



REMOTE ACCESS AND PROTECTION OF CRITICAL MACHINES

A digital lock for every machine.

How industry, infrastructure and healthcare can let the right person into the right machine – and make everything else invisible. Without rebuilding the network.

Swedish. Simple. Secure.

Xertified is a Swedish cybersecurity company based in Uppsala and Stockholm. We develop, manufacture and support everything in Sweden, under Swedish ownership. The hardware contains no components from the USA or China.

Our technology – XoT technology™ – places a lock in front of every critical machine. The machine keeps its address but becomes invisible to anyone without a key. The principle is the same for a pump at a waterworks, an X-ray machine at a hospital and a robot in a factory.

Xertified is on Ny Teknik's 33 list of Sweden's most promising tech companies and is delivered through partners such as Telia Cygate, Fujitsu, Orange Cyberdefense and NetNordic.

© Xertified AB 2026. The content is general information and does not replace technical or legal advice. Contact us and we will go through how the principles apply to your environment.

Six chapters. From the problem to a protected machine.

01	Everything connected can be reached	04
02	Third parties in the OT network	05
03	Why IT tools are not enough	06
04	Lock. Key. Policy.	07
05	Two services, one technology	08
06	How to get started	09

The firewall protects the edge. Breaches start on the inside.

Remote access no longer needs a business case. Every modern site depends on it. The question is how to provide it without opening the whole network.

More than half of all breaches in industrial networks start inside the firewall – through an employee, a consultant or a vendor with a VPN login. Once inside, you reach everything: control systems, historians, cameras, servers.

At the same time, machines live long. A protection relay, an X-ray machine or a PLC stays in place for twenty years, with an operating system the vendor does not allow you to patch. The vulnerabilities remain for its entire life.

Segmentation and VLANs slow attackers down, but do not stop them. Anyone inside the segment still sees every machine. The protection sits in the network – not at the machine.

No real boundary	Cannot be patched	Must be reachable
Insiders see every machine.	Equipment lasts twenty years.	Service is needed 24/7.

Three in four let vendors in. Few know what they do.

Machine builders, integrators and service partners need to get in. Today they often get a VPN account – and with it a clear view of everything.

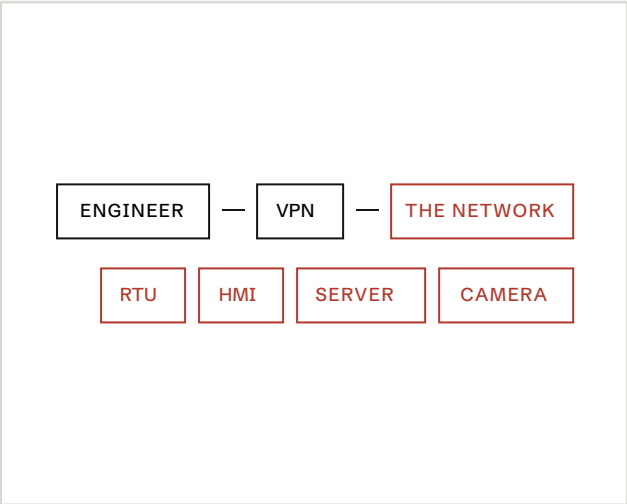


Fig. 1 Traditional remote access: one door in, then a clear view across the segment.

A typical site has a large number of external parties with access – often with administrator rights, often without a time limit and almost always without a log showing who did what, on which machine and when.

IT creates the accounts when a project starts and forgets them when it ends. Every forgotten account is a door left ajar.

What the asset owner needs is not more tools but fewer: a way to let one person into exactly one machine, during a set window, with a recording of what happened.

WHO	A named person from your directory – not a shared vendor account.
WHAT	One machine. Not the segment, not the network.
WHEN	One service window. The policy expires by itself.
PROOF	The session is recorded and logged. Ready for NIS 2.

VPN, jump servers and PAM are built for IT. Machines are not.

IT-centred tools assume that what needs protecting is a user with a modern computer that can run an agent, is updated every month and signs in with a password and two-factor. In OT, almost none of that applies.

A VPN lets the person into a network segment and then trusts the segmentation. A jump server gathers all traffic at one point – a bottleneck and a single point of failure. PAM handles privileged accounts well, but cannot see machines that have no accounts at all.

What they have in common is that the protection sits somewhere other than at the machine. If the machine moves, the network has to be redone. If the central point goes down, production stops.

What is needed is protection that sits at the machine, moves with it, works without an agent and keeps working even when the control plane is temporarily unreachable.

