



## DISPOSITIVO DE SEGURIDAD INDUSTRIAL CISCO ISA-3000

### Firewall para prevenir amenazas y asegurar sus sistemas de control industrial.

Las empresas de fabricación, energía, transporte y otras industrias están transformando sus operaciones a través de la digitalización. Esta integración más profunda entre redes de TI, nube e industrial está creando muchos problemas de seguridad que ahora están poniendo en riesgo la integridad de la producción, la continuidad y la seguridad. A medida que las organizaciones industriales conectan más dispositivos, permiten un acceso más remoto y crean nuevas aplicaciones, el enfoque de brecha aérea para proteger las redes industriales contra las amenazas cibernéticas ya no es suficiente. Las tecnologías operativas (OT) tienen necesidades específicas de protección contra amenazas, que requieren una solución robusta y una comprensión perfecta de los protocolos industriales.

Los dispositivos de seguridad industriales ISA3000 ofrecen soluciones a estas incesidades de protección contra intrusiones y las políticas de seguridad de red del software de firewall de próxima generación de Cisco. Desarrollados específicamente para su despliegue en los entornos industriales más duros, estos Firewalls industriales son la base para permitir operaciones industriales seguras y cumplimiento normativo.

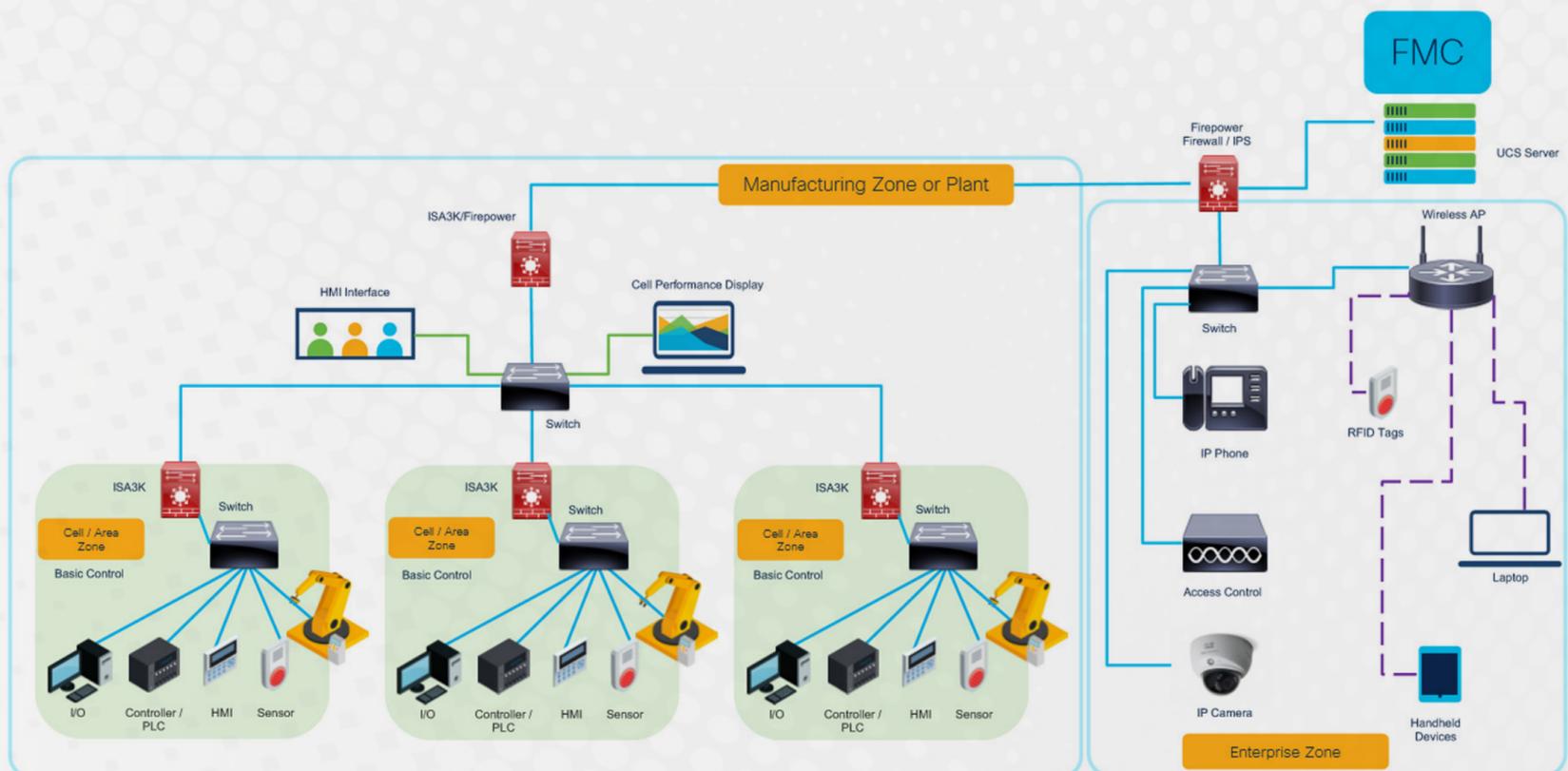
### Beneficios

- Reduzca el riesgo con el conocimiento de las aplicaciones: Controle el tráfico de la red industrial para ayudar a garantizar el tiempo de actividad y la integridad de la producción. El ISA3000 entiende los protocolos OT propietarios y estándar.
- Proteger los ordenadores OT del malware: Bloquear el tráfico malicioso antes de que sea demasiado tarde. El ISA3000 aprovecha talos® inteligencia de amenazas para analizar continuamente archivos y descubrir amenazas sigilosas
- Extender la seguridad de TI a OT: Aplicar políticas de seguridad consistentes en OT e TI. El ISA3000 es parte de la familia © Cisco Firepower y aprovecha las mismas herramientas de administración.
- Simplificar el cumplimiento y reducir el alcance de auditoría: Construir una red industrial segura que cumpla con los requisitos reglamentarios. El ISA3000 le ayuda a ajustarse a NERC-CIP, ISA99, IEC 62443, CFATS, ANSI/AWWA G430, y otro.

## PROTOSCOLOS SOPORTADOS POR ISA 3000

Protocolo/Detección de aplicaciones	Inspección profunda de paquetes
BACNet COSEM COTP DNP3 Emission control protocol Fujitsu device control GOOSE GSE IEC-60870-5-104 ISO MMS Modbus OPC-UA Q931 SRC TPKT CIP Honeywell Control Station/NIF Server Honeywell Experion DSA Server Monitor	Opciones para inspeccionar el encabezado, carga útil para filtrar en función de funciones, comandos y datos  Modbus DNP3 CIP IEC-60870-5-104 IEC-61850-MMS SIEMENS S7
<b>Política de control de acceso FTD/FMC</b>	<b>Política de intrusión FTD/FMC</b>

## POSICIONAMIENTO DEL FIREWALL ISA-3000 EN LA INDUSTRIA



## ¿POR QUÉ CISCO?

La Industria se está convirtiendo en una gran fuente de datos que requiere redes seguras y confiables

- Cartera completa de productos de red industrial (Wired & Wireless)
- Facilidad de gestión
- Productos seguros (por diseño) y soluciones de seguridad holísticas
- Alianza estratégica con Rockwell Automation
- Experiencia en la industria y soporte técnico de clase mundial.