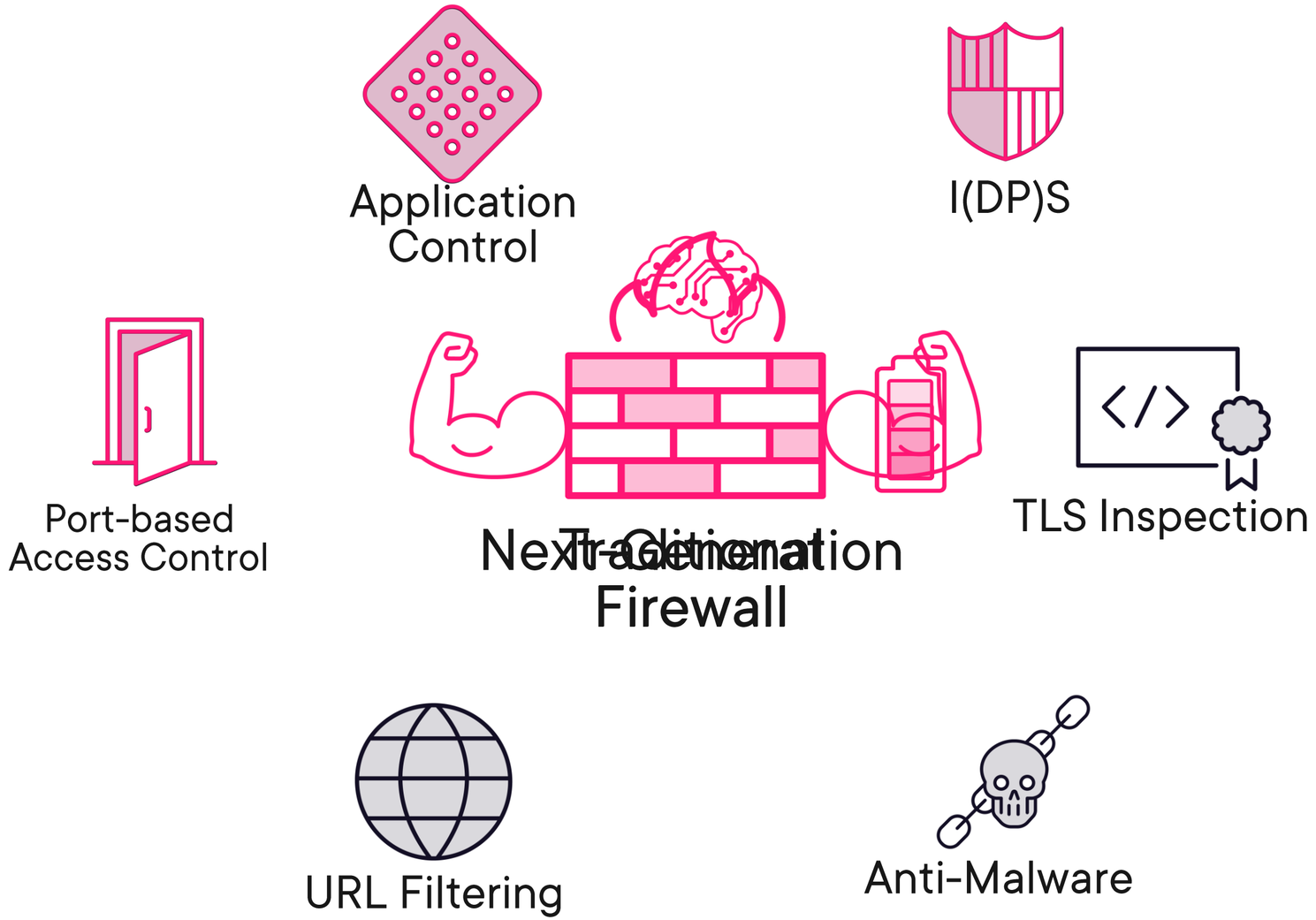
Securing the OT Network



Davy Cavens
OT Security Architect

linkedin.com/in/davycavens/

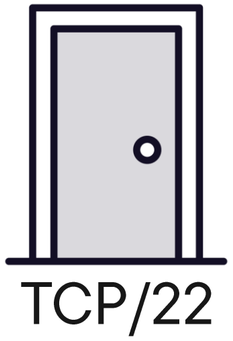
Firewall Types

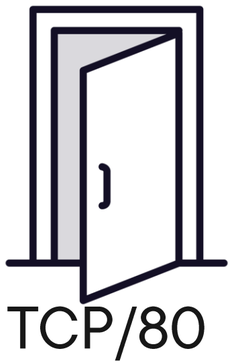


Port-based Access Control

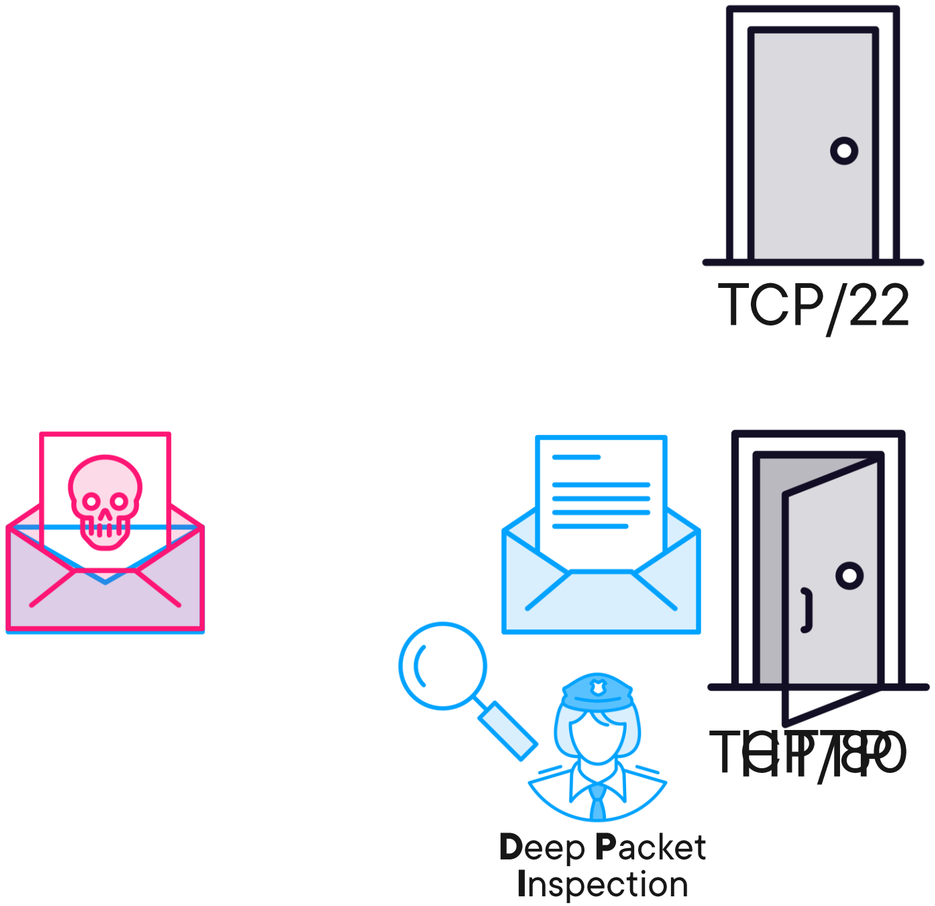




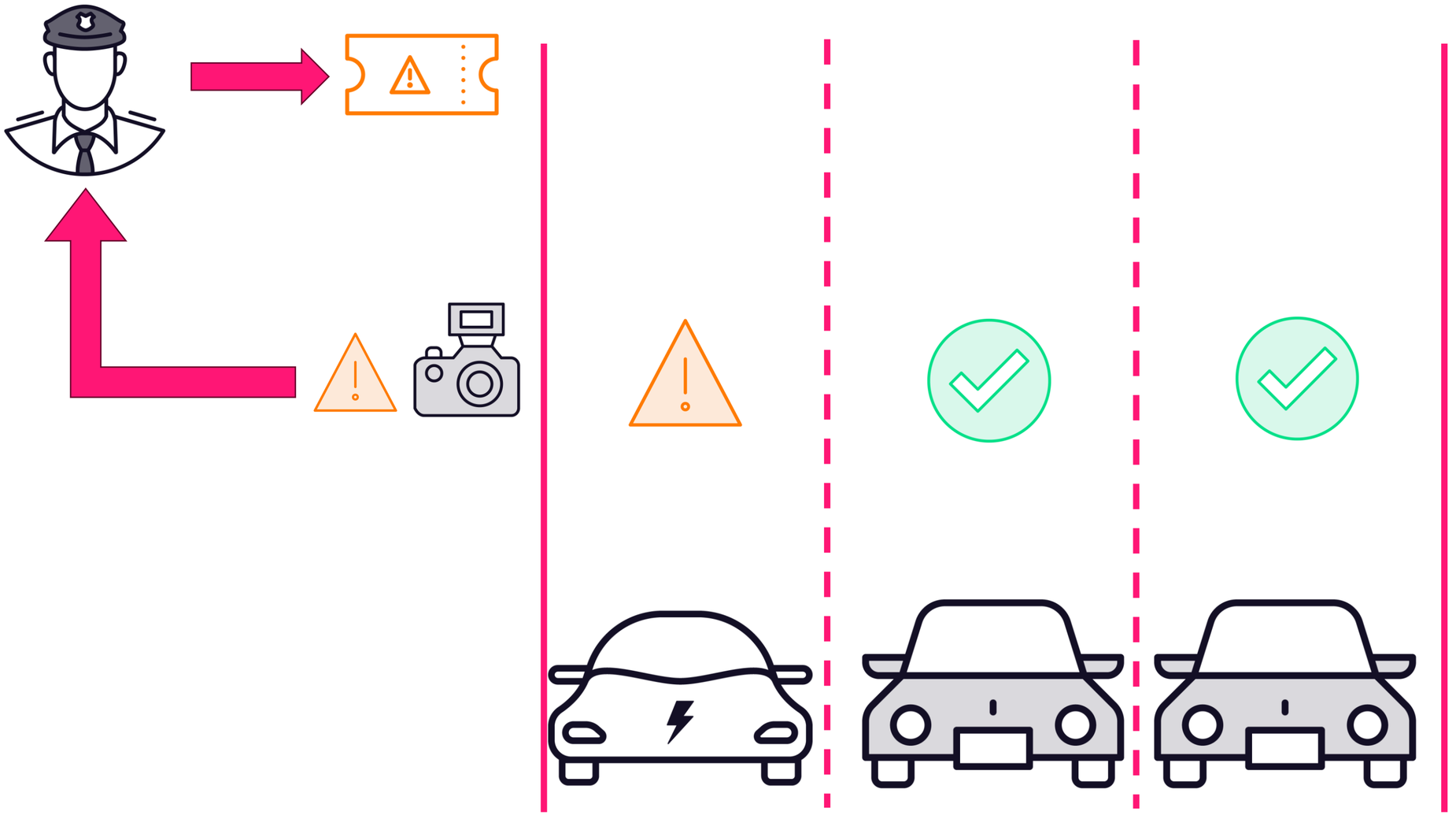




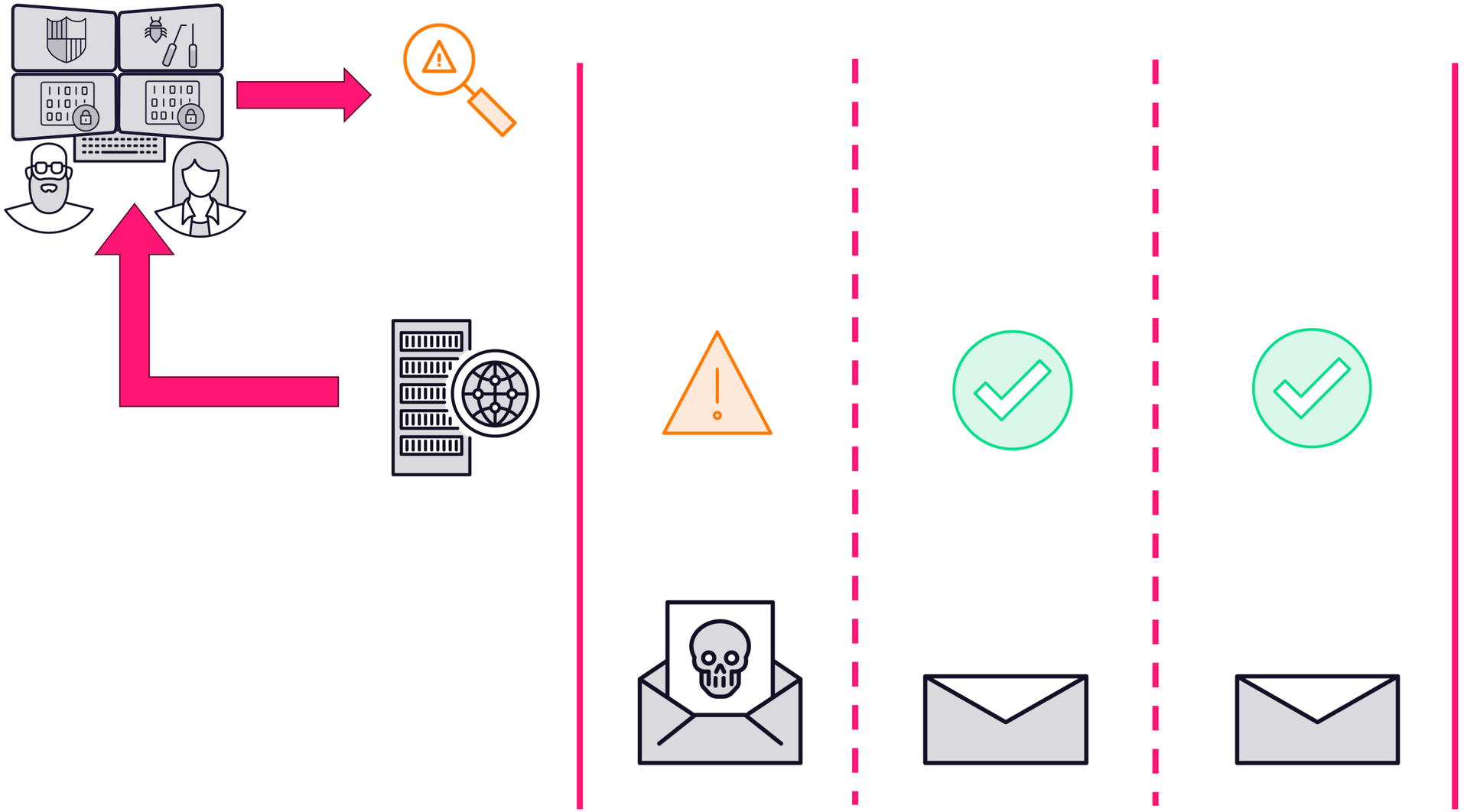
Application Control



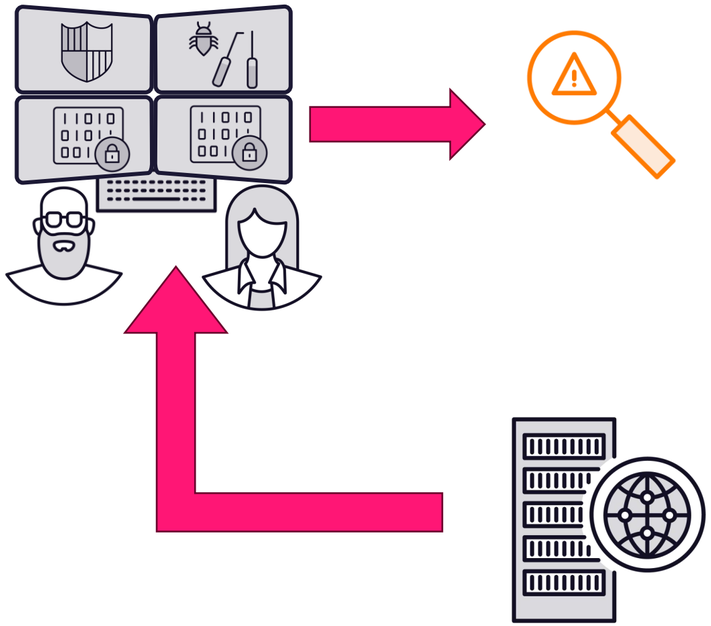
Intrusion Detection



Intrusion Detection



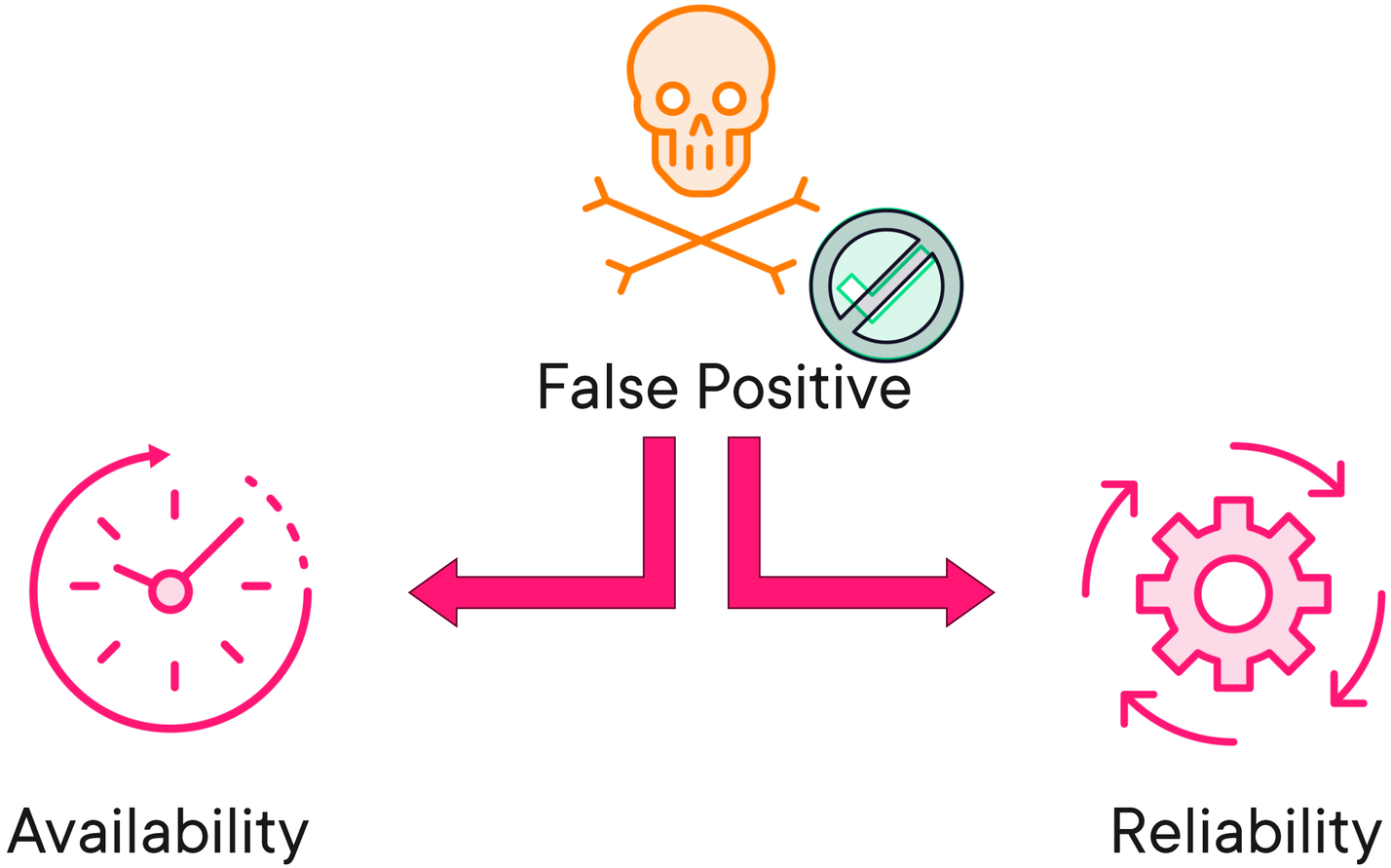
Intrusion Prevention



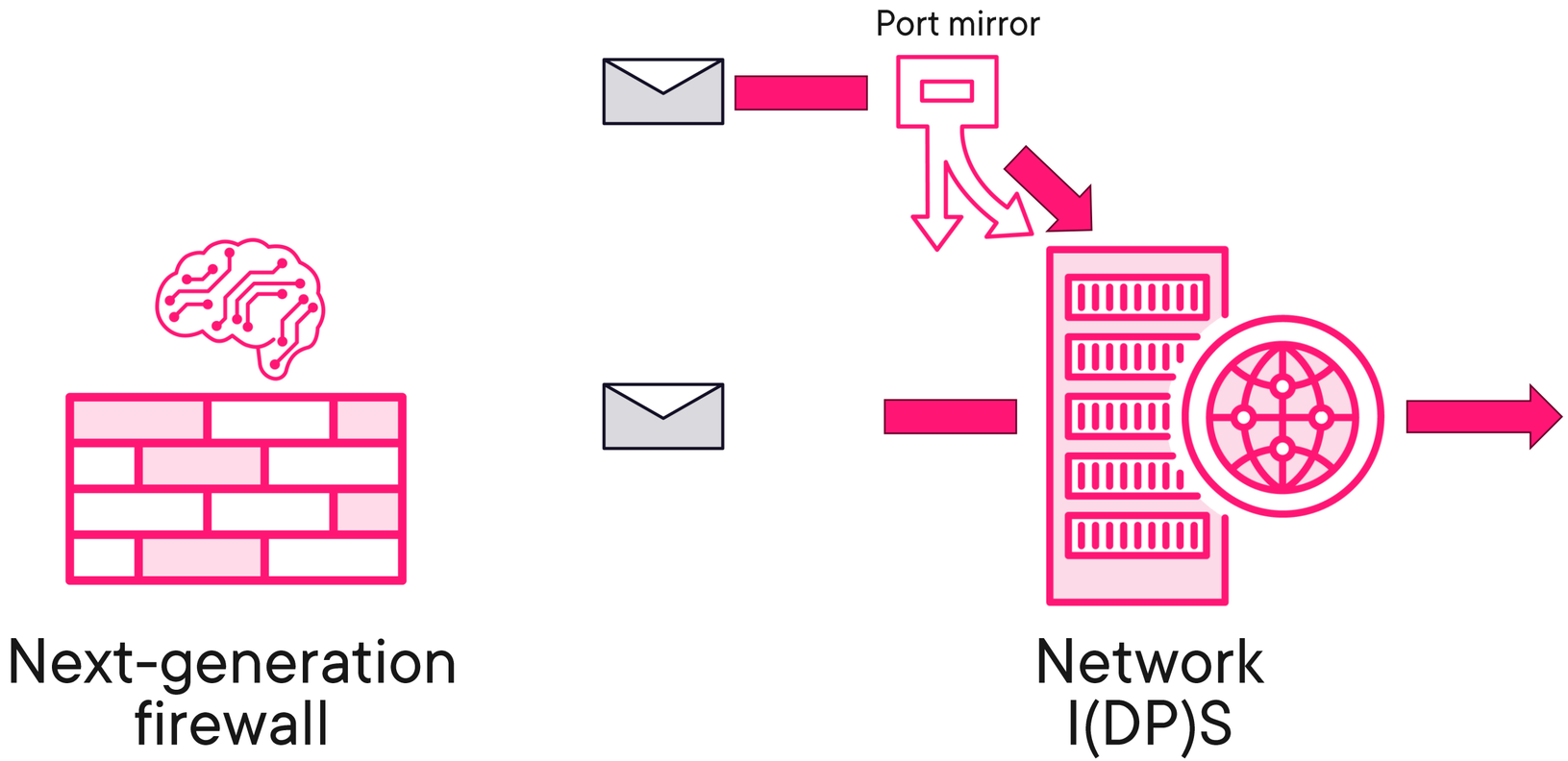




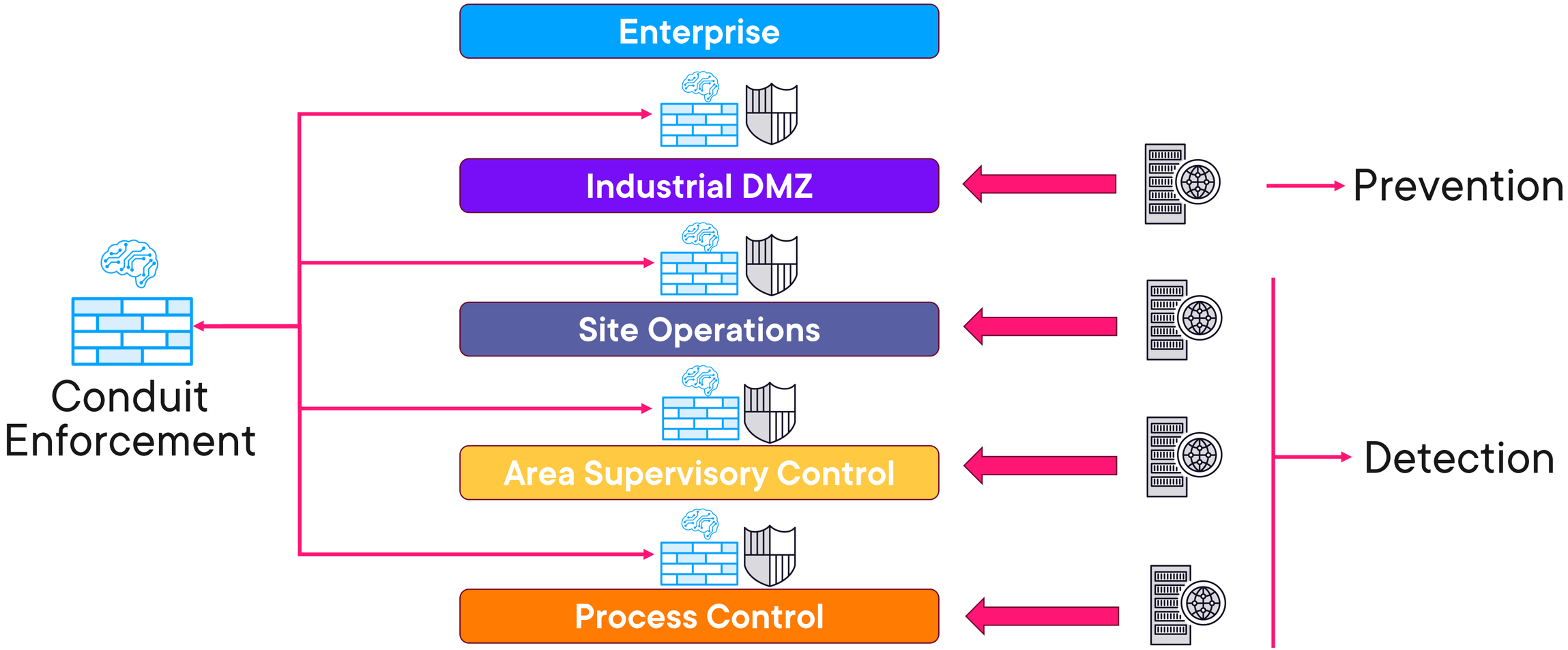
Detection or Prevention?



