MANAGED ENDPOINT SECURITY

ENDPOINT PROTECTION TAILORED FOR THE CEMENT INDUSTRY

Today's digital advances bring tangible benefits to cement plants in their quest to produce cement consistently, economically, and sustainably. But there are dangers here, too. Manufacturing sectors are facing a growing array of cyber threats including cement manufacturing . Increasing ransomware incidents that stop production, as well as advanced malware targeting Operational Technology (OT) systems, can result in significant effects on safety, productivity, and reputation.

Compounding the risk, cement plants often rely on legacy systems, while the criticality of continuous production provides limited windows for patching and updates.

FULLER

As plants become more integrated and interconnected, the need for proactive cybersecurity is becoming increasingly acute. Our Managed Endpoint Security (ENS) solution supports the operational cyber resilience that today's cement industry requires. Offered as part of our PlantLine™ Service Agreements or as a standalone service, it helps safeguard critical systems from known and emerging threats.

KEY BENEFITS

PROACTIVE CYBER THREAT PREVENTION

The service helps prevent cyber incidents before they impact production, offering a robust defence against ransomware, unauthorised access, and system compromise.

CYBERSECURITY TAILORED TO THE CEMENT INDUSTRY

Our Managed ENS service is specifically designed for OT environments in the cement industry, ensuring compatibility with existing systems, industrial protocols, and plant-specific workflows.

COMPLIANCE AND VISIBILITY

Gain clear visibility into your cyber hygiene across all protected systems. With built-in reporting on antivirus status, policy enforcement, and endpoint health, our Managed ENS service supports internal audits and regulatory compliance.

FLEXIBLE DEPLOYMENT MODELS

We offer centralised and localised ENS options, enabling you to select the model that best suits your site infrastructure, security posture, and operational requirements.

WHAT'S INCLUDED?

1 AGENT-BASED PROTECTION

Lightweight endpoint agents installed on OT systems provide continuous protection, reporting, and policy enforcement.

2 REAL-TIME THREAT DETECTION AND RESPONSE

Continuously monitors endpoint activity to identify and neutralise malware, ransomware, and suspicious behaviour before it impacts operations.

3 MANAGED WHITELISTING / MANAGED APPLICATION CONTROL

Prevents unauthorised software from executing on OT systems by enforcing strict application policies tailored to cement plant environments.

4 REPORTING

Generates regular reports on antivirus status, policy compliance, and threat activity to support internal audits and regulatory requirements.

5 ZERO-DAY THREAT MITIGATION

Uses behavioural analysis and heuristic scanning to detect and block previously unknown threats.

FLEXIBLE DEPLOYMENT MODELS

We offer two deployment models to suit digital infrastructure, security posture, and operational requirements.

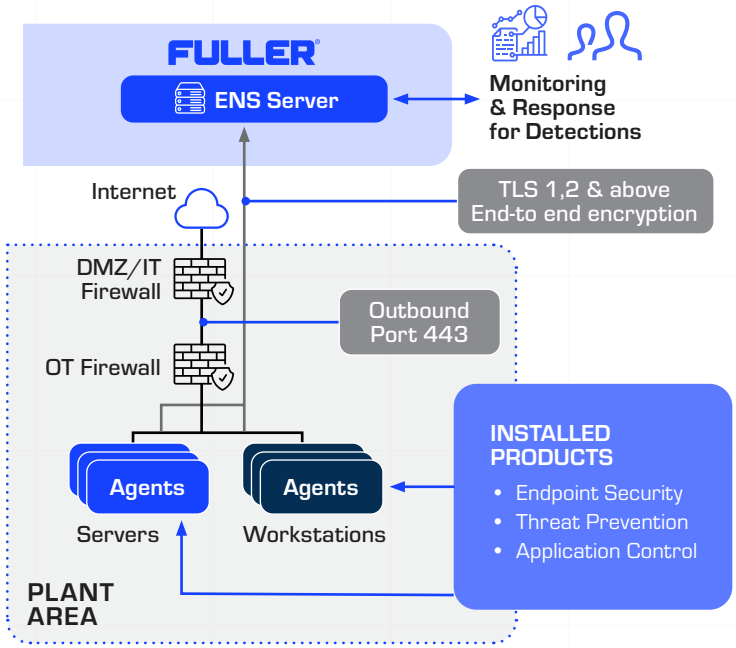
CENTRALISED ENS

This option provides a remotely managed ENS solution hosted securely on Fuller Technologies servers. Access is managed through our Secure Remote Access (SRA) solution Go2Cement - https://go2.cement1882.com, which provides secure and authenticated remote management and troubleshooting. OT systems are equipped with agent-based software that establishes encrypted TLS/443 connections to the central ENS server. This architecture enables:

- Centralised policy management aligned with OT product lifecycles.
- Rapid onboarding and redeployment of endpoint agents, enabling fast deployment across new or reconfigured systems.
- Real-time malware detection and response.
- Application control to block zero-day threats.
- Regular compliance reporting and anti-virus status updates.

