Discover assets, secure access, and get threat intelligence for OT

Joint Solution Brief

Operational Technology (OT) Security Challenges

Operational technology (OT) infrastructures are converging with IT, as these once closed OT environments adopt modern technologies to become more efficient. As a result, they are more open to new cyber risk.

A more IT driven OT environment increases the attack surface and allows bad actors to exploit infrastructures that were not built with cybersecurity in mind.

Connected IT/OT systems open opportunities for direct cyberattacks, as hackers are quick to identify unsecured industrial control systems (ICS) targets from infrastructures.

Discovering all ICS/OT assets, applying threat detection/analysis and ensuring assets are accessed - locally and remotely - in the most secure way possible, are all crucial elements in OT Infrastructure protection.

This is why we at SSH Communications Security (SSH) and at SCADAfence have joined forces to bring our security expertise for OT infrastructures under disruption bringing asset discovery, threat detection and access at industrial scale in one solution.

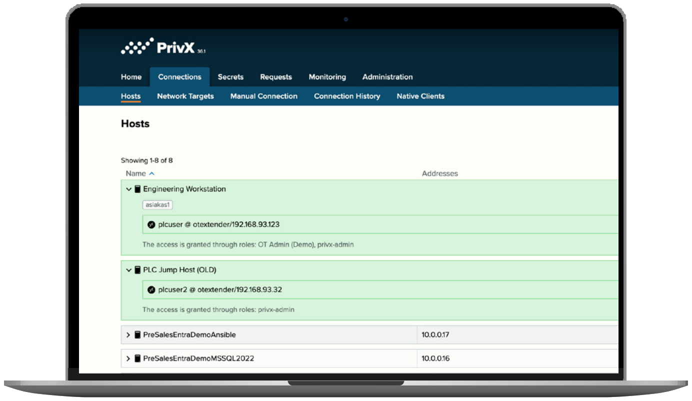
SSH and SCADAfence bring (OT) intelligence and industrial scale secure access across your IT/OT organization into a single solution. Protect ICS from unauthorized, indiscriminate and always-on access while streamlining workloads, getting prioritized alerts with meaningful context, and monitoring your OT environment.

Joint Solution

Integrating SCADAfence and SSH OT products offers organizations enhanced visibility, security, and control over OT environments with monitoring, asset visibility, and anomaly detection. This allows organizations to detect security risks, vulnerabilities, and unauthorized access to OT networks as well as provide secure, role-based access to critical OT systems without a need for passwords.

This just-in-time (JIT), ephemeral and role-based access ensures that high-impact credentials cannot be stolen, lost or misused while enforcing fine-grained permissions and logging of sessions.

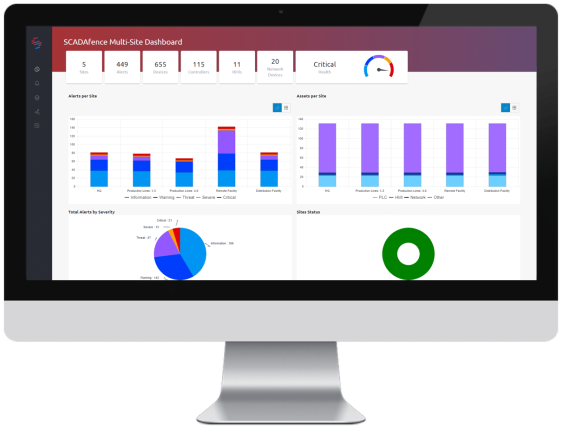
Integrating and combining SCADAfence's real-time network monitoring with SSH OT's secure access capabilities creates a robust security posture across your organization's OT networks.