I(DP)S



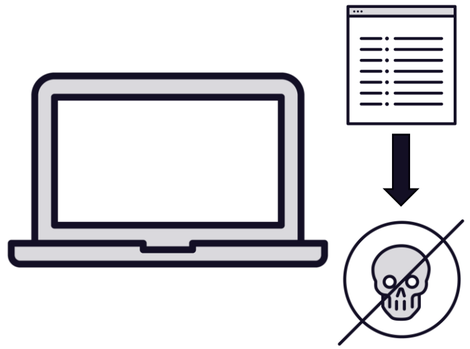
Asset Placement



Endpoint Security

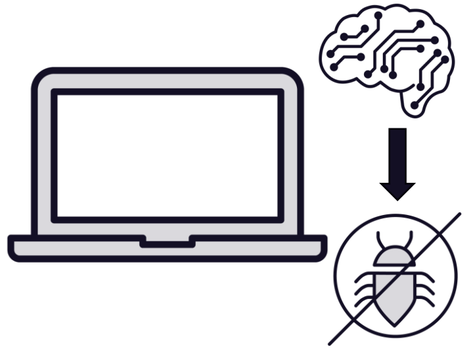
Endpoint Security Types

Antivirus



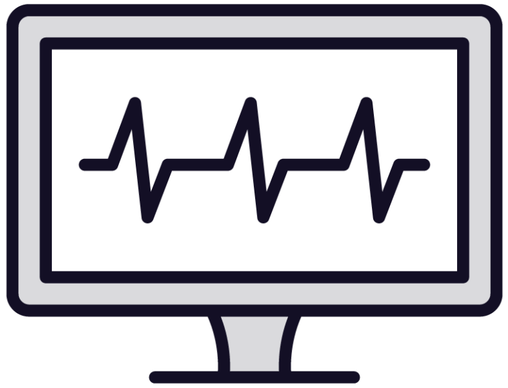
Hash values

Antimalware

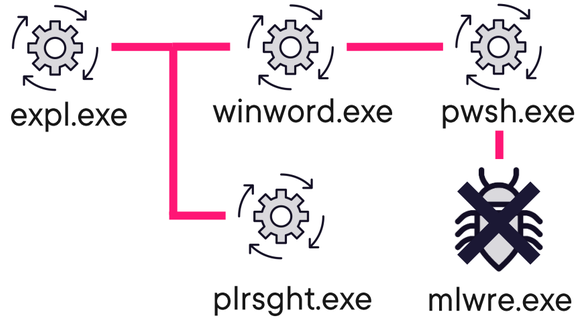


Advanced features

Antimalware Features

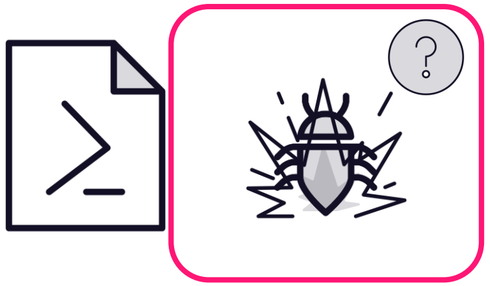


Endpoint
detection and response

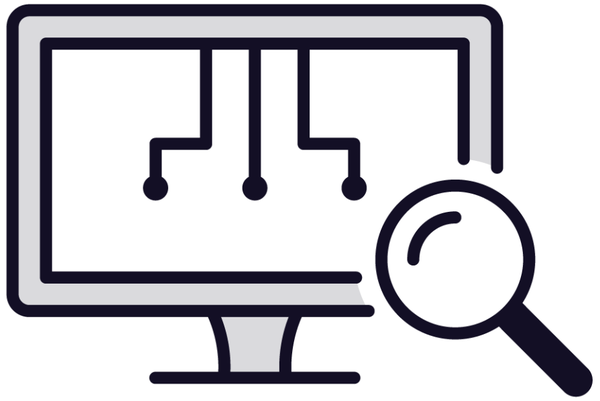




Sandboxing



Sandbox



Behavior Analysis

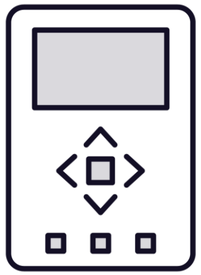


In-memory
analysis

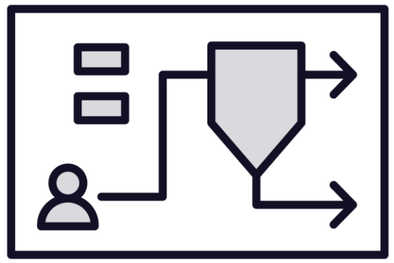


Host-based
intrusion prevention

Considerations



PLC



HMI

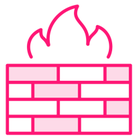


Endpoint security

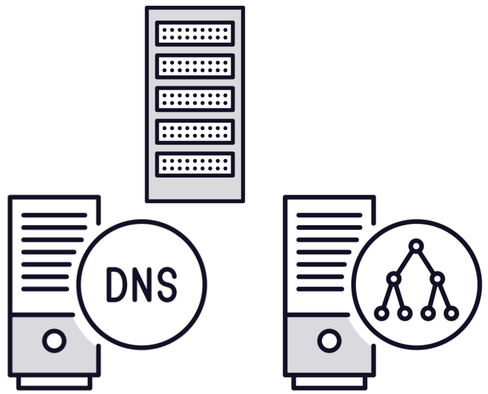


Additional controls

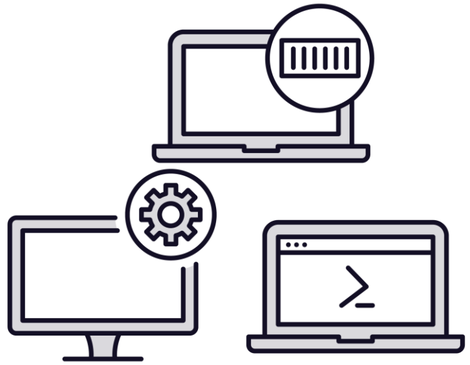




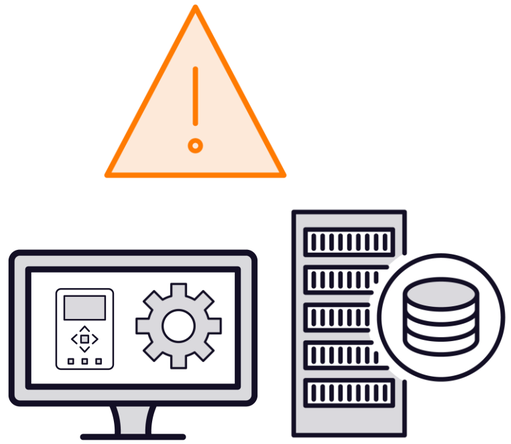
Installing Antimalware



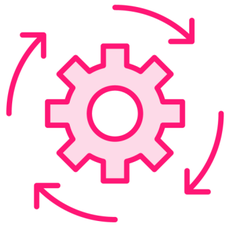
Supporting servers



OT End-user devices



OT servers

