



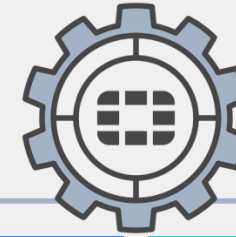
Notable Industry References For Standards & More



Standards, Regulations, Frameworks	Type	Governing Body	Origin	Scope	Applicability
NIS Directive	Regulation	ENISA	EU (+ UKI)	Multi-Industry IT/OT	EU
NERC CIP	Regulation	FERC	US	Electricity IT/OT	US
ISA/IEC 62443 (formerly ANSI ISA99)	Standard	ANSI, ISA, IEC	International	Multi-Industry OT	Multi
NIST CSF	Framework (Guideline)	NIST	US	Multi-Industry IT/OT	Multi
Critical Security Controls (CIS Top 20)	Guideline	CIS	US	Multi-Industry OT	Multi
IEC/ISO 27000 Series	Standard	ISO, IEC	International	Multi-Industry IT/OT	Multi
NIST SP 800-82	Guideline	NIST	US	Multi-Industry OT	Multi
NIST SP 800-53	Guideline	NIST	US	Multi-Industry IT/OT	Multi



OT Security Platform



IT

Cloud & External Zones

Cloud



MAJOR ENFORCEMENT BOUNDARY

Business & Enterprise Zones

IT



CONVERGED IT & OT



MAJOR ENFORCEMENT BOUNDARY

Operations & Control Zones

ICS / OT



MINOR ENFORCEMENT BOUNDARY

Process Control Zones

HMI



OT

MAJOR ENFORCEMENT BOUNDARY

Safety & Protection Zones



Secure Networking

Secure Digital Networks



FortiGate VM



SD-WAN / 5G



FortiGate NGFW



FortiSwitch



Ruggedized Products

Zero Trust

Secure Remote Access



FortiSASE



FortiSRA



FortiClient ZTNA



FortiAuthenticator



FortiToken



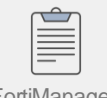
