Cybersecurity: Proponiendo una Infraestructura Física para la Seguridad del Mañana.

Neyton Avila – Consultant TSE

MBA, CCNPX3 (Enterprise, Data Center, Security)

Marcelino Vázquez – Territory Account Manager (México)

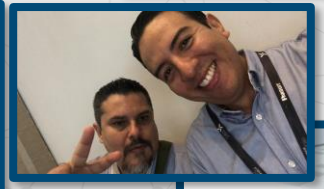
PANDUIT™

PRESENTACIÓN

JORGE NEYTON
34 | Tepic, Nayarit. MX
Maestría en **Informática Aplicada**
ITESO

Cisco CCNP Certiifcations:
Enterprise, Data Center, Security.
Business Development
Digital Transformation

Mobile: +52 3316068159
neyton.avila@panduit.com



Agenda

- Cybersecurity: aspectos fundamentales.
- Clasificación de Ataques Cibernéticos.
- El papel de la infraestructura física en la identificación, protección y detección de incidentes.
- ANSI / TIA-5017: Estándar de seguridad de redes físicas de telecomunicaciones
- Modelo de Arquitectura de Referencia para Redes Industriales: CPwE
- Conclusiones

GET TO KNOW PANDUIT

Cybersecurity

Aspectos Fundamentales de la Ciberseguridad

La **ciberseguridad** es la práctica de proteger sistemas, redes y programas de ataques digitales. Estos ataques cibernéticos generalmente tienen como objetivo acceder, cambiar o **destruir (Destruction of Service - DeOS)** información confidencial; extorsionar a los usuarios con dinero; o interrumpir los procesos comerciales normales.

La implementación de medidas efectivas de ciberseguridad es particularmente desafiante hoy porque hay más dispositivos que personas, y los atacantes se están volviendo más inovadores.

GET TO KNOW PANDUIT

La Humanidad está en guerra Cibernética

El cibercrimen es la nueva palabra de moda. Los **hackers** se han vuelto altamente sofisticados y organizados. Se han convertido en el nueva mafia, y la están manejando como una industria.

De acuerdo con la base de datos del Índice de Nivel de Infracción1, **1,792 violaciones** de datos fueron detectadas en 2016, lo que resultó en el robo de **1.3 billones de registros de datos**. Solo para aclarar, estas son las violaciones de datos informadas públicamente y no incluyen miles de incidentes de ciberataques y violaciones de datos no descubiertas.

1 http://breachlevelindex.com/assets/Breach-Level-Index-Report-2016-Gemalto.pdf
2 http://www.havocscope.com/black-market-prices/hackers/
3 http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by2019/#4af445823bb0

Fuente Oracle: http://www.oracle.com/us/technologies/linux/anatomy-of-cyber-attacks-wp-4124673.pdf

GET TO KNOW PANDUIT

Aquí hay algunos ejemplos de cómo los hackers han industrializado el cibercrimen[2]:

- Puede obtener los datos completos del seguro de salud de alguien pagando $ 1,250.
- Por solo $ 7 / hora, puede desatar un ataque de denegación de servicio (**DoS**) distribuido en su competencia.
- Puede comprar registros Fulz de los Estados Unidos (identidad de alguien, pasaporte, número de seguro social y otros). Puedes obtener todo eso por alrededor de $ 40.
- También puede obtener 10,000 seguidores falsos de Twitter por $ 15.
- Y si desea acceder a un servidor del gobierno, puede obtenerlo por $ 6.

Estás tratando con organizaciones profesionales que:

- **Proporcionar servicio al cliente 24/7**
- Ofrecer **ataques** de prueba gratuitos para demostrar su destreza;
- Pago después del ataque exitoso una vez que esté satisfecho con los resultados.

El costo del delito cibernético en 2016 se estima en alrededor de **$ 445 mil millones**, y se prevé que aumente a alrededor de **$ 2 Trillones** a nivel mundial para 2019.[3]

Estas estimaciones solo incluyen ataques conocidos, no delitos informáticos no detectados, **espionaje industrial** o patrocinio estatal ataques.

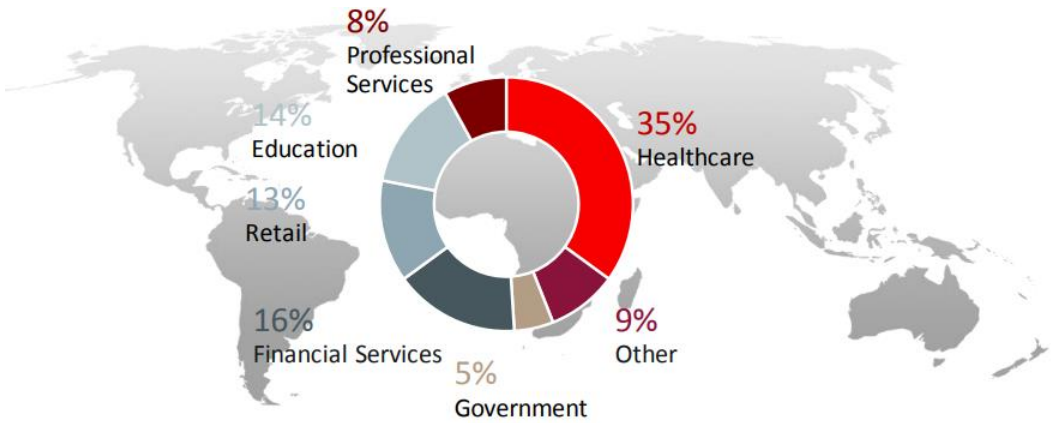
1 http://breachlevelindex.com/assets/Breach-Level-Index-Report-2016-Gemalto.pdf
2 http://www.havocscope.com/black-market-prices/hackers/
3 http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by2019/#4af445823bb0

Fuente Oracle: http://www.oracle.com/us/technologies/linux/anatomy-of-cyber-attacks-wp-4124673.pdf

GET TO KNOW PANDUIT

Nadie es inmune…

En 2016, aproximadamente el 35% de todos los ataques ocurrieron contra la **industria de la salud**.[4] En el pasado servicios financieros han sido el mayor objetivo Sin embargo, la industria de servicios financieros se ha vuelto más inteligente y se ha fortalecido. En 2016, el tipo de incidente más común fue el **phishing / hacking / malware** con un **43%**. Fue el tipo más grande de ataque / incidente en todos los sectores, excepto servicios financieros.[5] Hoy, todos los sectores empresariales deben asumir que están en riesgo.



[4] https://www.databreaches.net/bakerhostetler-2017-data-security-incident-response-report-based-on-450-incidents/
[5] https://www.databreaches.net/bakerhostetler-2017-data-security-incident-response-report-based-on-450-incidents/

Fuente Oracle: http://www.oracle.com/us/technologies/linux/anatomy-of-cyber-attacks-wp-4124673.pdf

GET TO KNOW PANDUIT

ANATOMÍA DEL ATAQUE

Aquí hay 7 componentes en la anatomía de un ciberataque, cada uno explicado por **Fortinet:**

1- **Reconocimiento**: el atacante debe comprender todo lo que pueda sobre una organización y su red para planificar su ataque. Entonces, en esta etapa, se investigan y prueban los mecanismos de defensa y respuesta de una organización. Los atacantes que **buscan dispositivos o sistemas operativos sin parches** utilizan las redes sociales para conocer a los empleados y buscar otra información importante de la compañía, como qué aplicaciones podría tener en su red. También pueden investigar a los socios comerciales de la víctima para evaluar si uno de ellos tiene una postura de seguridad más débil que puede convertirse en un camino hacia la red deseada.

2 - **Armamento:** una vez que se identifican las vulnerabilidades dentro de la organización objetivo, los atacantes crean **código malicioso** para explotarlas sin ser detectadas. Si el atacante es un actor del estado nación, es probable que use un **exploit de día cero**, pero la mayoría de los ciberdelincuentes usan kits de **exploit** centrados en vulnerabilidades conocidas públicamente. Muchos de estos kits utilizan técnicas de evasión que pueden evitar una serie de controles tecnológicos, como firewalls y antivirus.

3- **Entrega:** una vez que el arma cibernética es elegida y / o construida, el atacante necesita encontrar el mejor mecanismo para entregarla. Los vehículos de entrega incluyen sitios web infectados, publicidad maliciosa y uno de los más comunes: **correos electrónicos de phishing e ingeniería social**. Con tanta información en línea sobre los empleados, los correos electrónicos de phishing se están volviendo extremadamente personalizados y cada vez más difíciles de distinguir de uno legítimo. Desafortunadamente, todo lo que el actor de la amenaza necesita para tener éxito en esta etapa es engañar a un empleado para que haga clic en un enlace.

GET TO KNOW PANDUIT

4 - **Explotación:** una vez que se entrega el **exploit**, debe ejecutarse sin ser detectado. Con los correos electrónicos de phishing como una herramienta preferida, muchos ataques se realizan en el lado del cliente de la red, enfocados en el navegador del usuario y sus complementos vulnerables, como flash y java. Otros **exploits** entregan macros y scripts maliciosos ocultos dentro de los documentos enviados a otros usuarios.

5 - **Comando y control:** una vez ejecutado con éxito, el **exploit** intenta comunicarse con el actor de la amenaza detrás de él para descargar malware y otras herramientas para comprometer aún más la red invadida. Para comunicarse sin ser detectados, los comandos y las solicitudes generalmente se canalizan a través de protocolos como HTTP (S), DNS o TOR y las comunicaciones a menudo se cifran.

6 - **Reconocimiento interno:** dado que el primer punto de inserción suele ser una estación de trabajo vulnerable, los atacantes deben moverse lateralmente a través de la red de la víctima para mapear su infraestructura y encontrar los datos que buscan para completar su misión cibernética. Para hacer eso, necesitan comprometer otros dispositivos, **incluidos IoT y dispositivos de atención médica en la red**. Un buen lugar para comenzar es encontrar un servidor que almacene todas las credenciales de usuario y dispositivo, como un servidor de Active Directory.

7 -**Mantener:** los atacantes quieren permanecer el mayor tiempo posible en la red de la víctima, por lo que profundizan en ella para mantener un punto de apoyo, instalando cosas como rootkits para ocultar archivos o rootkits en modo kernel llamados **bootkits**. Los bootkits pueden infectar el código de inicio para obtener acceso sin restricciones a una computadora completa, por lo que el exploit puede controlar todo lo que el usuario puede ver. Pero puede ser un desafío para el atacante cuando los datos que desean robar no se encuentran en un dispositivo con acceso directo a Internet. En este caso, una vez que el actor de la amenaza ha apuntado los datos, es posible que necesite encontrar y comprometer otro servidor que tenga acceso a Internet para usarlo como un área de preparación, un área de almacenamiento intermedio que permite el proceso de extracción, como almacenes de datos u otros repositorios de datos.

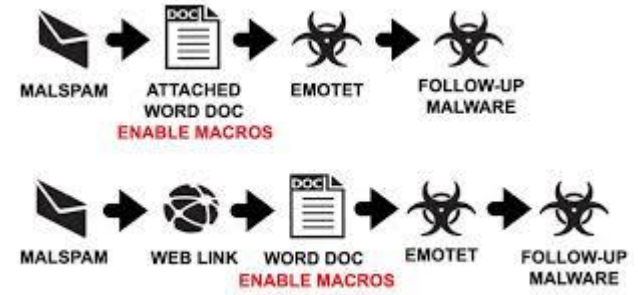
GET TO KNOW PANDUIT

Ataques de Emotet: un pico para comenzar el año 2020...

Es posible que haya escuchado hablar de Emotet en las noticias. ¿Qué es?: ¿Un rey del antiguo Egipto, el grupo emo favorito de su hermana adolescente? Nos tememos que no.

El troyano bancario Emotet fue identificado por primera vez por investigadores de seguridad en 2014. Emotet fue diseñado originalmente como un malware bancario que intentaba colarse en su ordenador y robar información confidencial y privada. En versiones posteriores del software se añadieron los servicios de envío de spam y malware, incluidos otros troyanos bancarios.
Emotet utiliza funciones que ayudan al software a eludir la detección por parte de algunos productos anti-malware.

Emotet utiliza capacidades similares a las de un gusano para ayudar a su propagación a otros ordenadores conectados. Esto ayuda a la distribución del malware. Esta funcionalidad ha llevado al Departamento de Seguridad Nacional de los Estados Unidos a la conclusión de que Emotet es uno de los malware más costosos y destructivos, que afecta a los sectores gubernamentales y privados, particulares y organizaciones, y cuya limpieza por incidente cuesta más de **1 millón de dólares**.



https://es.malwarebytes.com/emotet/

GET TO KNOW PANDUIT

Tipos de Amenazas Cibernéticas

Phishing

El **phishing** es la práctica de enviar correos electrónicos fraudulentos que se parecen a correos electrónicos de fuentes confiables. El objetivo es robar datos confidenciales como números de tarjetas de crédito e información de inicio de sesión. Es el tipo más común de ciberataque. Puede ayudar a protegerse a través de la educación o una solución tecnológica que filtra los correos electrónicos maliciosos.

GET TO KNOW PANDUIT

DEMO – Phishing attack

GET TO KNOW PANDUIT

Tipos de Amenazas Cibernéticas

Ransomware

El **ransomware** es un tipo de software malicioso. Está diseñado para extorsionar dinero bloqueando el acceso a los archivos o al sistema informático hasta que se pague el rescate. Pagar el rescate no garantiza que los archivos se recuperarán o que se restaurará el sistema.

GET TO KNOW PANDUIT

Ransomware – Anatomy of an Attack

https://www.youtube.com/watch?v=4gR562GW7TI

GET TO KNOW PANDUIT

Tipos de Amenazas Cibernéticas

Malware

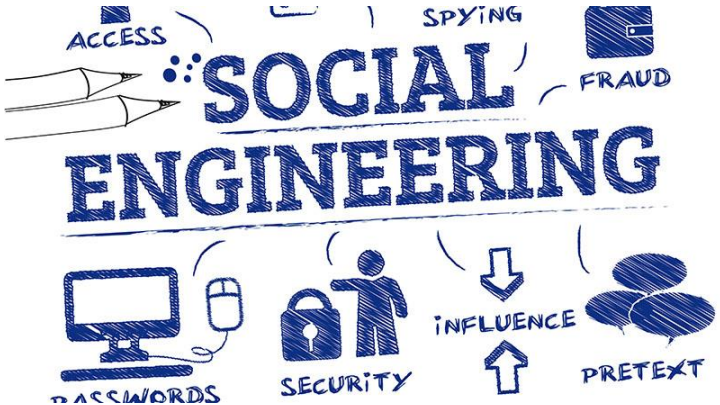
El malware es un tipo de software diseñado para obtener acceso no autorizado o para dañar una computadora.

GET TO KNOW PANDUIT

DEMO – MALWARE

GET TO KNOW PANDUIT

Tipos de Amenazas Cibernéticas



Social Engineering

La ingeniería social es una táctica que usan los adversarios para engañarte y revelar información confidencial. Pueden solicitar un pago monetario u obtener acceso a sus datos confidenciales. La ingeniería social se puede combinar con cualquiera de las amenazas enumeradas anteriormente para que sea más probable que haga clic en enlaces, descargue malware o confíe en una fuente maliciosa.

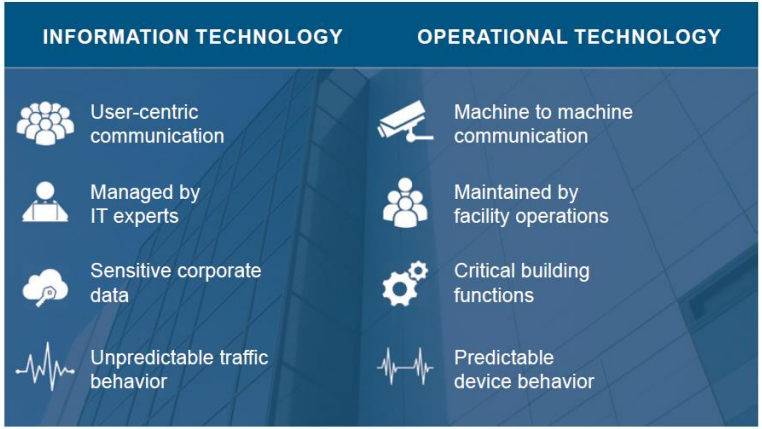
GET TO KNOW PANDUIT

El papel de la infraestructura física en la identificación, protección y detección de incidentes.

GET TO KNOW PANDUIT

Infraestructura física para la seguridad del mañana

Los sistemas de seguridad de red física correctamente planificados e instalados pueden proteger la infraestructura y los componentes críticos de telecomunicaciones contra robos, vandalismo, intrusiones y modificaciones no autorizadas. Es significativamente menos costoso y menos disruptivo instalar sistemas físicos de seguridad de red durante la fase de construcción o renovación del edificio que durante la fase de ocupación del edificio.



IT y OT son diferentes en muchos aspectos. Es importante que ellos trabajen en conjunto para diseñar sistemas robustos y seguros.

GET TO KNOW PANDUIT

¿Te suena familiar?

Twitter
330M records
A glitch stored passwords in readable text.

WorldPress
76.5M records
Security vulnerability

Facebook
29M records
Malicious 3rd party collected profile information

Uber
57M records
Uber paid hackers $100k to delete the stolen data.

Quora
100M records
Logins compromised

MyHeritage
92.2M records

British Airways
380k records
Customers personal and financial details were compromised

Orbitz
880K records
Payment Card info

T-Mobile
2M records

Marriott Hotels
383M records
Sensitive data leaked since 2014

Blur
2.4M records

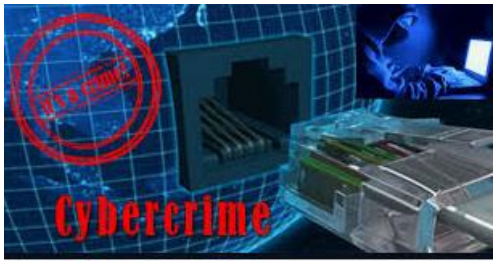
Amazon
100k records
Customer names and email addresses accidentally disclosed on its website.

Google
52.5M records
User's personal details could've been exposed. data.