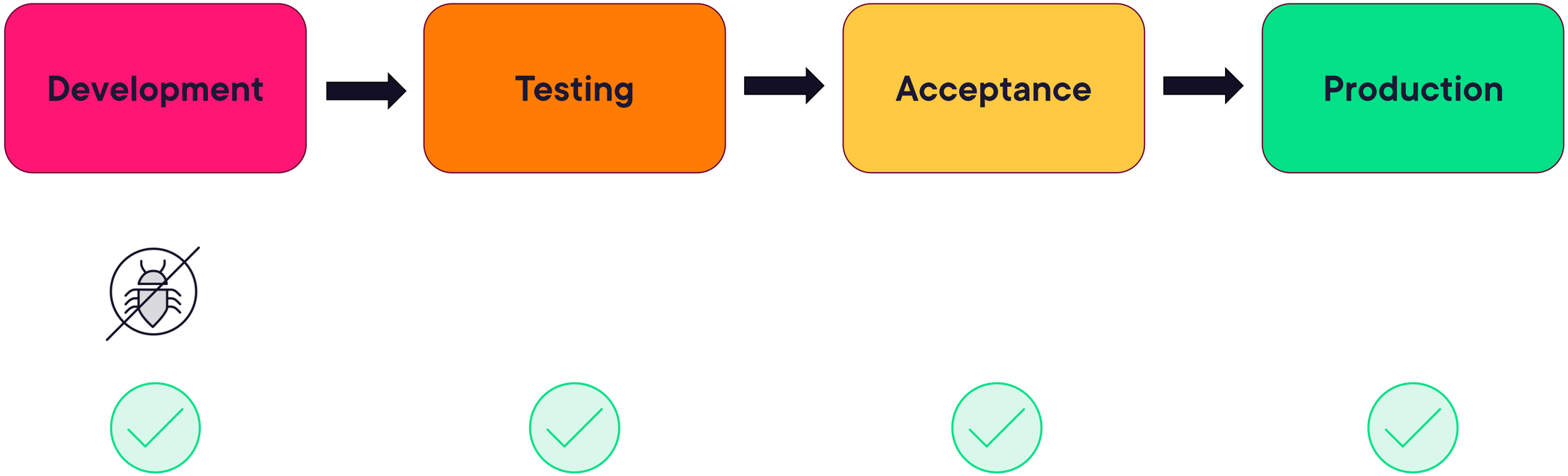


Reliability

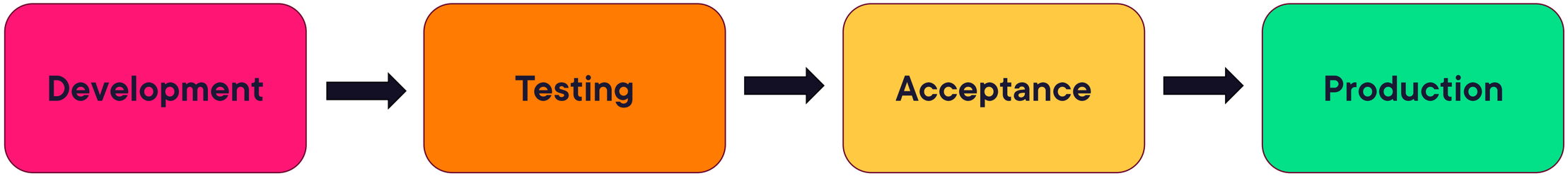


Availability

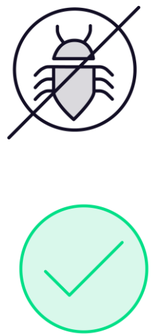
Considerations



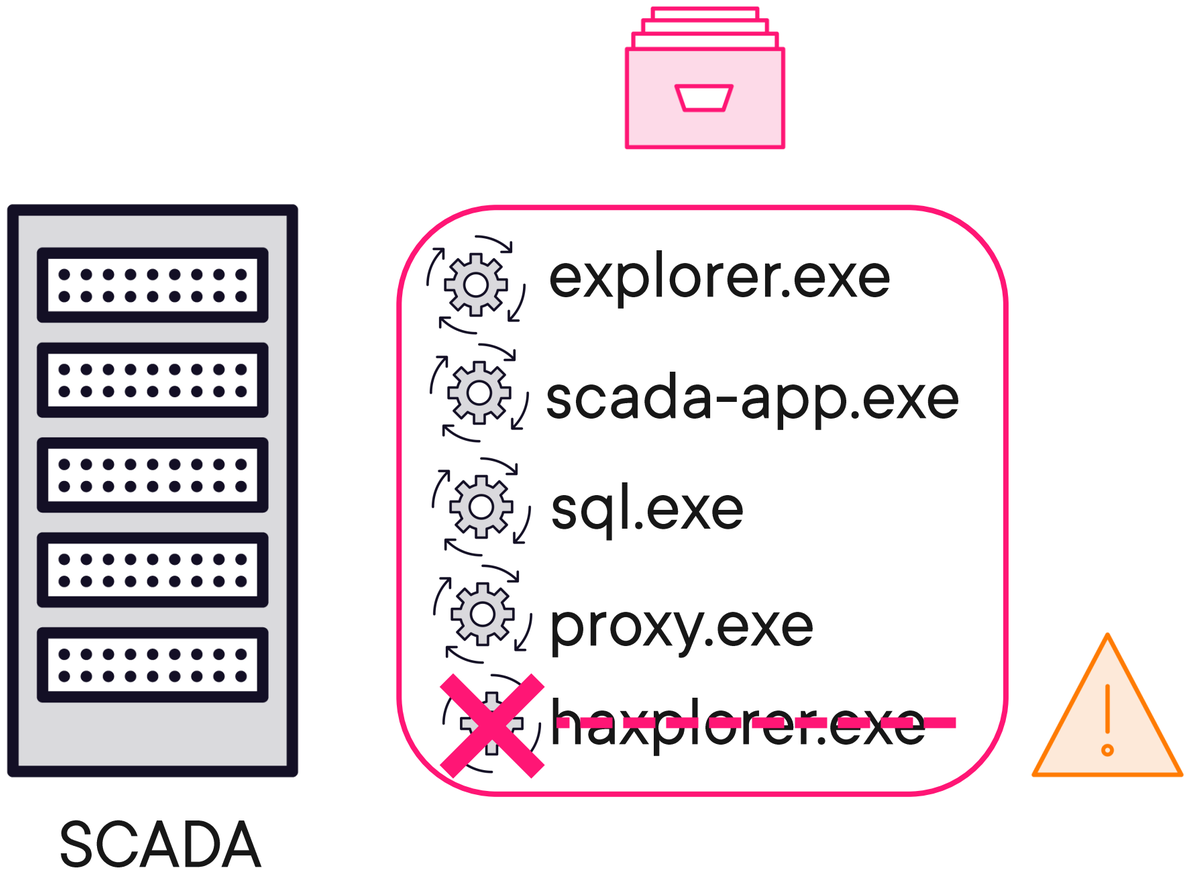
Considerations



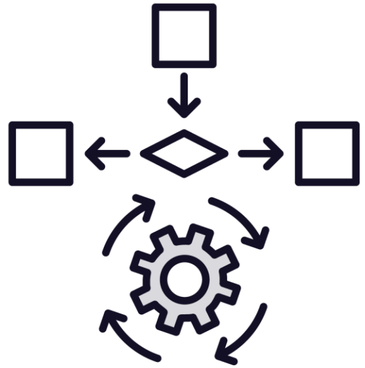




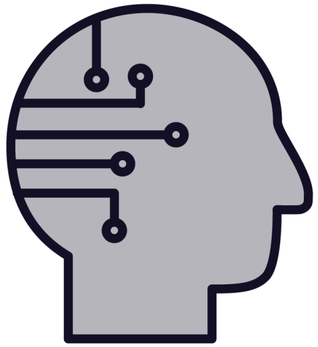
Application Whitelisting



Considerations



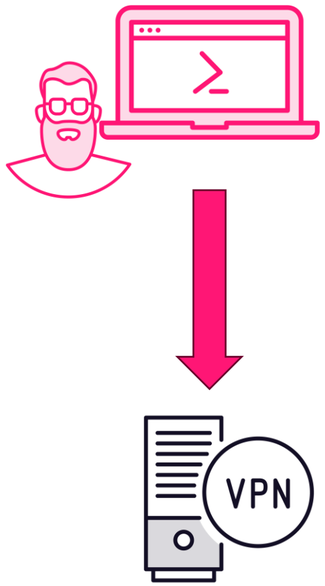
Static environment



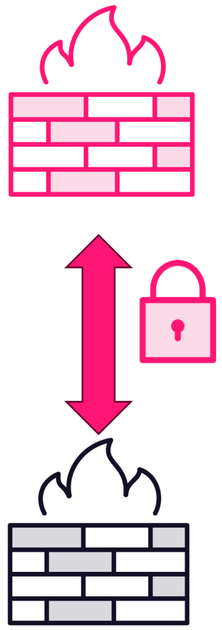
Overhead

Remote Access

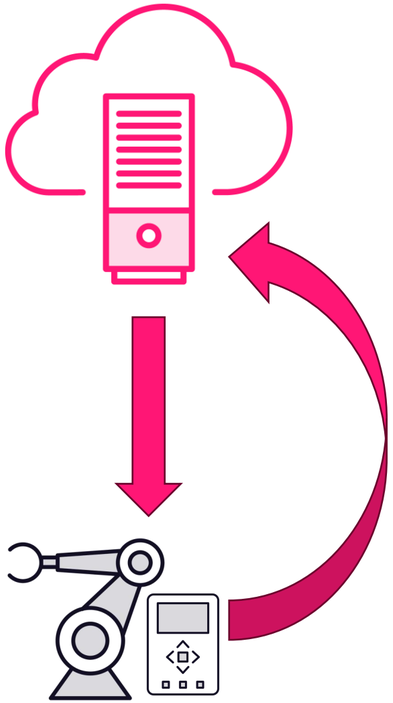
Remote Access



Client VPN

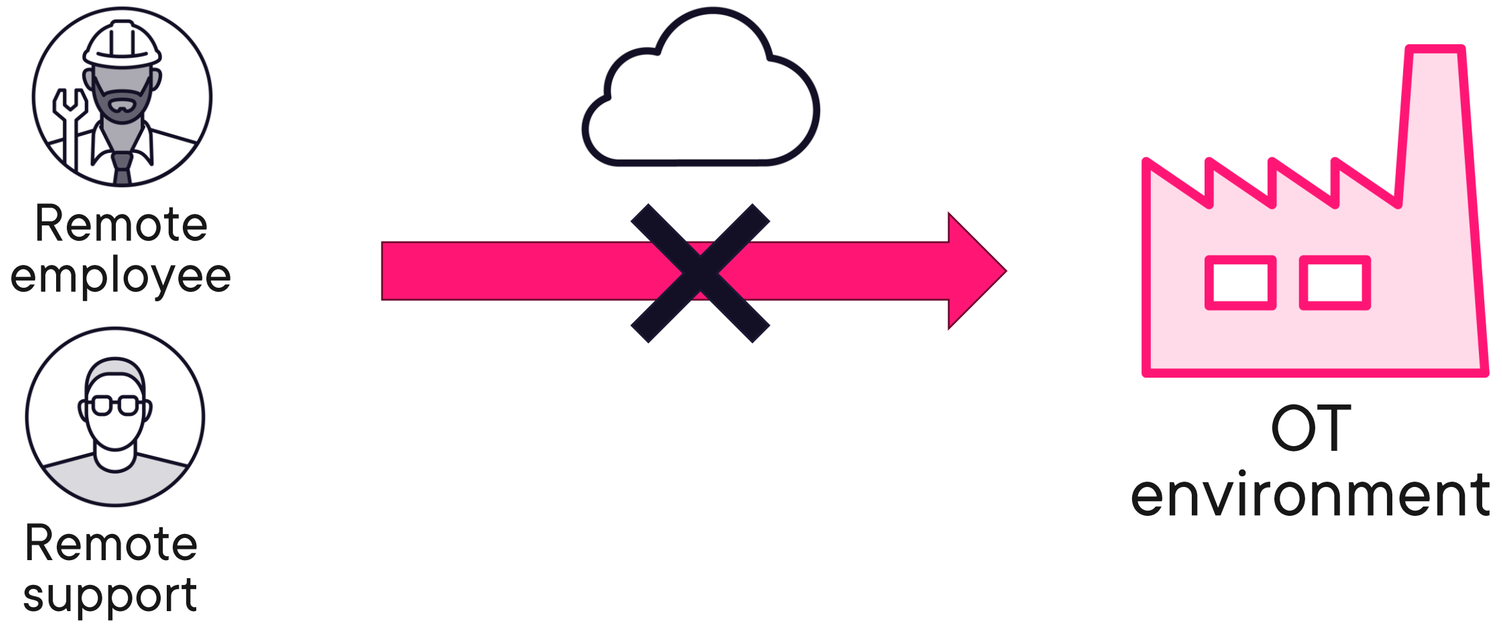


Site-to-Site VPN

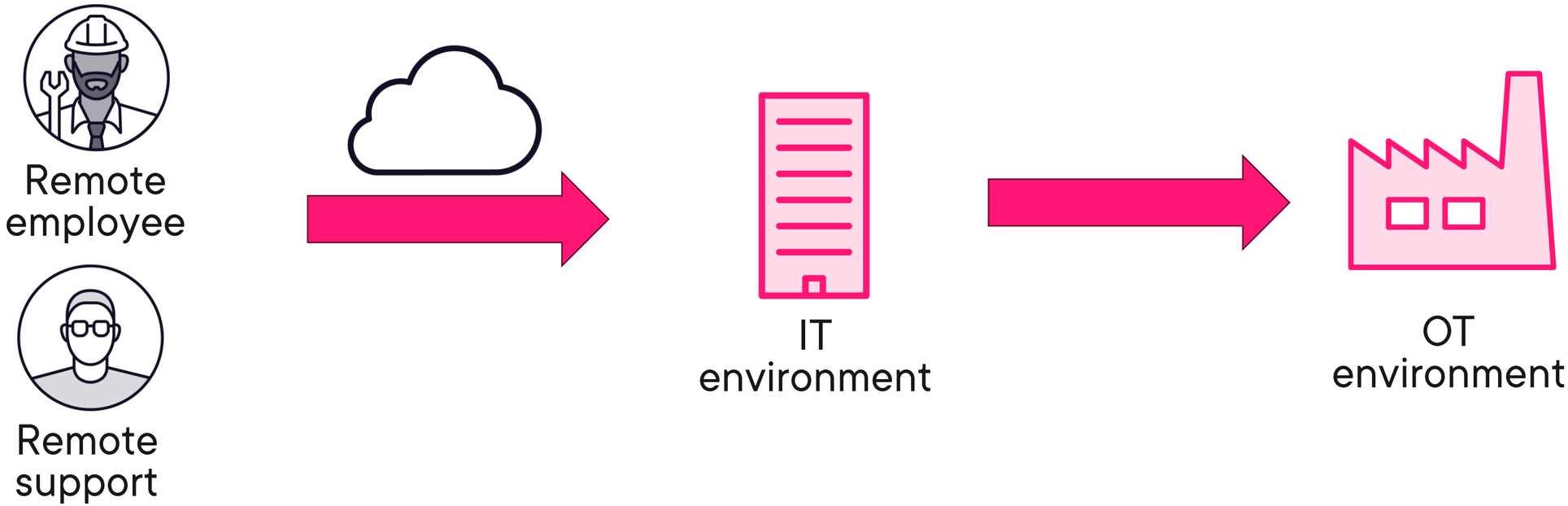


Service tunnel

Client VPN



Client VPN

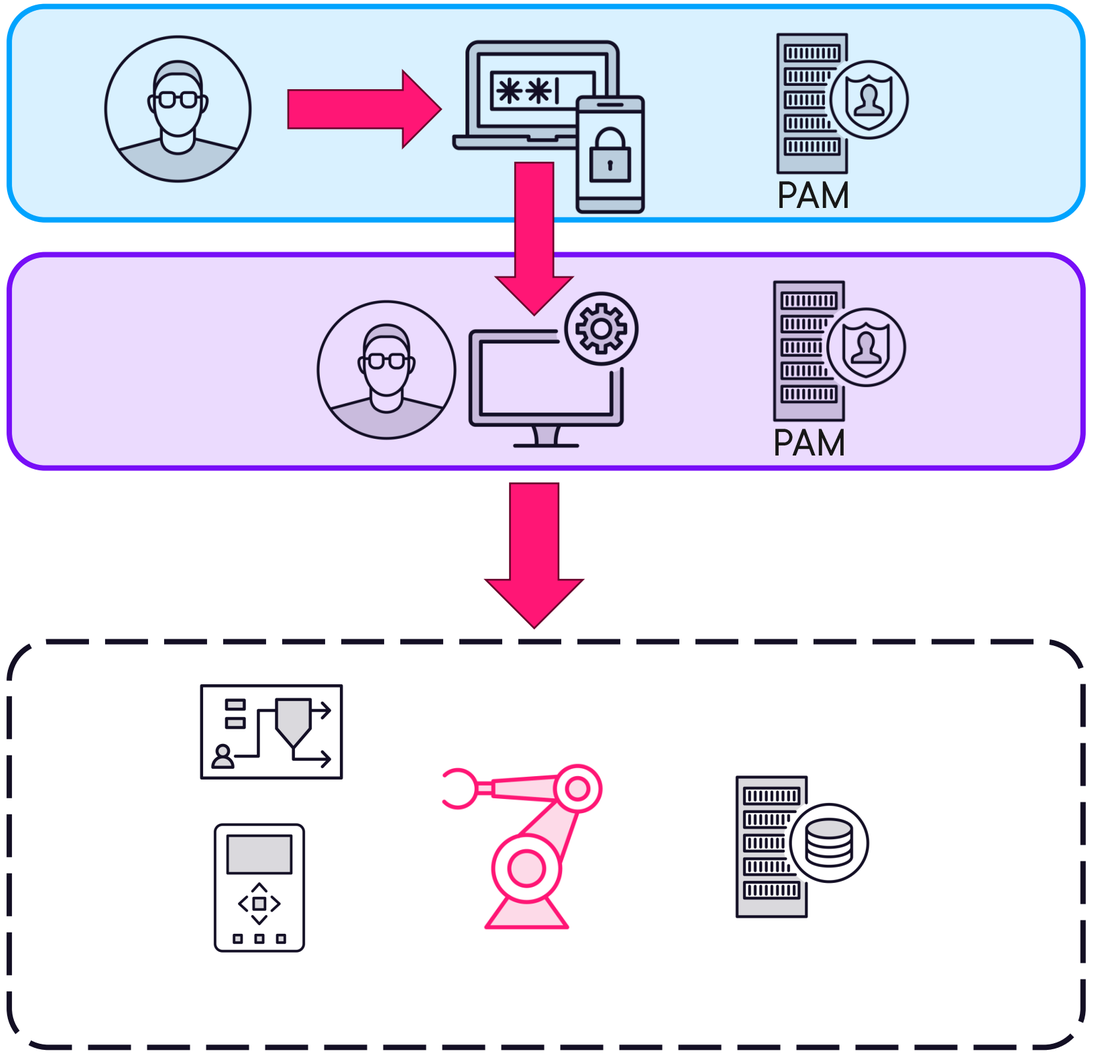

Remote employee
Remote support
IT environment
OT environment

Client VPN

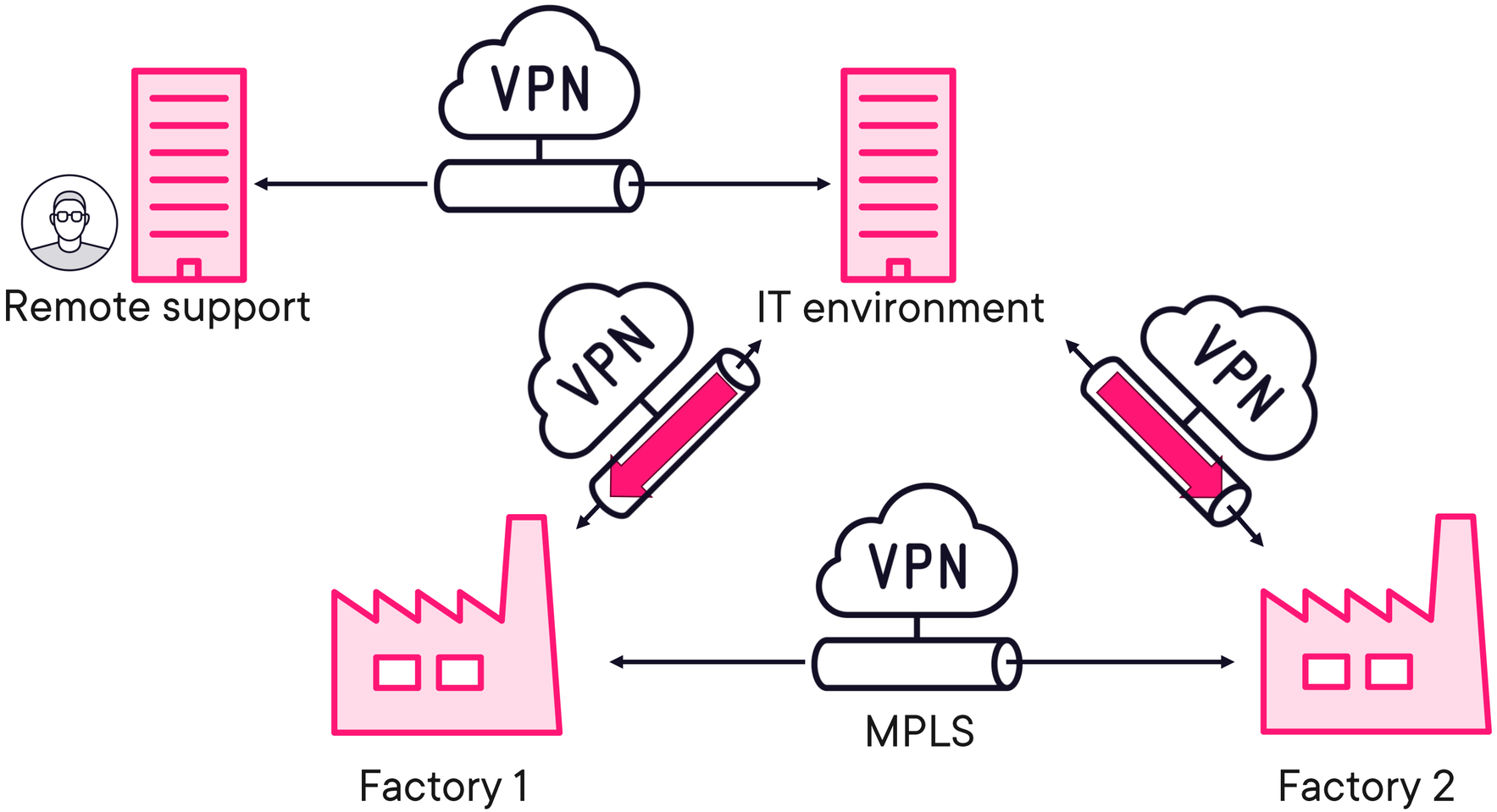
Enterprise

Industrial DMZ

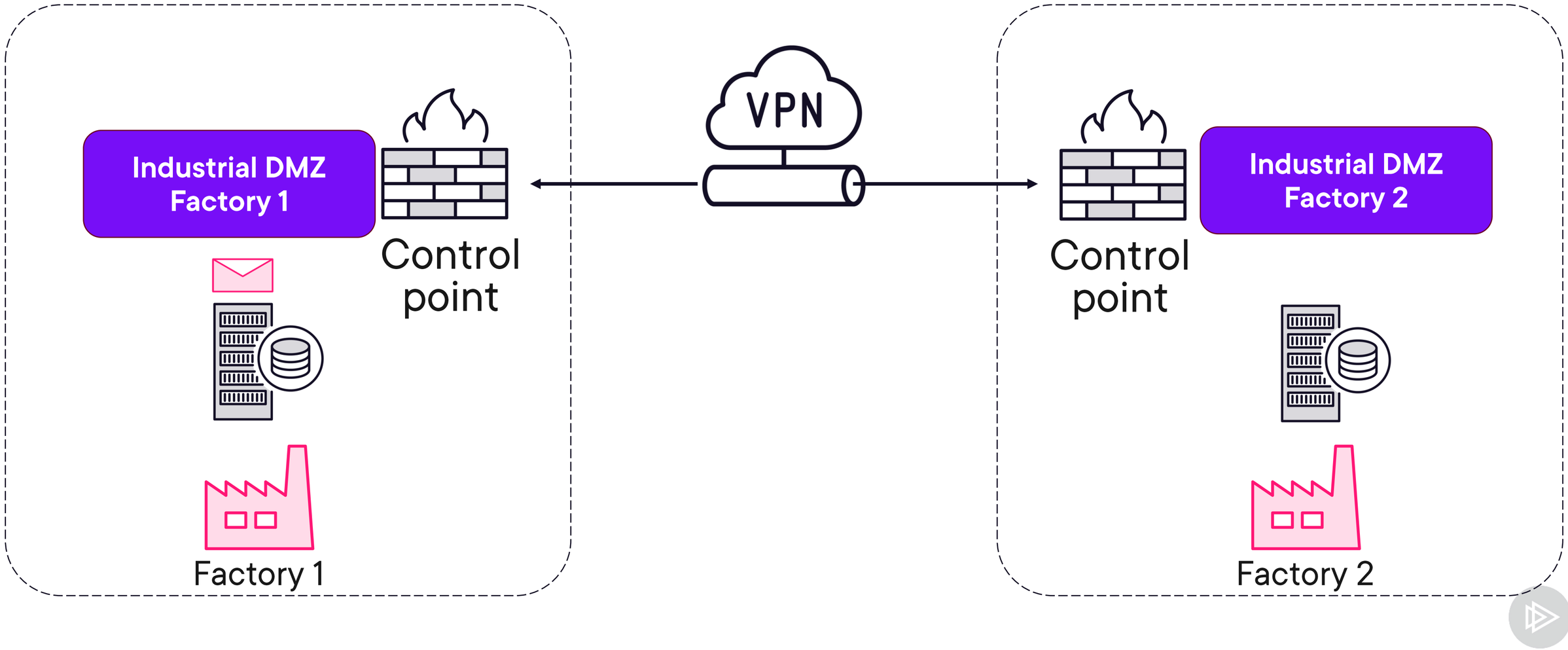
Internal OT network



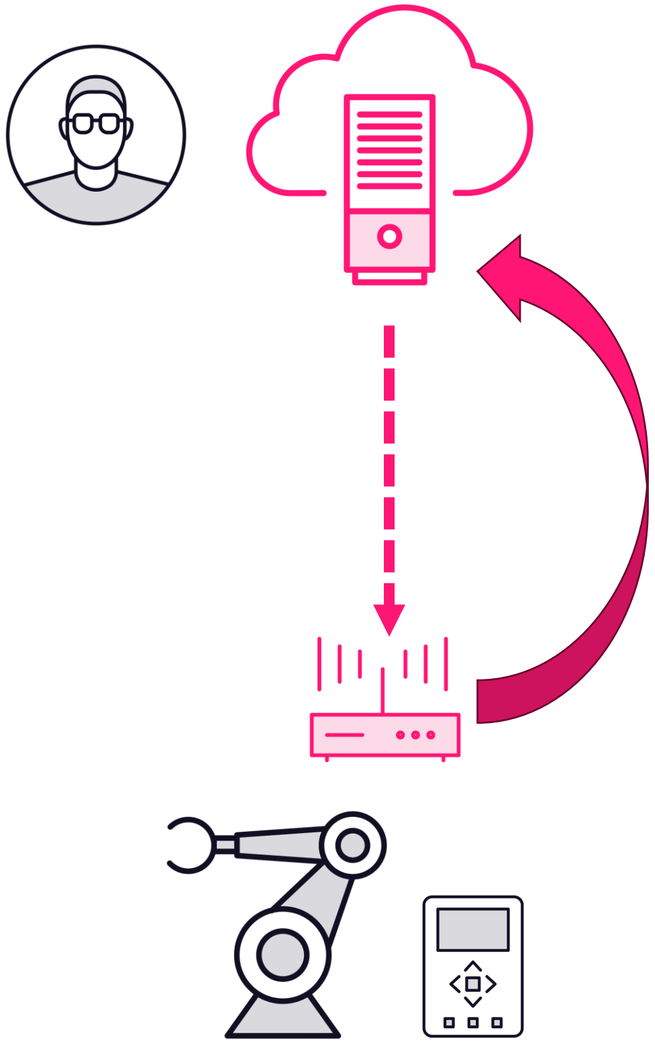