FortiNAC for OT

Security Operations

Secure IT/OT Convergence



FortiAnalyzer for OT



FortiManager



FortiSIEM for OT



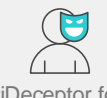
FortiSOAR for OT



FortiEDR



FortiNDR for OT



FortiDeceptor for OT

Security Services



OT Specialized FortiGuard Services



3,000+ OT Application Signatures



600+ OT Threat Signatures

Ecosystem Partners



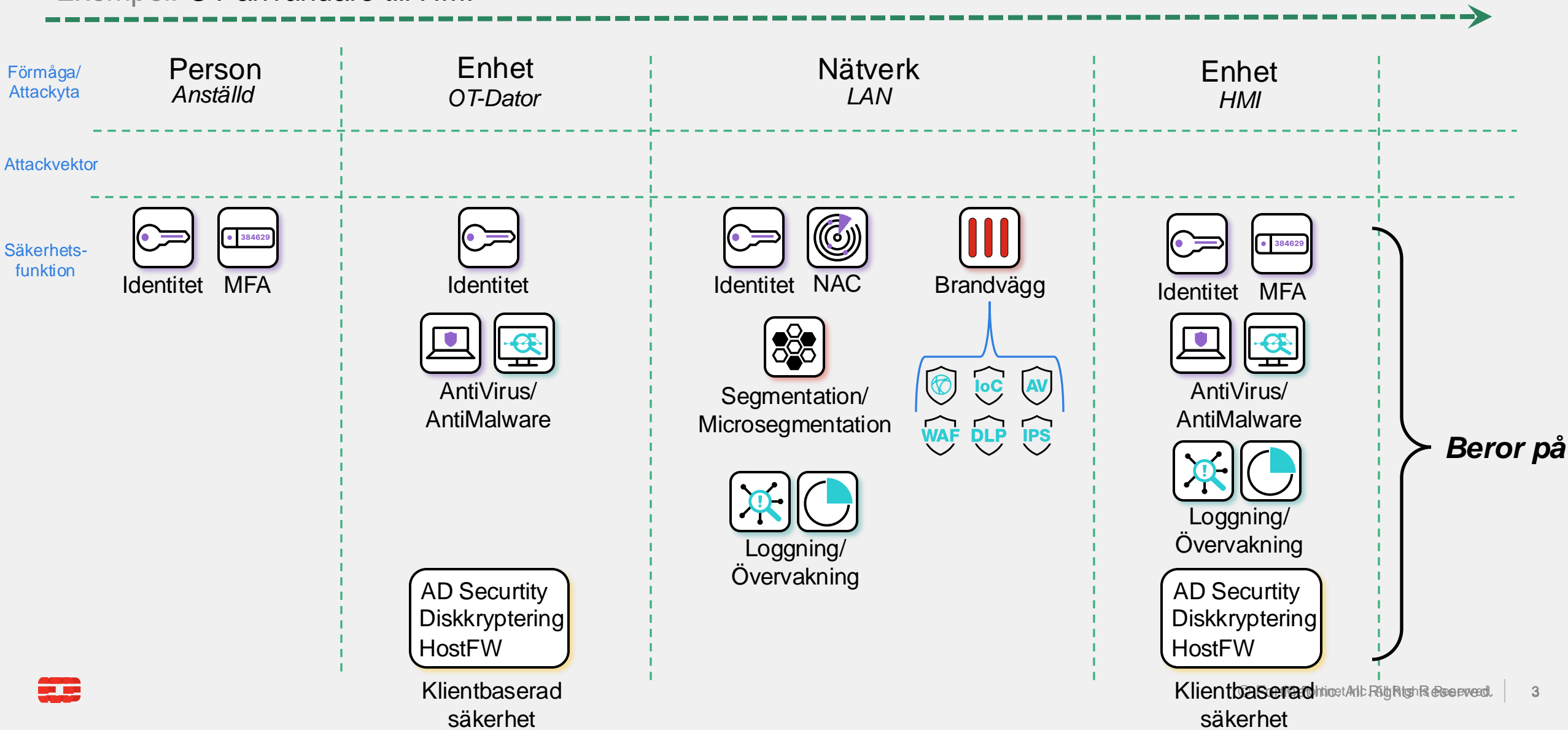
Fabric Ready Ecosystem



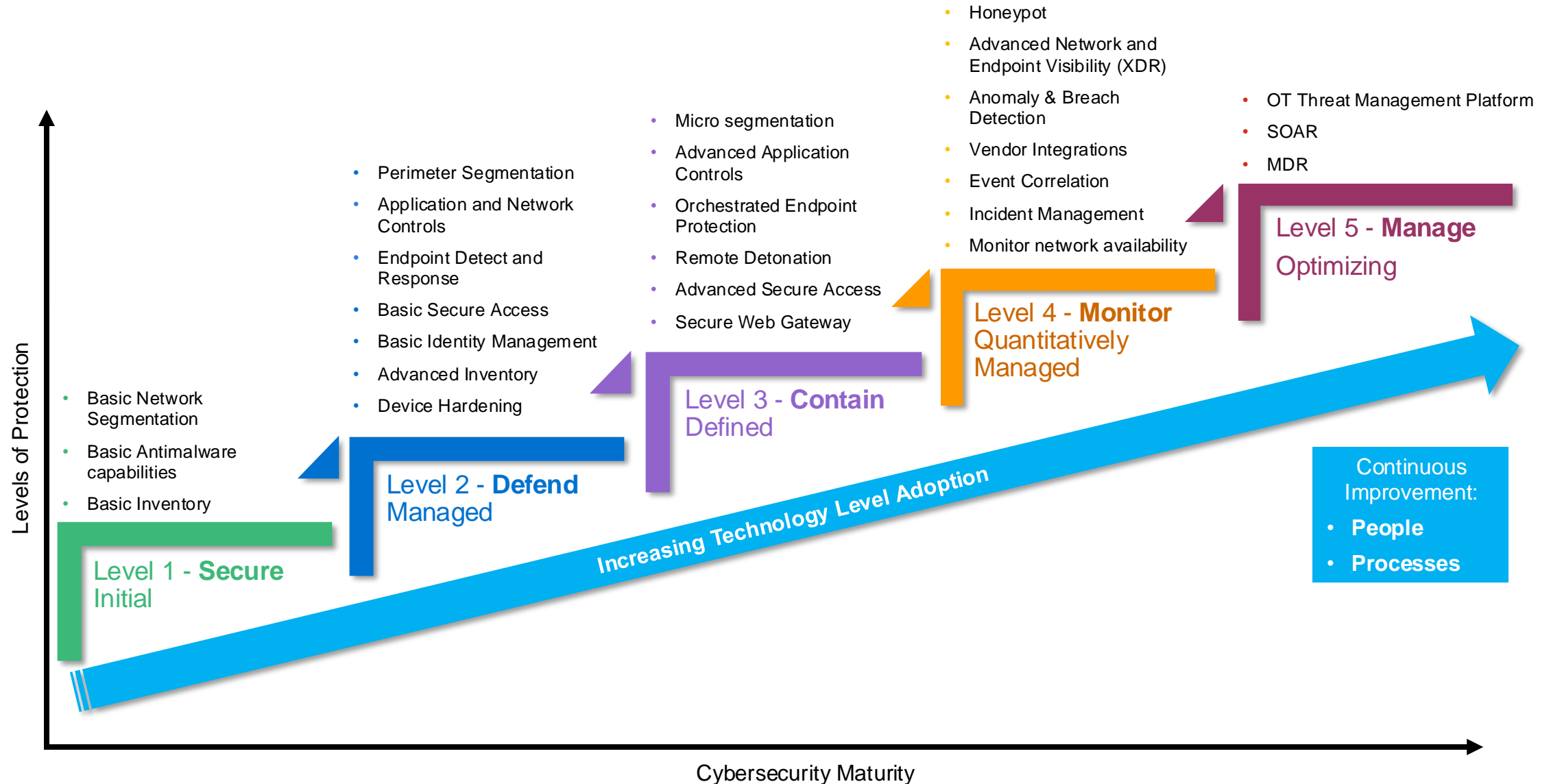
Säkerhet på Djupet

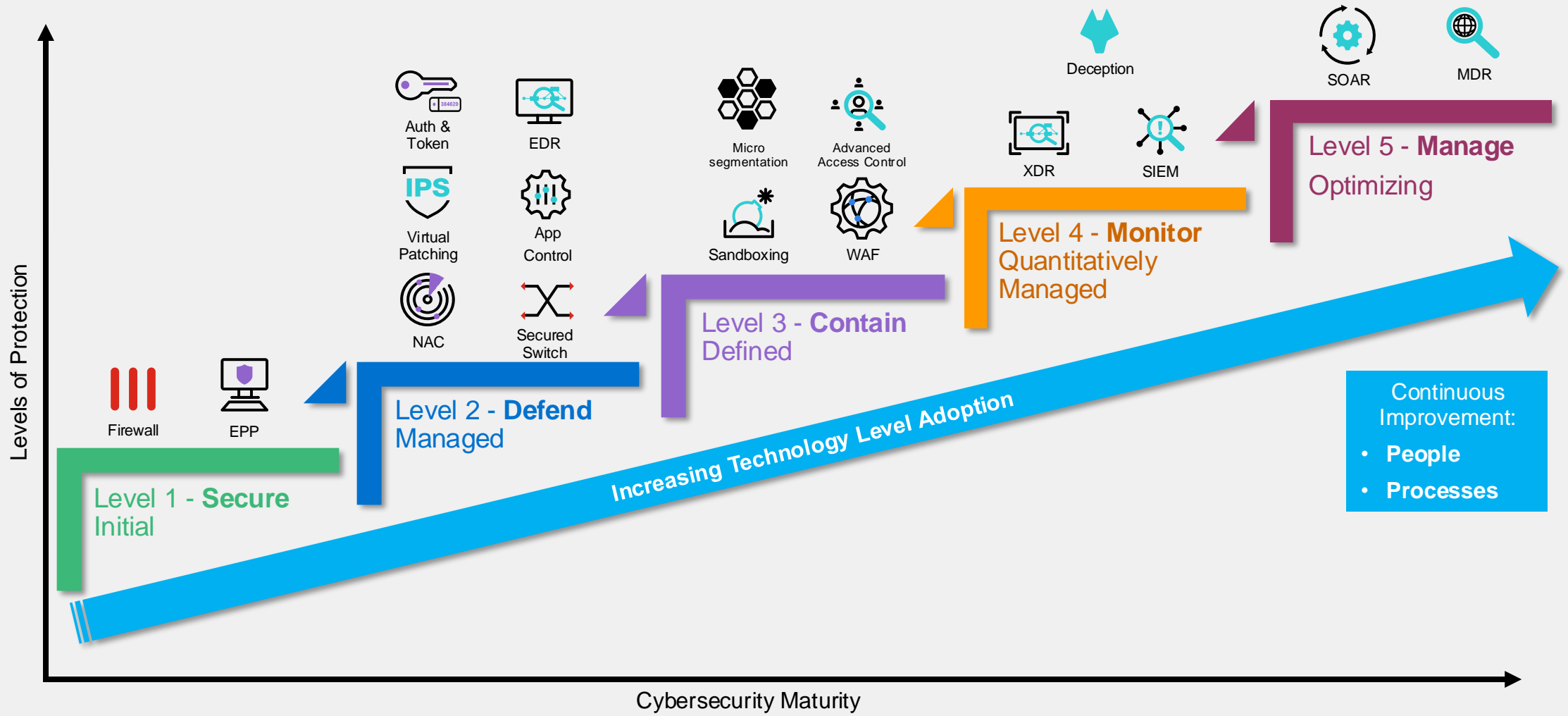
Klient
OT Användare

Exempel: OT-användare till HMI



Förmågor för IT och OT säkerhet