WITH IT TOOLS

The person gets into a whole network segment.

IT creates the account, and it is forgotten.

The log shows an IP address.

The protection sits in the network and requires rebuilding.

WITH XERTIFIED

The person reaches one machine.

Operations write the policy, and it expires by itself.

The log shows a person, a machine and a recording.

The protection sits at the machine and is connected in a minute.

Think hotel. The corridor is open, but every room has a lock.

Your key card only opens your room, during your stay. We do the same for machines.

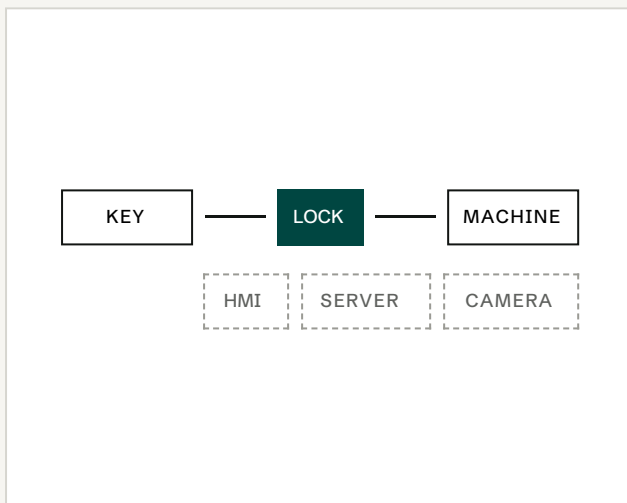


Fig. 2 The tunnel ends at the machine. The rest of the network stays untouched – and invisible.

01

The Lock

An XoT-S1 in the cabinet, or the XoT-Lock as software in the cloud, is placed in the traffic path in front of the machine. The machine keeps its IP and VLAN. Without a valid key, the Lock does not even answer a ping.

02

The Key

Every person and system gets its own cryptographic identity. The private key never leaves the device. People sign in through your existing directory – Entra, Google, Nexus, Pointsharp.

03

The Policy

Who, what, where, when and how. Anything that does not match is denied at the machine. A policy takes 20 seconds and can be managed by operations, not just IT.

04

XMS · the control plane

Hands out keys and policies but carries no traffic. If it goes down, traffic keeps flowing. Runs in the cloud, on your premises or fully air-gapped.

Choose what you need. Same Lock, same keys.

01 REMOTE ACCESS

Let the right person into the right machine.

Engineers and vendors reach exactly one machine, for a set time, through the browser or a small client. No VPN, no installation. Every session is recorded.

ACCESS	WebAccess or XoT-Desktop Client
PROTOCOLS	RDP · SSH · HTTPS · VNC · Modbus · OPC
PROOF	Recorded session, log to your SIEM

Engineer DE → X-ray CX4300 → Berlin →
Thu 09:00-13:30

02 HIDE AND PROTECT

Hide it from everyone else.

The machine keeps its IP and VLAN but becomes invisible to everything and everyone without a policy. What cannot be seen does not need patching at the same pace – the need drops by more than 90%.

INSTALLATION	Connected in a minute, enrolled with a QR code
--------------	--

BEST FOR	Equipment that cannot be updated or run an agent
----------	--

PROOF	Denied connections are logged at the Lock
-------	---

SCADA-RTU 12 · 10.20.4.12 · VLAN 20 →
invisible to all but 3

Energy and water

Protection relays, RTUs and SCADA that must be open around the clock – but not to everyone.

Manufacturing

Robots and HMIs from many vendors, often with remote service from abroad.

Healthcare

X-ray, labs and equipment that moves between departments. The protection moves with it.

Start with one machine. The rest stays untouched.

You do not need to replace everything at once. The firewall and the old remote access stay in place while you build trust. When the last machine is hidden, you switch off the old.

01

Sign in with your directory

No new passwords. Same account, same two-factor.

02

Enrol a Lock

XoT-S1 via a QR code on the screen, or the XoT-Lock as a container. Whoever stands at the cabinet can do it.

03

Choose what to hide

The machine keeps its address and vanishes from the network.

04

Give yourselves a key

A client on the computer, or a WebAccess link for an engineer.

05

Write the first policy

Who, what, where, when, how. Done in 20 seconds.



CONTACT

One Lock.
One key.
One policy.

Book a meeting and we will go through your
environment and pick the first machine together.

sales@xertified.com

+46 (0)18 265 06 06 · xertified.com