Site-to-Site VPN



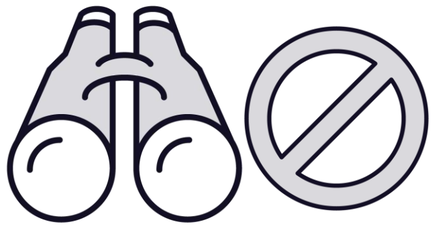
Connecting Industrial Environments



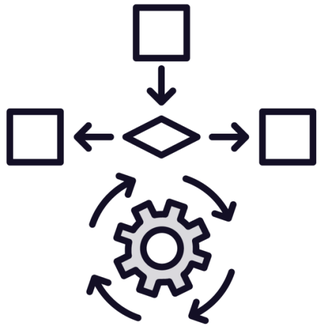
Service Tunnel



Service Tunnel Risks



Lack of visibility



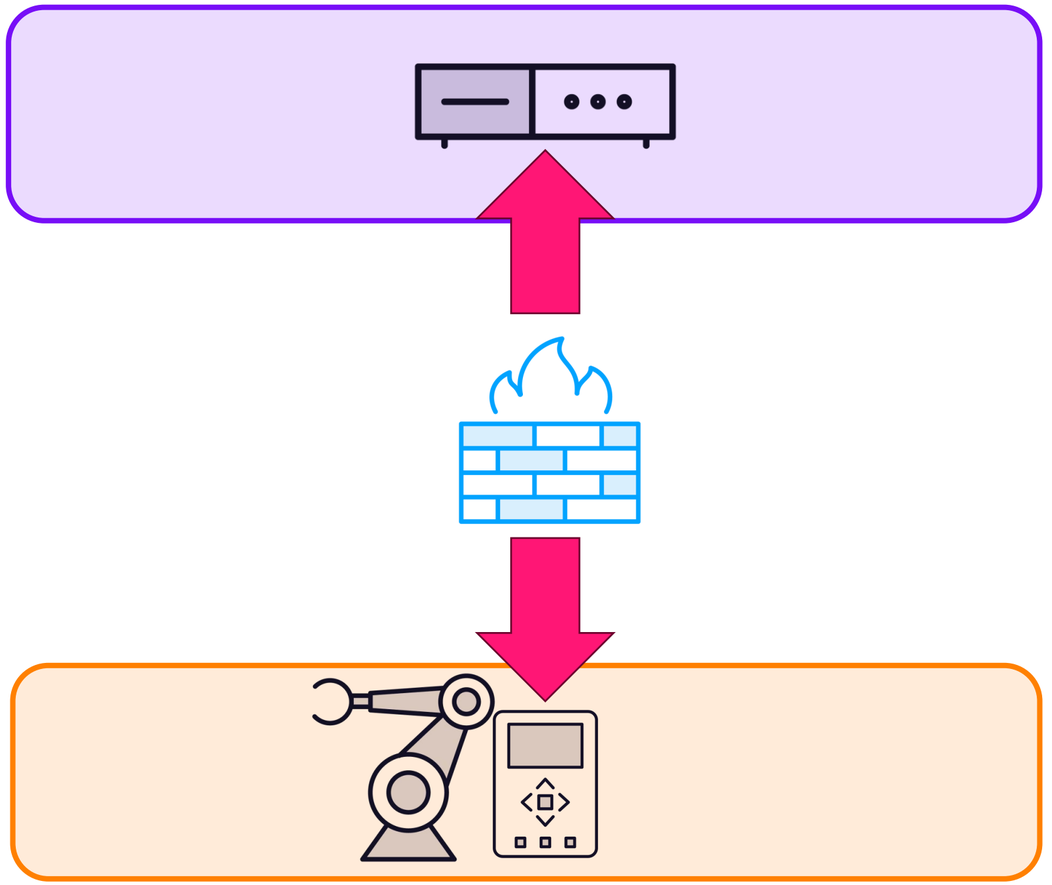
Lack of control



Risk to availability

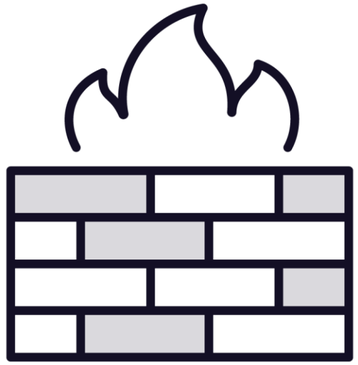
Service Tunnels

Industrial DMZ



Basic Control

General VPN Guidelines



Control points



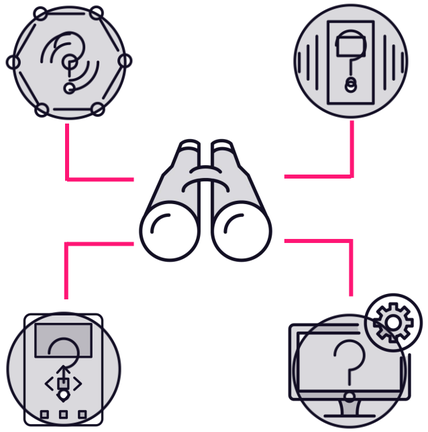
Least privilege



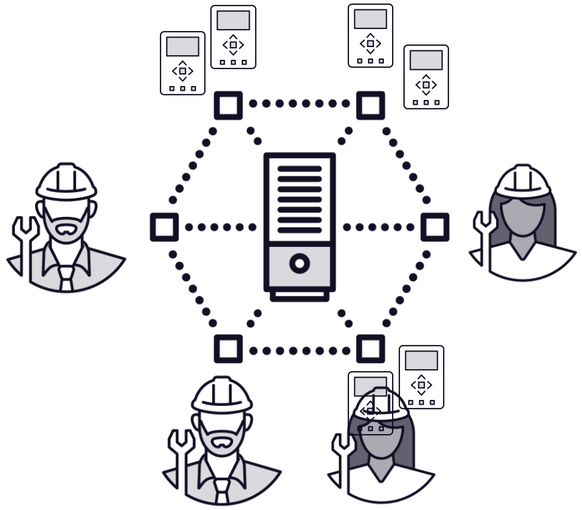
IT as proxy

Network Access Control

Why NAC?



Visibility



Segmentation



Prevent
unauthorized devices

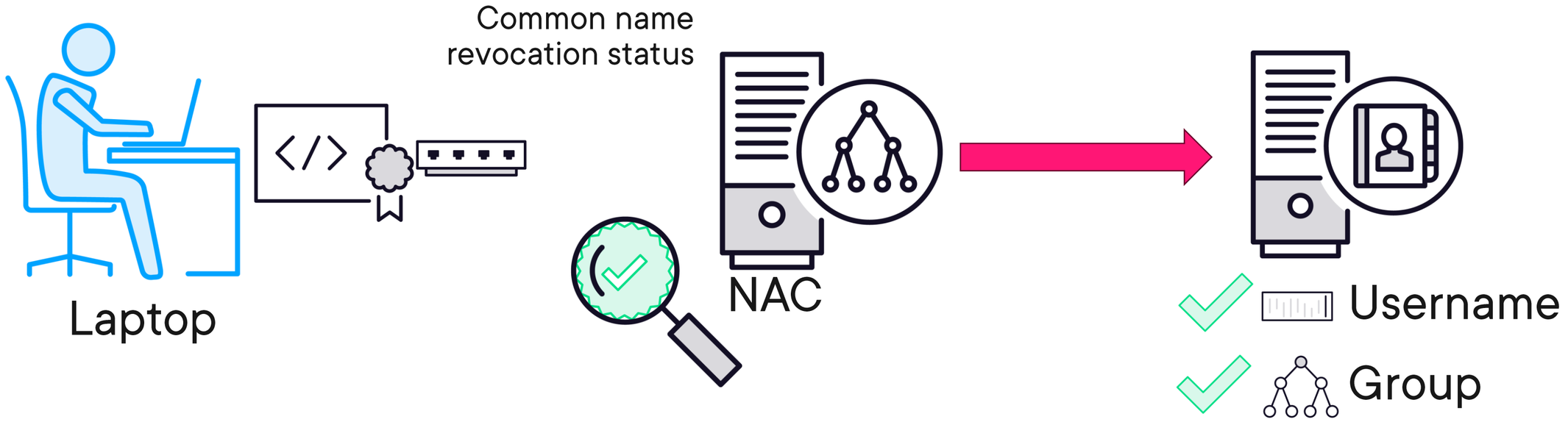
Network Access Control



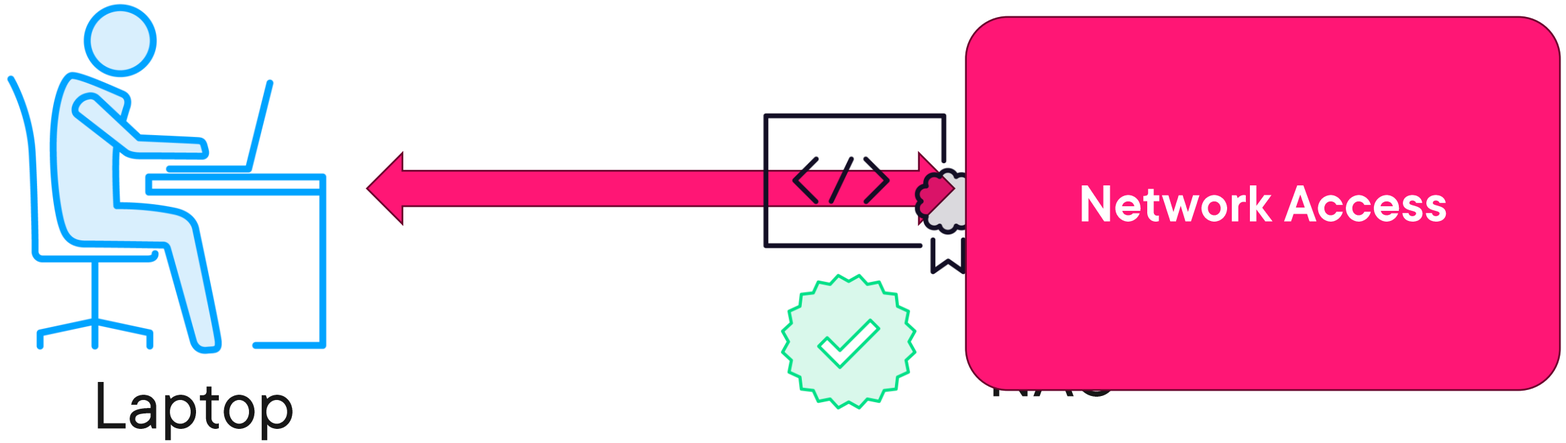
Network Access Control



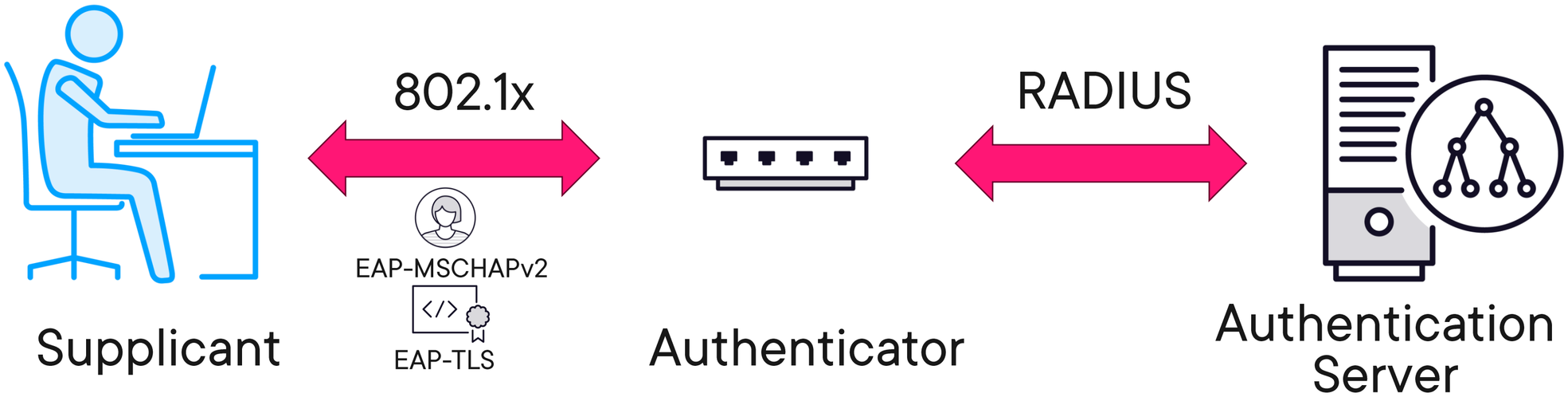
Network Access Control



Network Access Control



Protocols

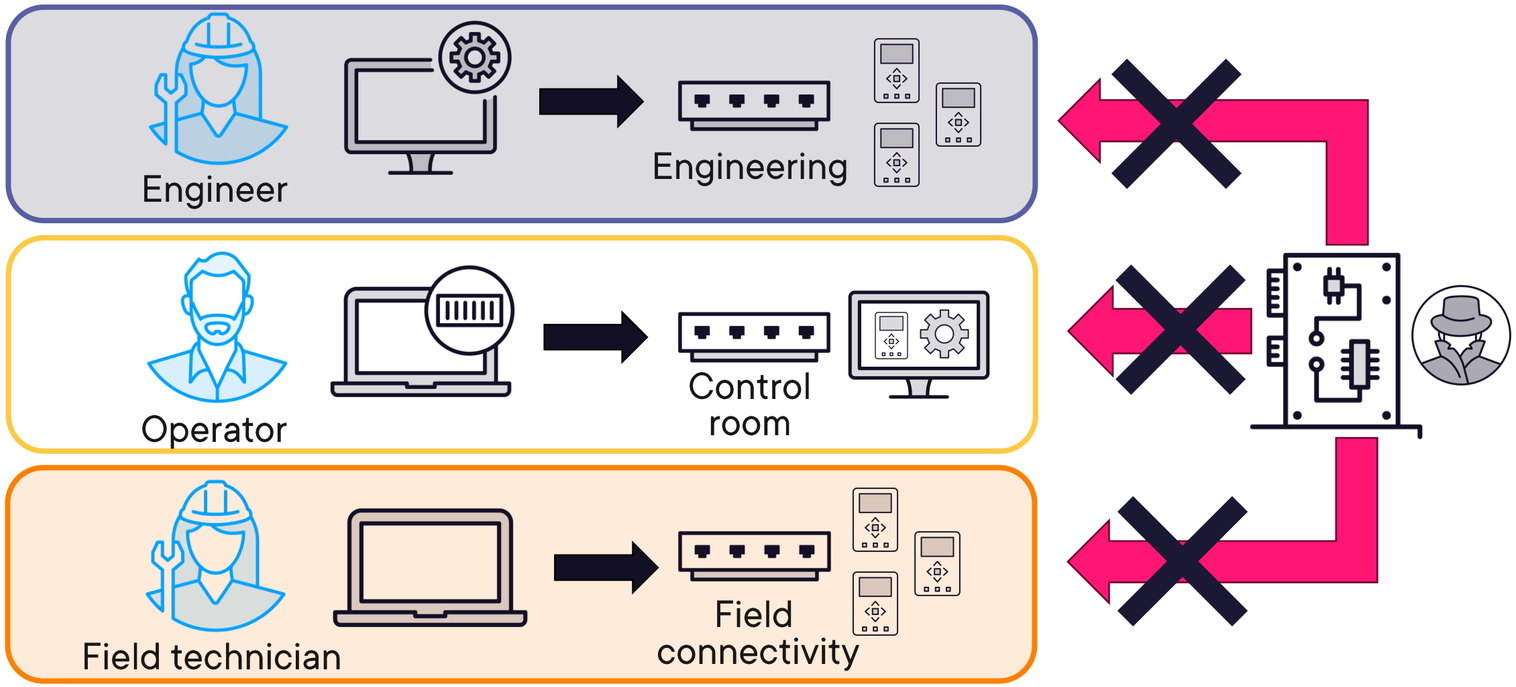

802.1x
EAP-MSCHAPv2
EAP-TLS
RADIUS
Supplicant
Authenticator
Authentication Server