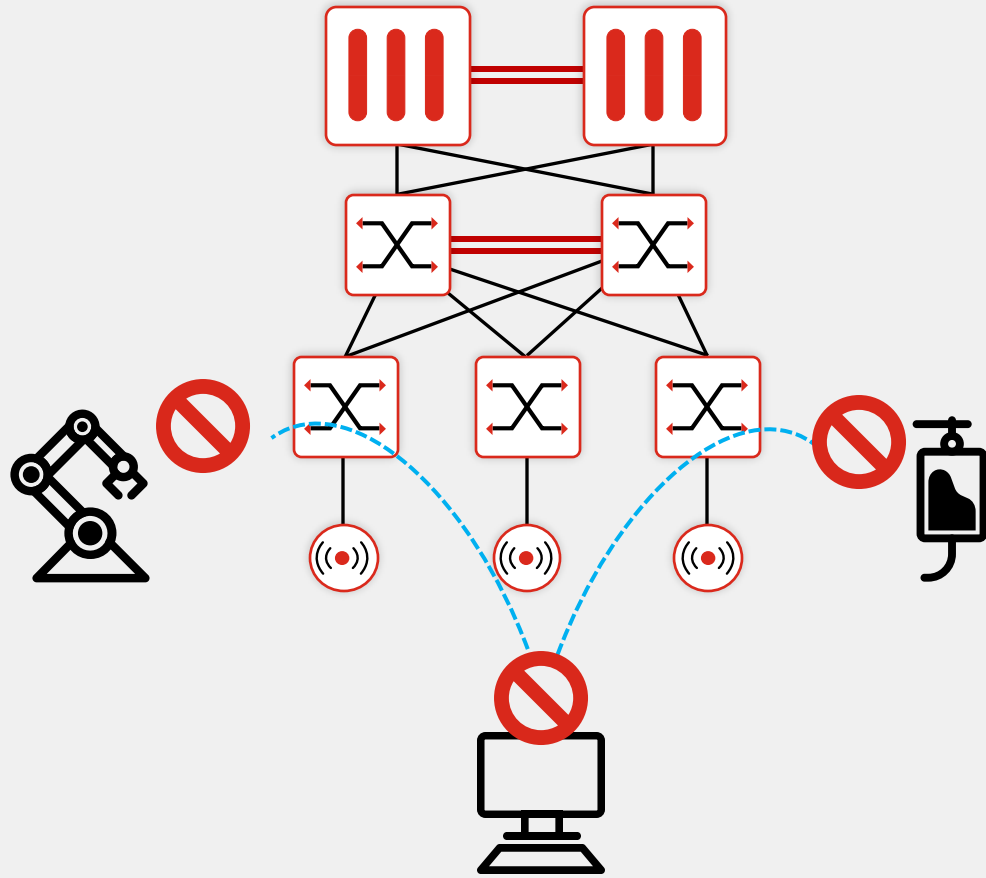




Assess Program Maturity against Proven Deployable Technologies



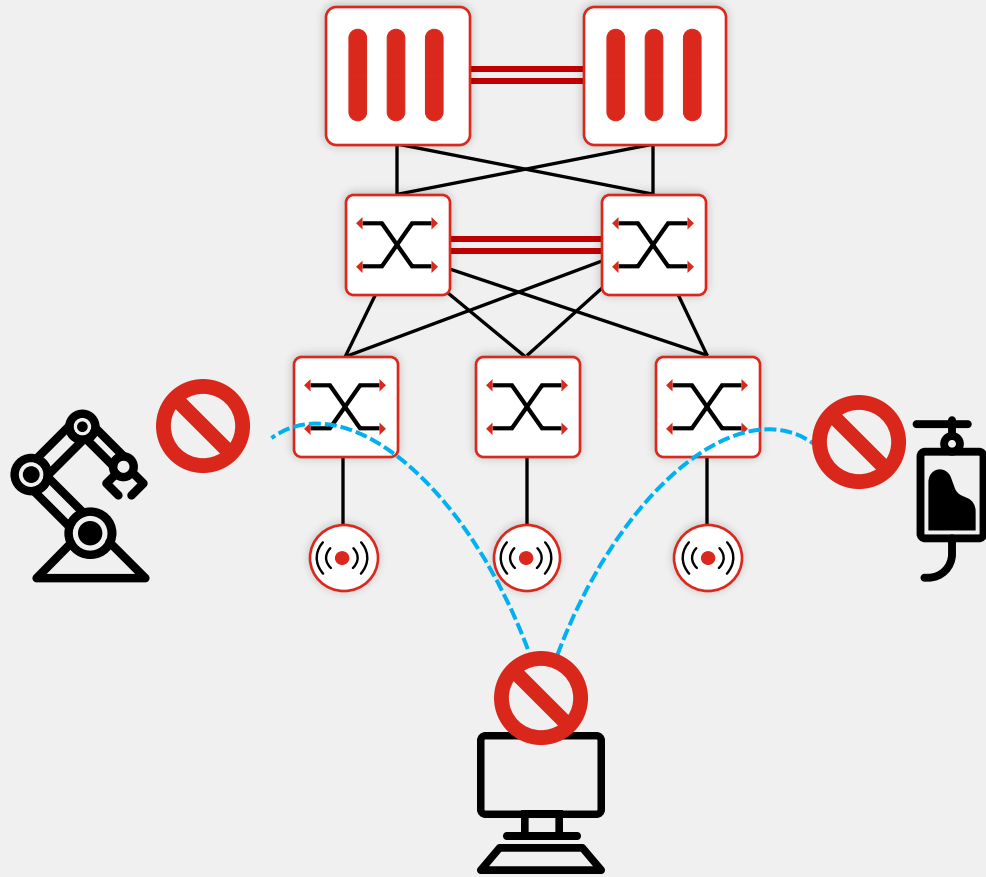
MICROSEGMENTING



Network	
Device detection i	<input checked="" type="checkbox"/>
IGMP snooping	<input type="checkbox"/>
DHCP snooping	<input checked="" type="checkbox"/>
Block intra-VLAN traffic	<input type="checkbox"/>
Security mode	<input type="checkbox"/>

MICROSEGMENTATION

& INSPEKTION



Network	
Device detection i	<input checked="" type="checkbox"/>
IGMP snooping	<input type="checkbox"/>
DHCP snooping	<input checked="" type="checkbox"/>
Block intra-VLAN traffic	<input type="checkbox"/>
Security mode	<input type="checkbox"/>