By centralising management, this model reduces the burden of maintaining additional hardware, software, and skilled resources at the plant, while ensuring consistent protection across multiple locations.

SOLUTION ARCHITECTURE : CENTRALISED



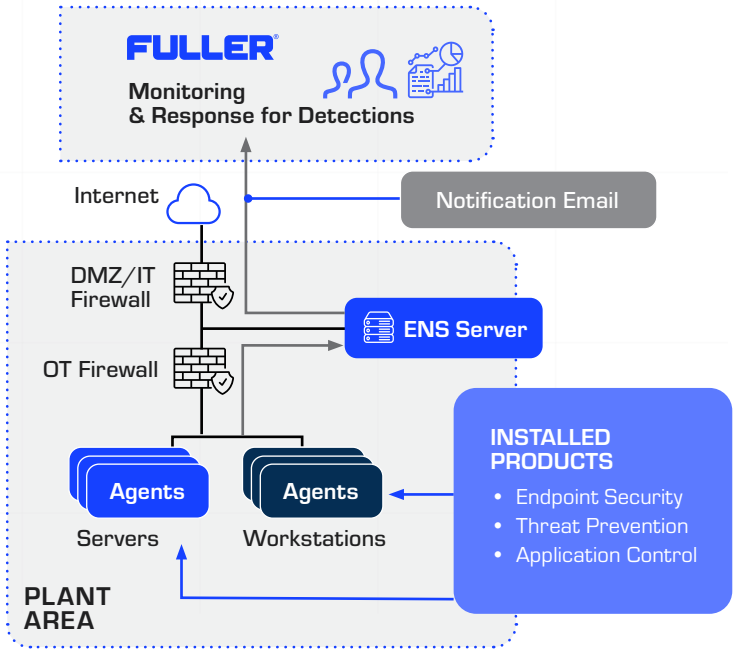
LOCALISED ENS (ON-PREMISES)

For sites with air-gapped networks or restricted internet access, we offer localised ENS deployment. The ENS server is installed within the plant's OT-DMZ or Industrial DMZ (IDMZ) segment, allowing complete control over endpoint agents without relying on external connectivity. Key features include:

- Site-specific policy customisation.
- Secure Remote Access (SRA) to manage the local ENS server via our SRA Solution – "Go2Cement"
- On-Demand Application whitelisting .
- Local malware detection and remediation.
- Antivirus and compliance reporting.

This model ensures that even isolated environments benefit from enterprise-grade security.

SOLUTION ARCHITECTURE : ON-PREMISES



WHICH ASSETS ARE COVERED?

Today, OT/ICS (Industrial Control Systems) are installed Windows Operating System, therefore these systems can access ENS server, those systems are covered with in the solution.

In today's industrial landscape, the OT systems are commonly operated on Windows-based platforms. This architecture allows seamless integration with the ENS server, ensuring that these critical systems are comprehensively protected as part of our solution.

WINDOWS BASED SYSTEMS USED AS:

1. PROCESS CONTROL SYSTEM (ECS/CONTROLCENTER™)
2. PLC ENGINEERING STATION
3. OPERATOR STATIONS
4. PROCESS EXPERT SYSTEMS (ECS/PROCESSEXPERT®)
5. HISTORIAN (ECS/ PLANTDATAMANAGEMENT)
6. LABORATORY SERVERS, WORKSTATIONS (QCX® ADVANCED QUALITY CONTROL SYSTEMS)
7. KILN SHELL MONITORING SYSTEM (ECS/CEMSCANNER™)
8. ANALYZER / EMS / POLLUTION MONITORING AND REPORTING SYSTEM
9. WINDOWS BASED HMI'S, KIOSKS USED FOR MONITORING AND CONTROL PURPOSES IN REMOTE LOCATIONS
10. OPC OR IOT GATEWAY SYSTEMS
11. WE CONTINUOUSLY INTRODUCE NEW APPLICATIONS - CONTACT US FOR DETAILS.

FULLER® TECHNOLOGIES

fuller-technologies.com

Copyright © 2025 FULLER Technologies. All Rights Reserved. FULLER® is a registered trademark of FULLER Technologies. This brochure makes no offers, representations or warranties (express or implied), and information and data contained in this brochure are for general reference only and may change at any time.

C 12-25 2000-19-ENG