GET TO KNOW PANDUIT

Violaciones de datos ... "la nueva normalidad"

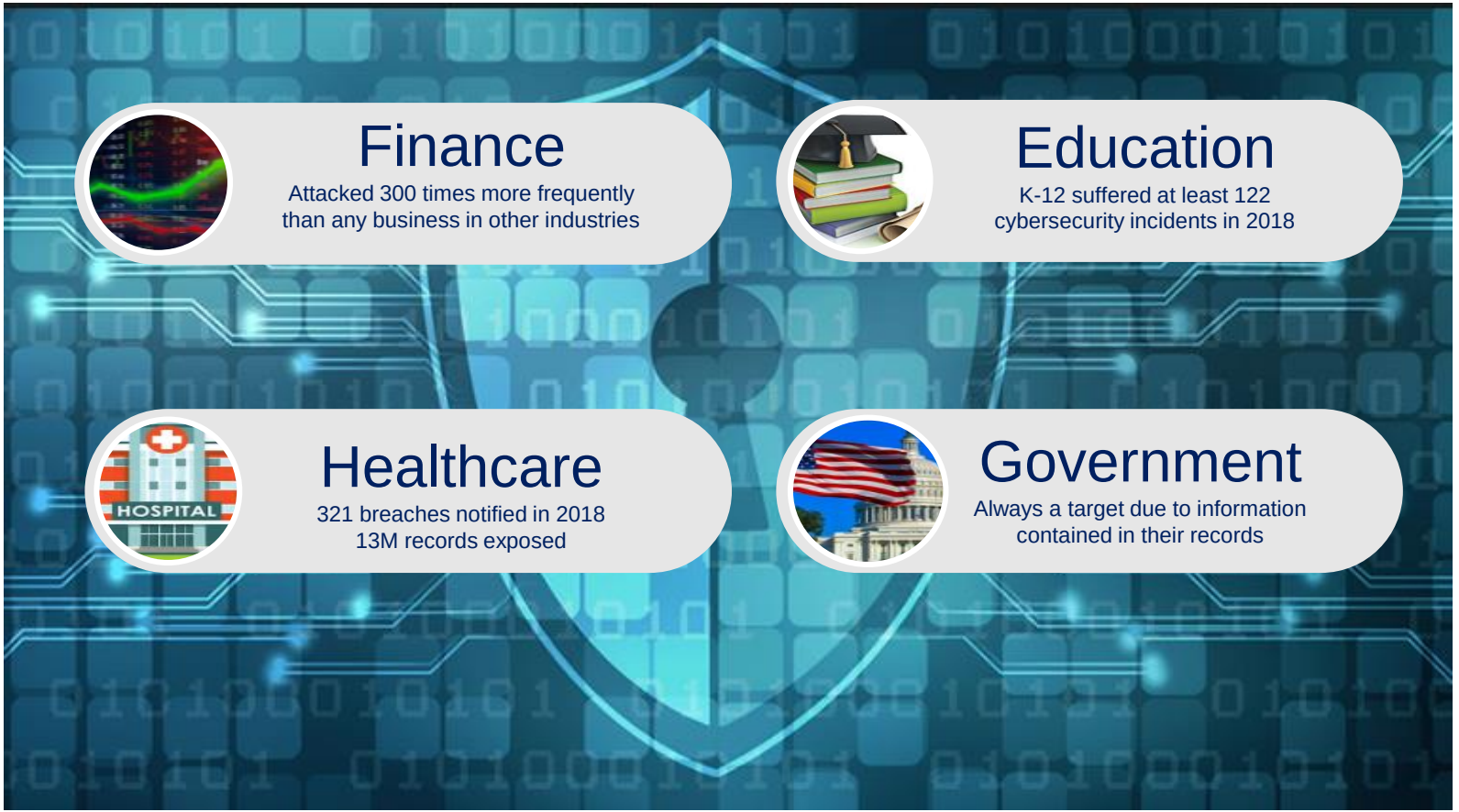
- Los riesgos de seguridad cibernética están aumentando debido a la creciente dependencia de los sistemas informáticos y los dispositivos inteligentes.
- Se estima que para 2020 habrá alrededor de 200 mil millones de dispositivos conectados.
- El 95% de las infracciones se deben a un error humano.
- El costo promedio de una violación de datos en 2020 superará los $ 150 millones de dólares.
- Un puerto abierto es una invitación para acceder fácilmente a sus datos ... ¡bloquéelos!



"El delito cibernético es la mayor amenaza para todas las empresas del mundo"
IBM's chairman, president & CEO Ginni Rometty

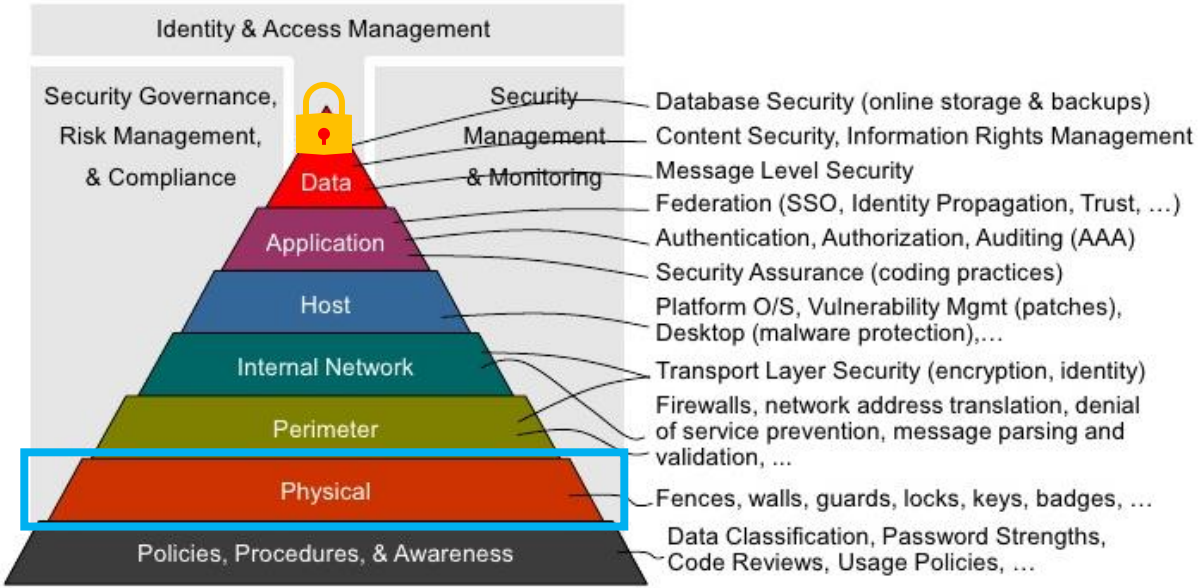
GET TO KNOW PANDUIT

Objetivos principales ...



GET TO KNOW PANDUIT

Proteja sus datos, agregue capas a su seguridad



GET TO KNOW PANDUIT

Ejemplos de algunas violaciones de datos:

En el Colegio de St Rose en Nueva York, un ex alumno usó un dispositivo USB armado llamado "USB Killer" que compró en línea para destruir 59 computadoras, 7 monitores y podios mejorados por computadora que tenían ranuras USB abiertas. 14 de febrero de 2019.

Marriott Hotels, reconocieron que una parte no autorizada había copiado y encriptado información perteneciente a clientes en su sistema de reservas Starwood. Accediendo a la información del pasaporte y los detalles de la tarjeta de crédito desde 2014. Después de una investigación, el tamaño del hack se estimó en alrededor de 383 millones. Nov. De 2018

Google descubrió un error en las API de Google+ durante su procedimiento de prueba estándar. Esta es la segunda vez que afecta a 52.5 millones de usuarios. Este sitio se cerró en abril de 2019 después de descubrirlo en noviembre de 2018

Toyota, se detectó un acceso no autorizado en los sistemas informáticos de múltiples filiales de ventas de Toyota y Lexus en Tokio, y se filtró información de aproximadamente 3,1 millones de clientes. Febrero 2019

GET TO KNOW PANDUIT

Panduit puede ayudar ...

- Nueva línea de dispositivos de bloqueo de seguridad de red con mecanismo de llave único

SKMKEY

UNA LLAVE
múltiples dispositivos

SKUSBA-V

SKUSBC

SKRJ45RD-X

GET TO KNOW PANDUIT

Dispositivo de bloqueo USB tipo A SKUSBA-V

- USB es una interfaz plug and play popular que permite a las computadoras comunicarse con otros dispositivos. También es una forma fácil de transferir **malware** o dañar equipos.

- Compatible con los puertos tipo A que se encuentran comúnmente en la mayoría de los dispositivos host
- Se monta al ras del puerto
- Instalación fácil de un solo empuje
- Desmontable con Panduit SmartKeeper Master Key
- Reemplazará la oferta existente de PSL-USBA

GET TO KNOW PANDUIT

Dispositivos de bloqueo USB tipo C

- Ampliamente adaptado desde 2015, se espera que el uso crezca al reemplazar varios tipos de conexiones que permiten que las computadoras se comuniquen con otros dispositivos, lo que lo convierte en un punto de fácil acceso a los datos.

- Compatible con puertos tipo C encontrados en una variedad de host y dispositivos periféricos.
- Mecanismo de bloqueo de un solo empuje fácil después de insertado en el puerto
- Desmontable con Panduit SmartKeeper Master Key

GET TO KNOW PANDUIT

Dispositivos de bloqueo RJ45

- Los puertos RJ45 se encuentran prácticamente en cualquier lugar, proporcionando acceso a la red y a sus datos. El puerto también puede ser dañado por un objeto extraño.

Locked Unlocked

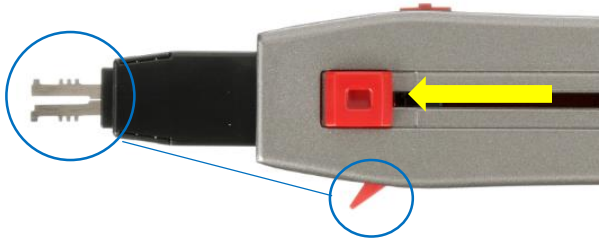
- Compatible con la mayoría de las aberturas RJ45
- Disponible en color rojo
- Construcción de dos piezas
- Mecanismo de bloqueo de un solo empuje fácil después de insertado en el puerto
- Desmontable con Panduit SmartKeeper Master Key

GET TO KNOW PANDUIT

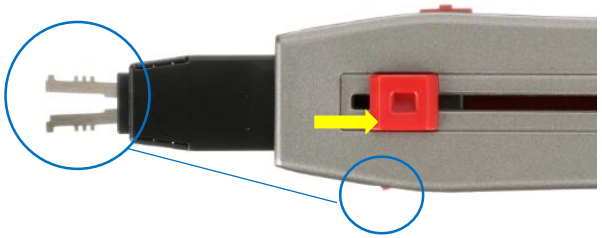
Llave Maestra SmartKeeper

- El patrón de la cuchilla es único y solo es compatible con los dispositivos de bloqueo SmartKeeper de Panduit
- El botón deslizante expulsa o retrae las cuchillas con llave; bloquea las cuchillas en el dispositivo para su extracción
- La palanca lateral también bloquea la llave en el dispositivo cuando se presiona
- Incluye luz que se activa mediante un interruptor
- Empuñadura de goma antiestática

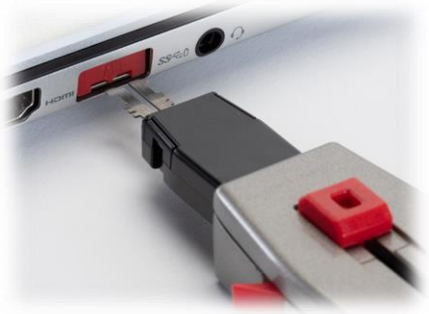
Master key – funcionalidades

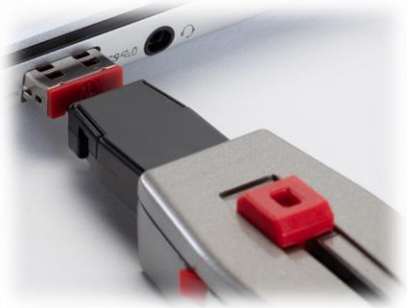


DESBLOQUEADO - (las cuchillas están juntas) Se usa para insertar o quitar del dispositivo



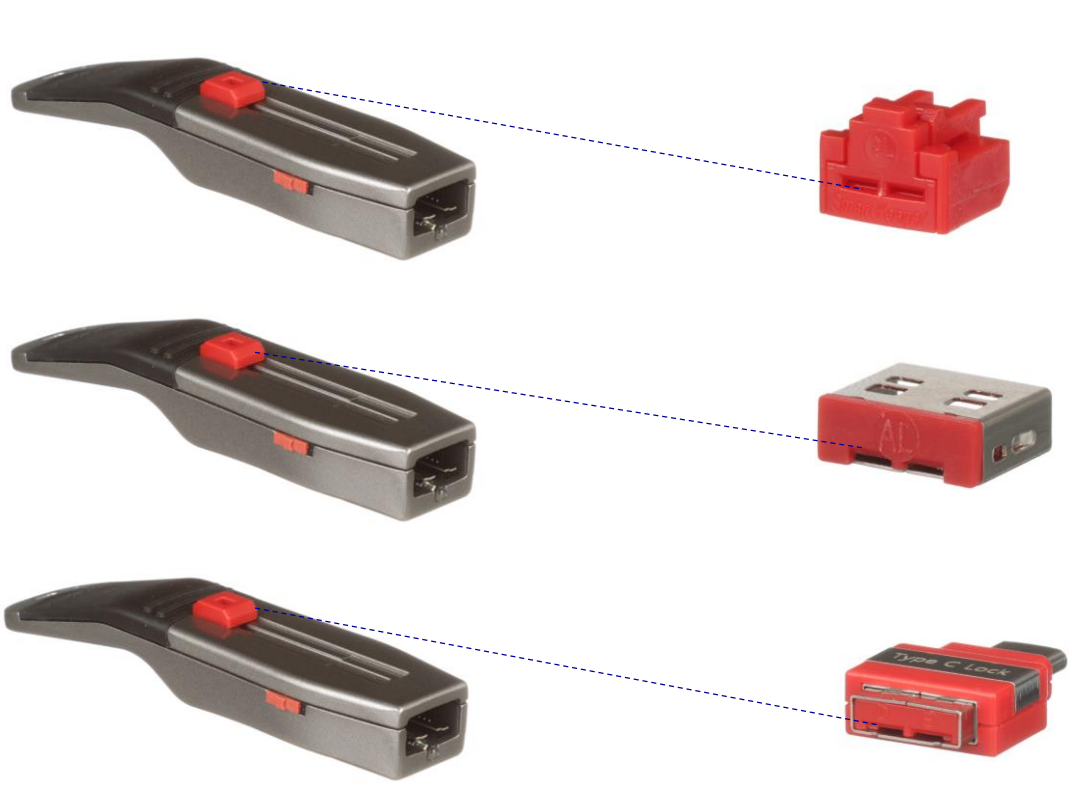
BLOQUEADO - (cuchillas abiertas) Se usa para recuperar el dispositivo del puerto





GET TO KNOW PANDUIT

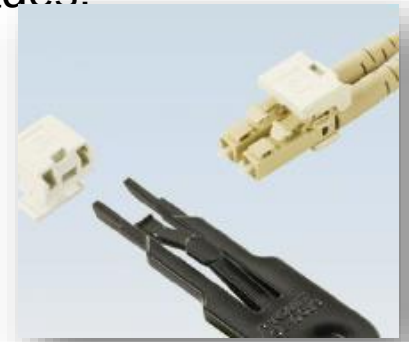
Llave Maestra - Orientación

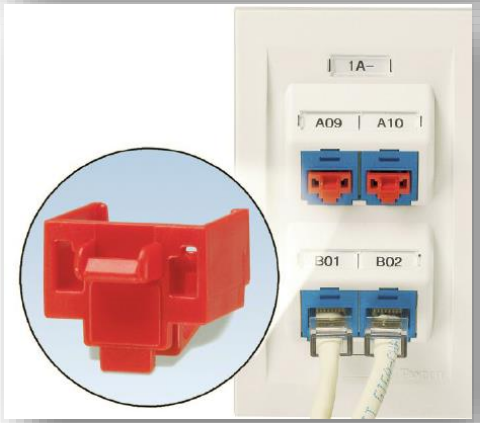


GET TO KNOW PANDUIT

Productos de seguridad física adicionales ...

- Panduit ofrece una amplia oferta de dispositivos de seguridad para satisfacer la mayoría de las necesidades.





GET TO KNOW PANDUIT

Recuerda….

- La interfaz común plug and play permite a las computadoras comunicarse con otros dispositivos
- No tiene que ser un dispositivo convencional
- Un puerto abierto es como entregar las llaves de tu casa a extraños
- Cierre todo el acceso abierto a sus datos con los dispositivos de seguridad de red SmartKeeper de Panduit.

ANSI / TIA-5017: Estándar de seguridad de redes físicas de telecomunicaciones

Estándar TIA para la Seguridad de Infraestructura de Red

ANSI/TIA-5017: Telecommunications Physical Network Security Standard

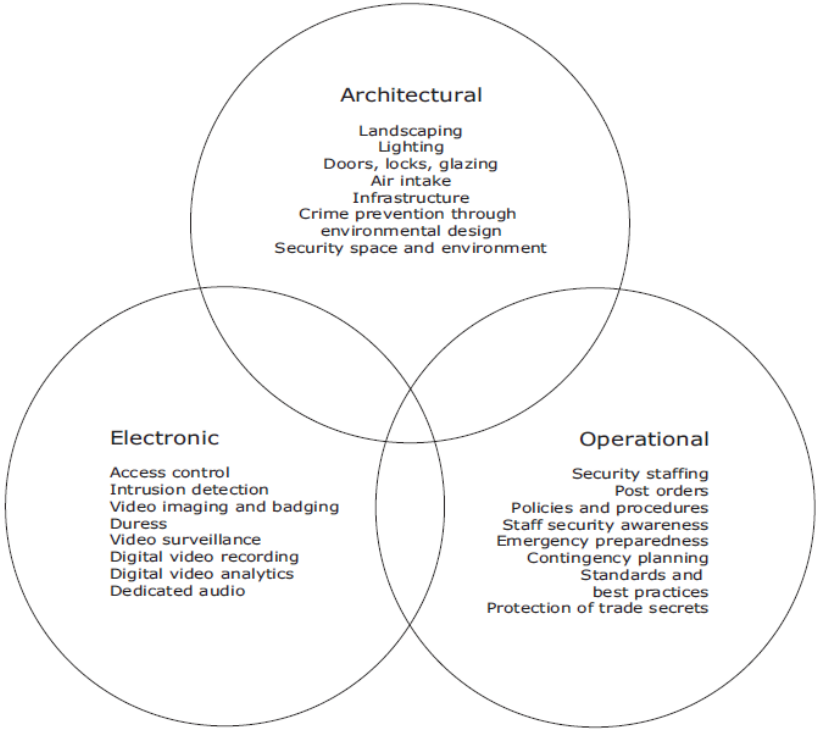
El estándar ANSI / TIA 5017, especifica los requisitos para analizar los niveles de seguridad y desarrolla un marco de seguridad individualizado para las infraestructuras de telecomunicaciones, ahora se está considerando oficialmente para convertirse en un estándar internacional. Fue desarrollado por el Subcomité de cableado de edificios comerciales TIA TR-42.1 y publicado en febrero de 2016.