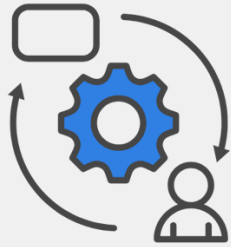
IPS PROTECT-CRITICAL

APP OFFICE365

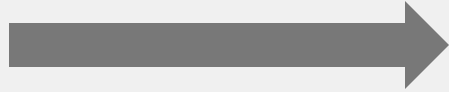
SSL DEEP-INSPECTION



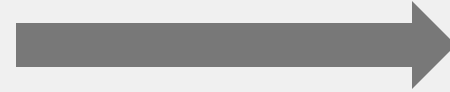
Fortinet Identity & Access Solutions



ZTNA



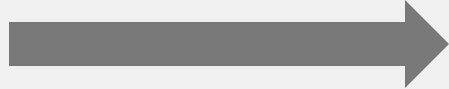
General Access



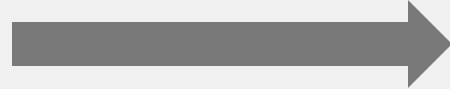
IT Applications



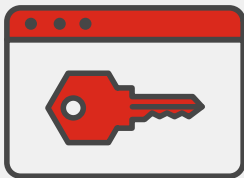
FortiPAM



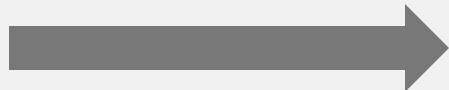
Privileged Access



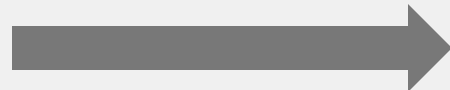
IT Systems



FortiSRA



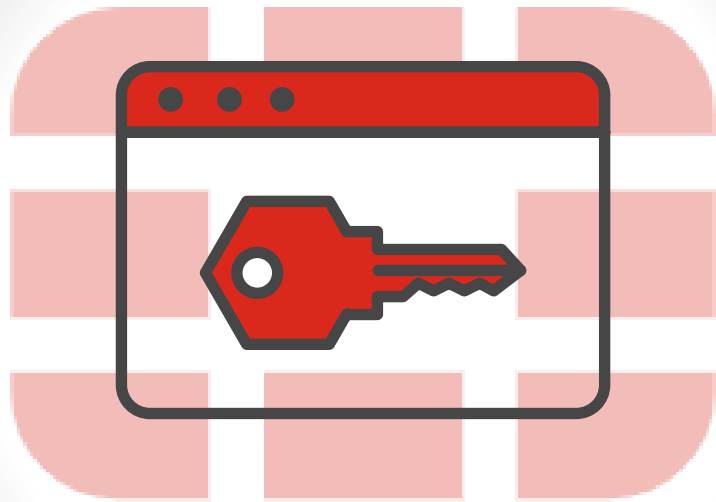
Remote Access



OT Systems

FortiSRA

**Agentless Secure Remote Access
from Fortinet**



for OT



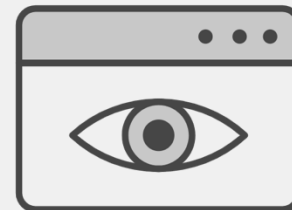
Manage Remote Access

Ensure only authorized users have access in a policy of least privilege



Manage Privileged Credentials

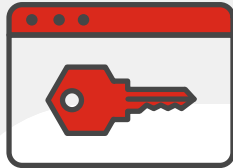
Store credentials securely and automatically create and rotate passwords



Monitor and Record Sessions

Post session audit and ability to terminate sessions in real-time

FortiSRA Solution Components



Web Browser Extension

Remote Clients

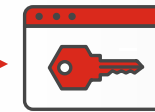
Windows and Linux

Web Browsers

Chrome, Firefox & Edge

Target Systems

ICS machines & HMIs, Cisco devices, FortiGate NGFWs, Windows and Linux servers, etc.



