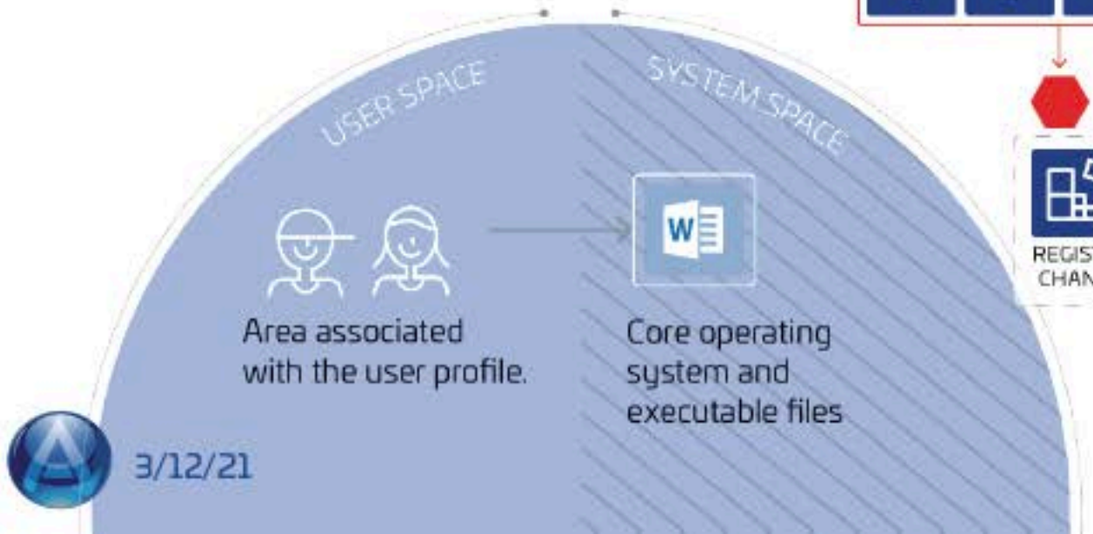
Prevent Breaches with 3-Point Policy Protection

LAUNCH POLICY | POST-LAUNCH POLICIES

Zero Trust Space
LOCATION-BASED POLICY

Key operating system folders are separated into System Space. **Applications and utilities can only launch from the System Space** unless a "trusted" exception is granted.

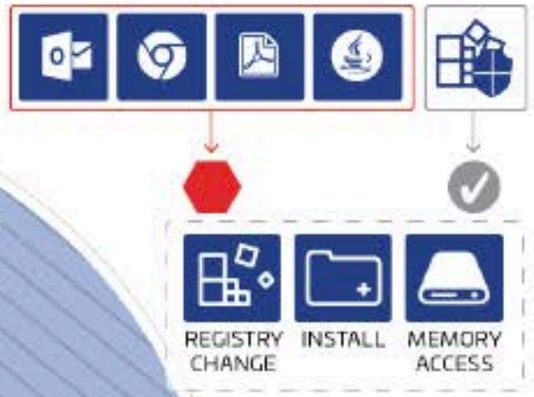
User Space is "untrusted" territory, where executables are blocked from launching.



Isolation
OS INTERACTION POLICY (PATENTED)

Applications in System Space are grouped into **high-risk** and "normal" applications.

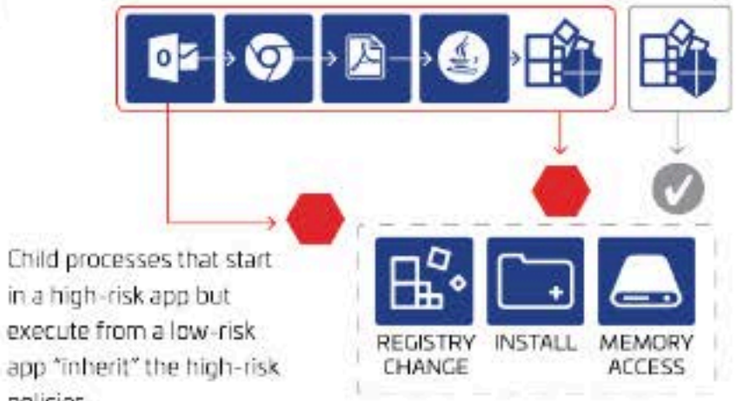
High-risk apps are blocked from executing processes malware requires to cause harm.