Esta Norma especifica los requisitos y las pautas para proteger y asegurar la infraestructura de telecomunicaciones (por ejemplo, cables de telecomunicaciones, vías, espacios y otros elementos de la infraestructura física) en locales propiedad del cliente. Establece tres niveles de seguridad de la infraestructura física y proporciona pautas de diseño, prácticas de instalación, administración, gestión y otras consideraciones adicionales para mejorar la seguridad física de la infraestructura de telecomunicaciones.

GET TO KNOW PANDUIT

Funciones y características de seguridad en ANSI/TIA-5017

- Directrices de evaluación de riesgos para establecer el nivel de riesgo.
- Tres niveles diferentes de seguridad que el cliente puede implementar para igualar el nivel de riesgo
- Requisitos de seguridad para cada elemento de telecomunicaciones en cada nivel de seguridad elegido
- Requisitos de seguridad adicionales para aquellas instalaciones que protegen los sistemas de distribución (PDS)
- Requisitos de detección de intrusiones
- Requisitos de vigilancia especialmente para instalaciones educativas.
- Uso de sistemas AIM (Gestión Automatizada de Infraestructura) para mejorar la seguridad general de la premisa



Niveles de seguridad de infraestructura física ANSI / TIA-5017

TIA-5017 reconoce tres niveles de seguridad de la infraestructura de cableado para diversas necesidades de seguridad:

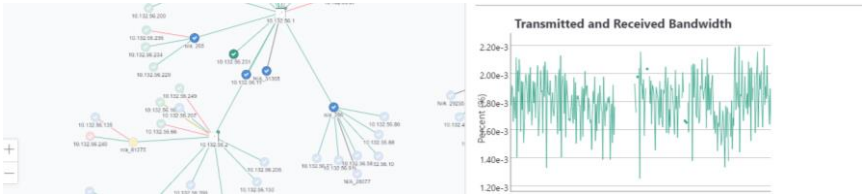
- SL1 - Instalación de seguridad básica
- SL2 - Instalación de resistencia a la manipulación
- SL3 - Instalación de seguridad crítica

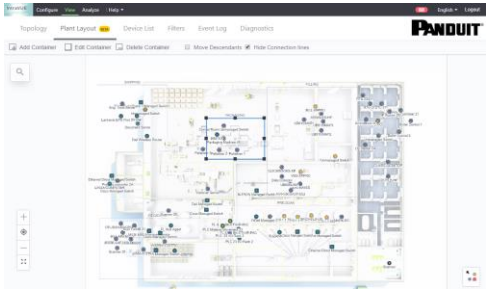
ANSI / TIA-5017 Gestión automatizada de infraestructura (AIM) para seguridad

TIA-5017 recomienda que un sistema AIM se considere como un medio adicional para mejorar la seguridad de la infraestructura de cableado.

Se mencionan las siguientes capacidades de administración automatizada:

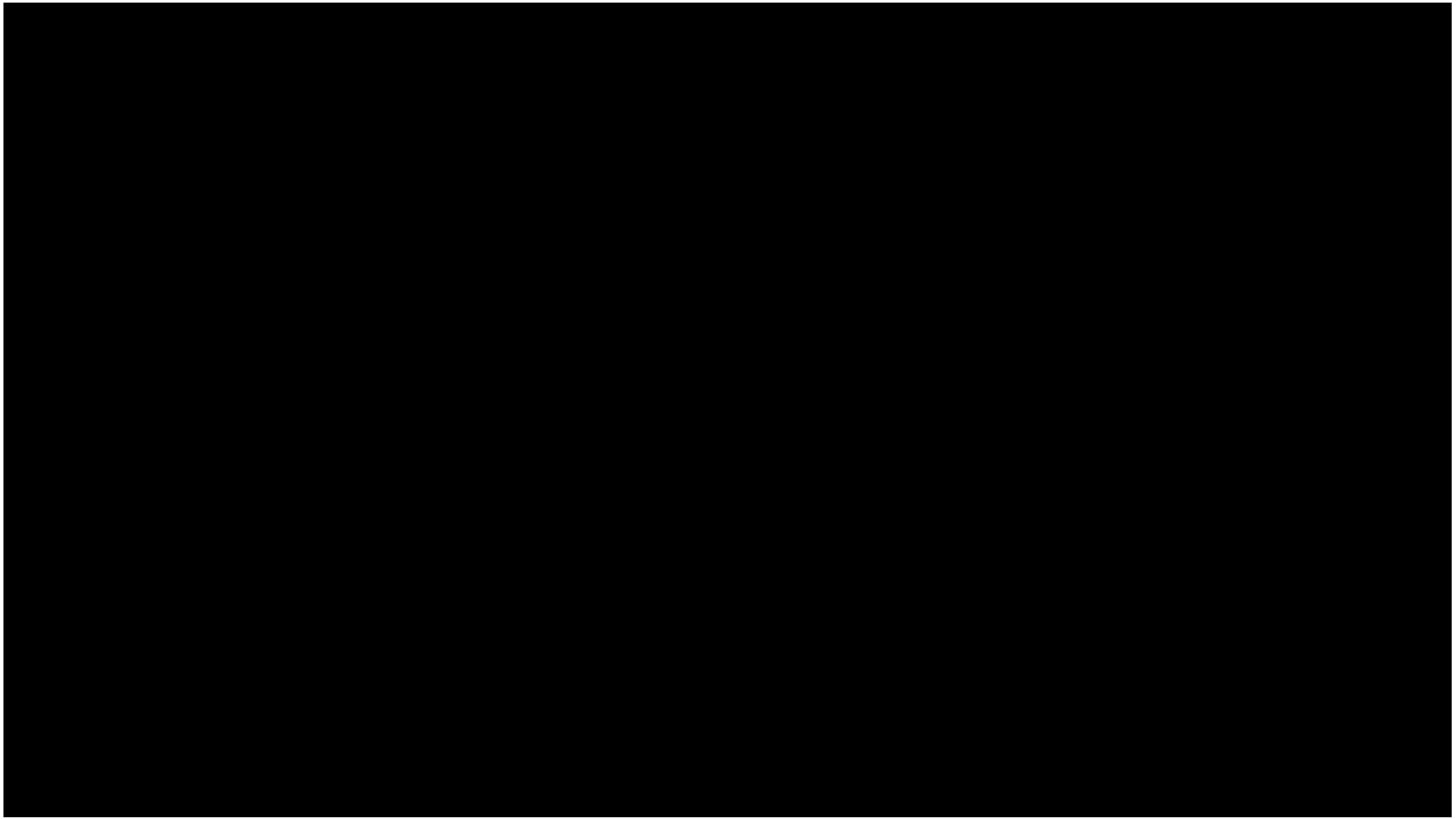
- **Se pueden detectar cambios en la conectividad del cable de conexión**
- El estado de **disponibilidad de puertos** en el equipo de red se puede **monitorear en tiempo real**
- Se pueden identificar los circuitos críticos de la red y reportar las infracciones en tiempo real
- Las conexiones del dispositivo se pueden **detectar e informar** y se puede identificar **su ubicación**
- La integración con **cámaras de seguridad** puede ser compatible para grabar eventos
- Se admite la comunicación y el intercambio de datos con otros sistemas y bases de datos.
- La ubicación de origen de la llamada de emergencia se puede identificar e informar
- Los componentes de AIM se pueden asegurar





Modelo de Arquitectura de Referencia para Redes Industriales: CPwE

GET TO KNOW PANDUIT



Simplificando la implementación robusta de redes industriales

Una infraestructura de capa física de red de extremo a extremo confiable desde la empresa hasta el borde

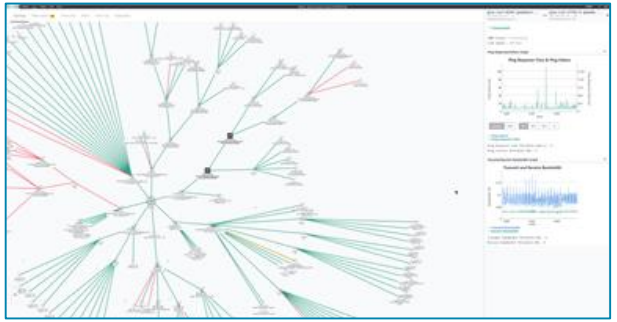
- Conectando la empresa a la planta
- Distribución de Ethernet en toda la planta
- Conexión de máquinas y dispositivos a la arquitectura de la planta
- Implementación de Ethernet en la máquina
- Fortalecimiento de la red desde cero

GET TO KNOW PANDUIT

Conectando la red Empresarial a la Planta

- Optimizar la comunicación y el enlace
- Agrupar equipos de red
- Mantener un rendimiento sólido de la red
- Garantizar la seguridad de la red

MICRO DATA CENTER



INTRAVUE

GET TO KNOW PANDUIT

CPwE - Ethernet convergente en toda la planta

- **ARQUITECTURAS DE REFERENCIA PROBADAS Y VALIDADAS**
- Una colección de arquitecturas de referencia basadas en casos de uso
- Diseñado para ser robusto y escalable
- Creado por Cisco y Rockwell Automation hace 10 años
- Panduit ha sido un contribuyente activo durante más de 2 años.

www.panduit.com/cpwe

GET TO KNOW PANDUIT

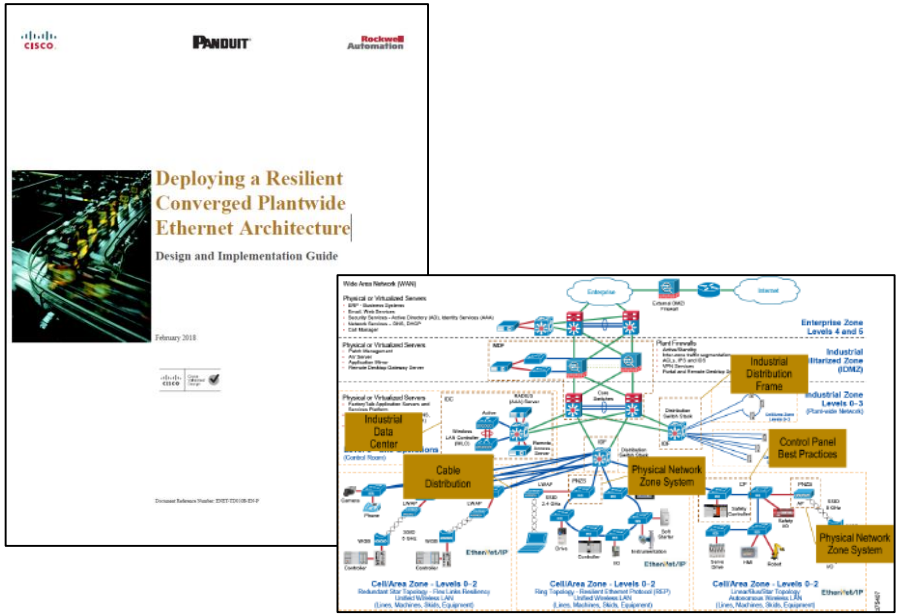
Ethernet convergente en toda la planta (CPwE)

Una colección de arquitecturas probadas y validadas desarrolladas por las autoridades de la materia en Cisco y Rockwell Automation y que siguen el programa Cisco Validated Design (CVD).

Cisco y Rockwell Automation han colaborado con **Panduit** para incluir su enfoque de bloques de construcción para la implementación de infraestructura física en arquitecturas específicas.

Para la implementación de una guía de diseño e implementación de arquitectura Ethernet en toda la planta convergente resiliente (DIG), Panduit documentó los siguientes casos de uso:

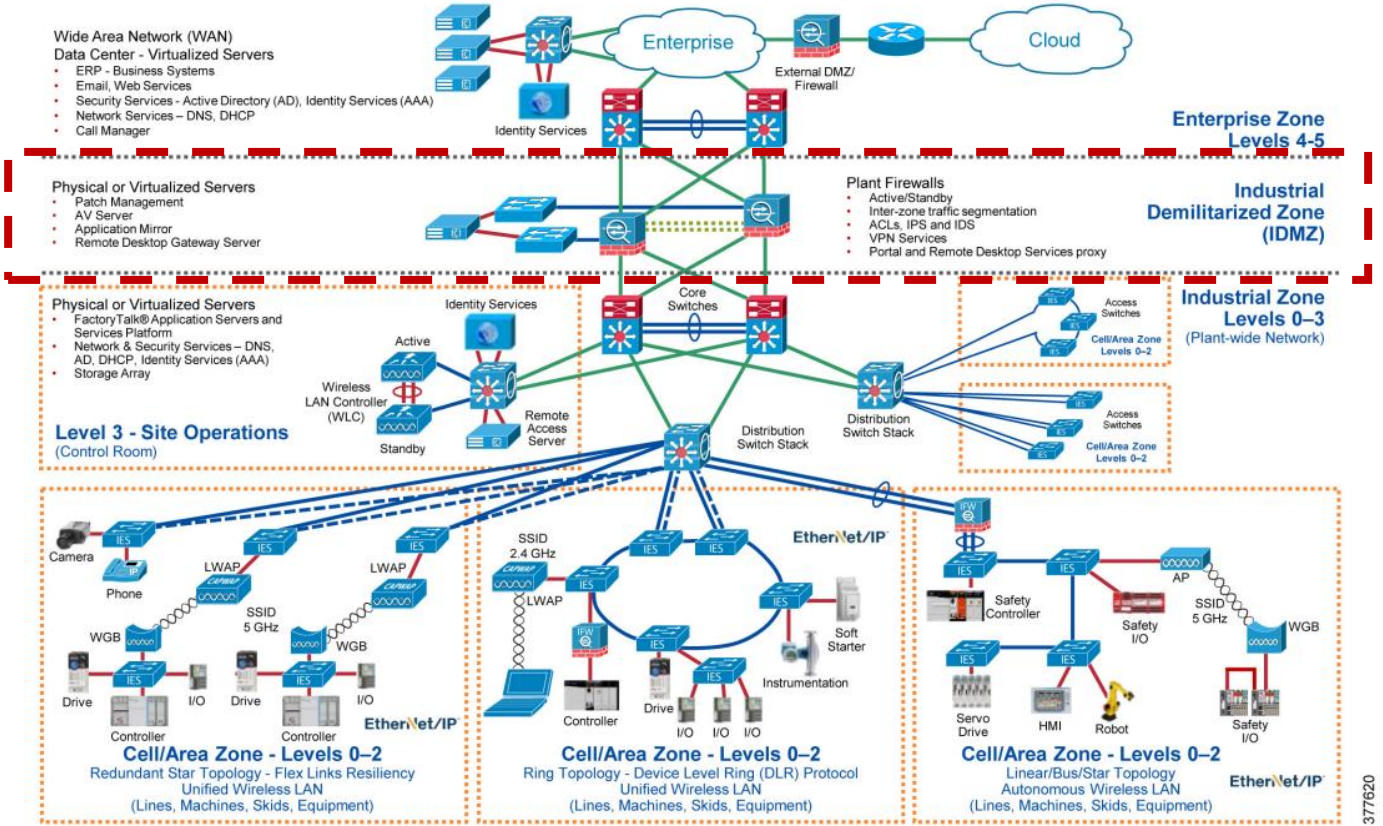
- **Panel de control**:
  - Mitigación de ruido de interferencia electromagnética (EMI) a través de la unión, blindaje y conexión a tierra.
  - Implementación del conmutador Ethernet industrial (IES) dentro de la zona de celda / área
- **Sistema de zona de red física**:
  - Despliegue de IES y punto de acceso (AP) dentro de la zona de celda / área
  - Distribución de cables en la zona industrial.
- **Marco de distribución industrial (IDF):**
  - Implementación de conmutadores de agregación / distribución industrial dentro de la zona industrial
- **Centro de datos industriales (IDC):**
  - Diseño físico y despliegue de las operaciones del sitio de nivel 3



Robust Physical Infrastructure for the CPwE Architecture

GET TO KNOW PANDUIT

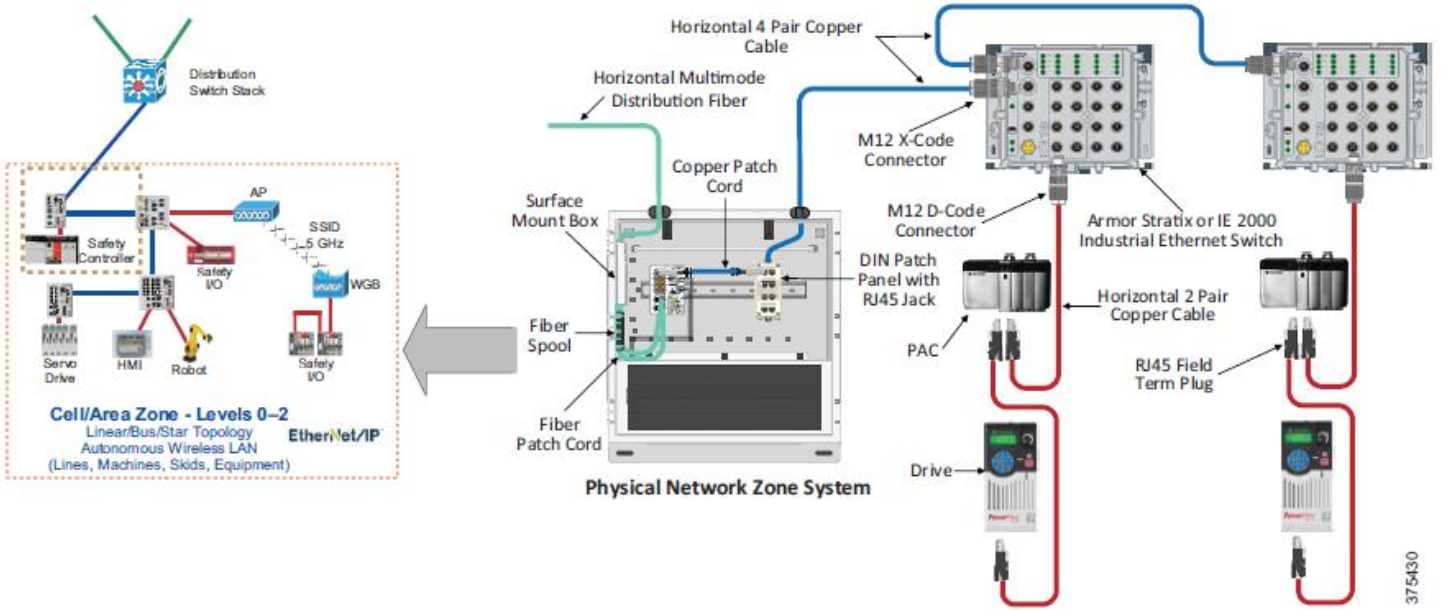
Arquitectura CPwE (Converged Plantwide Ethernet)