FortiSRA

Target System

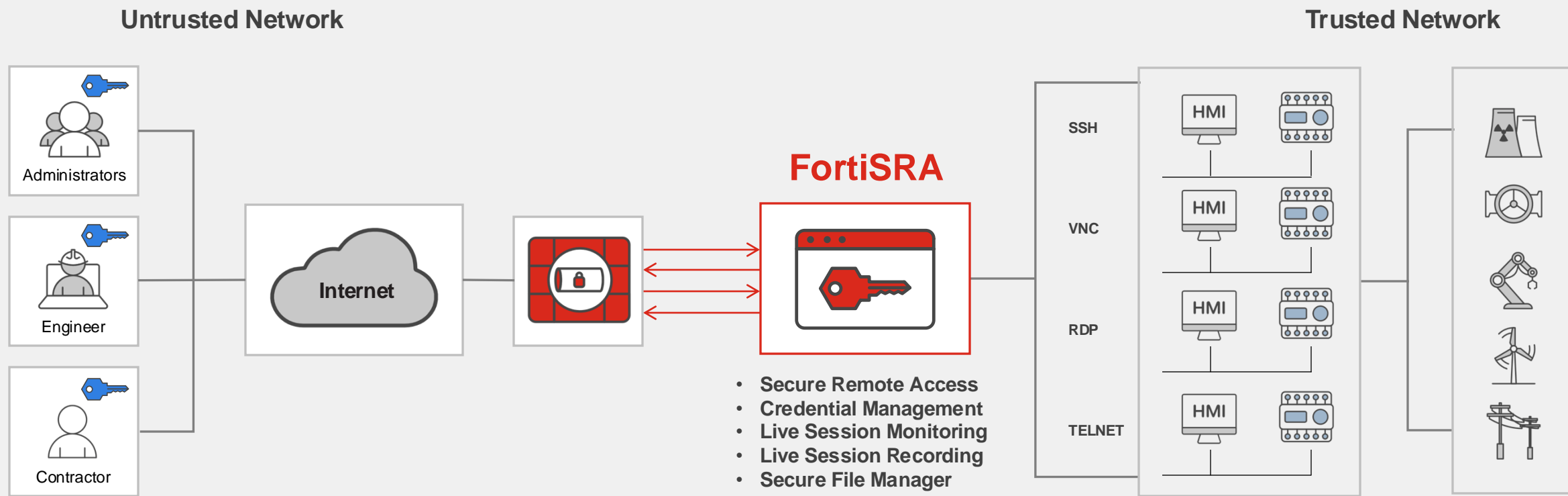
FORTINET



Integrations



Secure Remote Access – An Agentless Solution



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



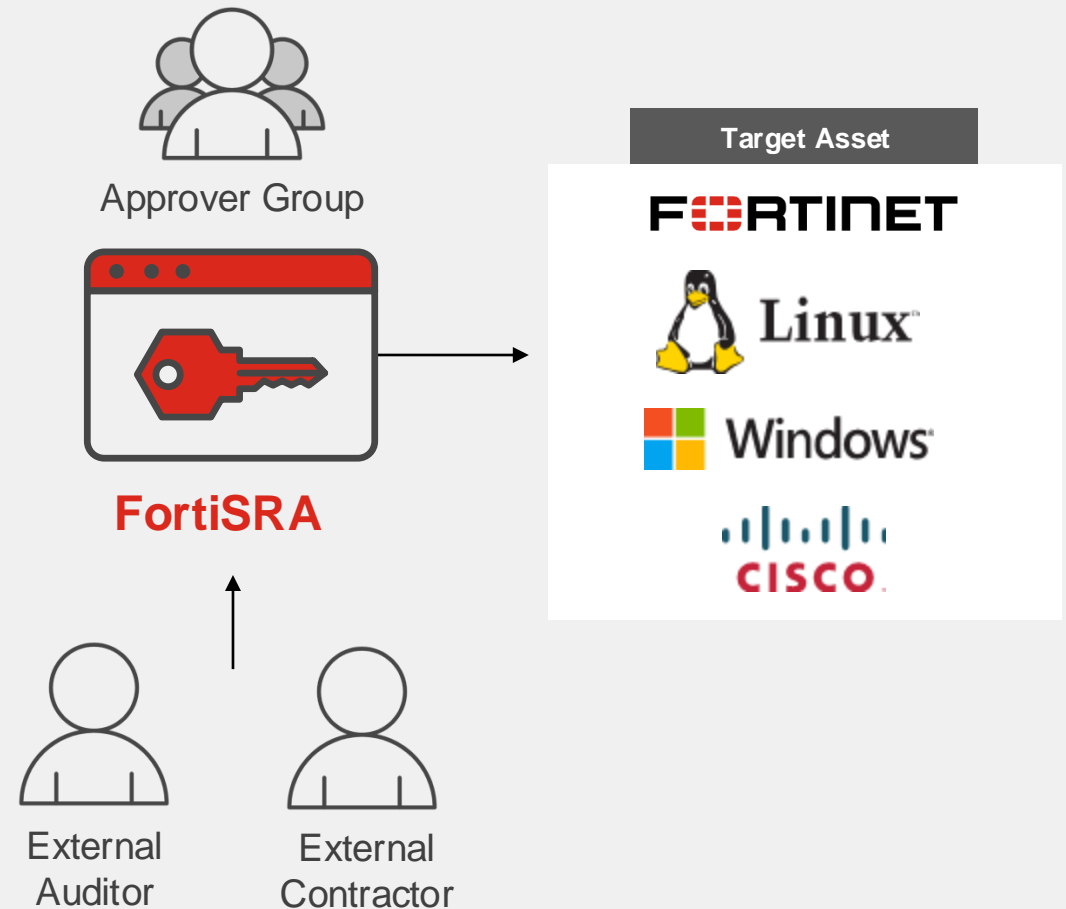
FortiSRA Key Functions

Hierarchical approval

Session Surveillance and Audit

Scheduled credential changing

Target Systems check-out/check-in



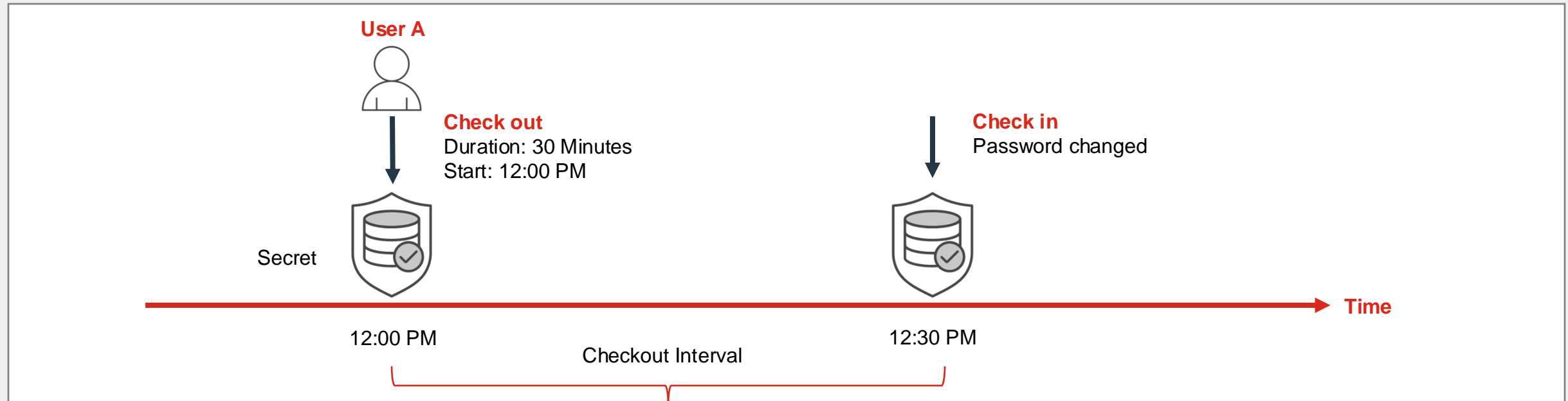
Credential Check in and Check out

Allows FortiSRA users to have exclusive access to a credential for a limited time

- Secret owner or admin enables check out feature
- Only User A can launch the credential during checkout interval unless user A checks in manually

Checkout Enable Disable

↳ Checkout Duration Minutes (3-120)