OT Network Access Control

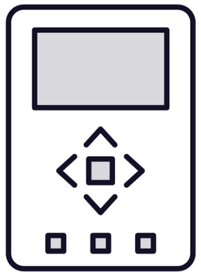
Site Operations

Area Supervisory Control

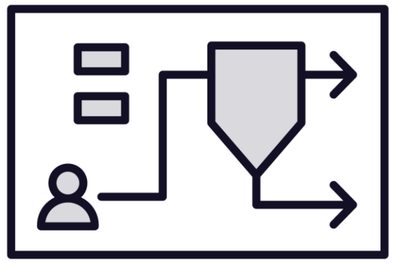
Basic Control



Considerations



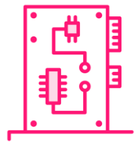
PLC



HMI



802.1x



MAC
Authentication
Bypass



Profiling

Practical Usecase

Overview

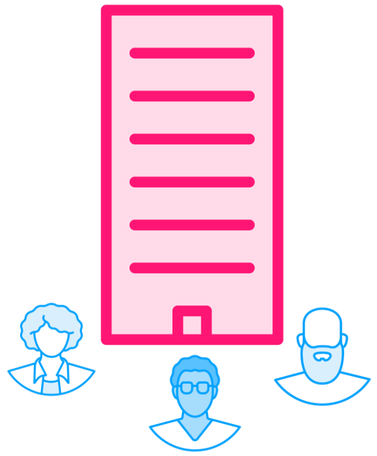


Sam

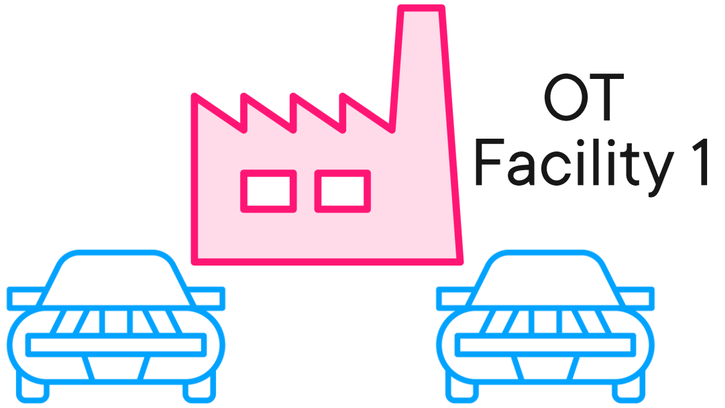


Dan

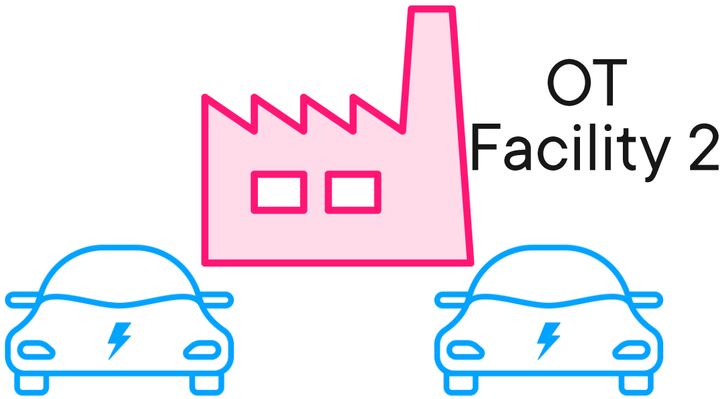
ACME-CAR



IT datacenter
HQ

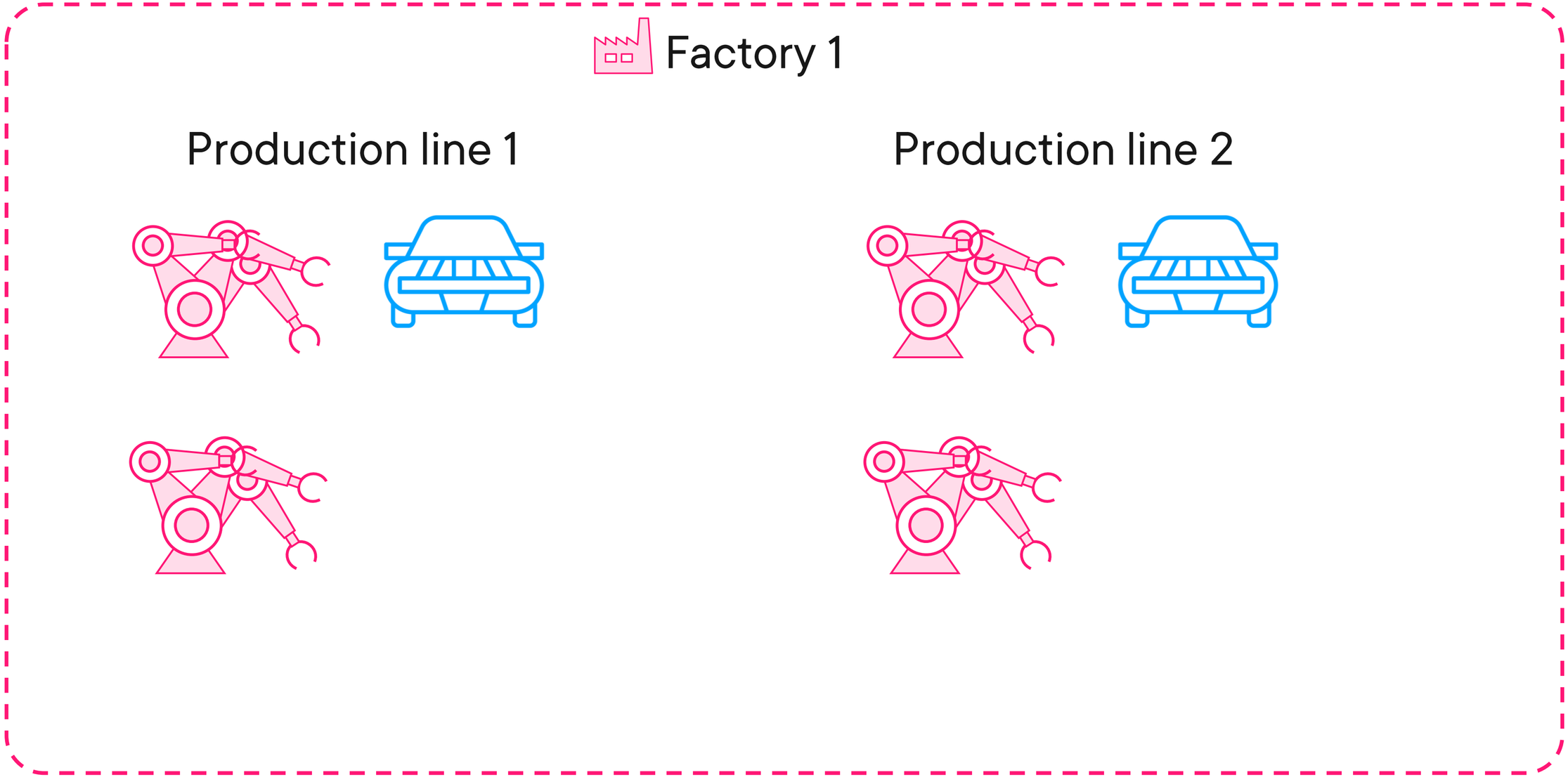


OT
Facility 1

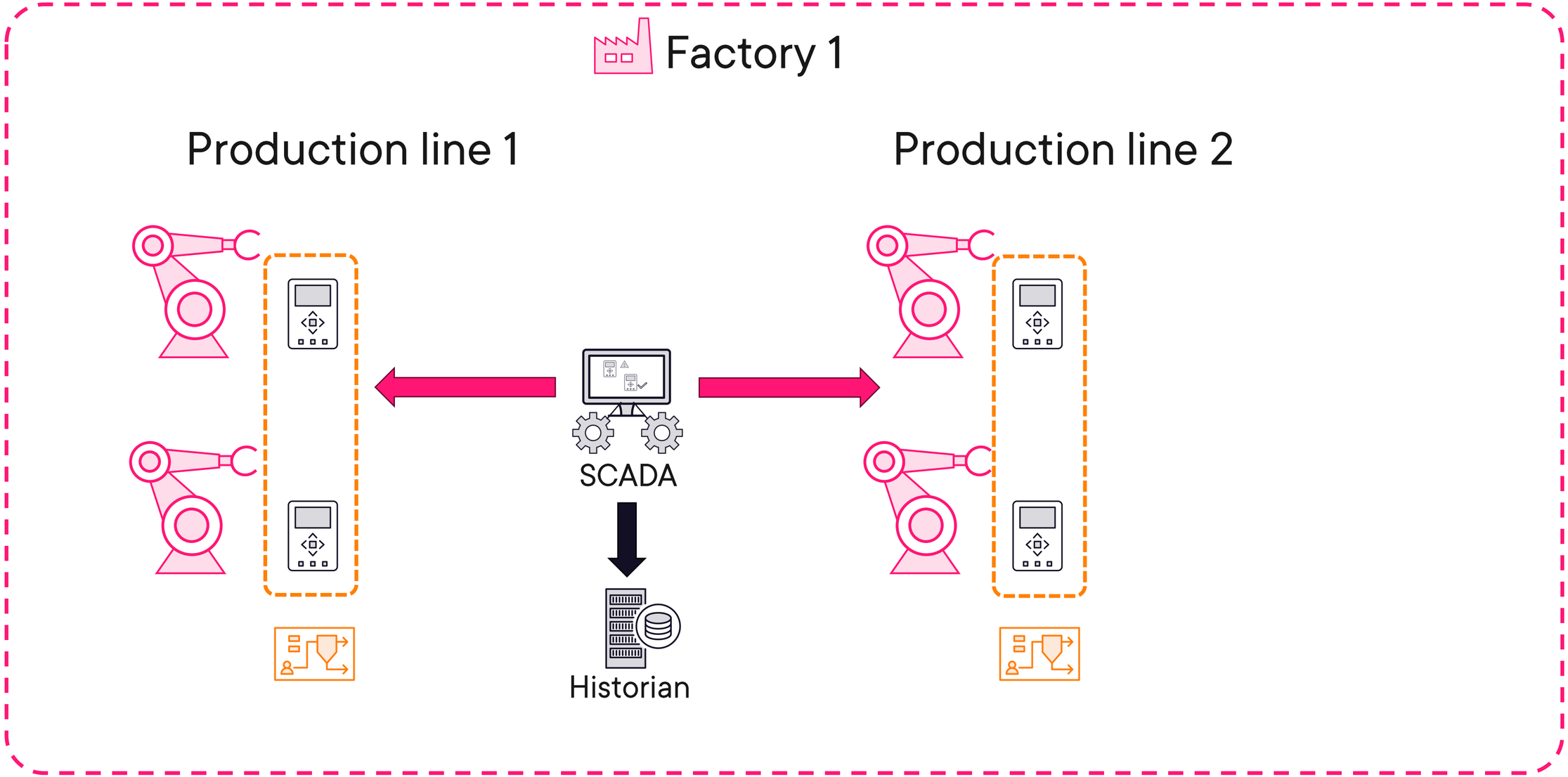


OT
Facility 2

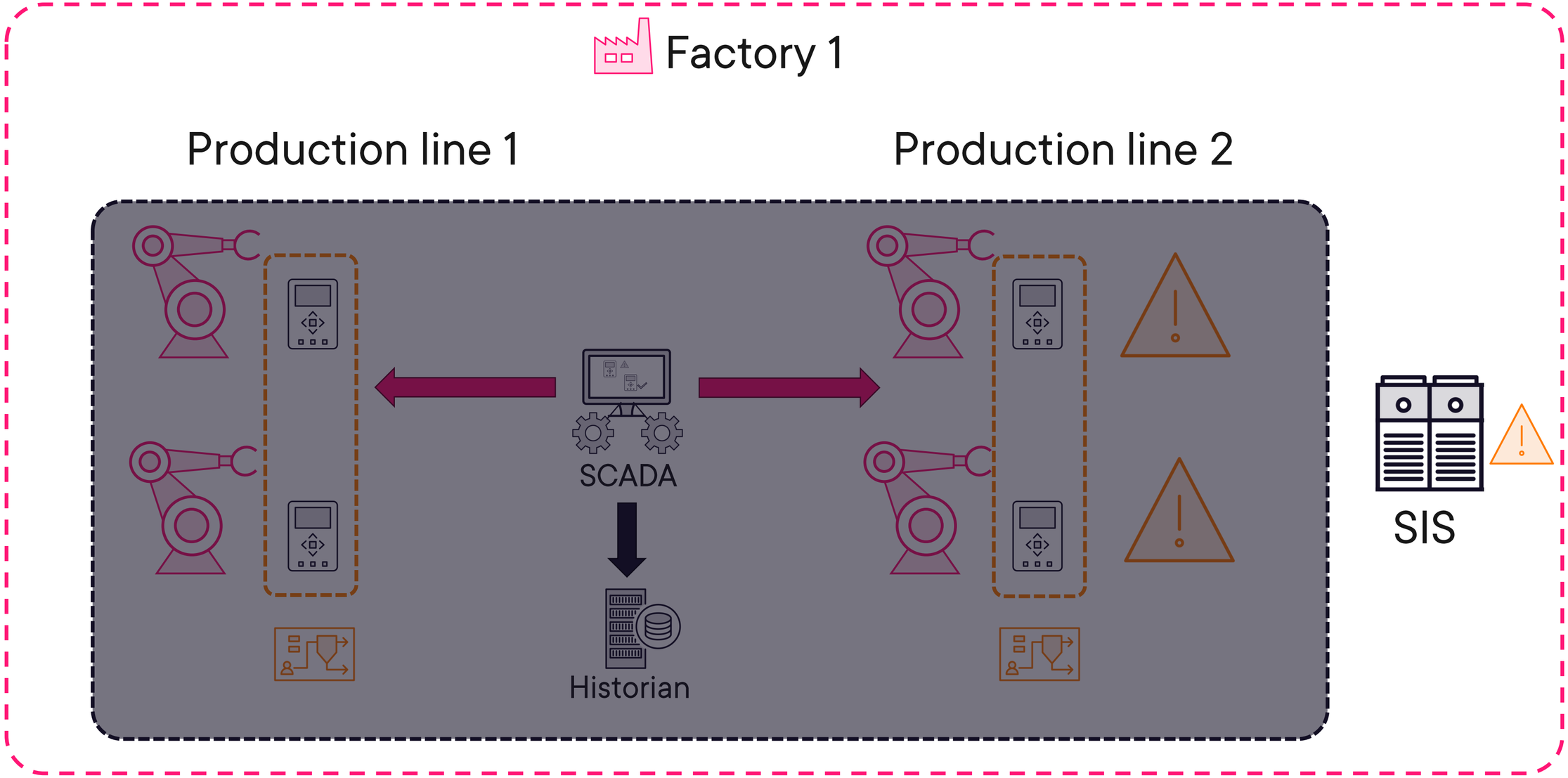
Inside the Facility



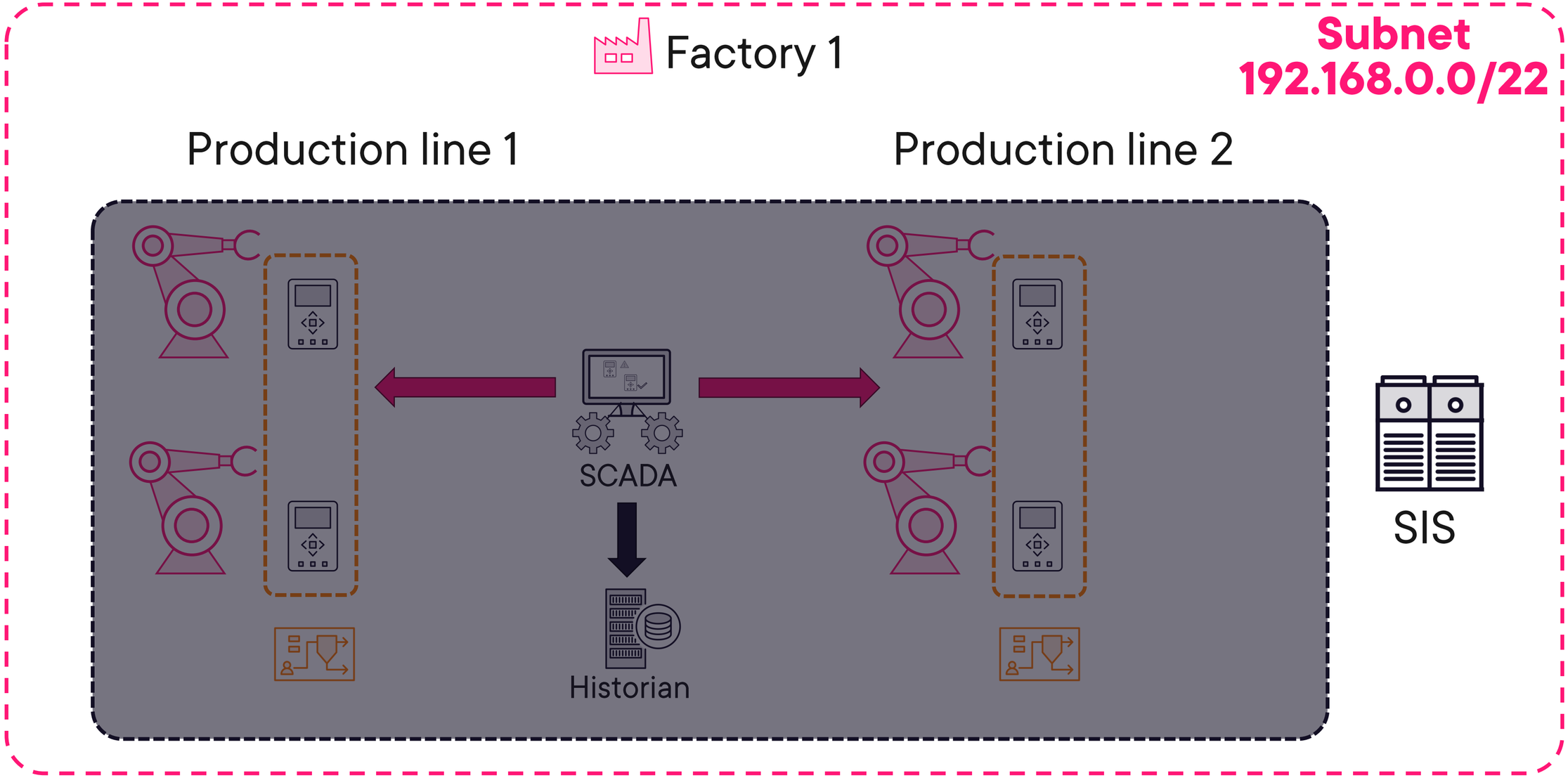
Inside the Facility



Inside the Facility

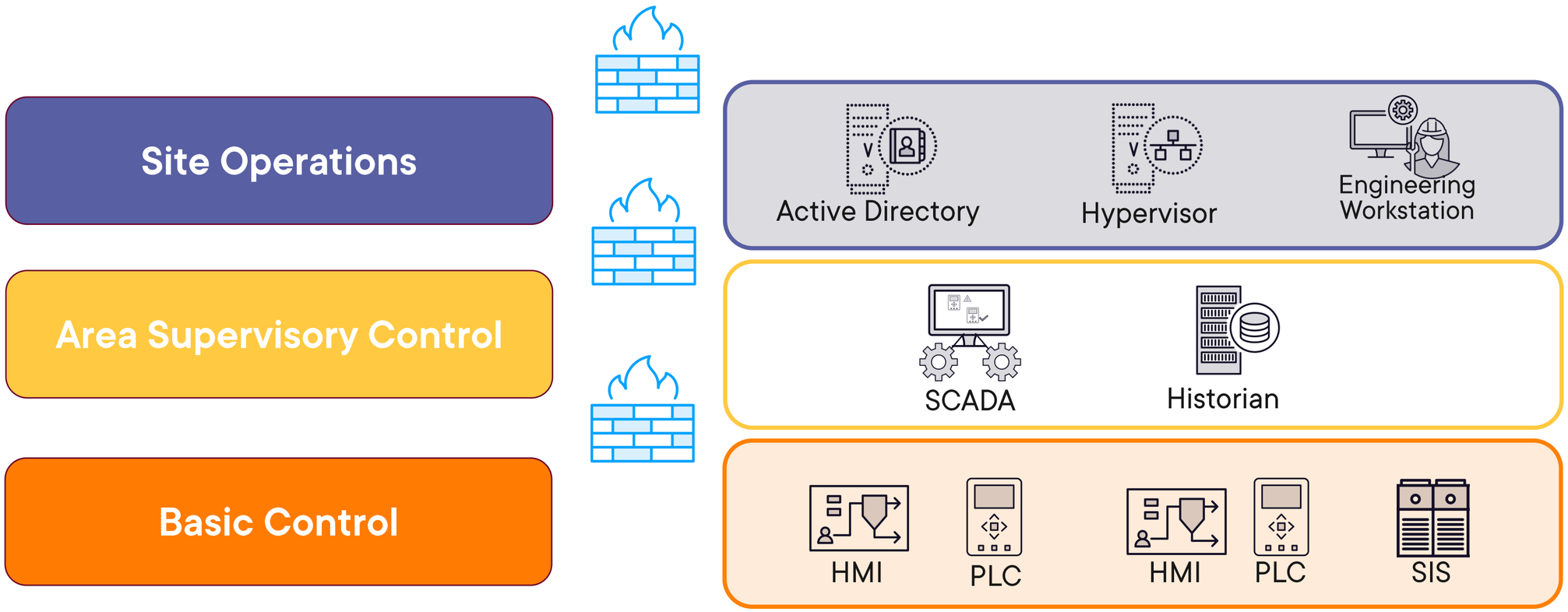


Inside the Facility

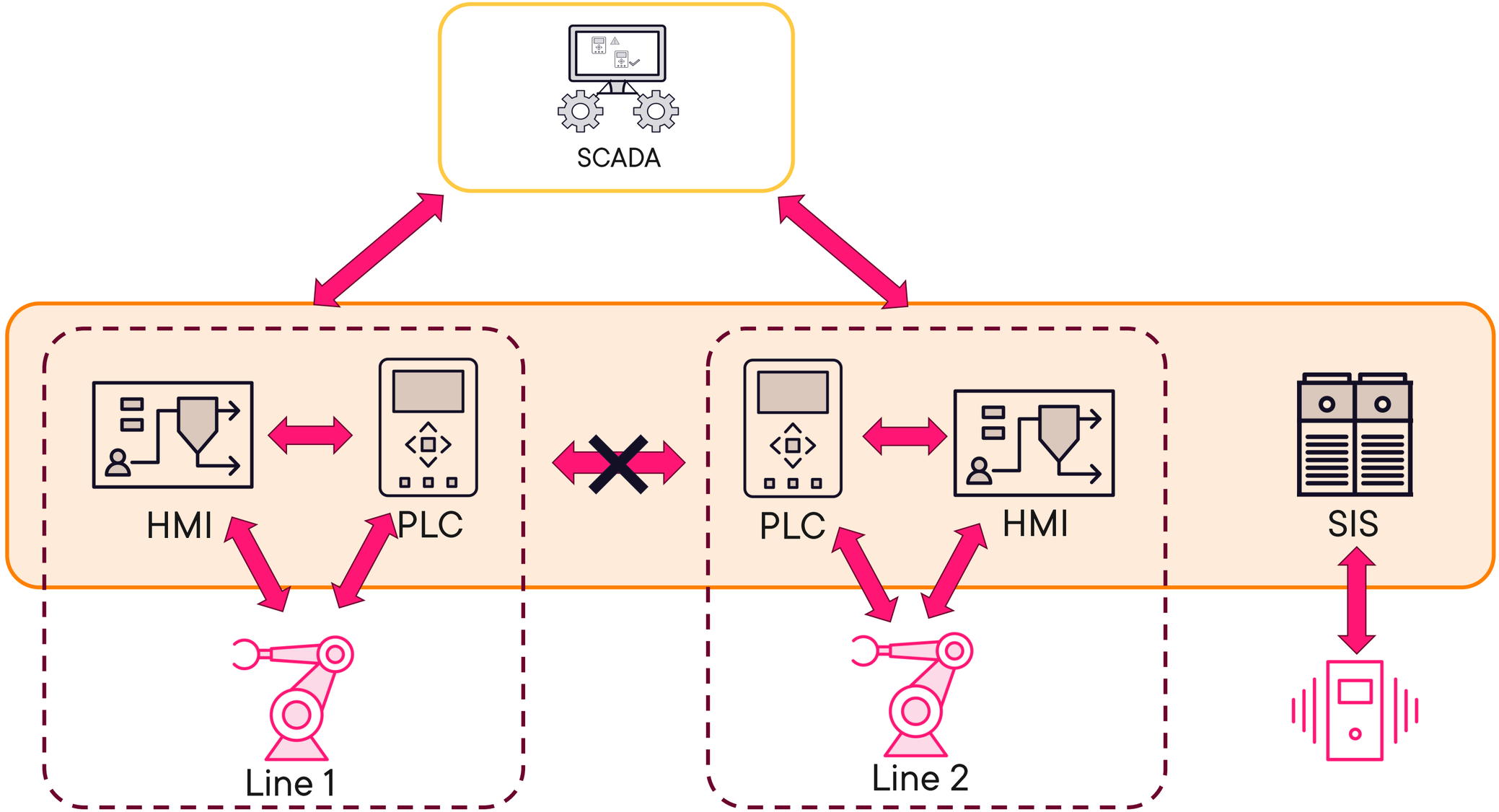