Inheritance
PROCESS EXECUTION FLOW POLICY (PATENTED)

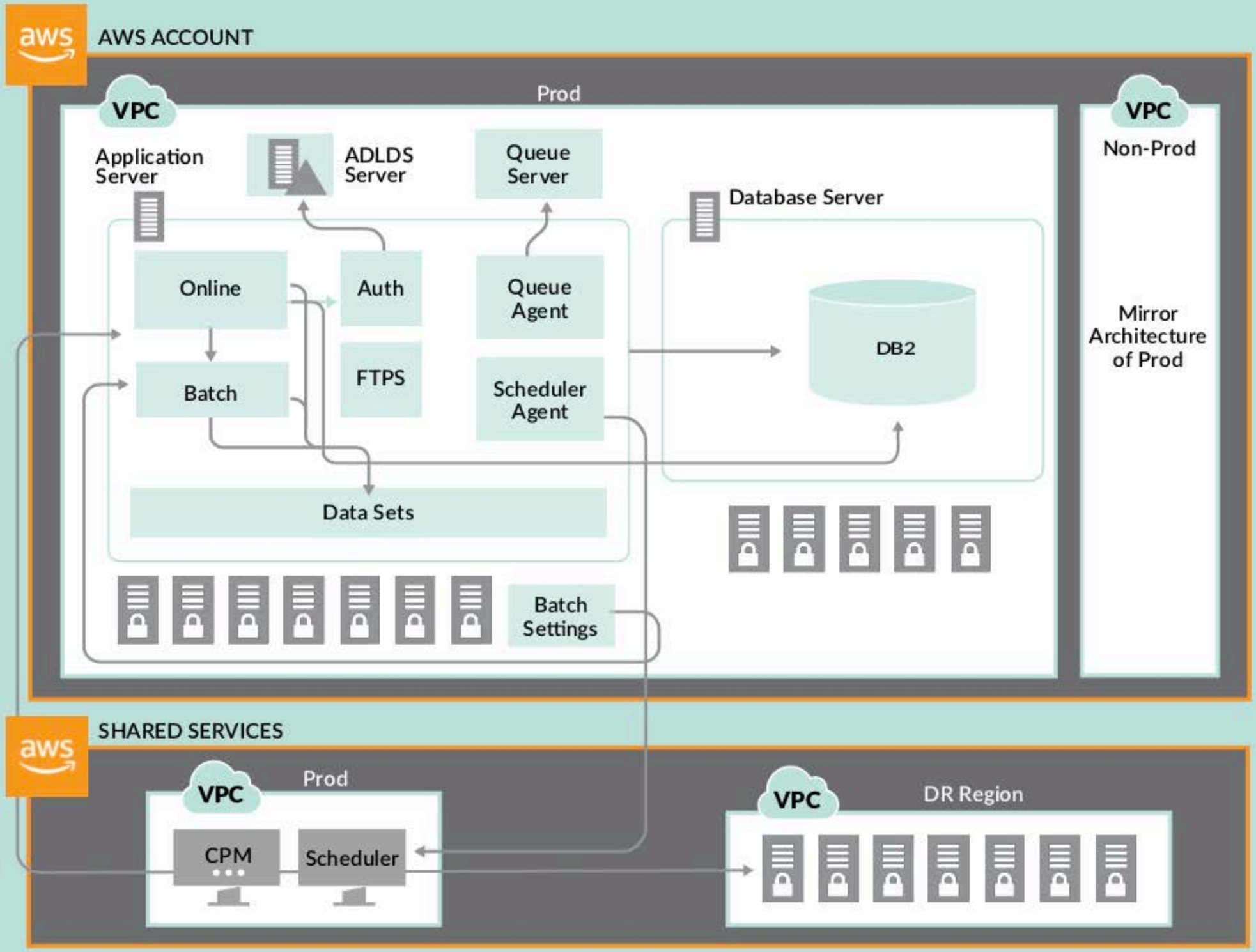
Inheritance ensures that isolation rules are automatically adapted for more precise controls with less management burden.

