerings. While SAE is targeted at privileged remote access, SCE is deployed across an entire PC fleet to protect against social engineering attacks such as phishing and ransomware.

Sure Access Enterprise for OT Remote Access: Solution Benefits

Unlike almost all endpoint security products, SAE is purpose-built to secure remote access to critical systems. It starts with the premise that the "known important" activity must be protected from everything else, turning the normal endpoint security paradigm on its head.

Sure Access Enterprise delivers benefits across all three key areas:

EXAMPLE USE CASE: WATER TREATMENT FACILITY HMI/SCADA

HMI/SCADA systems in water treatment plants are the control point for chemical additives such as chlorine. Too much or too little chlorine can cause serious public health hazards. This means that there is an urgent need to protect these HMI/SCADA systems against unauthorized access and malware attacks, as these systems often have unpatched vulnerabilities.
An analysis of recent attacks confirms that Sure Access Enterprise and Sure Click Enterprise prevents such attacks from exploiting such vulnerabilities, helping keep the plant operational and the public safe.

RISK MITIGATION

- Hardware-enforced micro-virtualization keeps OT assets safe
- Full audit trail of privileged access to support primary or compensating control

USER EXPERIENCE

- Single workstation can be used for OT remote access, as well as other tasks, without worrying about cross-domain attacks
- Transparent to remote access applications; consistent operational experience across remote access protocols
- Portability across workstations: policies can be moved securely across PCs

EFFICIENT SECURITY OPERATIONS

- Single workstation for all user activity
- Centralized policy control & distribution
- No need to physically touch remote access PCs to support them
- Effective visibility and monitoring

Summary

OT remote access activity creates significant risk to operations availability and safety. Sure Access Enterprise is an innovative secure-by-design solution that prevents attackers from using a remote technician's PC to access critical OT systems. Because the solution helps organizations across all three key dimensions of IT efficiency, user experience, and security, SAE should be strongly considered for all OT environments.

CHOOSE HP BUSINESS PCs FOR GREATER SECURITY

SAE supports both HP and non-HP PCs. However, for the highest level of assurance, organizations should consider HP business-class PCs. These secure the underlying platform, with additional security at the hardware and BIOS levels. These devices provide a highly resilient platform for all applications and data, including OT remote access.

[1] Industrial Defender, Florida Water Treatment Plant hit with Cyber Attack, Feb 2021.

[2] HP Sure Access Enterprise is sold separately. For full system requirements, please visit System Requirements for HP Sure Access Enterprise for details.

[3] HP Sure Click Enterprise is sold separately. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed. For full system requirements, please visit System Requirements for HP Sure Click Enterprise for details.

4AA8-2073ENW, October 2022