Secrets: Approvals

- If a secret is configured with an approval policy, approval must be granted before a user may access that secret
- Hierarchical - up to 3 tiers of approval
- Minimum number of approvals may be required for each layer of approval
- Both users and groups may be selected as approvers

FortiSRA KVM

Secret Details - Control-HMI (id: 1)

★ Add Favorite ↻ Change Password ❤️ Verify Password

General Service Setting ⓘ Permission ⓘ Dependency Credential History

Name: Control-HMI

Folder: OT

Target: Control-HMI

Privileged Account: Yes No

Template: Ubuntu_SSH_RDP

Server Information: Inherit Server Information from Template

Associated Secret: No associated secret

Description: Control-HMI for Lightbox Demo

Fields

Host: 172.20.4.22

User: user

Password: ●●●●●●

Secret Setting ⓘ

Automatic Password Changing: Not available

Automatic Password Verification: Not available

Session Recording: Disable Enable

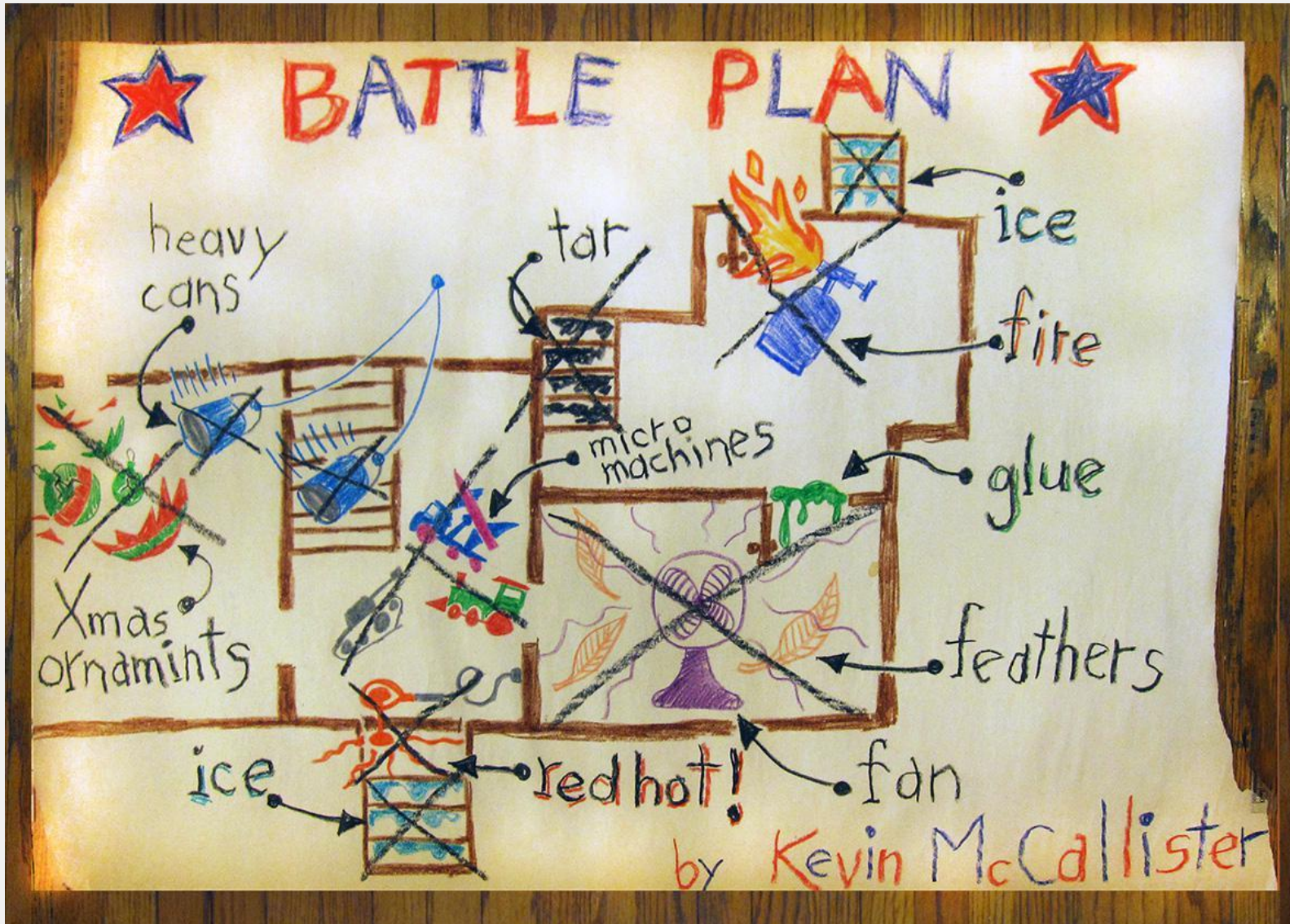
Proxy Mode ⓘ: Disable Enable

Tunnel Encryption: Disable Enable

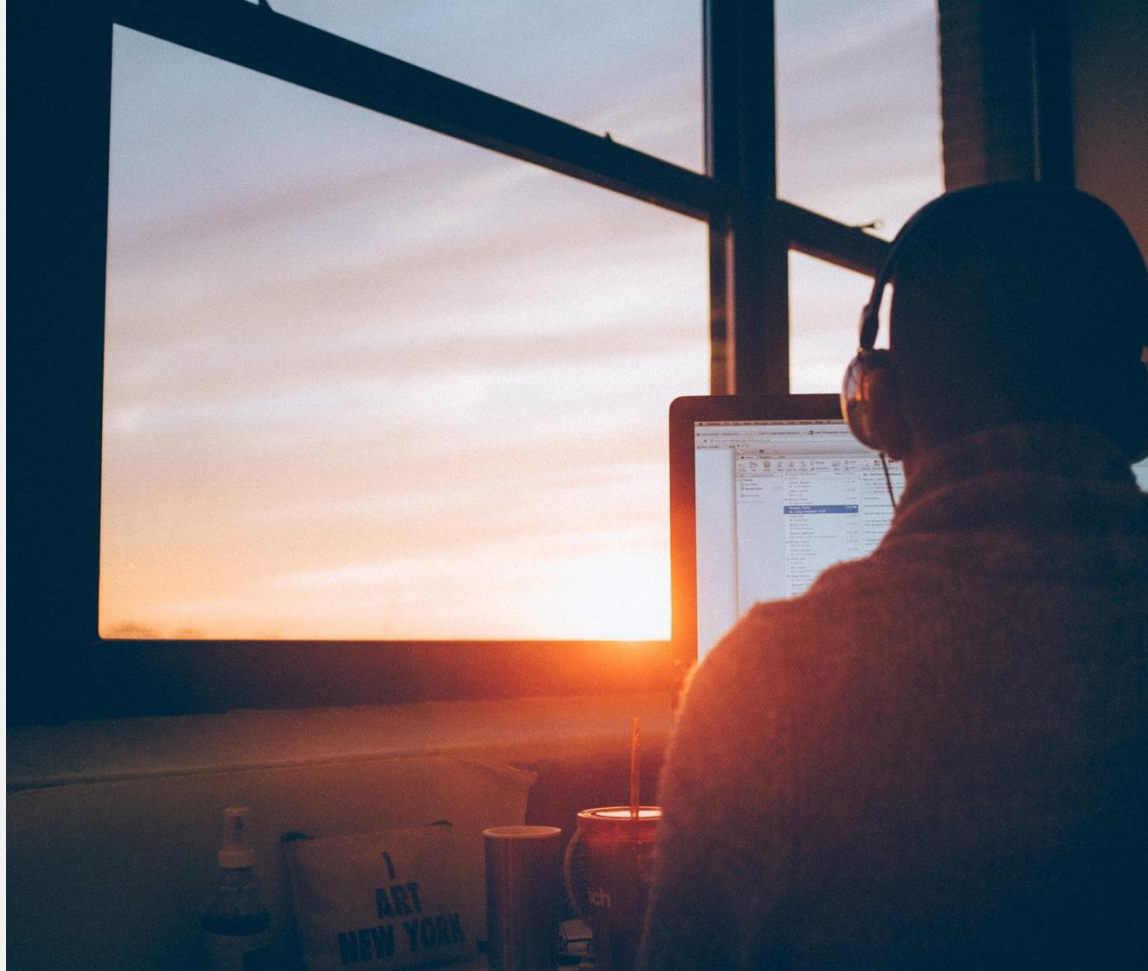
Save Back

FORTINET v1.4.0

FortiDeceptor



VAD ÄR **FORTIDECEPTOR**



DECOYS

- Falska resurser
- Falska applikationer
- Falska tjänster

LURES

- Falska tjänster på en Decoy

NÄTVERKSTRAFIK

- Falsk trafiksignalering

BRÖDSMULOR

- Falska resurser placerade på riktiga system

INTEGRATIONER

Fabric Upstream

Enabled:

Upstream IP Address/URL: Port:

Authorization Status: The device is authorized by upstream. [FGT

Quarantine Via Upstream:

Quarantine Severity: Low Medium High Critical

Quarantine Expiry: seconds