Implementación de una Arquitectura Ethernet convergente en toda la Planta

Guía de diseño e implementación

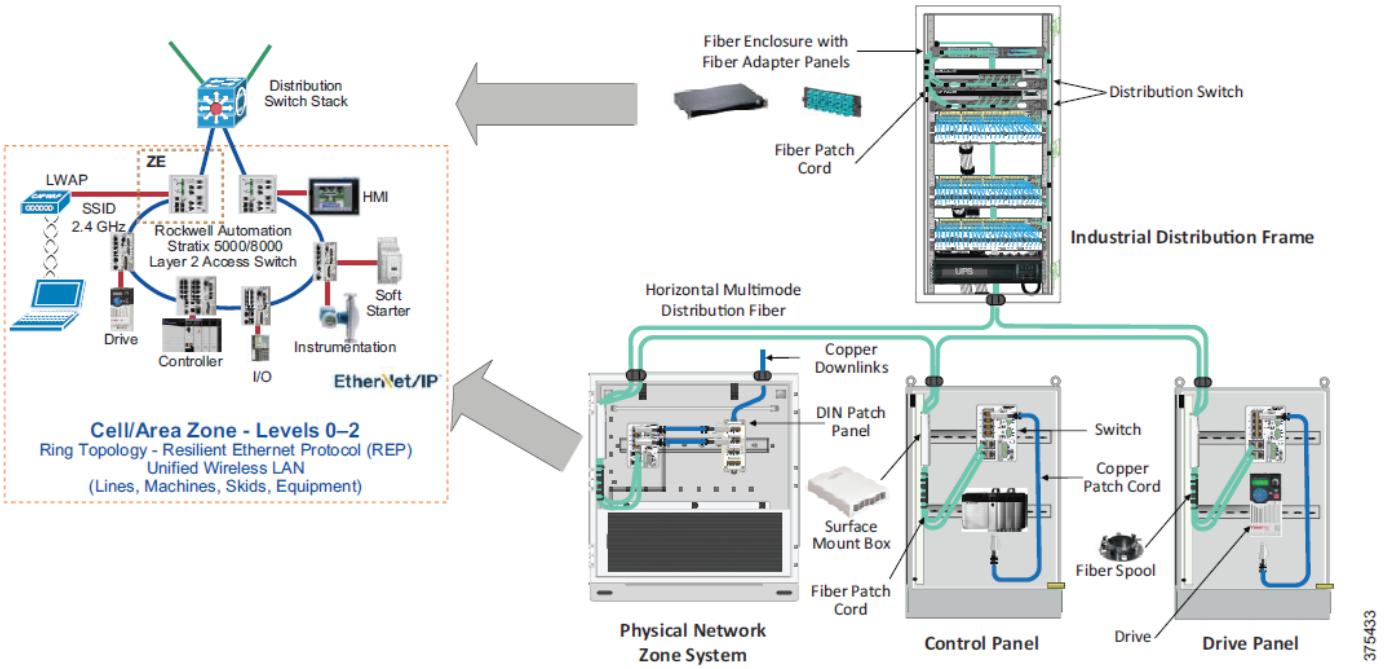
Figure D-6 Linear Connectivity Deployment Example



Implementación de una Arquitectura Ethernet convergente en toda la Planta

Guía de diseño e implementación

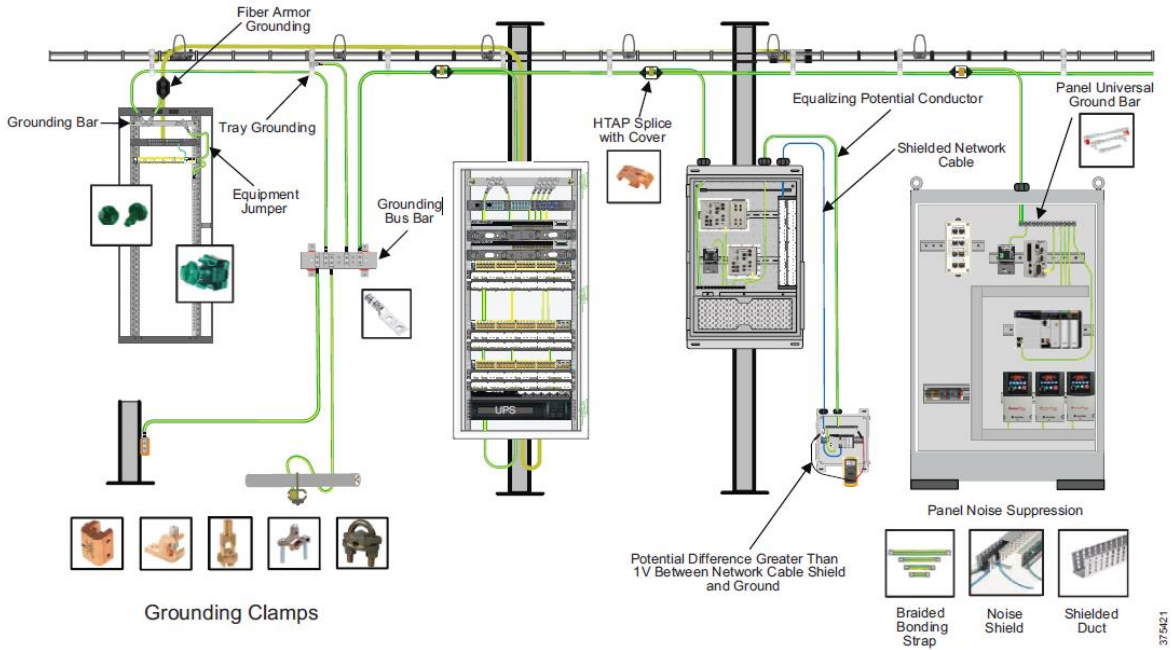
Figure D-9 Switch-level Ring Topology in the Cell/Area Zone



Implementación de una Arquitectura Ethernet convergente en toda la Planta

Guía de diseño e implementación

Figure C-10 Industrial Grounding Network

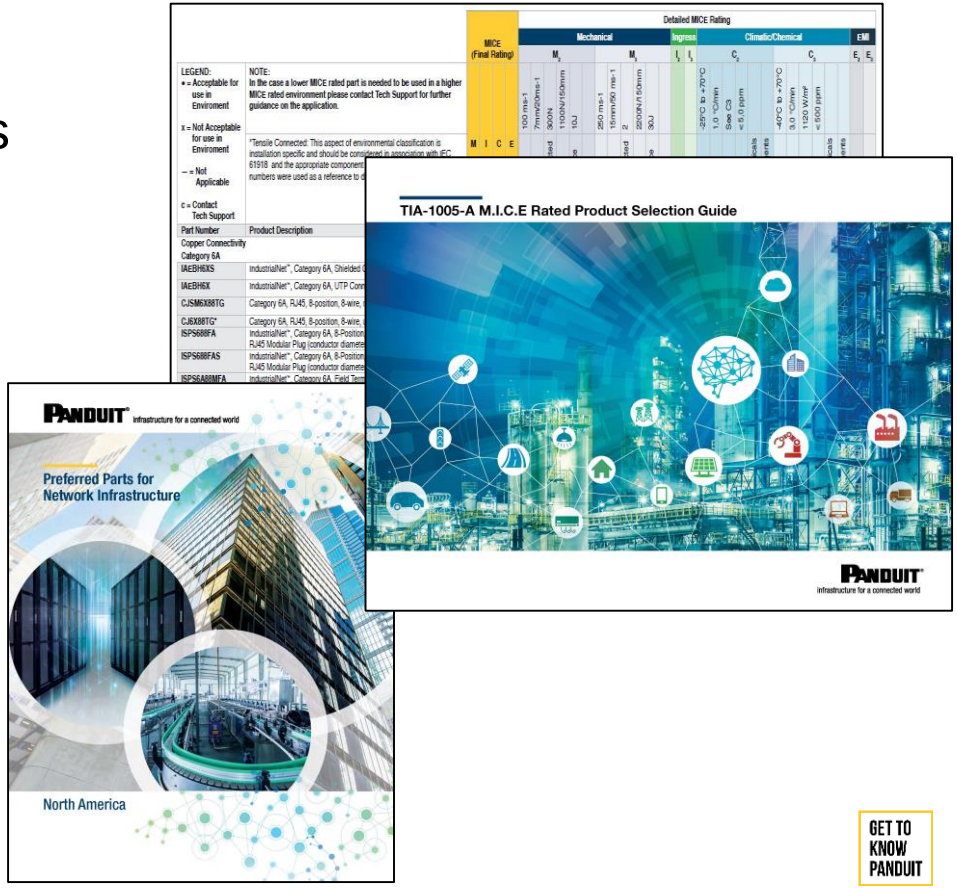


Applicable Grounding and Bonding Standards

- NEC Article 250 and 645.15
- IA 607-B and 1005
- BICSI
- Industrial Grounding Network

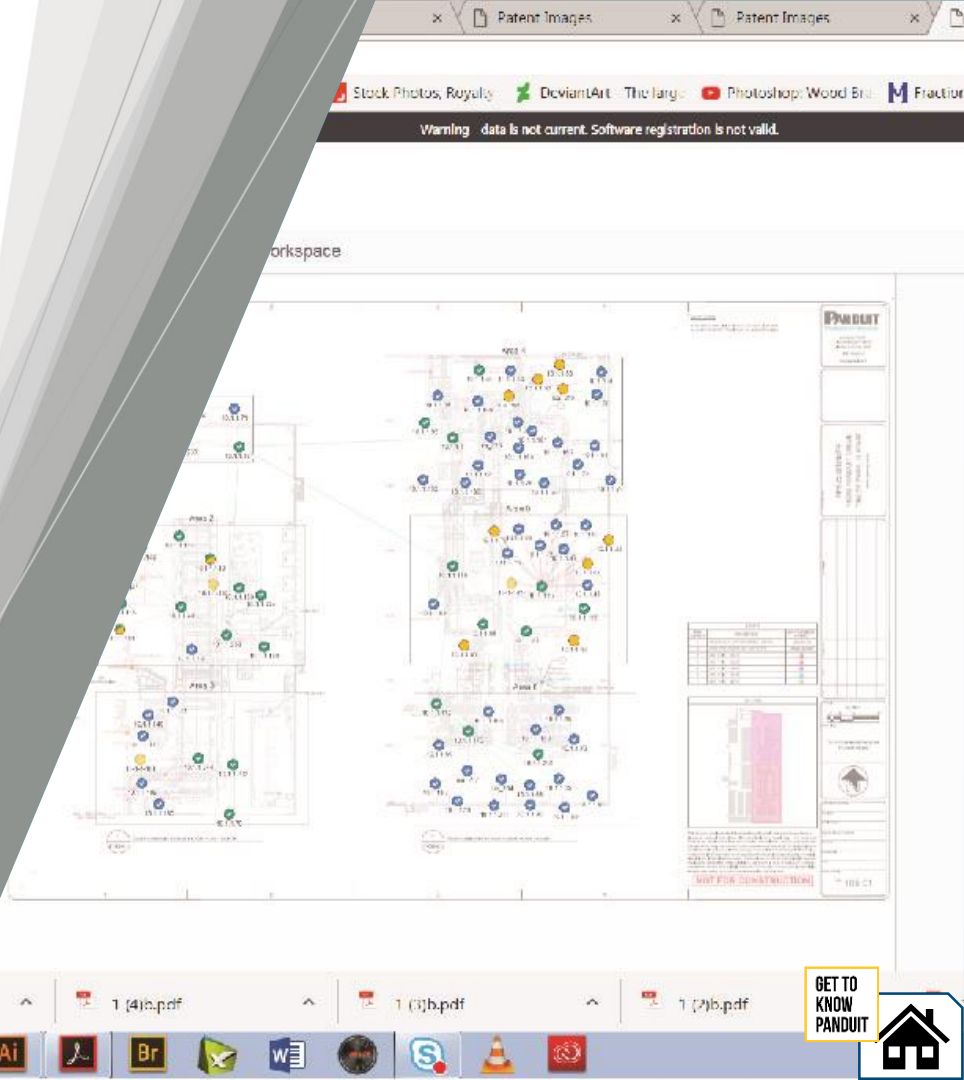
M.I.C.E Resources

- Guía de selección: representa los productos de red de Panduit que generalmente se consideran en entornos industriales
  - www.panduit.com/miceguide
- Catálogo de piezas preferidas: Representa las ofertas de nivel 1
- www.panduit.com/networkpartsamerica



IntraVUE™

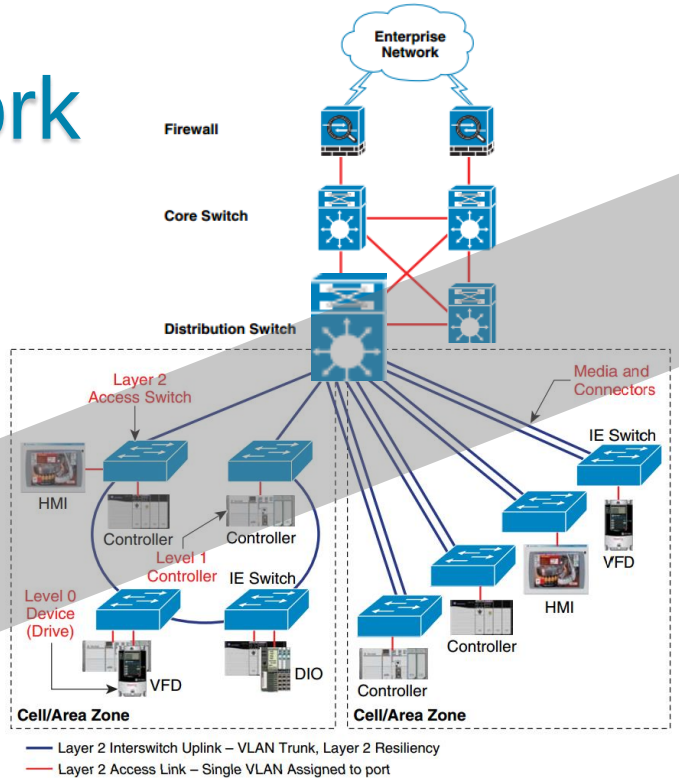
For a Reliable Plant Infrastructure



PANDUIT™

INTRAVUE Ayuda a TI y OT a trabajar juntos

IT Network Admin



Controls and Maintenance Operations

"Keep the Plant Producing"

GET TO KNOW PANDUIT

¿Por qué IntraVUE ™?
Diferentes formas de ver el monitoreo

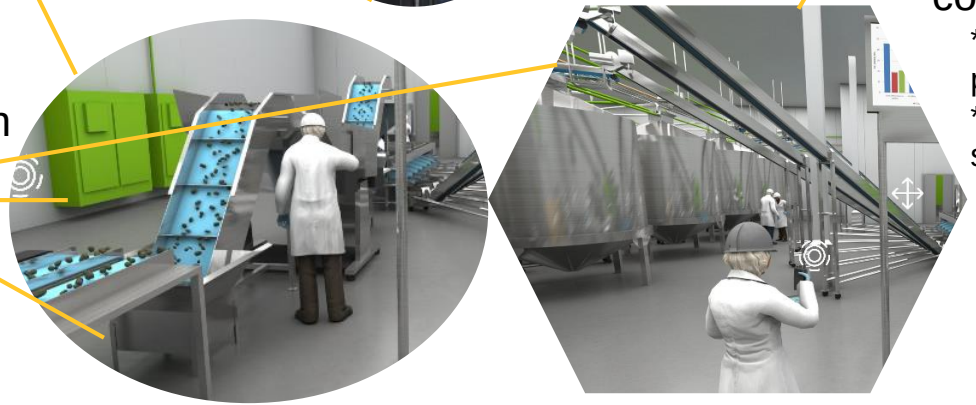
Network / Switch Monitoring
Focuses on switch/server performance

Deep Packet Inspection
Pulls all packet information from switches, analyzes content of traffic

*switches must support port mirroring or equivalent
*may not see traffic that stays local to system

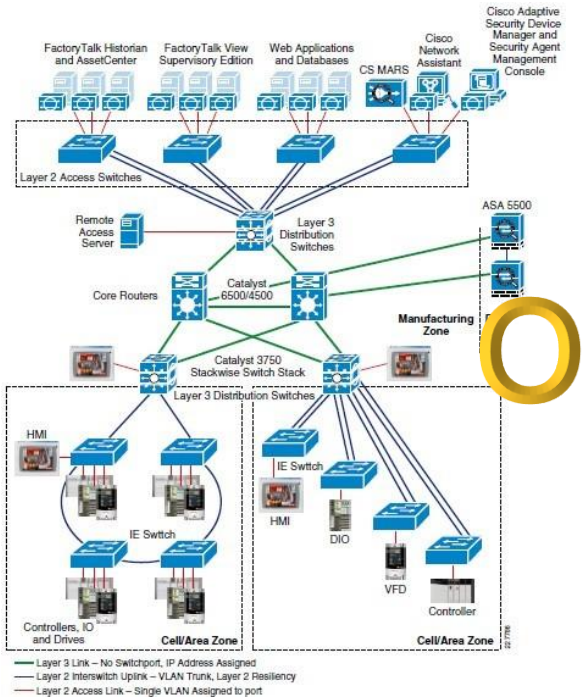
Device Monitoring
Focuses on documentation and monitoring of automation device connections.