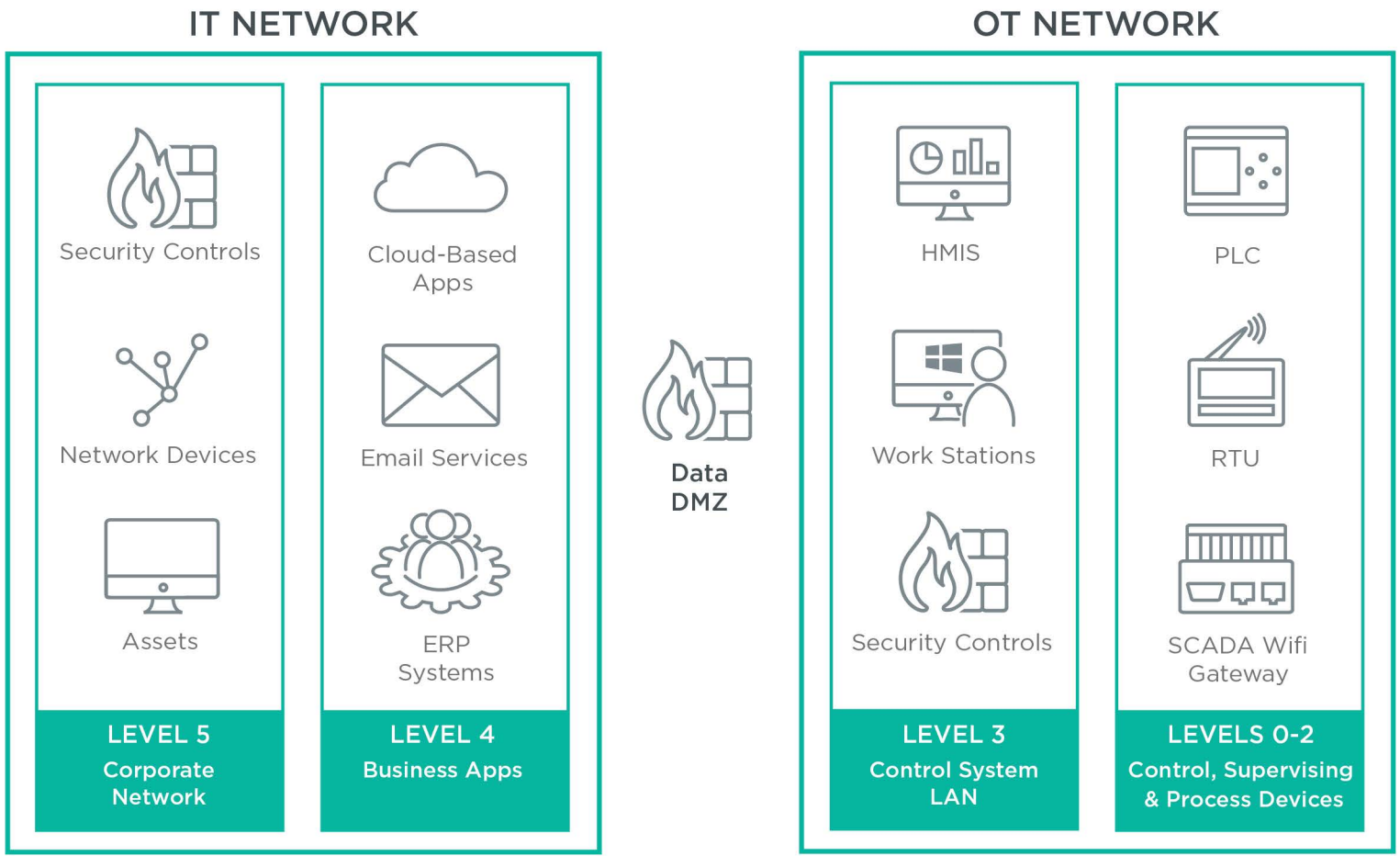
Advanced malware cannot hide its actions using a normally unrestricted application.