Secure Segmentation

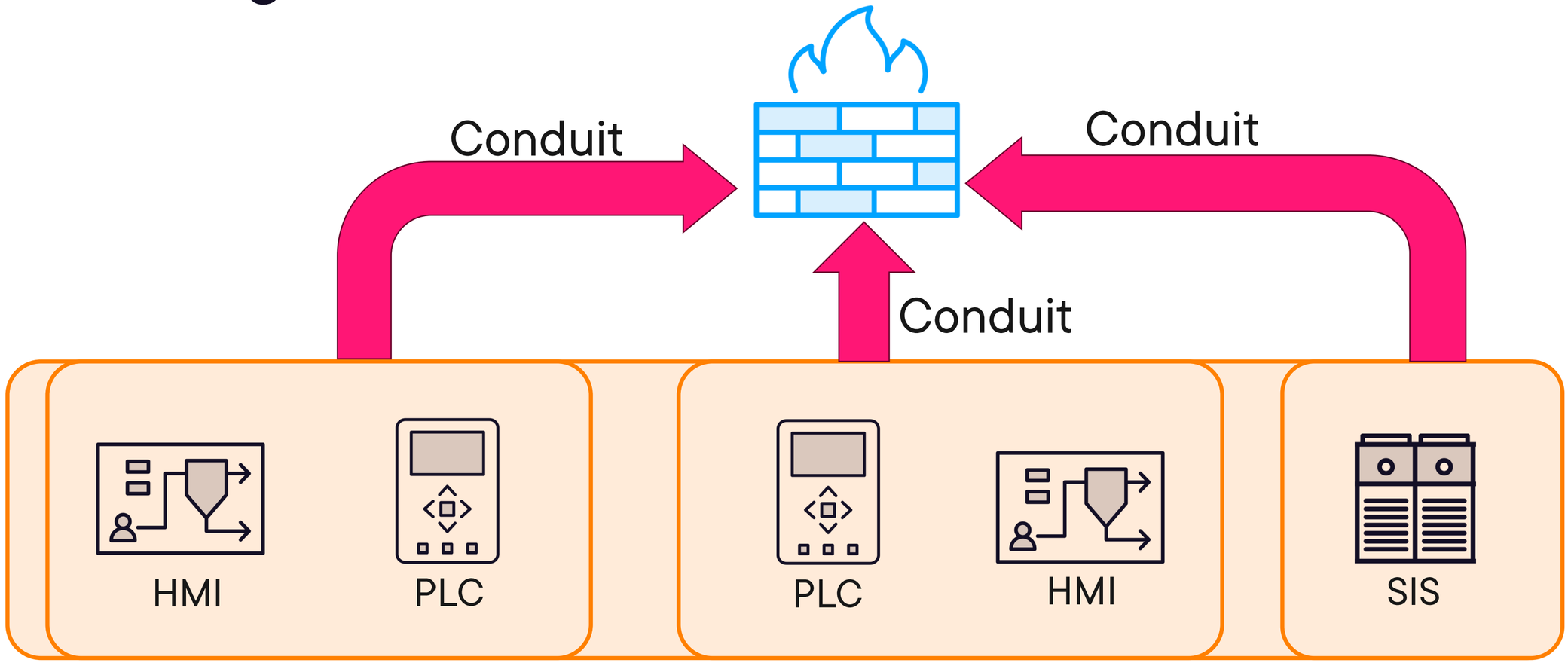
Secure Segmentation



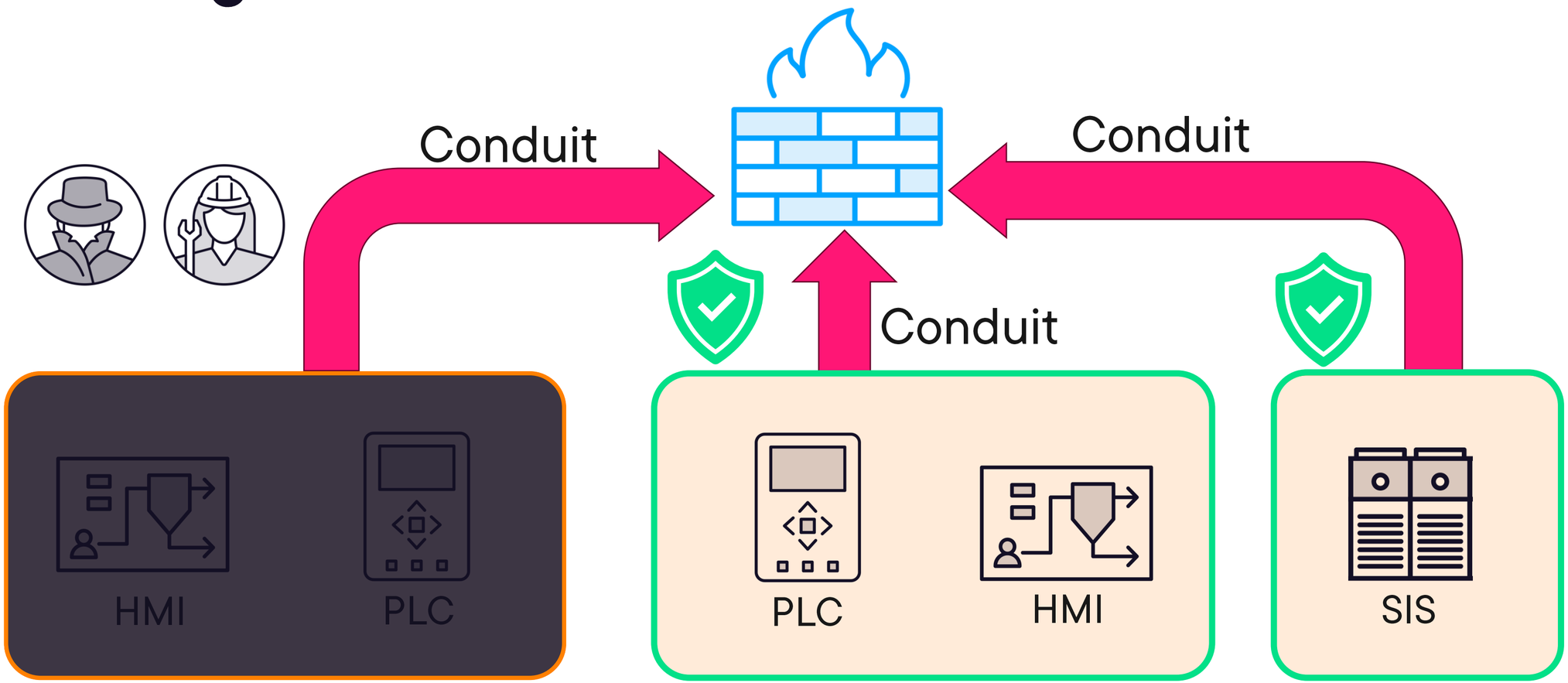
Secure Segmentation



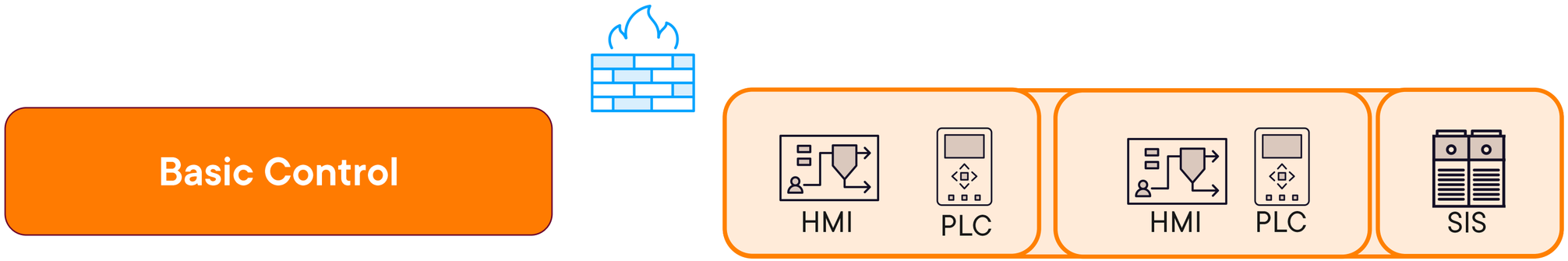
Secure Segmentation



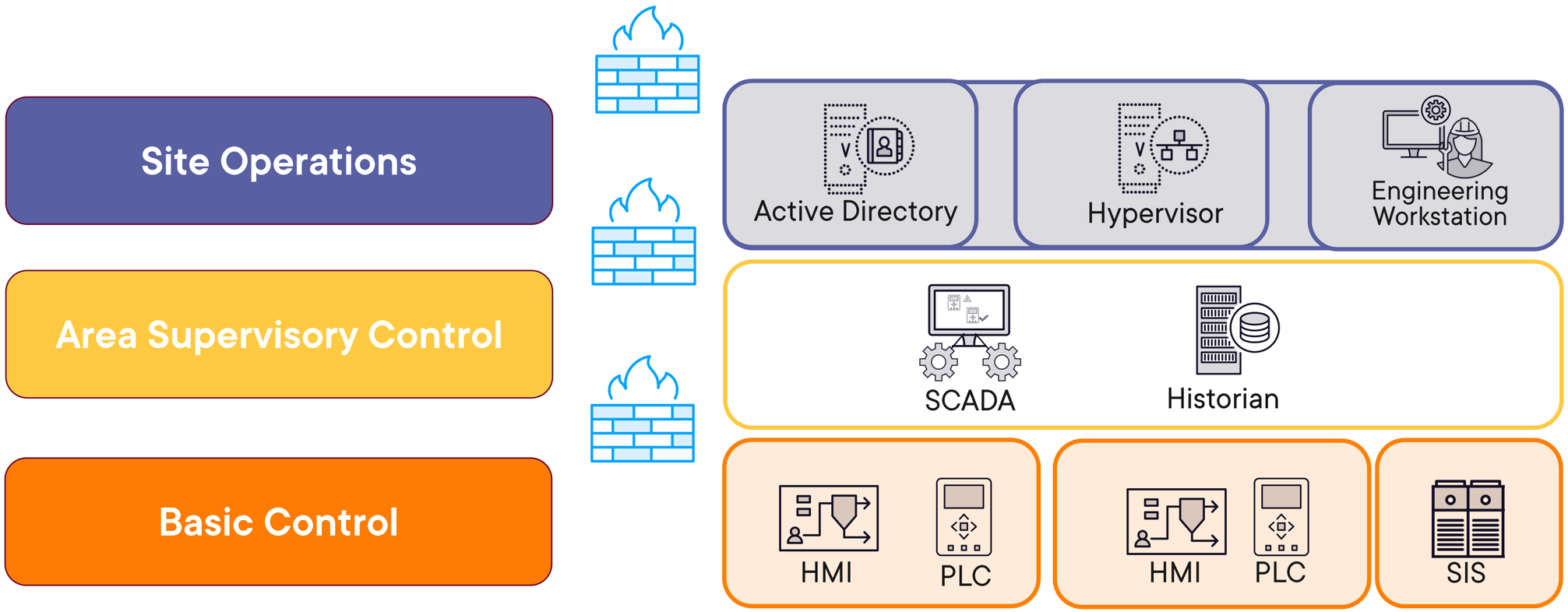
Secure Segmentation



Secure Segmentation

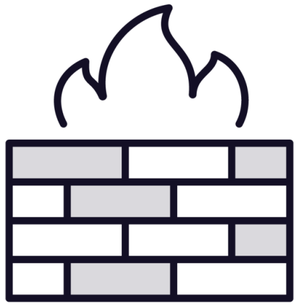


Secure Segmentation

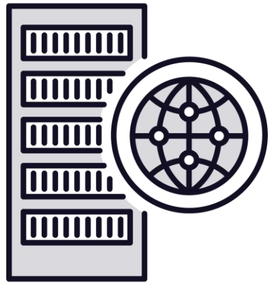


Securing the OT Network

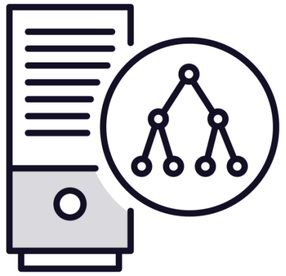
Security Tools



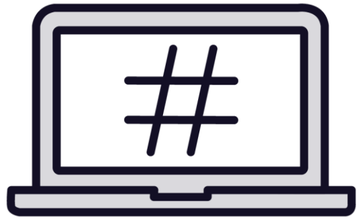
Firewall



Intrusion
Detection System

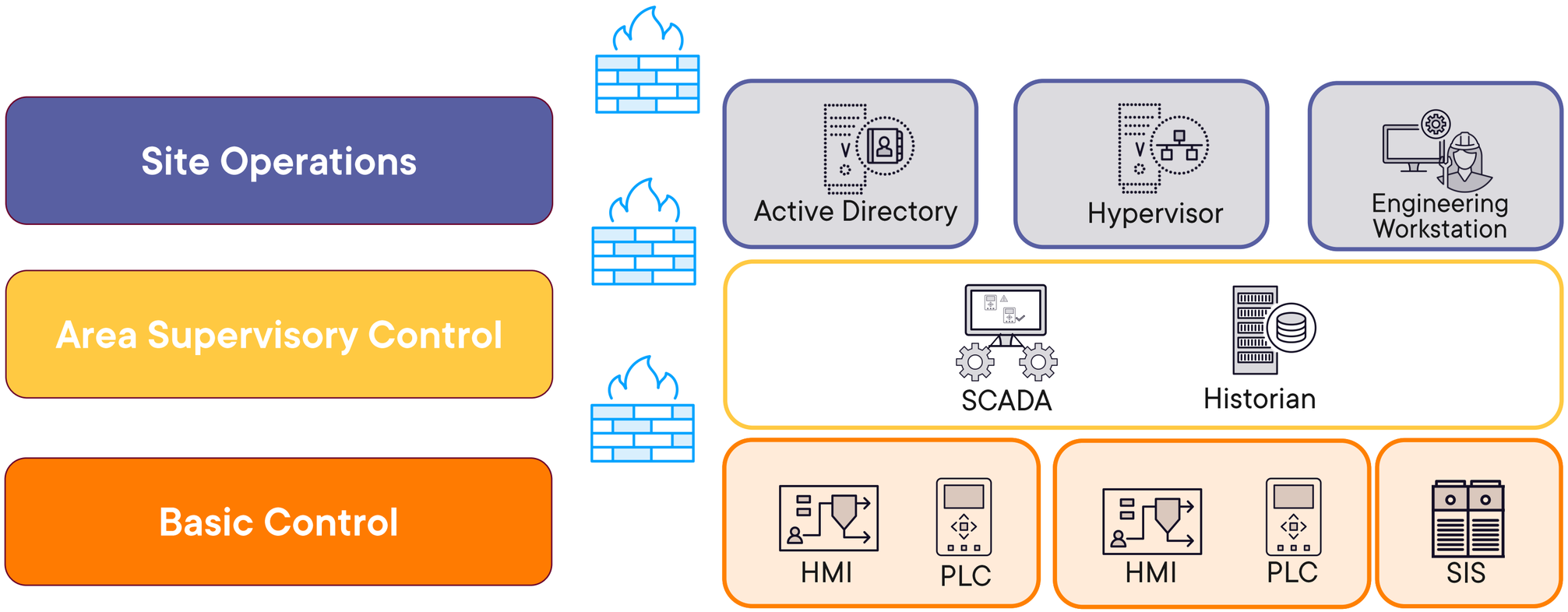


Network
Access Control

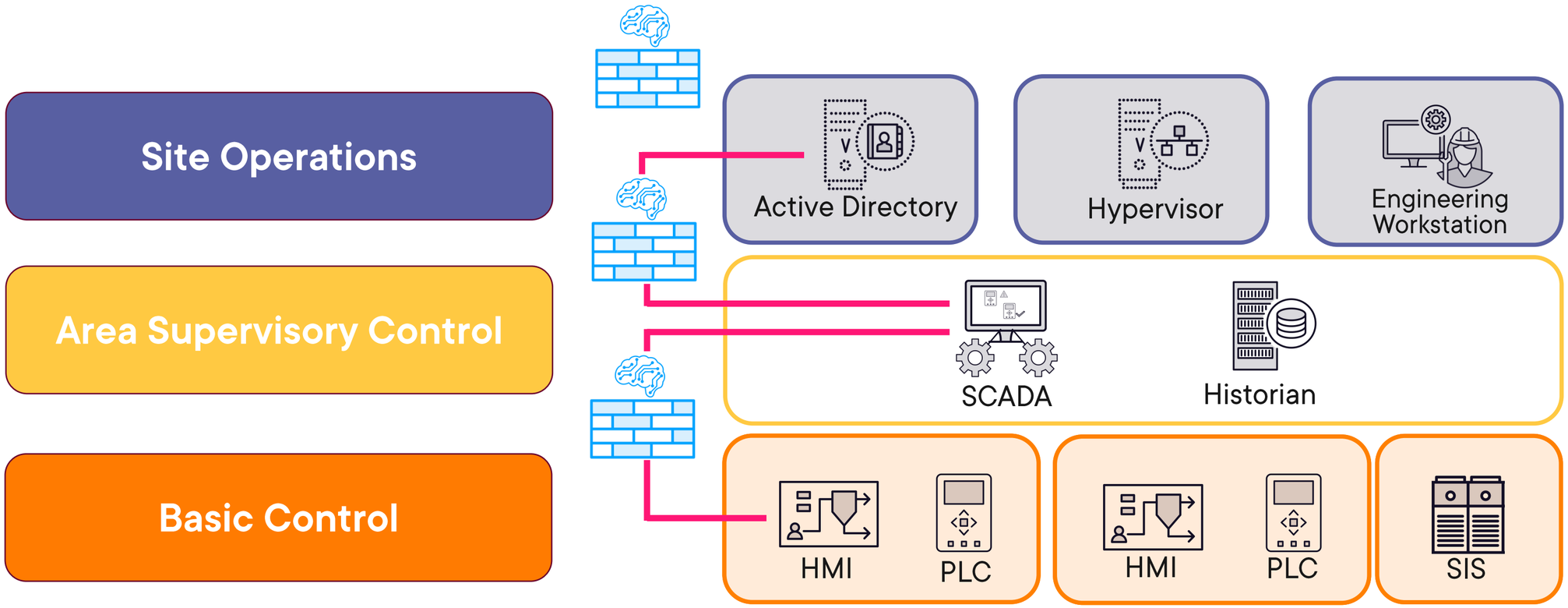


Endpoint
Security

Firewall


Site Operations
Area Supervisory Control
Basic Control
Active Directory
Hypervisor
Engineering Workstation
SCADA
Historian
HMI
PLC
HMI
PLC
SIS