Target of IntraVUE®

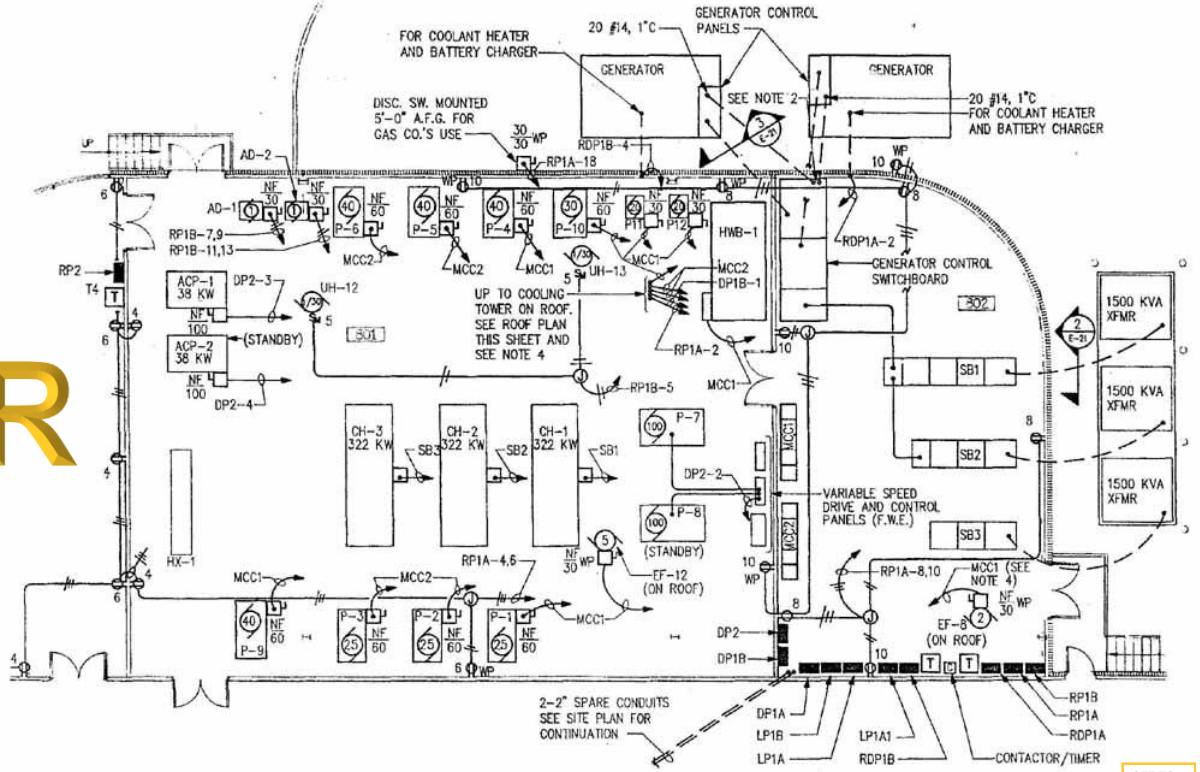


GET TO KNOW PANDUIT

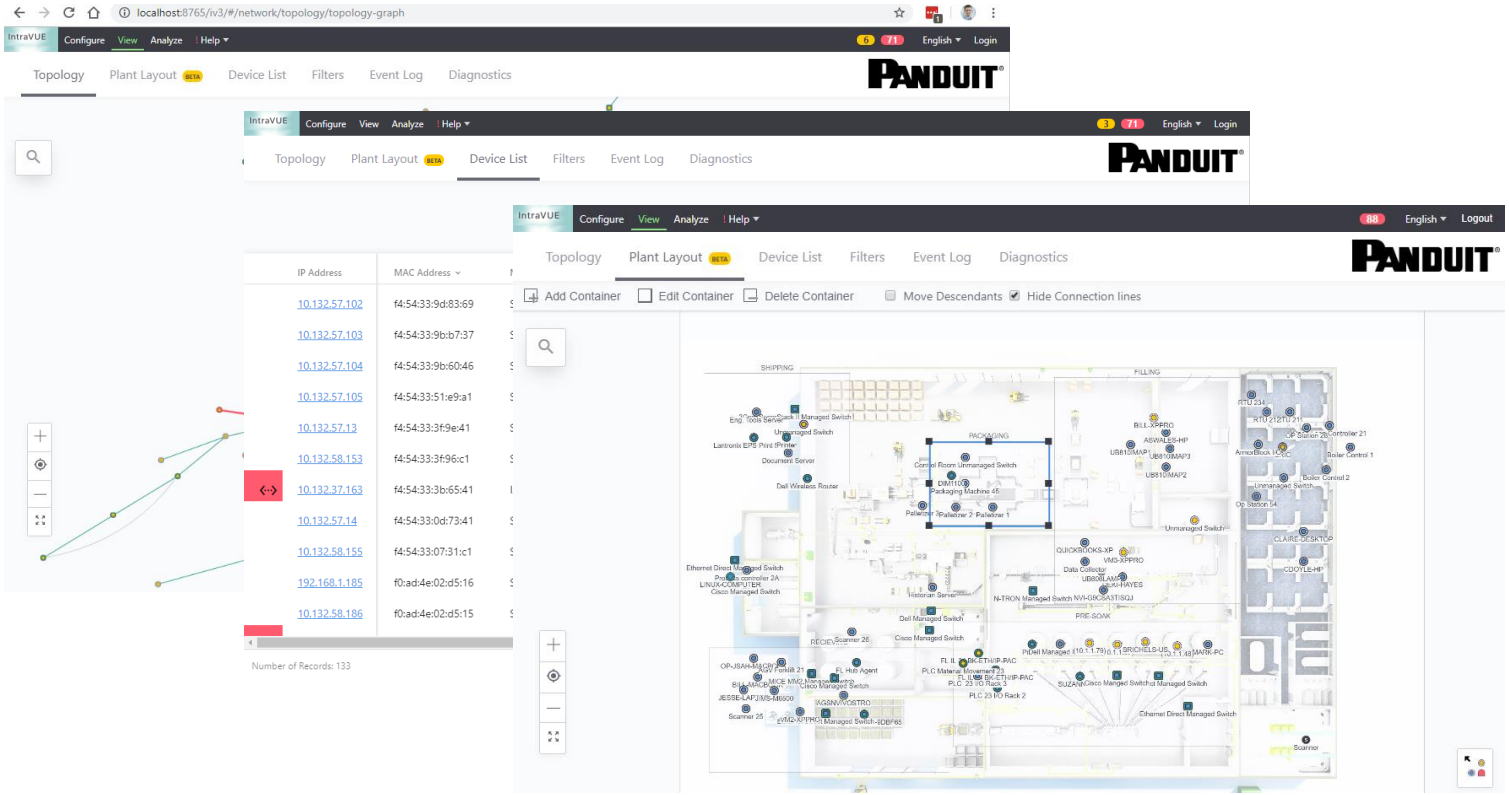
¿Las plantas necesitan una mejor documentación?



OR



Capacidades de documentación



¿Qué podría hacer con evidencia de fallas en la red?

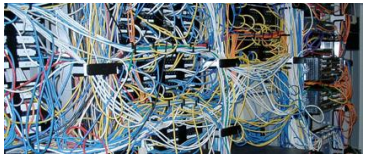
Controls Engineer:

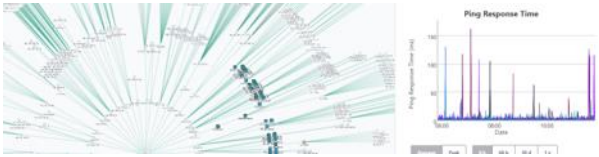
“Tengo constantes dolores de cabeza con la confiabilidad relacionada con la red; ¿Cómo puedo mostrarle a la gerencia que necesitan invertir en mejoras?

GET TO KNOW PANDUIT

Potentes diagnósticos neutrales para proveedores

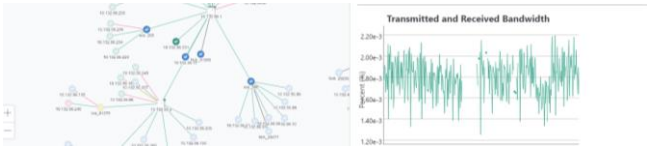
Damaged Connections



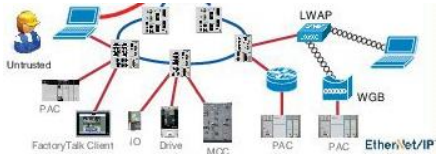


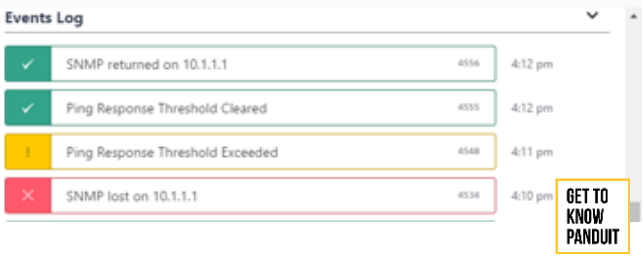
Failed Devices

Application Problems



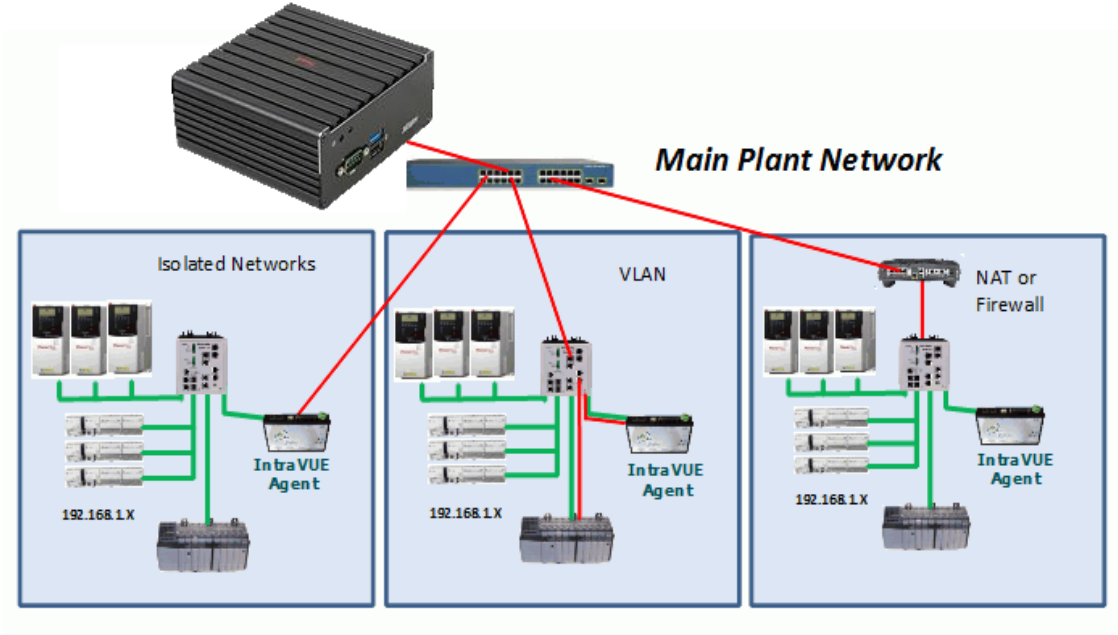
Architecture Problems





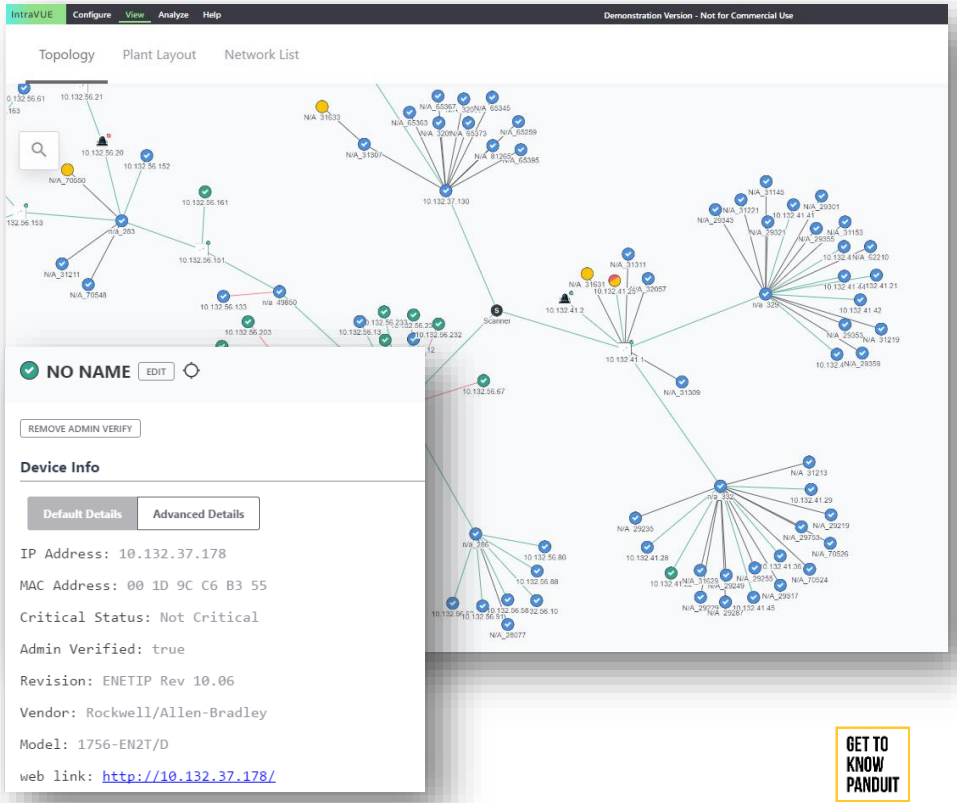
Agente IntraVUE

- Configuración común del Agente IntraVUE para entornos industriales con distintas redes.



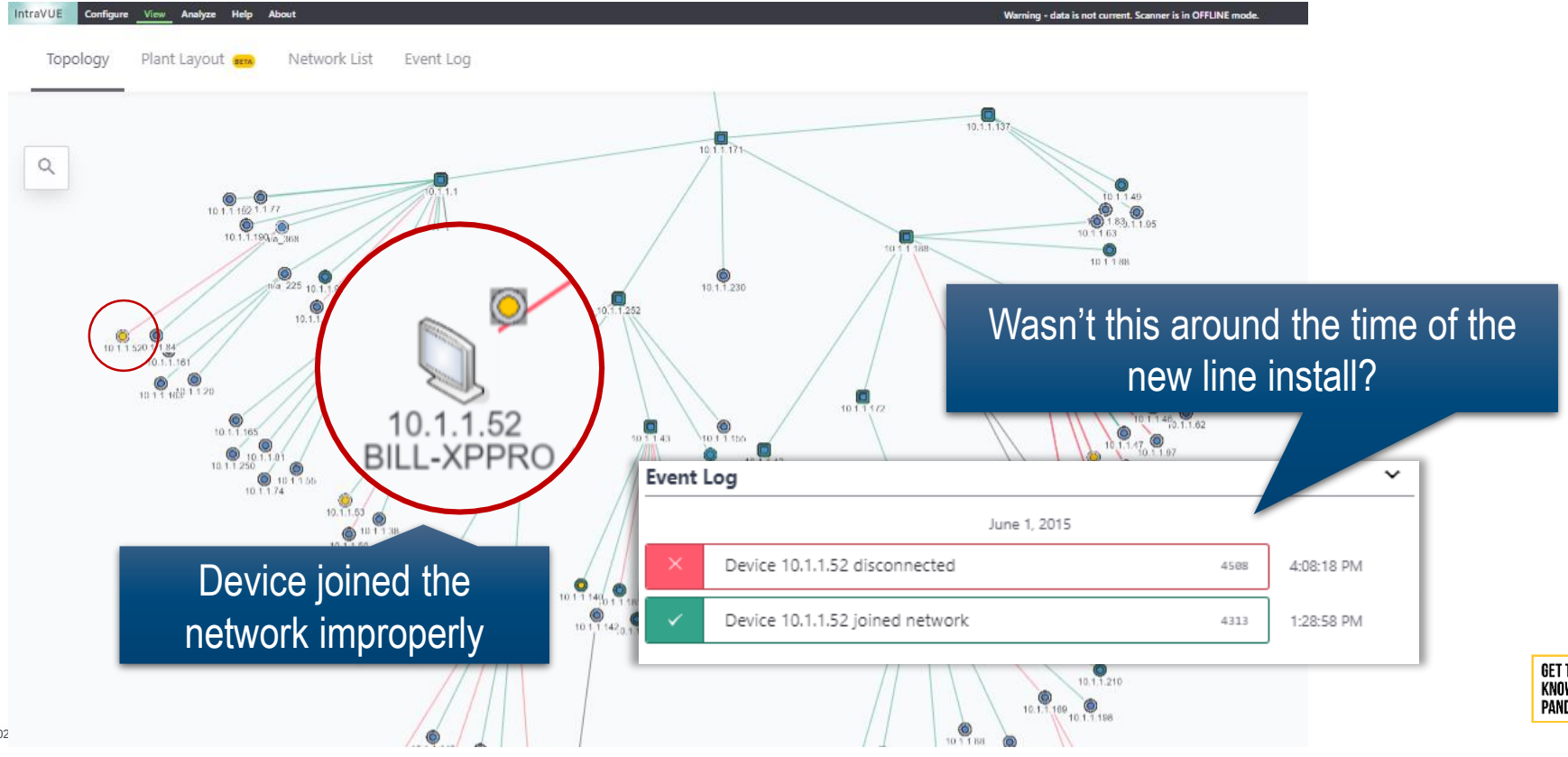
Mejorar la visibilidad de su entorno Industrial

- Fácil de configurar y con un potente software de visualización gráfica.
- Mapas automáticaos de su red.
- Visualice una imagn en vivo de las comunicaciones entre todos los dispositivos de su red Industrial!