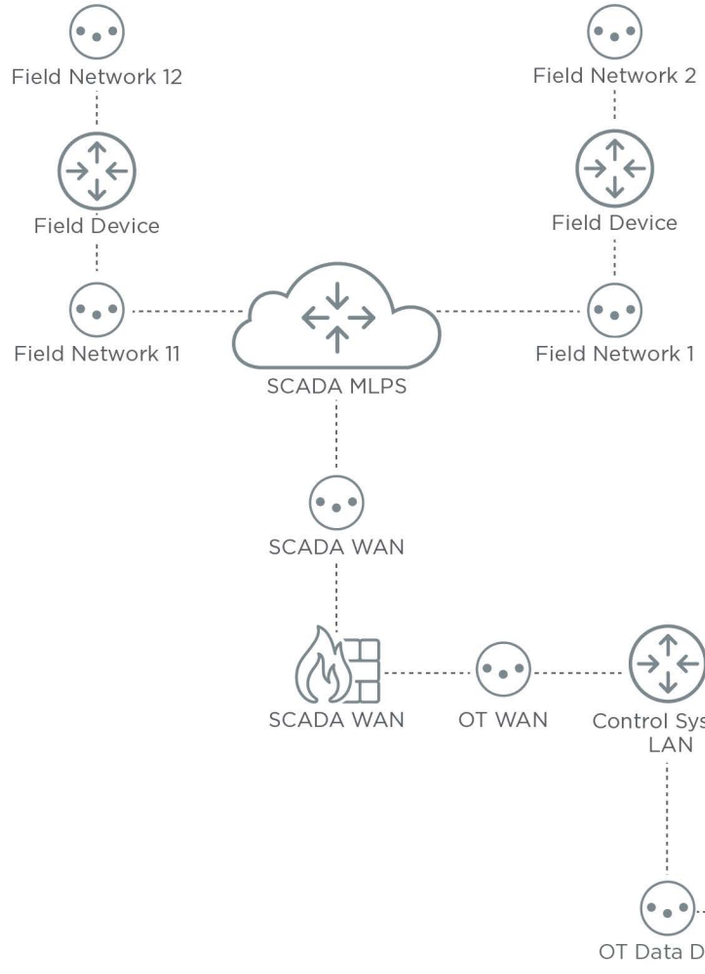
TYPICAL CLOUD-BASED ARCHITECTURE

The system architecture of one cloud-based environment is shown in this diagram.

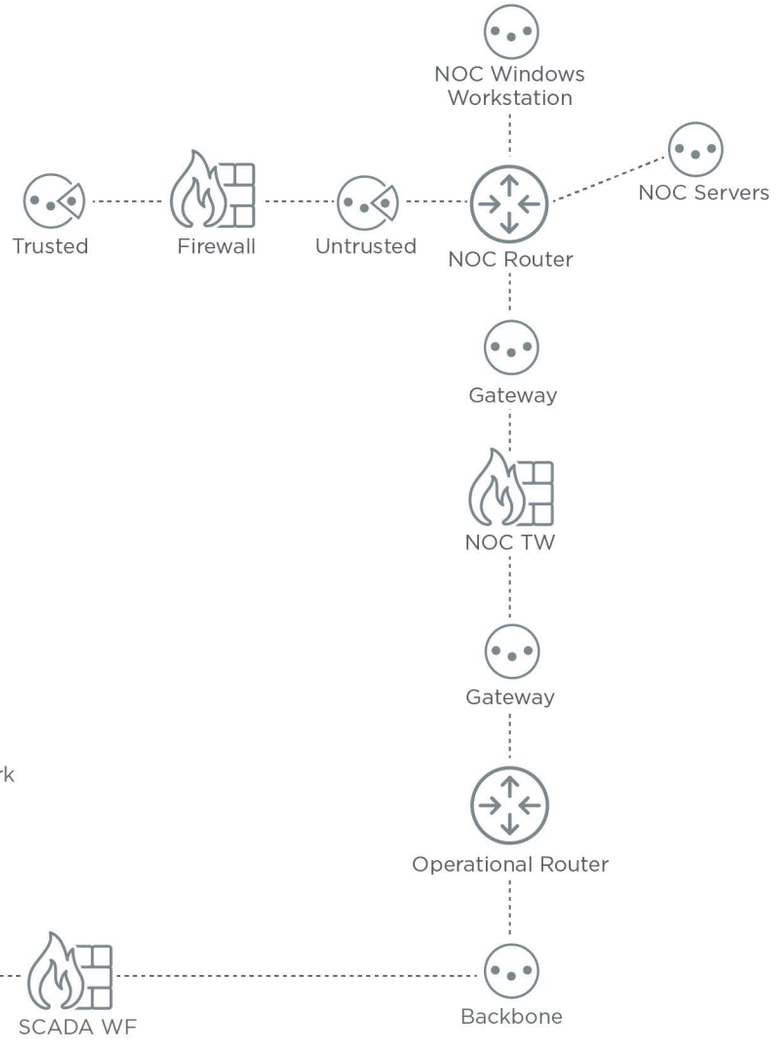



IT NETWORK
Security Controls
Network Devices
Assets
LEVEL 5
Corporate Network
Cloud-Based Apps
Email Services
ERP Systems
LEVEL 4
Business Apps
Data DMZ
OT NETWORK
HMIS
Work Stations
Security Controls
LEVEL 3
Control System LAN
PLC
RTU
SCADA Wifi Gateway
LEVELS 0-2
Control, Supervising & Process Devices