Hosts

Showing 1-8 of 8

Name	Addresses
Engineering Workstation asiakas1 plcuser @ otextender/192.168.93.123 The access is granted through roles: OT Admin (Demo), privx-admin	
PLC Jump Host (OLD) plcuser2 @ otextender/192.168.93.32 The access is granted through roles: privx-admin	
PreSalesEntraDemoAnsible	10.0.0.17
PreSalesEntraDemoMSSQL2022	10.0.0.16



SCADAfence Multi-Site Dashboard

5 Sites · 449 Alerts · 655 Devices · 115 Controllers · 11 HMIs · 20 Network Devices · Critical Health

Benefits of Integration

- Unified view of security environments across IT and OT and landscapes
- Centralized, uniform access across IT and OT environments with task approvals
- Intelligence-driven threat detection, detailed audit logs, session monitoring & recording
- Discovery of all ICS/OT assets within the OT Infrastructure
- StrongID based (biometric) authentication with an option for external authorization for high-impact sessions
- Block anomalous access attempts based on alerts
- OT asset management and scanning of file uploads for malicious payloads, leading to reduced risk of malware shutting down production
- Secrets management (passwords and keys) and a path to true Zero Trust, just-in-time passwordless and keyless authentication
- Secure Remote Access Management protected with classical encryption, Quantum-Safe Cryptography (QSC) or hybrid

How the Role-based Access Enforcement and Compliance are provided

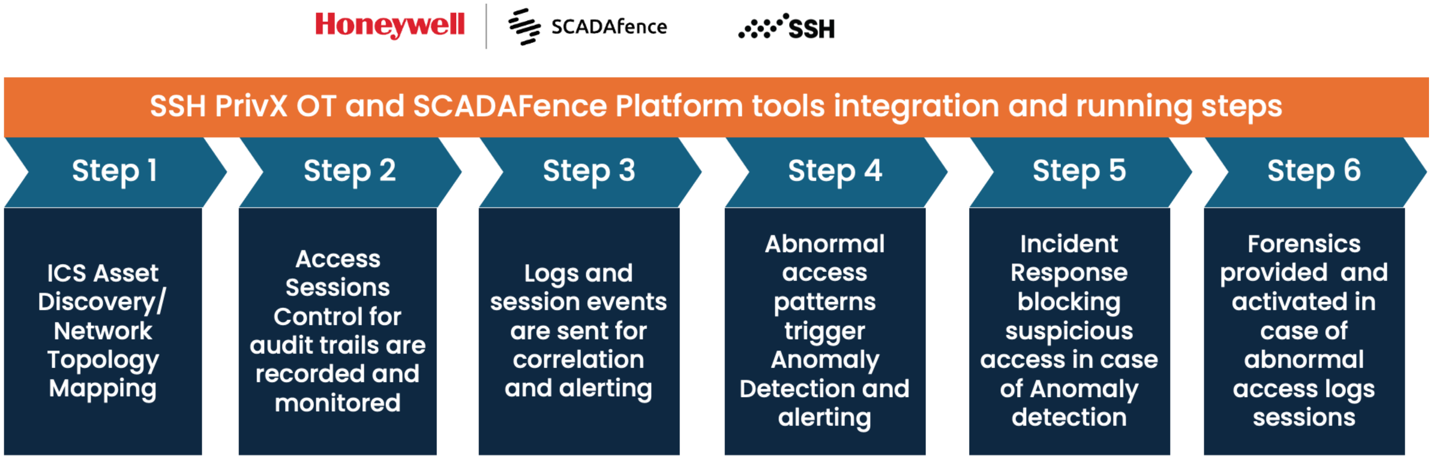
PrivX OT's role-based access features, paired with SCADAfence's device-level visibility, help ensure that users only access specific assets according to their role. SCADAfence can verify that all access aligns with pre-established roles and permissions.

Combining PrivX OT session logs with SCADAfence network logs offers a unified and comprehensive view into compliance posture and is a big step towards meeting regulatory requirements.

