GUIDE · 2026

FJÄRRÅTKOMST OCH SKYDD AV KRITISKA MASKINER

Ett digitalt lås för varje maskin.

Hur industri, infrastruktur och sjukvård kan släppa in rätt person till rätt maskin – och göra allt annat osynligt. Utan att bygga om nätet.

XERTIFIED AB · UPPSALA · STOCKHOLM

XERTIFIED.COM

Svenskt.
Enkelt. Säkert.

Xertified är ett svenskt cybersäkerhetsbolag med säte i Uppsala och Stockholm. Vi utvecklar, tillverkar och supportar allt i Sverige, med svenska ägare. Hårdvaran innehåller inga komponenter från USA eller Kina.

Vår teknik – XoT technology™ – sätter ett lås framför varje kritisk maskin. Maskinen behåller sin adress men blir osynlig för alla som inte har nyckel. Det är samma princip för en pump i ett vattenverk, en röntgen på ett sjukhus och en robot i en fabrik.

Xertified finns på Ny Tekniks 33-lista över Sveriges mest lovande techbolag och levereras genom partners som Telia Cygate, Fujitsu, Orange Cyberdefense och NetNordic.

© Xertified AB 2026. Innehållet är allmän information och ersätter inte teknisk eller juridisk rådgivning. Kontakta oss så går vi igenom hur principerna kan tillämpas i er miljö.

Sex kapitel. Från problemet till en maskin skyddad.

01	Allt som är uppkopplat kan nås	04
02	Tredje part i OT-nätet	05
03	Varför IT-verktygen inte räcker	06
04	Lås. Nyckel. Regel.	07
05	Två tjänster, en teknik	08
06	Så kommer ni igång	09

Brandväggen skyddar kanten. Intrången börjar på insidan.

Det behövs inget affärscase för fjärråtkomst längre. Varje modern anläggning är beroende av den. Frågan är hur den ska ske utan att öppna hela nätet.

Mer än hälften av alla intrång i industriella nät börjar redan innanför brandväggen – via en anställd, en konsult eller en leverantör som fått en VPN-inloggning. Väl inne når man allt: styrsystem, historiker, kameror, servrar.

Samtidigt lever maskinerna länge. Ett reläskydd, en röntgenapparat eller en PLC står i tjugo år, med operativsystem som leverantören inte tillåter att man patchar. Sårbarheterna följer med genom hela livslängden.

Segmentering och VLAN bromsar, men stoppar inte. Den som är inne i segmentet ser fortfarande varje maskin. Skyddet sitter i nätet – inte vid maskinen.

Nätet är inte gränsen

Den som är inne ser varje maskin.

Kan inte patchas

Utrustning lever i tjugo år.

Måste nås utifrån

Service är nödvändig, dygnet runt.

Tre av fyra släpper in leverantörer. Få vet vad de gör där.

Maskinleverantörer, integratörer och servicepartners behöver komma in. Idag får de ofta ett VPN-konto – och med det fri sikt.

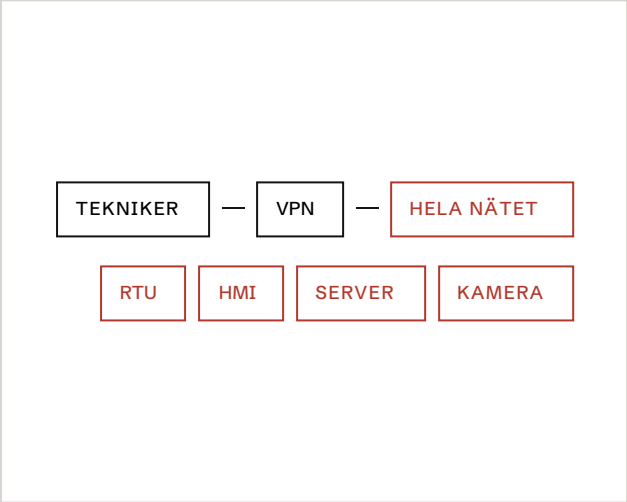


Fig. 1 Traditionell fjärråtkomst: en dörr in, sedan fri sikt över segmentet.

En anläggning har i snitt ett stort antal externa parter med åtkomst – ofta med behörigheter på administratörsnivå, ofta utan tidsgräns och nästan alltid utan en logg som visar vem som gjorde vad, mot vilken maskin och när.

Kontona skapas av IT när ett projekt startar och glöms bort när det avslutas. Varje kvarglömt konto är en dörr som står på gläntt.

Det asset-ägaren behöver är inte fler verktyg utan färre: ett sätt att släppa in en person till exakt en maskin, under ett bestämt fönster, med en inspelning av vad som hände.

VEM	Namngiven person via er katalog – inte ett delat leverantörskonto.
VAD	En maskin. Inte segmentet, inte nätet.
NÄR	Ett servicefönster. Regeln upphör av sig själv.
BEVIS	Sessionen spelas in och loggas. Redo för NIS 2.

VPN, jump-server och PAM är byggda för IT. Maskinerna är inte det.

IT-centrerade verktyg utgår från att det som ska skyddas är en användare med en modern dator, som kan köra en agent, uppdateras varje månad och identifiera sig med lösenord och tvåfaktor. I OT gäller nästan inget av det.

En VPN släpper in personen i ett nätsegment och litar därefter på segmenteringen. En jump-server samlar all trafik på en punkt – en flaskhals och en enskild felpunkt. PAM hanterar privilegierade konton väl, men ser inte maskiner som inte har några konton alls.