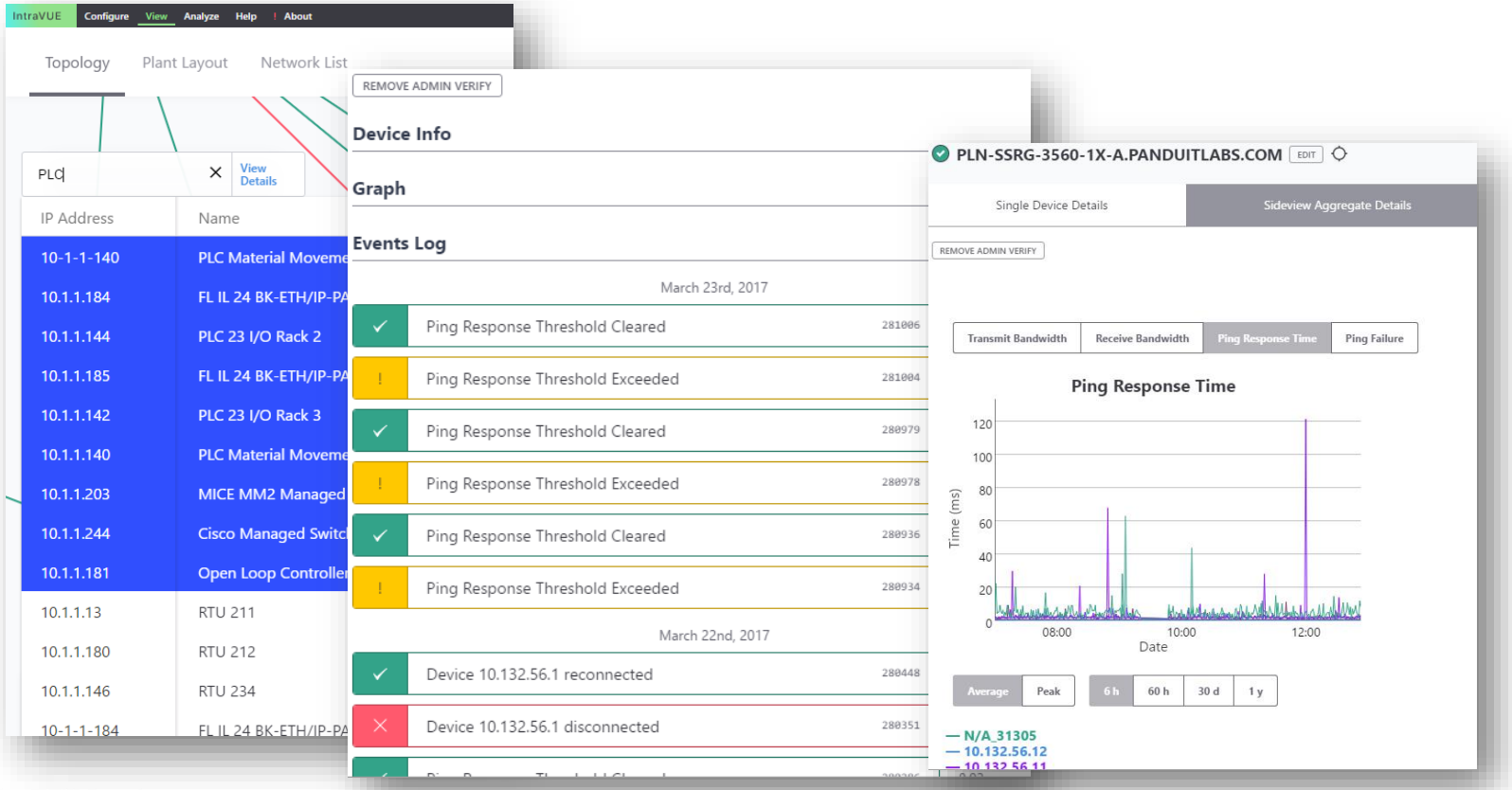


GET TO KNOW PANDUIT

Detección en tiempo real de nuevos dispositivos (TIA-5017)



Monitoreo en tiempo Real de Redes Industriales



IntraVUE™ Edge

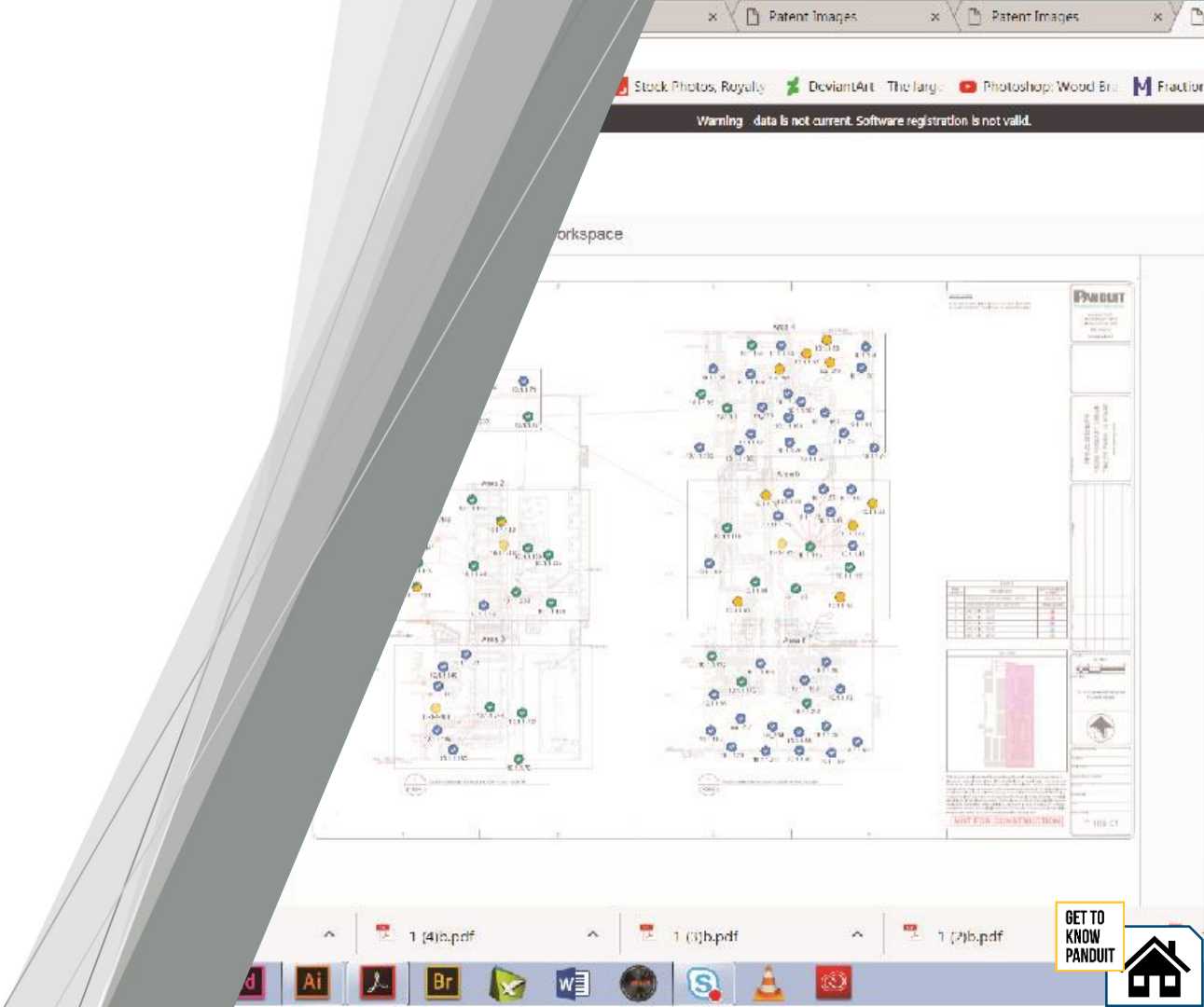
- Uso perpetuo, sin contratos.
- Descubrimiento de dispositivos
- Mapa de conexión y Diseño de Planta
- Acceso remoto
- Monitoreo y Alertas

Part Number: PNPIV

GET TO KNOW PANDUIT

IntraVUE™

DEMO



PANDUIT™

GET TO KNOW PANDUIT

Infraestructura física para la seguridad del mañana

A través de los ojos del gerente del centro de datos, hay es el rango de monitoreo de dispositivos ambientales, limpieza del poder y eficiencia energética del poder uso, a la capacidad de energía general y análisis para evitar tiempos de inactividad no planificados e interrupciones.

Sumado a esto está el necesita monitorear y recibir información sobre cómo asegurar el centro de datos es 24/7.

GET TO KNOW PANDUIT

Soluciones de Monitoreo de Infraestructura Física

GET TO KNOW PANDUIT

Panduit's DCIM Solutions

SYNAPSENSE

Se enfoca en la optimización de enfriamiento en el Centro de Datos

smartzone™

Monitorea y analiza datos de sensores de Energía, Medio Ambiente, Activos y Conectividad

GET TO KNOW PANDUIT

SmartZone Overview

SmartZone™ Solutions, a suite of data center infrastructure management (DCIM) solutions, help you **manage risk and change within the physical infrastructure** by **providing real-time data** on the status of power, temperature, connectivity, physical security, and environmentals from the enterprise to individual devices in data center cabinets.

- Collects data and provides visualization
  - Power
  - Environmental
  - Asset
  - Connectivity
- Monitors thresholds
- Models assets and floor plan
- Sends alarms
- Reporting and dashboards

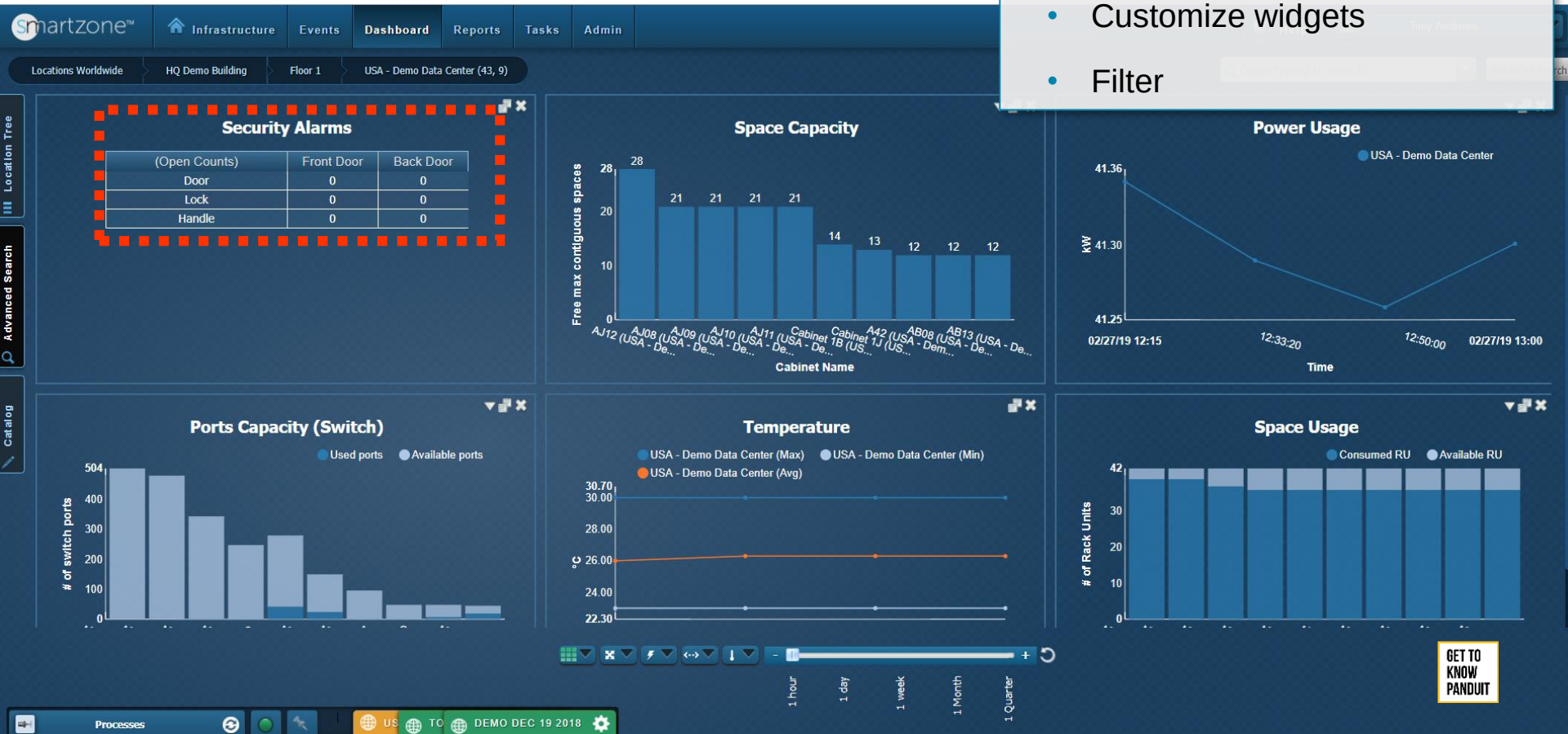
GET TO KNOW PANDUIT

Infrastructure

- Navigation Tree
- Map (workspace)
- Health Status/Capacity of each Infrastructure Pillar
  - System Configuration
- Power Management at Data Center/Cabinet/PDU level
- Access Control
- Environmental Monitoring
- Connectivity Management

Dashboards *easily view high level information*

- Use up to 6 dashboard widgets
- Customize widgets
- Filter

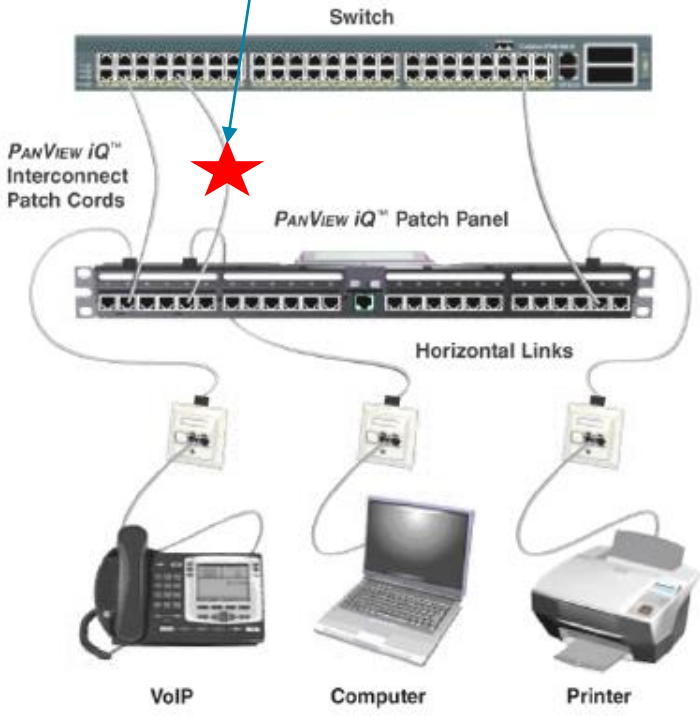


PViQ™ Standalone Solution

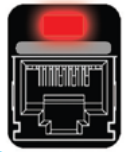
smartzone™ Connectivity PViQ Standalone Solution

Establecer una política de seguridad portuaria para interconexión y conexión cruzada

Desconexión del cable o alerta de seguridad de conexión:

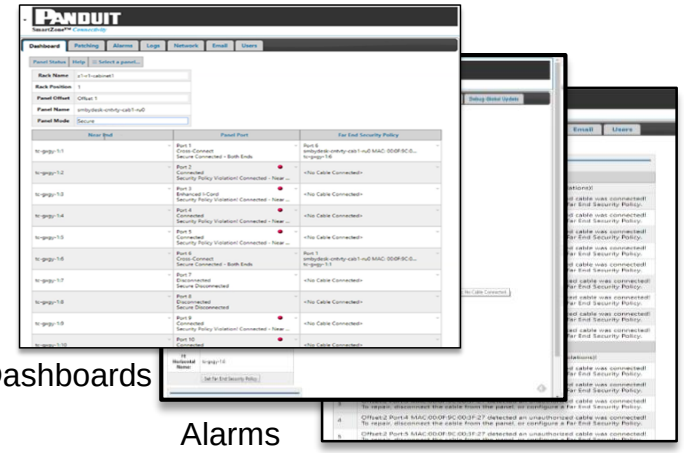


- Alerta visual local
- Instrucciones de recuperación
- Auditoría completada
- Alerta de evento enviada

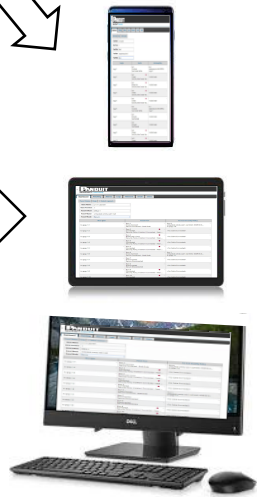


Real-Time Traps & Email (Disconnect, Connect, etc.)

WebGUI para acceso remoto, configuración y actualización



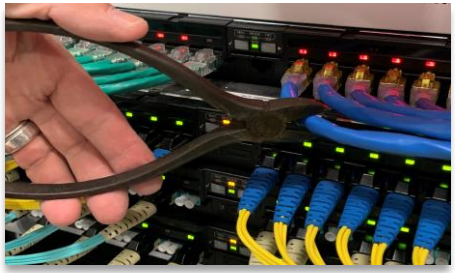
BYOD & Browser



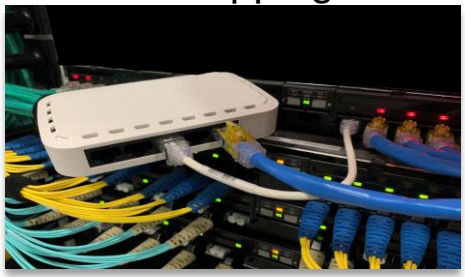
Casos de uso de soluciones: infracciones de seguridad

Sitios de inquilinos de EdgeDC y ColoDC con equipo remoto aislado

Malicious Disconnect



Line Tapping



Port Tapping

Accidental Disconnect

Consolidated Alarm Server

SmartZone DCIM CONNECT

Alarm Trap

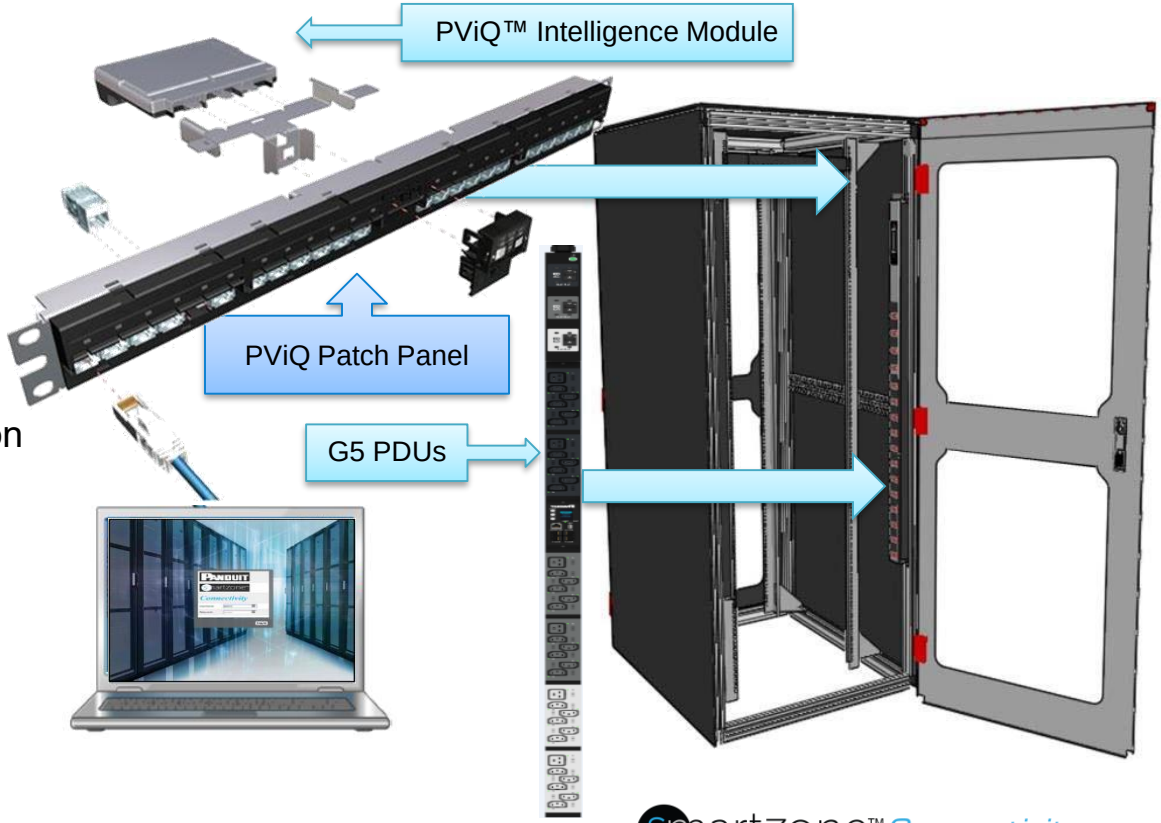
Alarm Email

Alarm Email

smartzone™ Connectivity

El firmware **SZ Connectivity** y un conjunto compatible de dispositivos de hardware inteligente PViQ ™ proporcionan una gestión de conectividad activa y pasiva.