How SCADAfence and SSH tools integration works

- Start by centralizing Access Control and Monitoring where the access requests are managed so that SCADAfence can monitor network traffic and detect access requests to OT devices that PrivX governs. This ensures that all traffic, including SSH connections, are scrutinized.
- PrivX OT handles the Session Control and provides audit trails and session recordings, which SCADAfence can monitor for anomalous access attempts, unauthorized connections, or suspicious behavior within the OT environment.
- Next step will be taking care of the event correlation and alerts by configuring PrivX to forward logs and session events to SCADAfence. This can enable SCADAfence to correlate access attempts with network activity for more comprehensive alerting.
- Anomaly Detection is handled by SCADAfence by alerting based on abnormal PrivX access patterns, for example, detecting new access from unusual locations, which could signal potential compromise or insider threats.
- To handle Enhanced Incident Response, API configurations automate information sharing between SCADAfence and PrivX OT. This enables automatic responses such as blocking suspicious access attempts in PrivX based on SCADAfence alerts.
- SCADAfence provides Forensics by using its network monitoring capabilities that correlate access logs from PrivX sessions with observed network anomalies, enabling faster forensic investigations.

Here are the SCADAfence and SSH PrivX OT tools integrations and running steps:



Honeywell | SCADAfence SSH

SSH PrivX OT and SCADAFence Platform tools integration and running steps

Step 1
ICS Asset Discovery/ Network Topology Mapping

Step 2
Access Sessions Control for audit trails are recorded and monitored

Step 3
Logs and session events are sent for correlation and alerting

Step 4
Abnormal access patterns trigger Anomaly Detection and alerting

Step 5
Incident Response blocking suspicious access in case of Anomaly detection

Step 6
Forensics provided and activated in case of abnormal access logs sessions

About SSH Communications Security

SSH Communications Security is a European cybersecurity company that helps businesses secure critical data and communications between systems, automated applications, and people with defensive cybersecurity.

SSH solutions defend and safeguard business communications, business secrets, and access to them - now and in the future. SSH Communications Security is the market leader in developing advanced security solutions since 1995 when the company's founder, Tatu Ylönen, invented the Secure Shell protocol, which soon became the gold standard for data-in-transit security.

Today Secure Shell is one of the most widely used protocols in the world and SSH Communications Security has grown to serve over 3,000 customers around the globe. Throughout SSH Communications Security history, we have developed leading-edge security solutions that enable organizations to protect themselves against a rapidly growing threat landscape that includes both internal and external actors.

SSH Communications Security platform-based approach to Secure Shell deployment and management provides the only solution on the market that addresses the need for security, compliance, and operational efficiency in today's complex enterprise environments.

About SCADAfence

SCADAfence is the global technology leader in OT & IoT cybersecurity. SCADAfence offers a full suite of industrial cybersecurity products that provides full coverage of large-scale networks, offering best-in-class network monitoring, asset discovery, governance, remote access, and IoT device security.

A Gartner "Cool Vendor", SCADAfence delivers proactive security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAfence enables organizations in critical infrastructure, manufacturing, and building management industries to operate securely, reliably, and efficiently.

Helsinki

Global and EMEA headquarters
SSH Communications Security Oyj
Tel. +358 20 500 7000
emea.sales@ssh.com

New York City

AMER headquarters
SSH Communications Security Inc.
Tel. +1 781 247 2100
info.us@ssh.com

Singapore

APAC headquarters
SSH CommSec Pte. Ltd.
Tel. +65 6338 7160
sales.asia@ssh.com

The information in this document is provided “as is” without any warranty, express or implied, including without any warranties of merchantability, fitness for a particular purpose and any warranty or condition of non-infringement. SSH Communications Security products are warranted according to the terms and conditions of the agreements under which they are provided. SSH Communications Security may make changes to specifications and product descriptions at any time, without notice. SSH® and NQX™ are a registered trademark or trademarks of SSH Communications Security Corporation and are protected by the relevant jurisdiction-specific and international copyright laws and treaties. Other names and marks are the property of their respective owners.