OT NETWORK



IT NETWORK



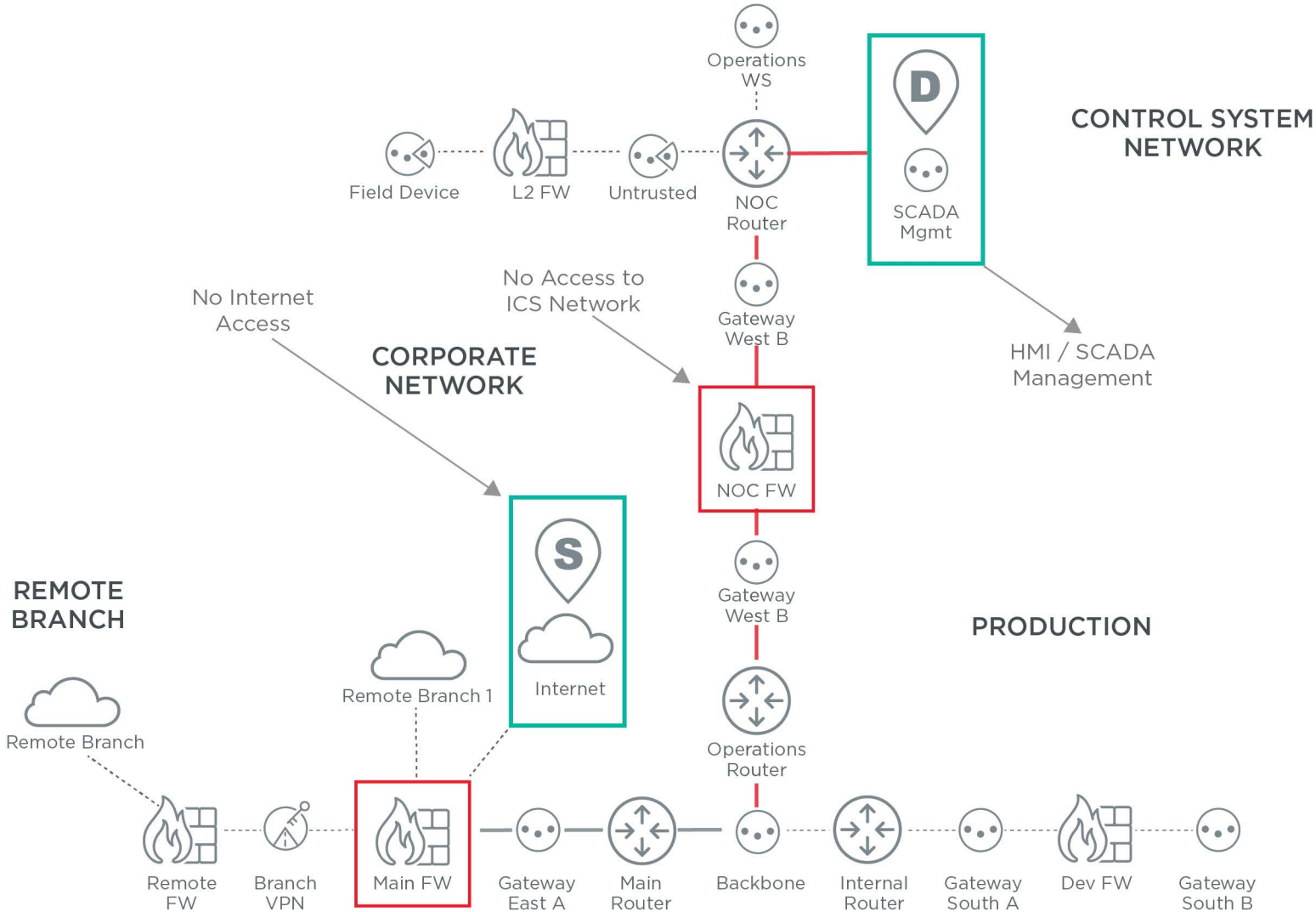
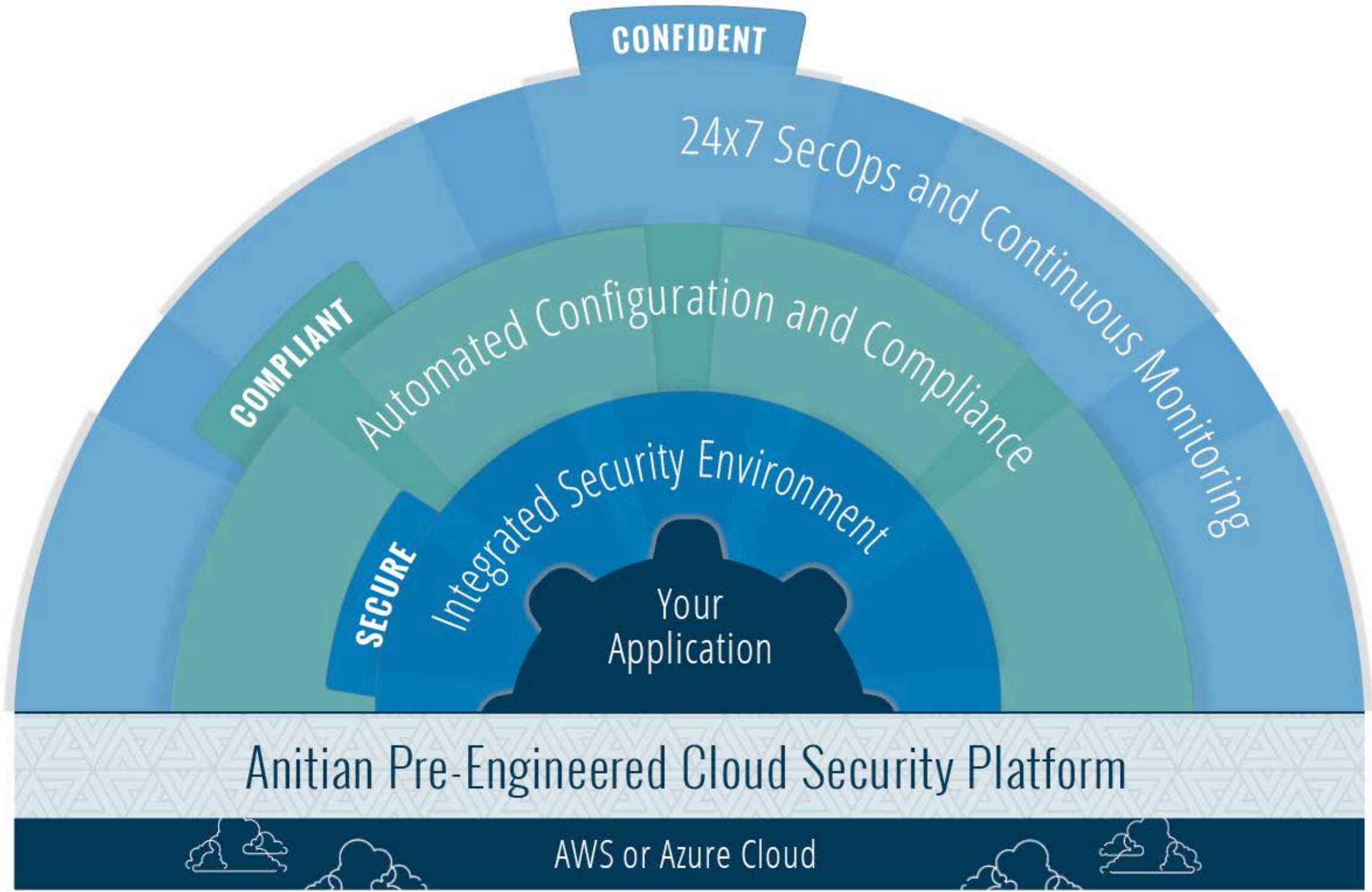


Figure 3: Path analysis from the corporate to production network showing the path to the HMI system is blocked.

AWS AND AZURE

Security 'OF' the cloud is provided by your cloud service provider


CONFIDENT
24x7 SecOps and Continuous Monitoring
COMPLIANT
Automated Configuration and Compliance
SECURE
Integrated Security Environment
Your Application
Anitian Pre-Engineered Cloud Security Platform
AWS or Azure Cloud