Juntos, reducen los errores de implementación con correcciones de violación controladas y guiadas, e información de recursos de red para ayudar al proceso de planificación de capacidad.



Hardware

PViQ™ Patch Panels

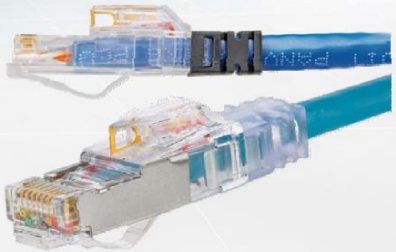
- **Industry-First Innovation**
- Interfaces seamlessly with WebGUI or DCIM to:
  - Provide intelligent, real-time monitoring of patch field connectivity
  - Modular approach provides installation options; Fully Managed or Managed Ready
  - Does not impact data traffic

PViQ Fiber Tray

- Provides Fiber Channel support by utilizing Mini-Com LC Fiber Optic Adapters
  - Multimode and single mode connections supported
- Internal Fiber Management protects splices and pigtails from damage while maintaining bend radius control
- Rack or Cabinet Mounted Mounts to either a rack or cabinet for flexible installations

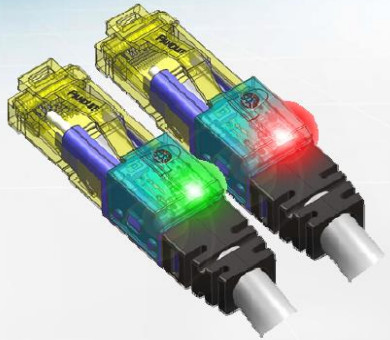
PViQ Intelligent Patch Cords

- Shielded and Unshielded Patch Cords
- Different options available to accommodate several preferred installation options such as cross-connect or interconnect
- Performance Tested Assures reliability of performance for maximum uptime
- 9th Wire technology provides accurate connectivity monitoring & tracing without affecting network traffic



PViQ Intelligent Patch Cords

- Enhanced Interconnect Patch Cords incorporate Integrated LEDs
- Guided Switch Port Disconnects
  - Reduce risk and enable secure disconnects
- Visual Traceability Enables port tracing between PViQ Panels and network switches connections



Violaciones de seguridad - Notificación de hardware

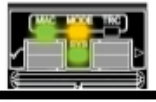
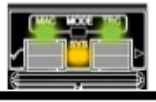
–**Conexión no autorizada:**
• Se realizó una conexión de puerto inadecuada debido a una conexión al puerto o conexión incorrecta sin aprovisionarlo primero.

–**Desconexión no autorizada:**
• El puerto espera estar en una conexión de doble extremo, pero está desconectado.

Port LED Status & Alerts

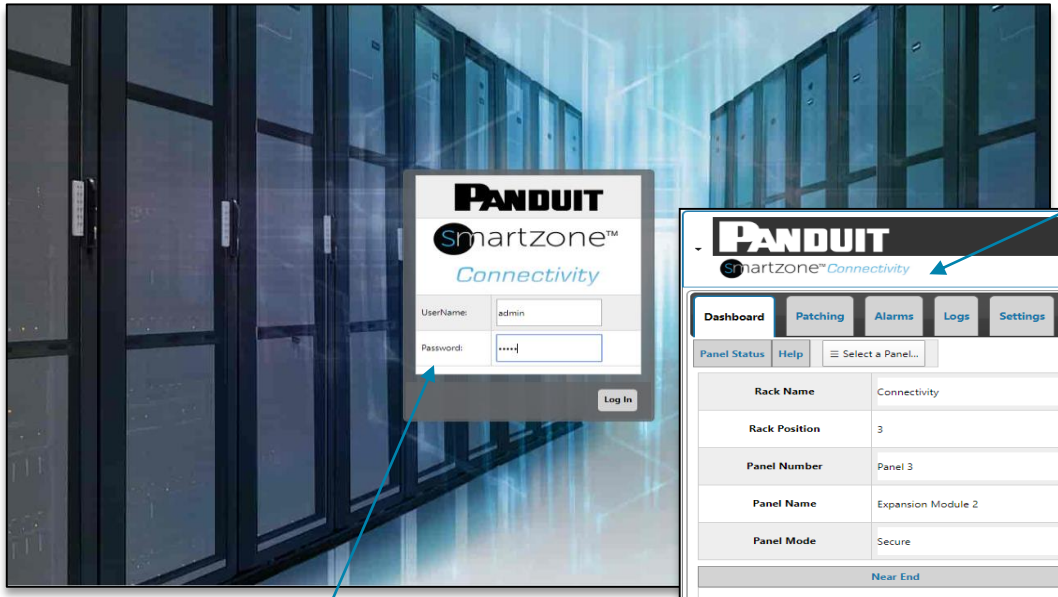
LED	Status	Meaning	LED	Status	Meaning
	off	Normal Operating State		Flashing Red	Move, Add, or Change (MAC) is pending on this port. Waiting for remove.
	Solid Red (*One Port*)	Secure Mode Violation		Flashing Green	Move, Add, or Change (MAC) is pending on this port. Waiting for insert.
	Solid Amber	Panel is in Learn Mode, with a single ended connection on this port		Flashing Green/Red	Trace is active on this port. If a patch cord is connected, the far end port will also flash.
	Solid Green	Connection successfully "learned."		Solid Red (*ALL Ports*)	Panel is in Maintenance Mode

Panel LED Status & Alerts

IU Display	MODE	Meaning	IU Display	MODE	Meaning
	SECURE	Normal operating state		MAC	Notifies users when change orders are pending
	LEARN	Commit the current patch field to the database (9-wire cross connect)		MAC	MAC in progress – single sided connection
	TRACE	Directs users to the near and far end of patch field for end-to-end connectivity		Firmware Update	A firmware update of the PM is in progress

MODE	Meaning	Full Panel Display
MAINTENANCE	Perform system resets	
LOCATION	Identify where a specific panel resides	
FIRMWARE UPDATE	An update of the panel firmware is in progress	

Multi-Device & User-Friendly WebGUI



One-Click Navigation

Graphical Secure Web Login

Alarm Viewing

PANDUIT
Smartzone™ Connectivity
Log Out

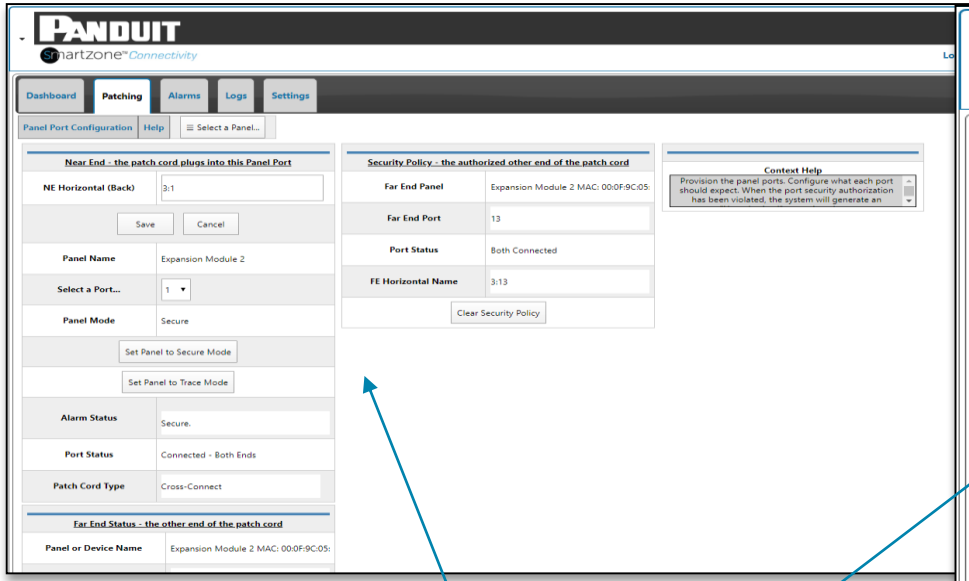
Dashboard | Patching | Alarms | Logs | Settings

Panel Status | Help | ☰ Select a Panel...

Rack Name	Connectivity
Rack Position	3
Panel Number	Panel 3
Panel Name	Expansion Module 2
Panel Mode	Secure

Near End	Panel Port	Security Policy
3:1	Port 1 Cross-Connect Security Policy Violation! Connected - Both Ends	<No Cable Connected>
3:2	Port 2 Cross-Connect Security Policy Violation! Connected - Both Ends	<No Cable Connected>
3:3	Port 3 Cross-Connect Security Policy Violation! Connected - Both Ends	<No Cable Connected>
3:4	Port 4 Cross-Connect Security Policy Violation! Connected - Both Ends	<No Cable Connected>
3:5	Port 5 Cross-Connect Security Policy Violation! Connected - Both Ends	<No Cable Connected>
3:6	Port 6 Cross-Connect Security Policy Violation! Connected - Both Ends	<No Cable Connected>
3:7	Port 7 Disconnected Secure, Disconnected	<No Cable Connected>

Multi-Device & User-Friendly WebGUI

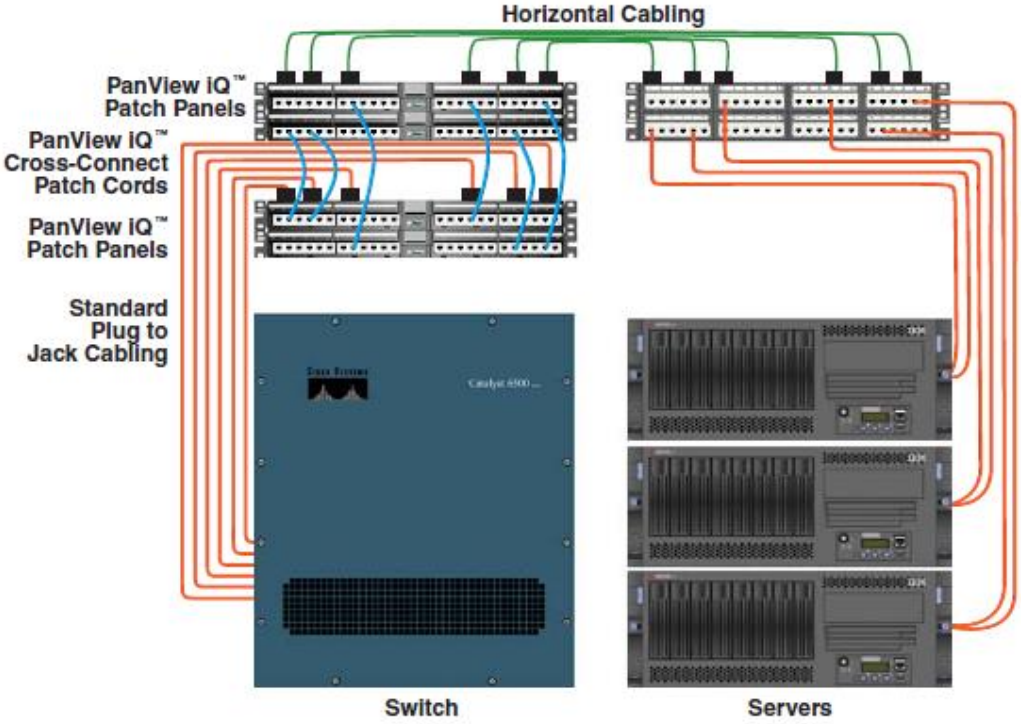


Patching/Connectivity Details

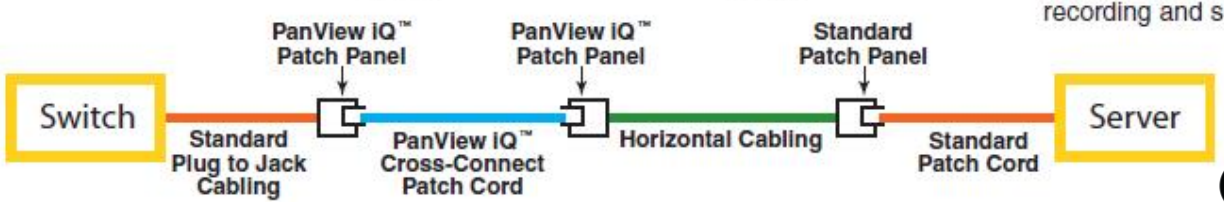
Security Violation Location Alarm

Unauthorized Cable Connection Alarm

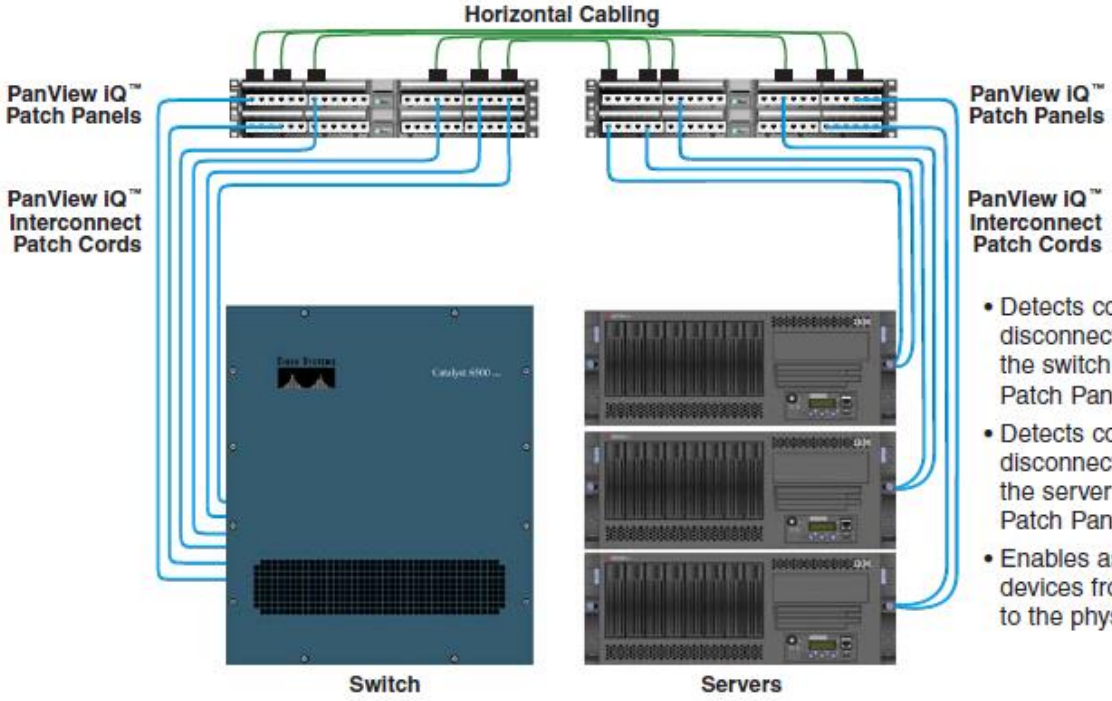
Trazabilidad de conexión - Cross-Connect



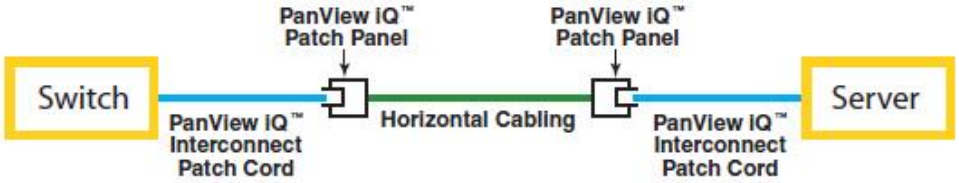
- Helps prevent damage to switch and server ports by creating protected patch field between PanView iQ™ Patch Panels. Each switch and server port is represented at the patch panel level
- PanView iQ™ Cross-Connect Patch Cords guarantee switch to server traceability to support critical moves, adds, and changes
- PanView iQ™ Patch Panels detect and send notifications of connect and disconnect status for event recording and security purposes



Trazabilidad de conexión - Interconexión



- Detects connections and disconnections made between the switch and PanView iQ™ Patch Panels
- Detects connections and disconnections made between the server and PanView iQ™ Patch Panels
- Enables asset tracking of devices from the logical layer to the physical layer