A/D Connector Isolation

AWS Key

CheckPoint-FW-Isolation

Cisco-ISE

CrowdStrike-Isolation

FGT-REST-API

FGT-WEBHOOK

FNAC-WEBHOOK

FSM-Watch-List

FortiEDR-Isolation

GEN-WEBHOOK

Microsoft-ATP

PAN-XMLAPI

Windows Network Isolation



SÄKERHET PÅ DJUPET

Minska Risken

Taktisk

Strategisk

Deception

SD/NDR

FW/EDR/NAC

SIEM/SOAR

- Malware Analys
- Threat Intelligence
- IOC

- Stoppa intrång
- Policyhantering
- Karantänsättning

- Larma
- Korrelera attacken
- Hot från insidan

- Säkra larm
- Intrångsdetektion
- Automatiska åtgärder
- Profilera motståndaren



Bra länkar

MSB om NIS2

<https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/krav-och-regler-inom-informationssakerhet-och-cybersakerhet/nis-direktivet/det-har-ar-nis2-direktivet/>

NIS2 artikel 6 och 21

https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32022L2555#art_6

https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32022L2555#art_21

NCSC Cybersäkerhet i Sverige

<https://www.ncsc.se/siteassets/publikationer/cybersakerhet-i-sverige-2024.pdf>

The logo features the word "FORTINET" in a bold, white, sans-serif font. The letter "O" is replaced by a red square icon with a white grid pattern. The background is black with several large, semi-transparent gray shapes: a large "F" shape at the top, a large "R" shape at the bottom, and a large "I" shape on the right. There are also three red horizontal bars: one at the top left, one in the middle right, and one at the bottom left. A grid of small white dots is located in the bottom right area, and a vertical gray bar is on the far right edge.

FORTINET