Next-Generation Firewall

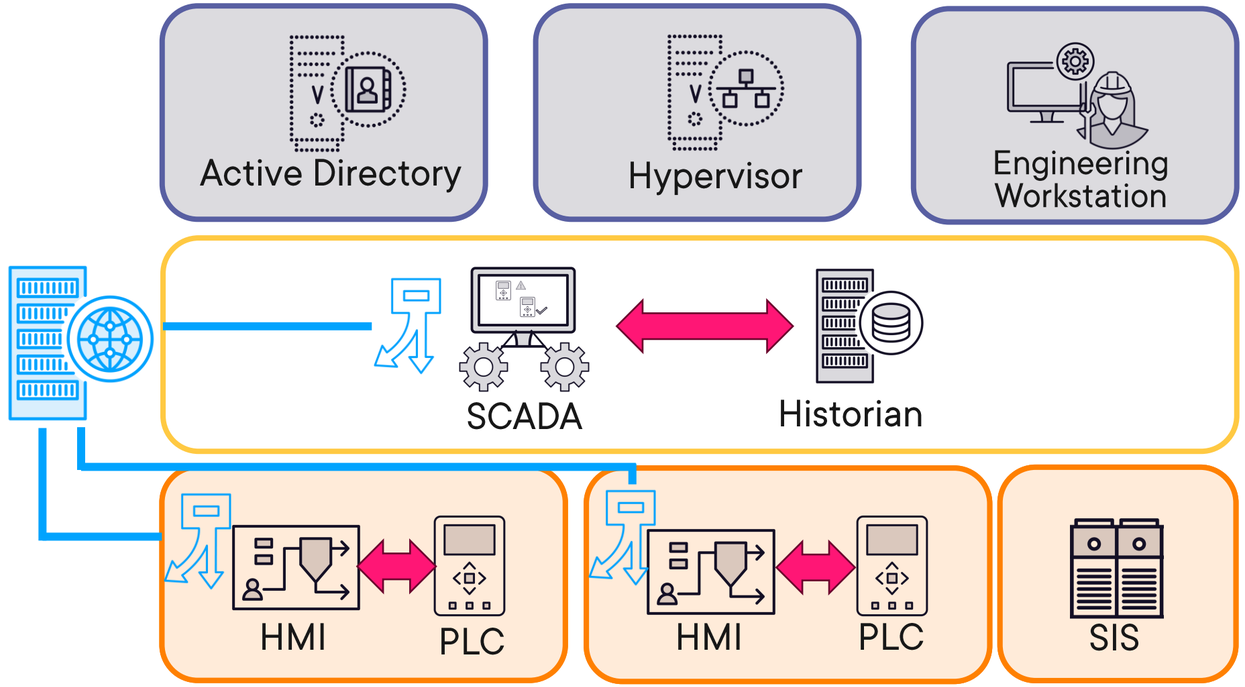


Intrusion Detection

Site Operations

Area Supervisory Control

Basic Control

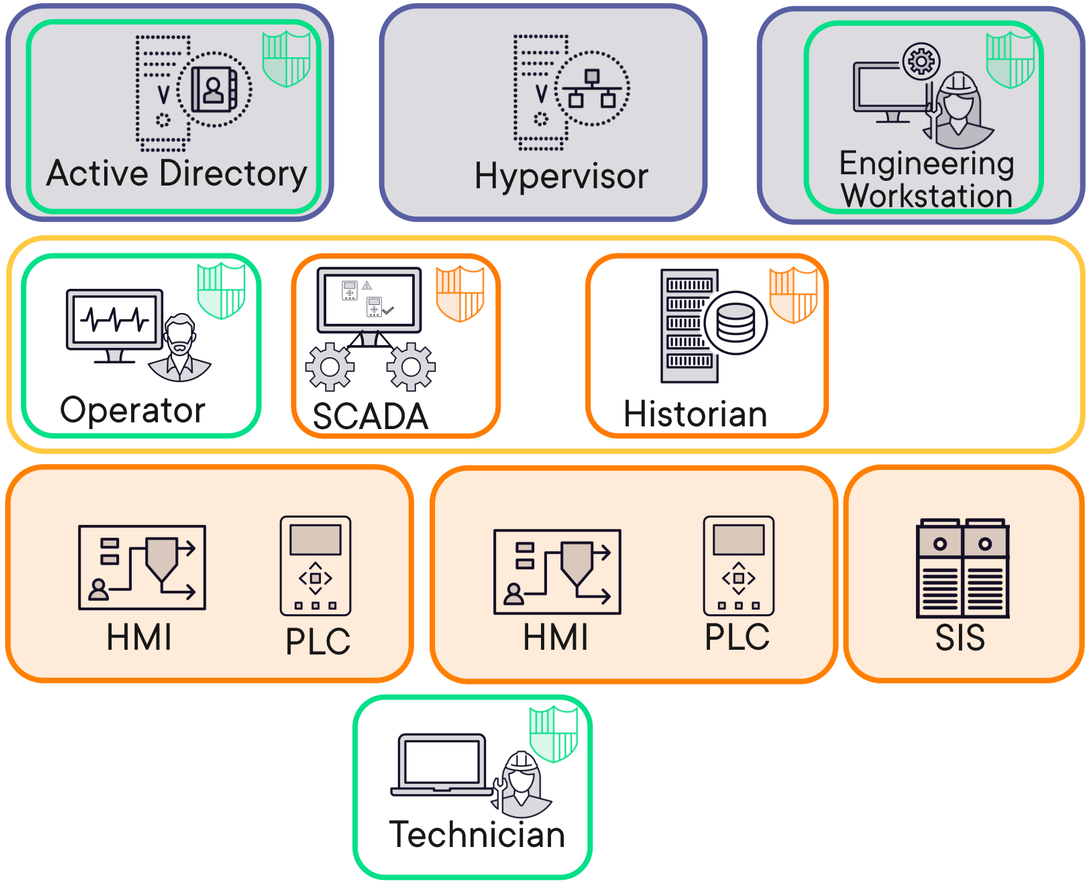


Endpoint Security

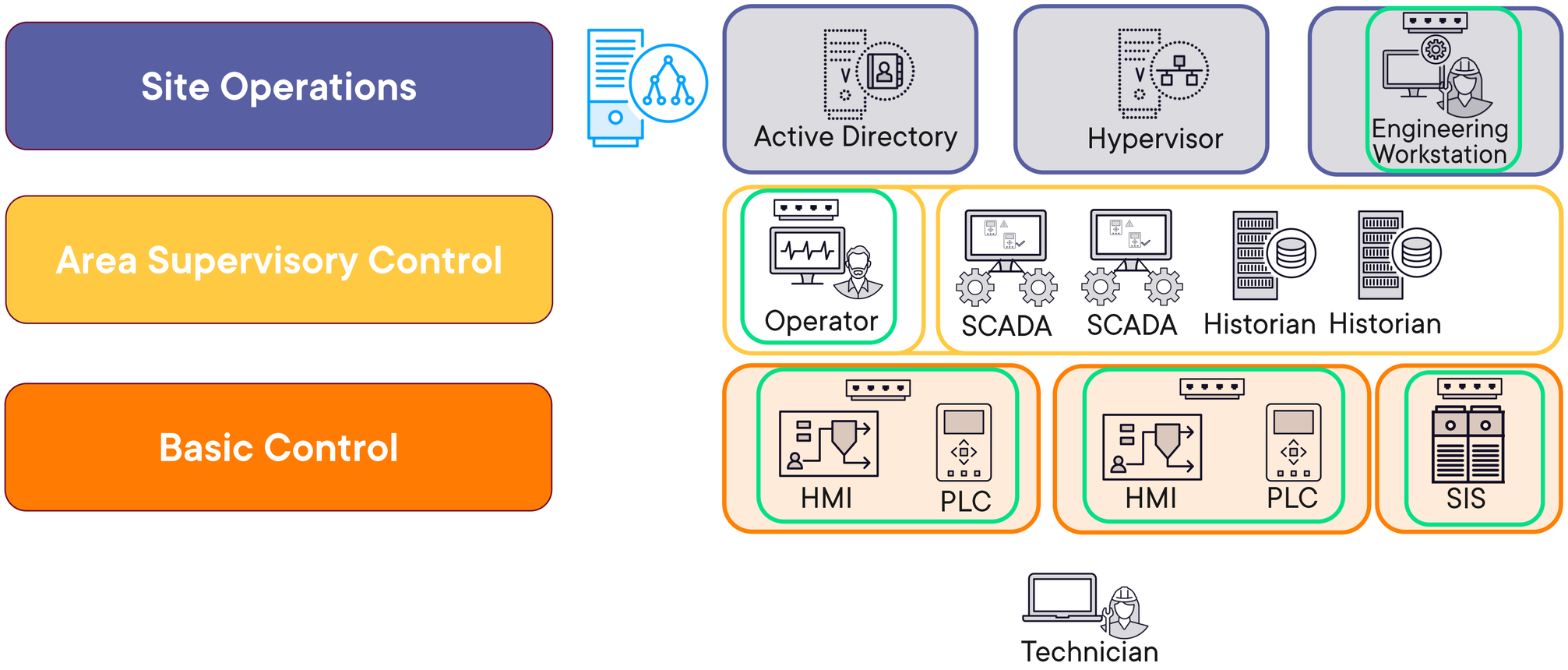
Site Operations

Area Supervisory Control

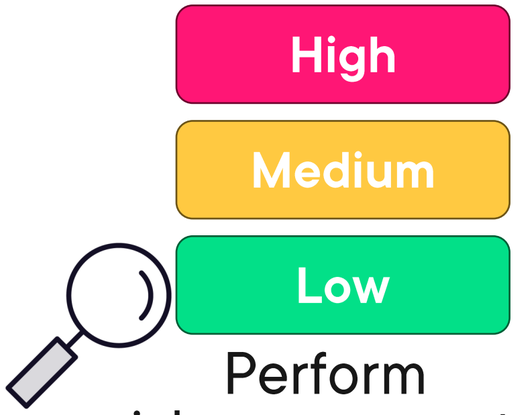
Basic Control



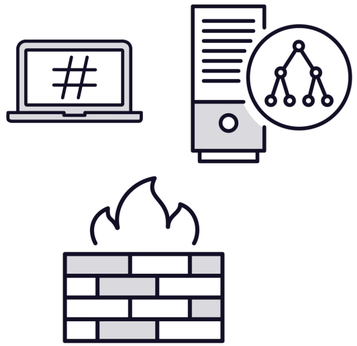
Network Access Control



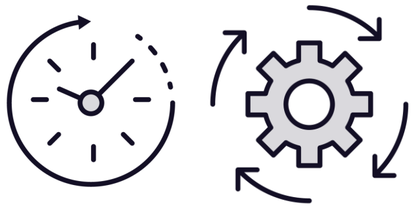
Key Topics



Perform
risk assessments



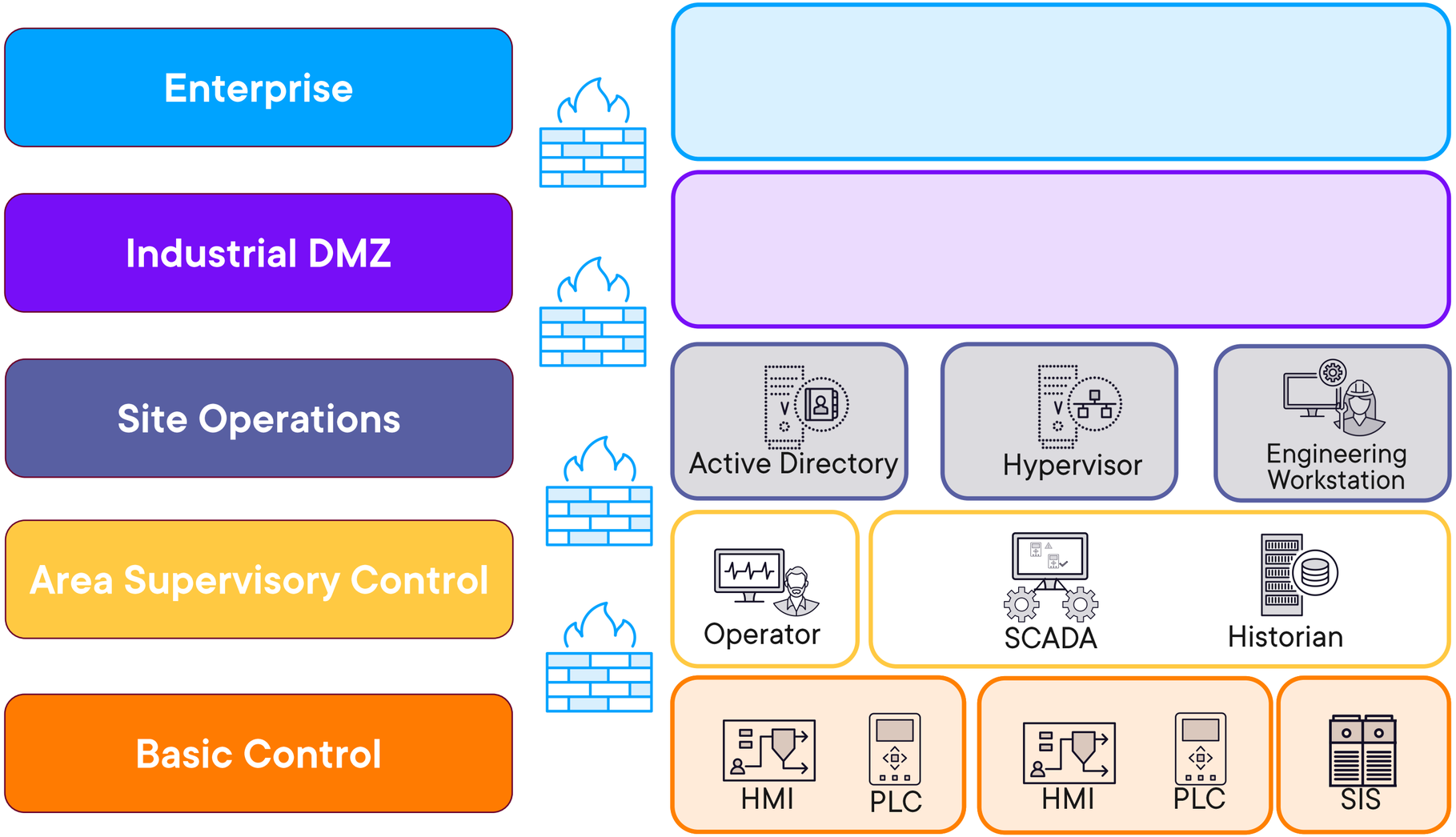
Construct
a baseline