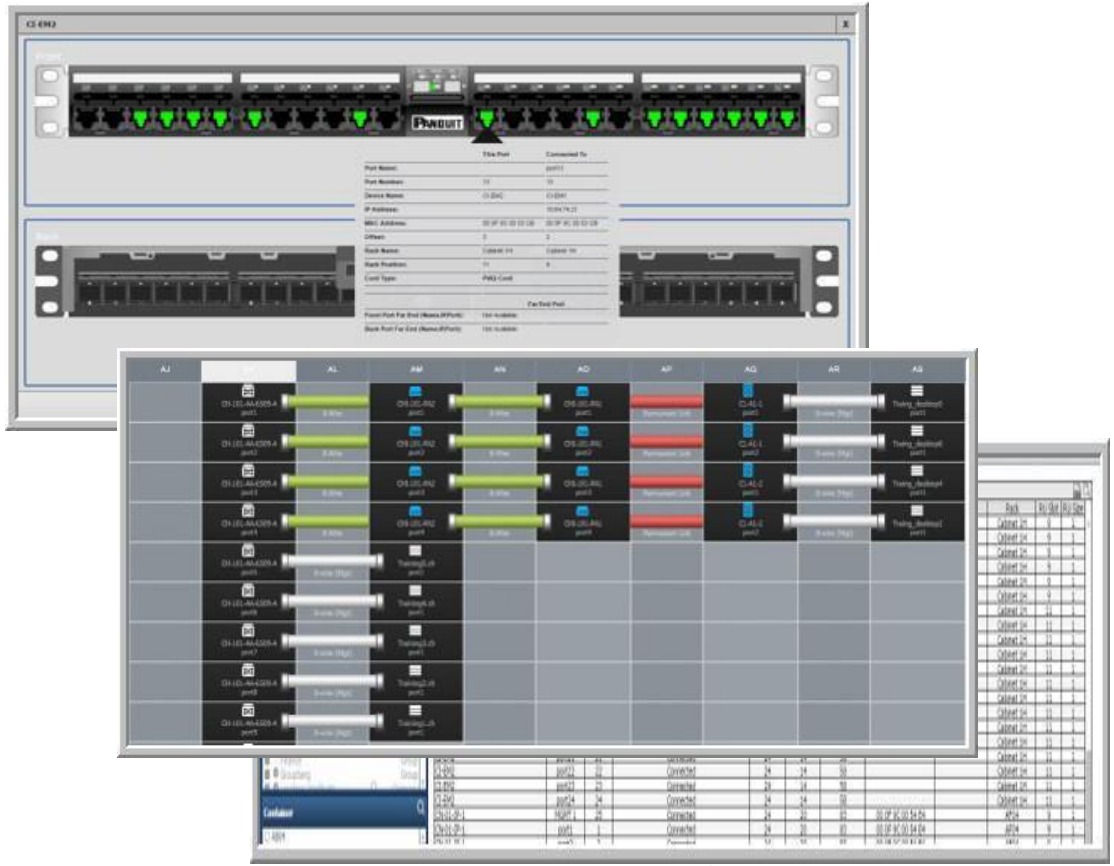
Solución de software de conectividad DCIM SmartZone(Opcional)

Características clave

- Gestión de conectividad de red de extremo a extremo **CENTRALIZADA.**
- Capacidad de cableado
- Notificación automática del estado del enlace
- Dispositivos de reconciliación automática

Valor:

- Acorta el tiempo de resolución de problemas de conectividad
- Proporciona capacidad de cableado para una implementación de activos más rápida
- Notificaciones de dispositivos en línea / fuera de línea
- Notificación de dispositivos que necesitan ser reconciliados

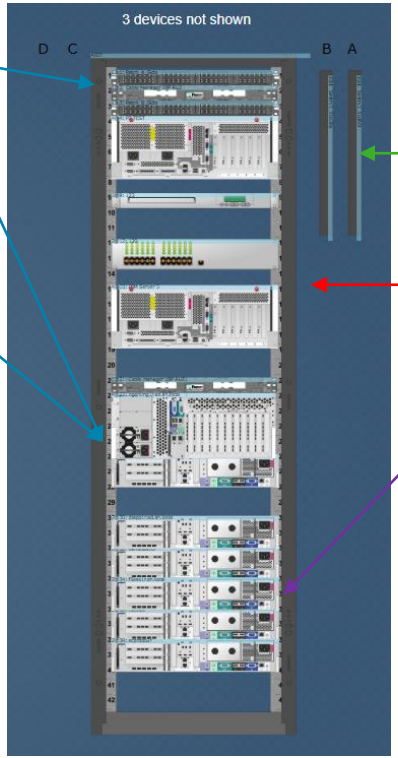


Monitoreo permanente de la Infraestructura (MicroData Center)

La infraestructura toma relevancia de manera **crítica**, ya que todos los elementos que integran las aplicaciones críticas se concentran en un solo Gabinete de Alta Densidad de Cómputo, Almacenamiento, Red y Conectividad por lo que el monitoreo permanente es necesario adoptando las recomendaciones de las normativas y estándares internacionales.

TIA-942 Estándard Data Center

ASHRAE



Conectividad

HCI

Monitoreo

Energía (PDU´s)

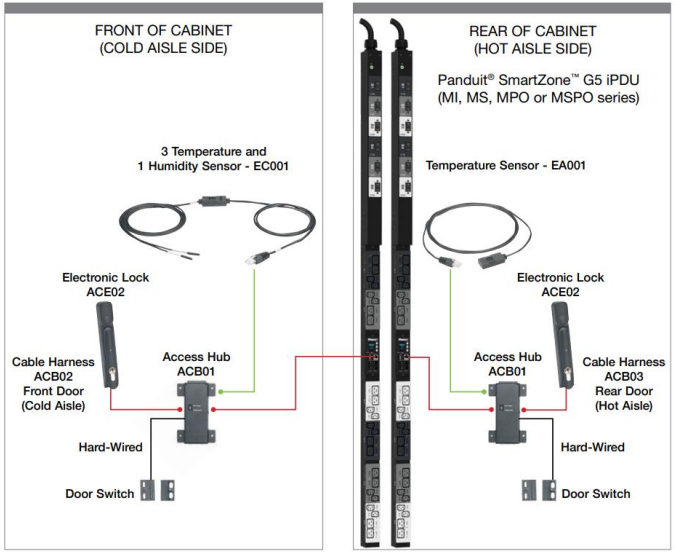
Temperatura (Sensores)

Equipo

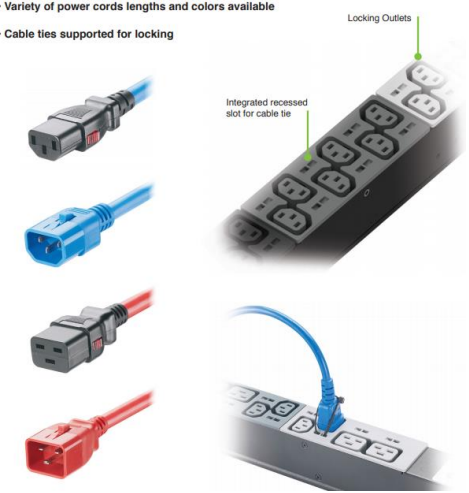
PUE (Power Usage Effectiveness)

HCI = Cómputo + Redes + Storage + Conectividad

Panduit G5 PDU´s (Monitoreo Ambiental + Energético + Control de Accesos)



- Locking outlets compatible to V and W power cords
- W power cords provide locking at both end (PDU and equipment)
- Variety of power cords lengths and colors available
- Cable ties supported for locking



Quality & Reliability
- 3-Year standard and 5-Year extended warranty

High Temp
- Built with high-temperature grade premium components to withstand 60°C high temperature at full load for an extended period to provide high quality and reliability

High Power Density
- Unique outlets design for high power density, and compact form-factors minimizing cabinet space

Hot-Swappable and Upgradable
- Hot-Swappable Controller with large OLED display and high contrast ratio

Hardened Security
- Enhanced security with (SNMPv3 and RESTful/TLS) with certificate-based advanced asymmetric encryption, validated and hardened with multiple security scanning tools

1G Redundant Network Access
- High Networking speed (1G) and with Redundant Network Access (RNA) for connectivity redundancy or for allowing separate Colo/Tenant Network connectivity.

Real-Time Monitor
- Real-time Monitoring of Power Environmental and Physical Access Security

Environmental Plug & Play Sensors
- Variety of Plug-n-Play Environment and Access Security accessories through U-Ports

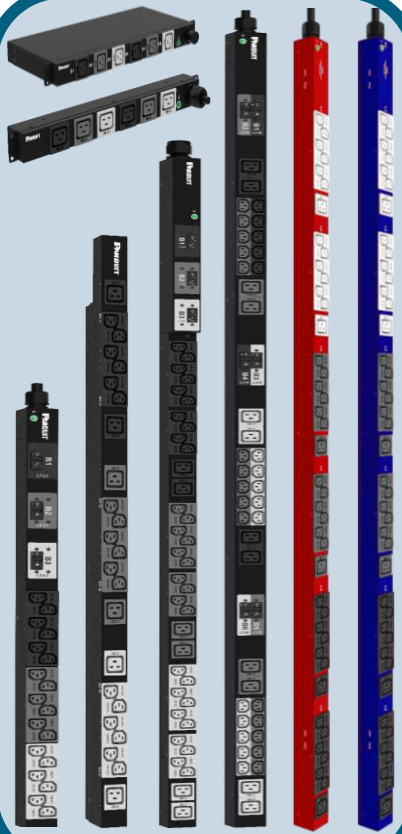
Multi-Device WebGUI
- Enhanced User-Experience with/BYOD WebGUI and colored PDU, cords and cable ties

Multi-Color
- A variety of colored PDU chassis, power cords and cable ties

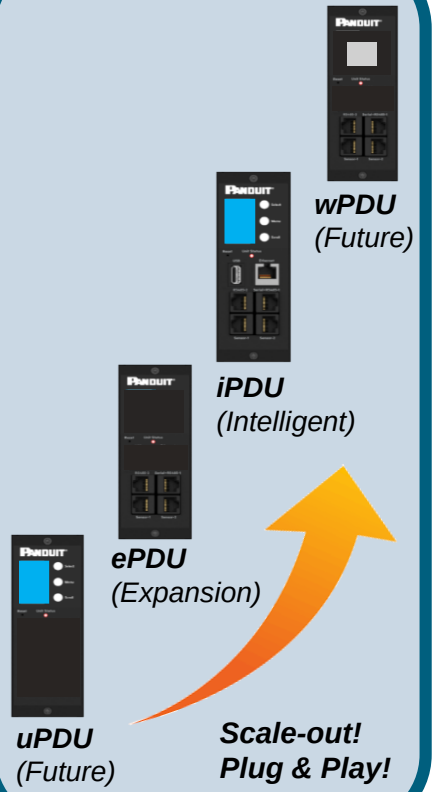
GET TO KNOW PANDUIT

Value Summary!

Extensive Configurations w/ Best-in-Class Form-factors



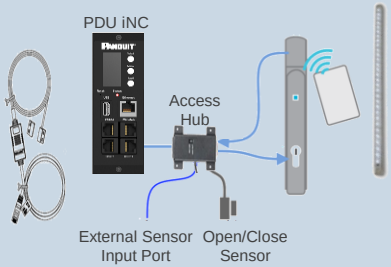
Multiple Hot-Swappable Intelligent Network Controller (iNC)



Plug-n-Play Accessories

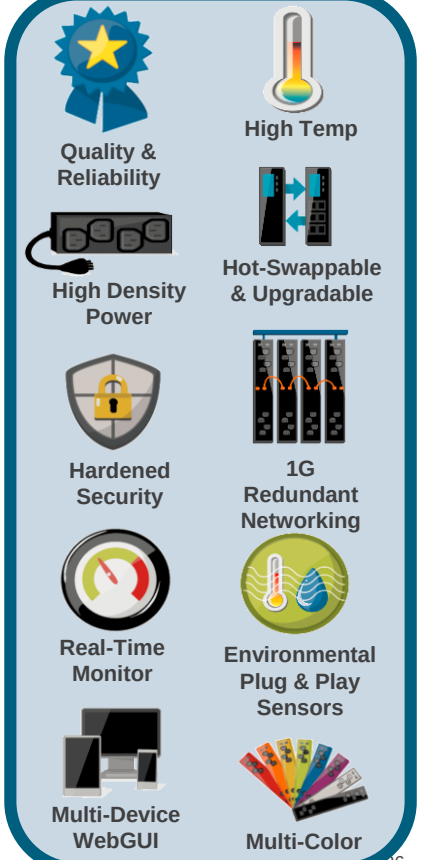
Environmental

Security



Power Cord & Cable Ties

Best-in-Class Performance & Features



Panduit Enclosures y Gabinetes + G5 PDU´s

ZDF48-EADD2

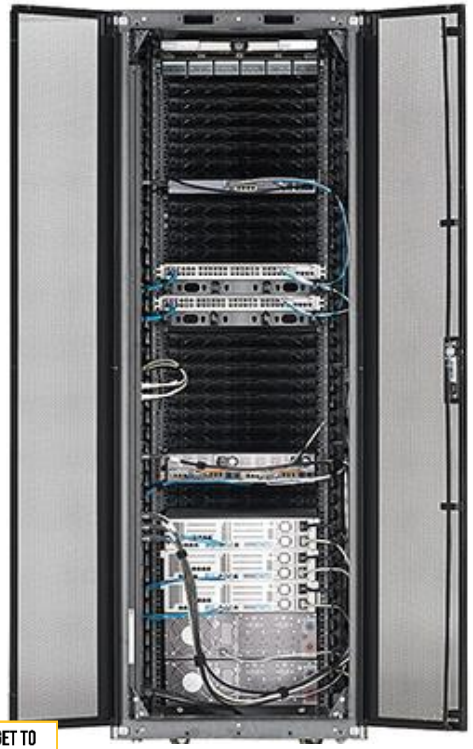
Pre-Configured Industrial Distribution Frame With Access Control

ZDF242430DB2

Pre-Configured Industrial Distribution Frame With Access Control

GET TO KNOW PANDUIT

ICE Alliance 2.0 – Micro Data Center



MDC82NN

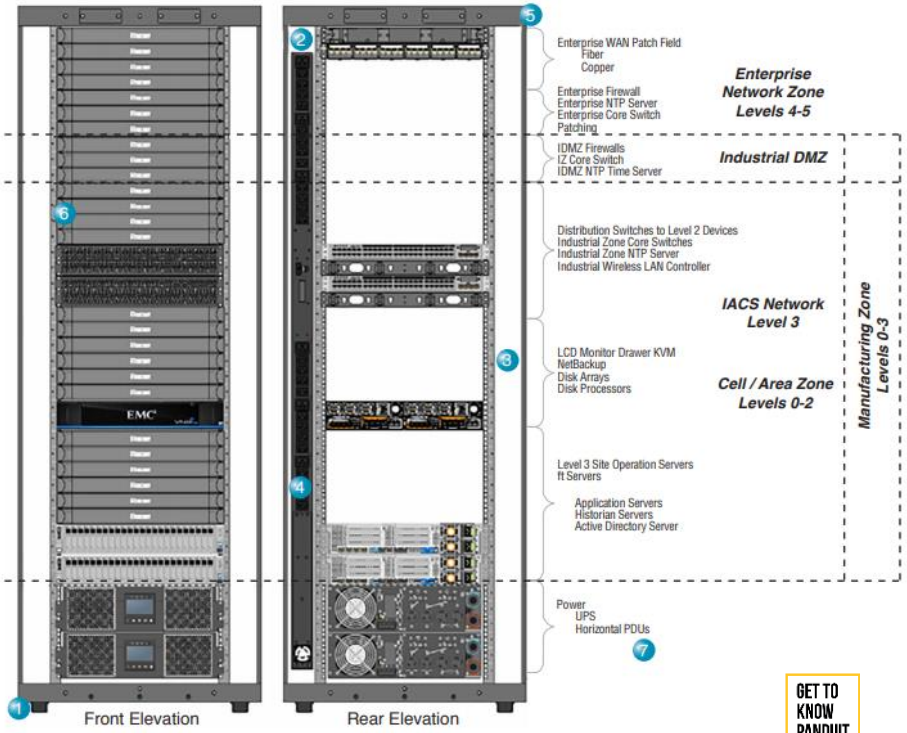
ICE Alliance 2.0

STULZ PANDUIT EATON CISCO

(Disponible solo para México)

82" Micro Data Center (Full Rack)

The 42 RU NEMA MDC is designed to protect active hardware and enable up to 200 devices within the manufacturing floor. It is designed to house switches, firewalls, storage, servers, and UPS equipment.



GET TO KNOW PANDUIT

GET TO KNOW PANDUIT

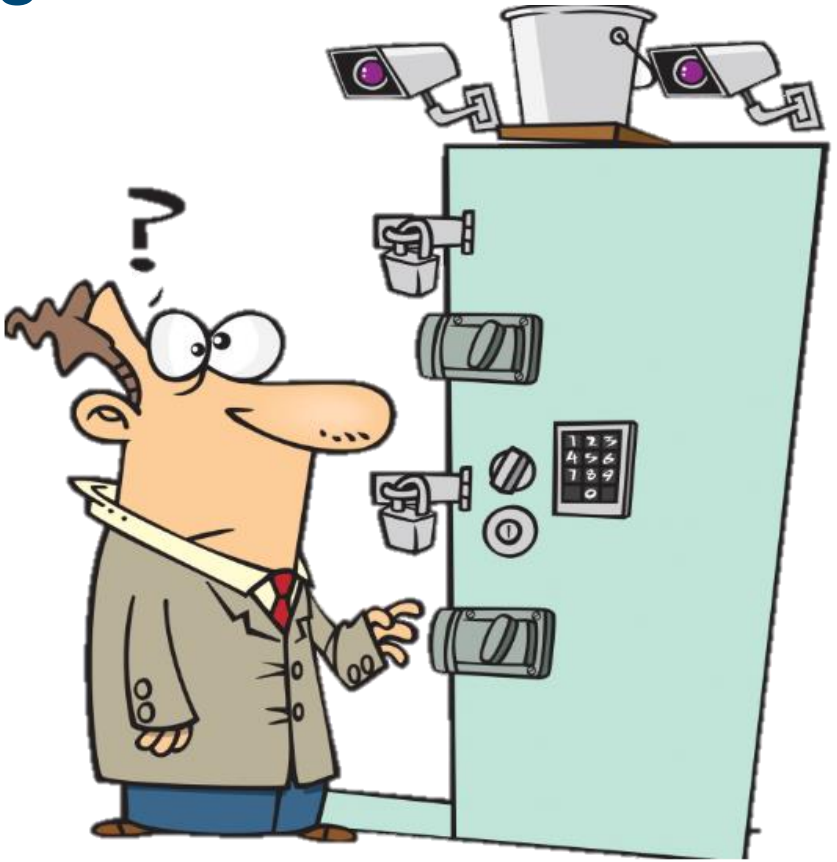
Conclusiones

GET TO KNOW PANDUIT

GET TO KNOW PANDUIT

No lo hagas fácil: Protege tu Red.

- Seguir las recomendaciones de las normativas y estándares internacionales (TIA-5017)
- Monitoreo permanente de la Infraestructura física y lógica.
- Crea múltiples obstáculos
  - No confíes solo en el software
- No dejes ninguna puerta abierta
  - Un puerto abierto es un acceso potencial a sus datos.
- "Cerrar y bloquear la entrada"
  - Bloquee los puertos que conducen a sus datos.



GET TO KNOW PANDUIT

Enterprise Security and Safety Solutions

Network infrastructure for security and safety systems.

PANDUIT®

GET TO KNOW PANDUIT

Próximo webinar – Viernes 17 de abril a las 10hrs (GMT-5)

Gracias

#Panduit #accelleratethepossible

GET TO KNOW PANDUIT