Gemensamt för dem är att skyddet sitter någon annanstans än vid maskinen. Flyttas maskinen måste nätet göras om. Går den centrala punkten ner står produktionen.

Det som krävs är ett skydd som sitter vid maskinen, följer med den, fungerar utan agent och fortsätter fungera även när kontrollplanet tillfälligt inte går att nå.

MED IT-VERKTYG	MED XERTIFIED
Personen kommer in i ett helt nätsegment.	Personen kommer fram till en maskin.
Kontot skapas av IT och glöms bort.	Regeln skrivs av verksamheten och upphör av sig själv.
Loggen visar en IP-adress.	Loggen visar en person, en maskin och en inspelning.
Skyddet sitter i nätet och kräver ombyggnad.	Skyddet sitter vid maskinen och kopplas in på en minut.

Tänk hotell. Korridoren är öppen, men varje rum har ett lås.

Kortet fungerar bara till ditt rum, under din vistelse. Vi gör samma sak med maskiner.

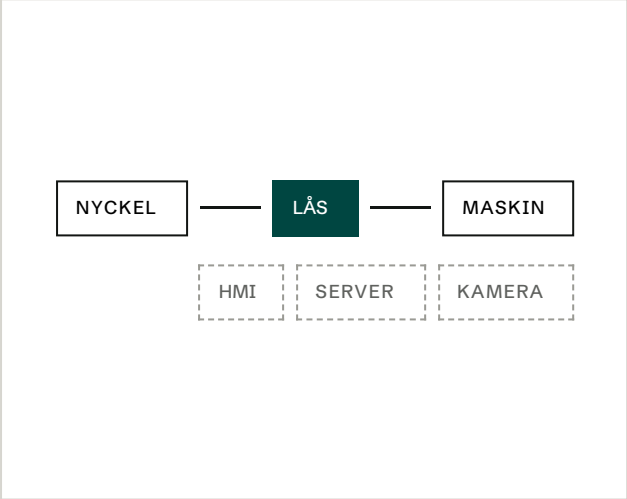


Fig. 2 Tunneln slutar vid maskinen. Resten av nätet står orört – och osynligt.

01

Låset

Ett XoT-S1 i skåpet, eller XoT-Lock som mjukvara i molnet, sätts i trafikvägen framför maskinen. Maskinen behåller IP och VLAN. Utan giltig nyckel svarar låset inte ens på ping.

02

Nyckeln

Varje person och system får en egen kryptografisk identitet. Den privata nyckeln lämnar aldrig enheten. Personer loggar in via er befintliga katalog – Entra, Google, Nexus, Pointsharp.

03

Regeln

Vem, vad, var, när och hur. Allt som inte matchar nekas vid maskinen. En regel tar 20 sekunder och kan skötas av verksamheten, inte bara IT.

04

XMS · kontrollplanet

Delar ut nycklar och regler men bär ingen trafik. Går det ner flyter trafiken vidare. Kör i molnet, hos er eller helt luftgapat.

Välj det ni behöver. Samma lås, samma nycklar.

01 REMOTE ACCESS

Släpp in rätt person till rätt maskin.

Tekniker och leverantörer når exakt en maskin, under en bestämd tid, via webbläsaren eller en liten klient. Inget VPN, ingen installation. Varje session spelas in.

ÅTKOMST	WebAccess i webbläsaren eller XoT-Desktop Client
PROTOKOLL	RDP · SSH · HTTPS · VNC · Modbus · OPC
BEVIS	Inspelad session, logg till er SIEM

`Tekniker DE → Röntgen CX4300 → Berlin → tors 09.00–13.30`

02 HIDE AND PROTECT

Göm maskinen för alla andra.

Maskinen behåller sin IP och sitt VLAN men blir osynlig för allt och alla som inte har en regel. Det som inte syns behöver inte heller patchas i samma takt – behovet minskar med över 90 %.

INSTALLATION	Kopplas in på en minut, registreras med QR-kod
PASSAR	Utrustning som inte kan uppdateras eller köra agent
BEVIS	Varje nekad anslutning loggas vid låset

`SCADA-RTU 12 · 10.20.4.12 · VLAN 20 → osynlig för alla utom 3`

Energi och vatten

Reläskydd, RTU:er och SCADA som måste vara öppna dygnet runt – men inte för alla.

Tillverkande industri

Robotar och HMI:er från många leverantörer, ofta med fjärrservice från utlandet.

Sjukvård

Röntgen, labb och utrustning som flyttas mellan avdelningar. Skyddet följer med.

Börja med en maskin. Nätet står kvar orört.

Ni behöver inte byta allt på en gång. Brandväggen och den gamla fjärråtkomsten står kvar medan ni bygger förtroende. När den sista maskinen är gömd stänger ni det gamla.

01 **Logga in med er katalog**
Inga nya lösenord. Samma konto, samma tvåfaktor.

02 **Registrera ett lås**
XoT-S1 via QR-kod på skärmen, eller XoT-Lock som container. Den som står vid skåpet klarar det.

03 **Välj vad låset ska gömma**
Maskinen behåller sin adress och försvinner från nätet.

04 **Ge er själva en nyckel**
Klient på datorn, eller en WebAccess-länk till en tekniker.

05 **Skriv den första regeln**
Vem, vad, var, när, hur. Klart på 20 sekunder.

Ett lås.
En nyckel.
En regel.

Boka ett möte så går vi igenom er miljö och väljer den första maskinen tillsammans.

sales@xertified.com

+46 (0)18 265 06 06 · xertified.com