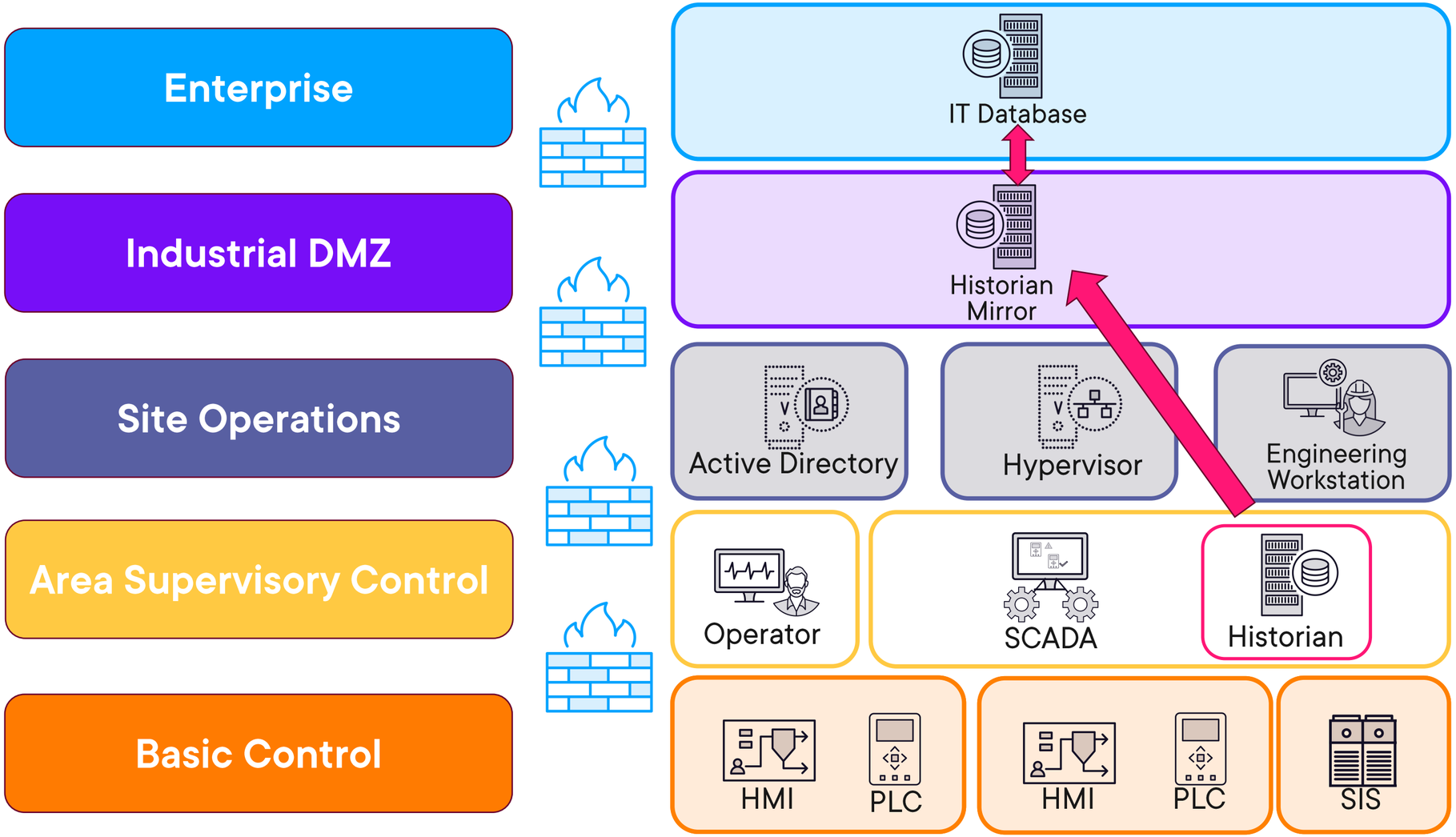
Availability &
reliability

IT – OT Bridge

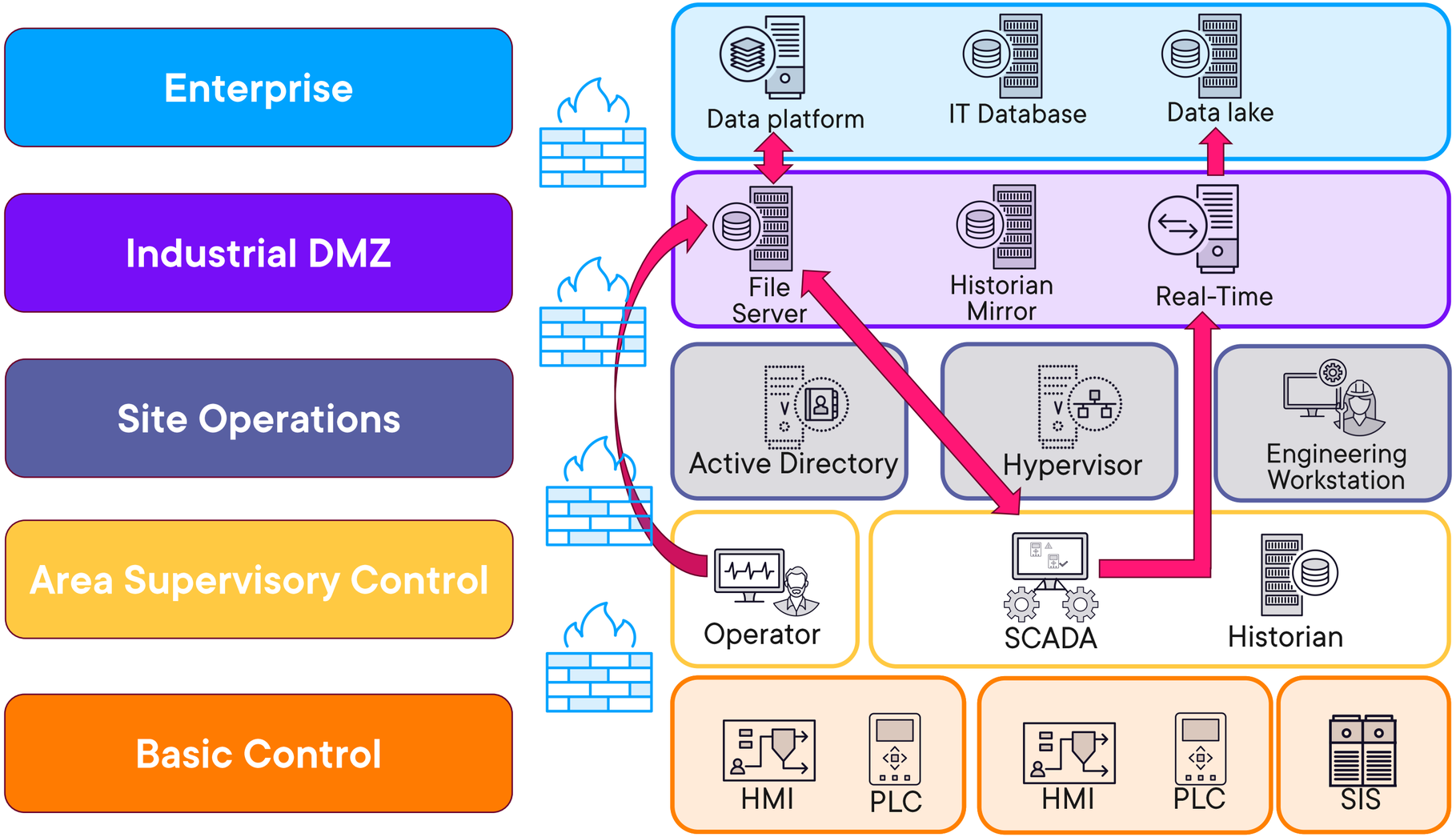
Secure Data Exchange



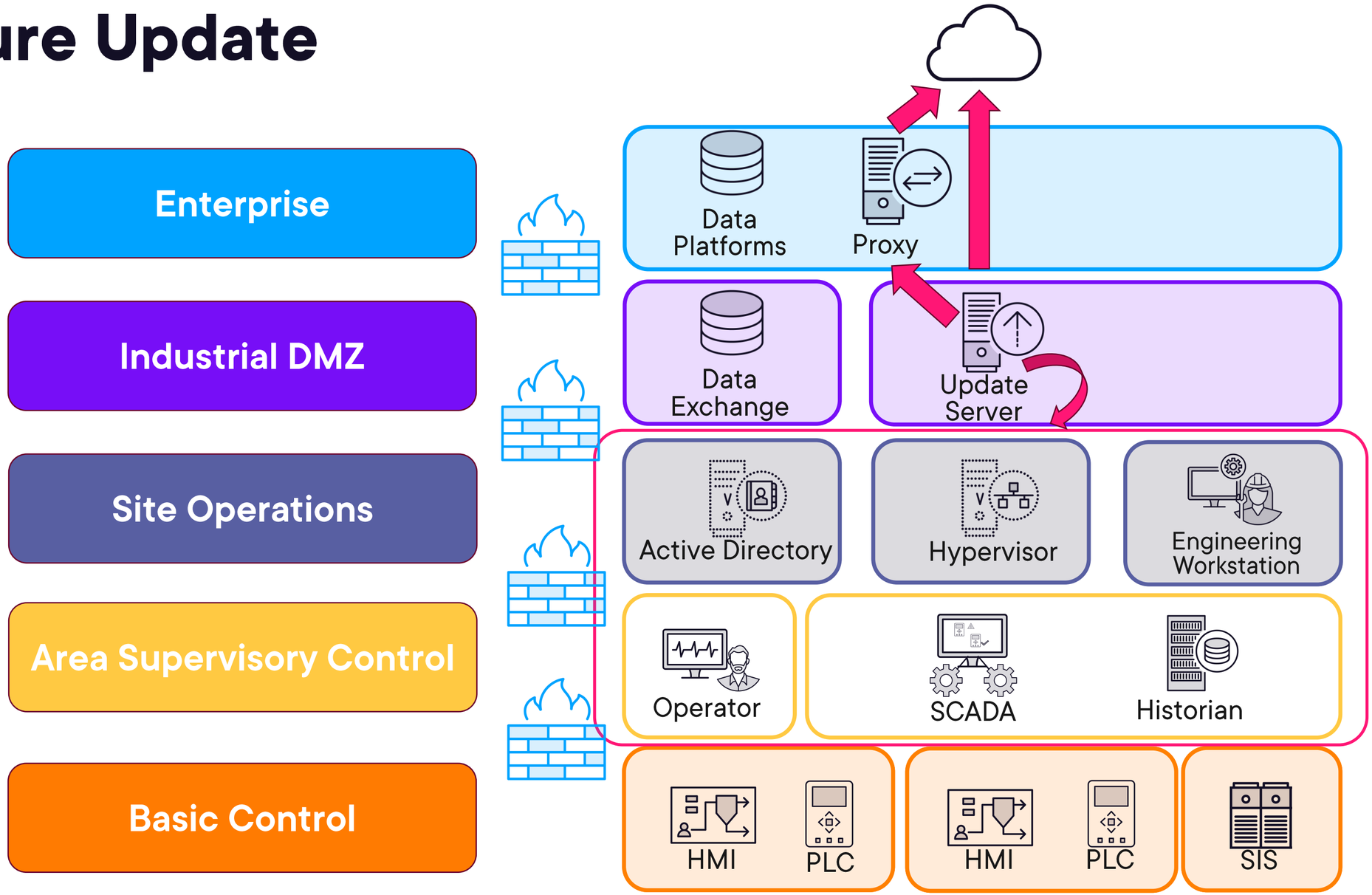
Secure Data Exchange



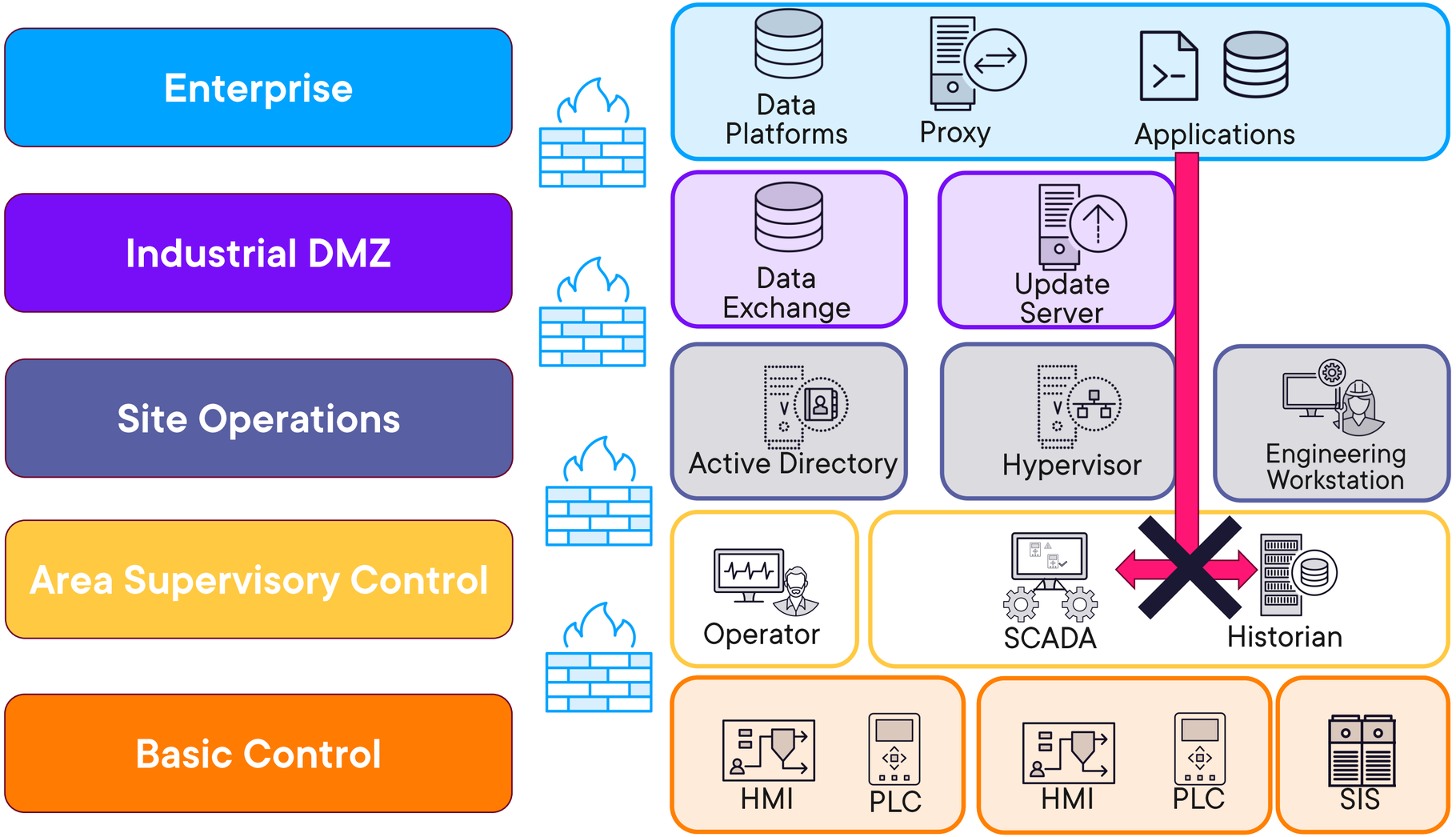
Secure Data Exchange



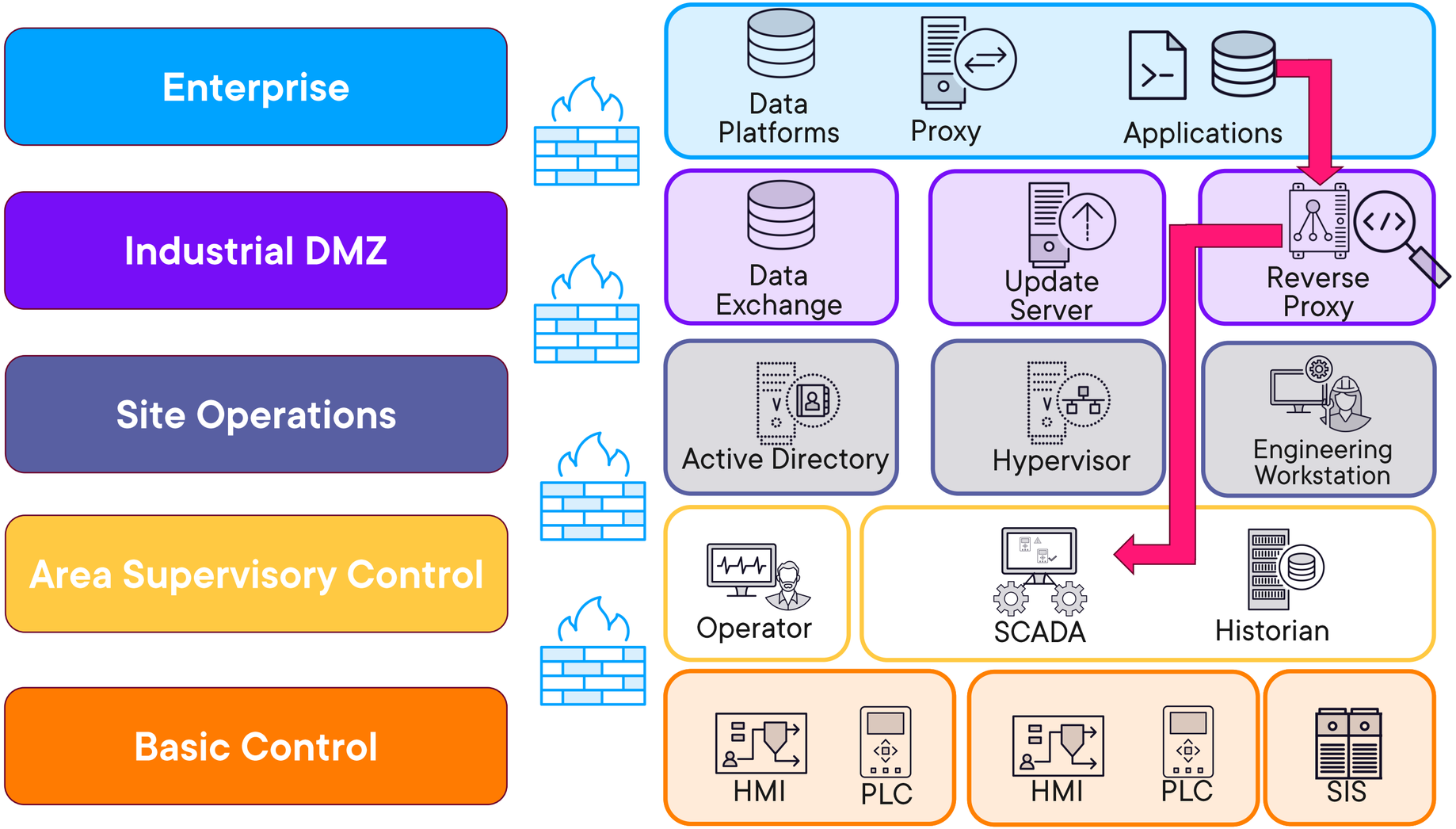
Secure Update



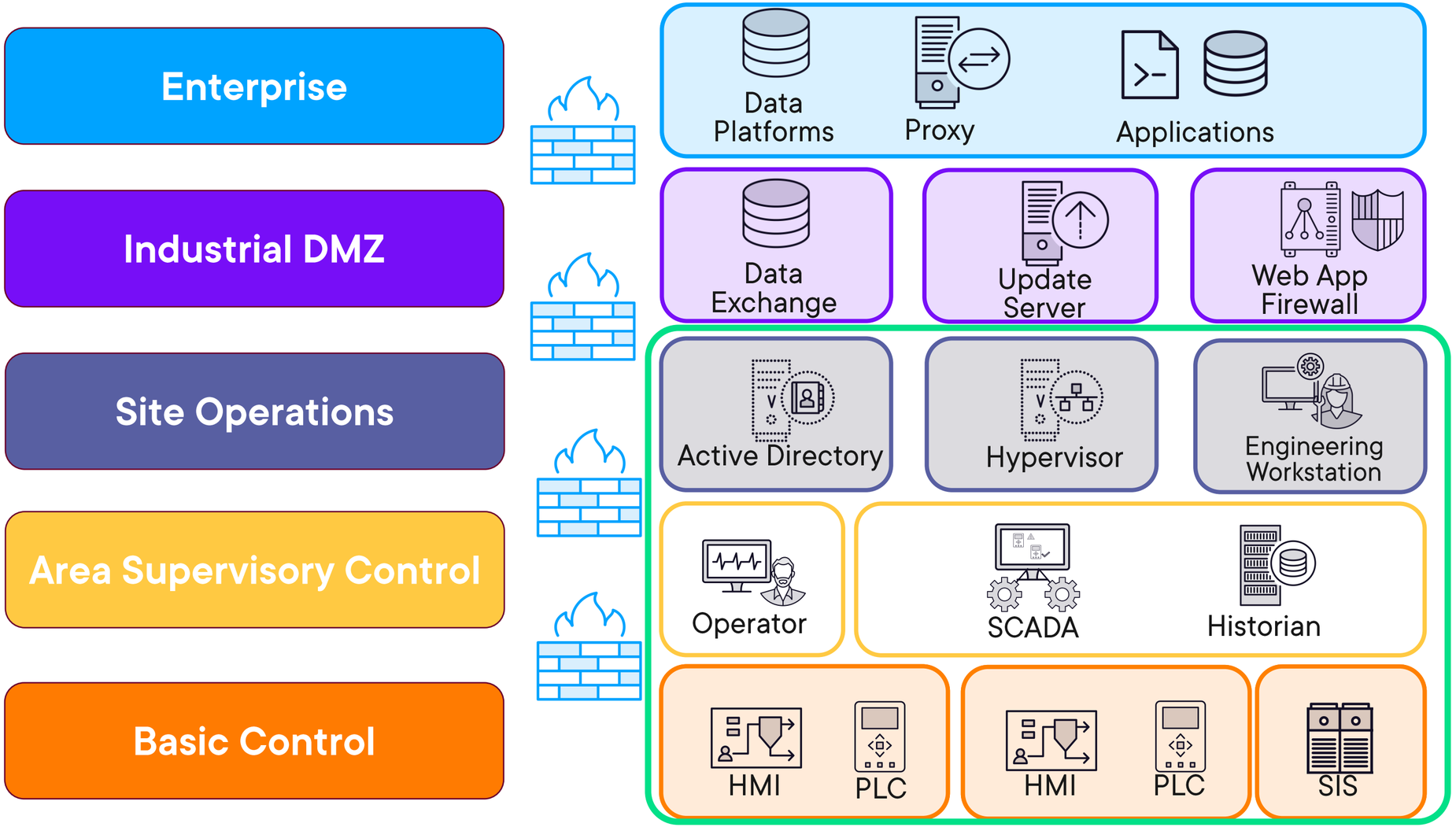
Secure Application Connectivity



Secure Application Connectivity



Secure Application Connectivity



Summary

ACME-CAR setup

Secure Segmentation

Implementing Security Controls

IT-OT Bridge Usecases