SANGFOR

PERFIL CORPORATIVO

Maury Pineda | Sales Director - Colombia, Peru & Chile
maurypineda@sangfor.com
Sangfor Technologies México

Expansión Global

SANGFOR

#1 Compañía con mayor capitalización de mercado en China

23 Años

9500+ Empleados

60+ Oficinas regionales

100K+ Clientes en el mundo

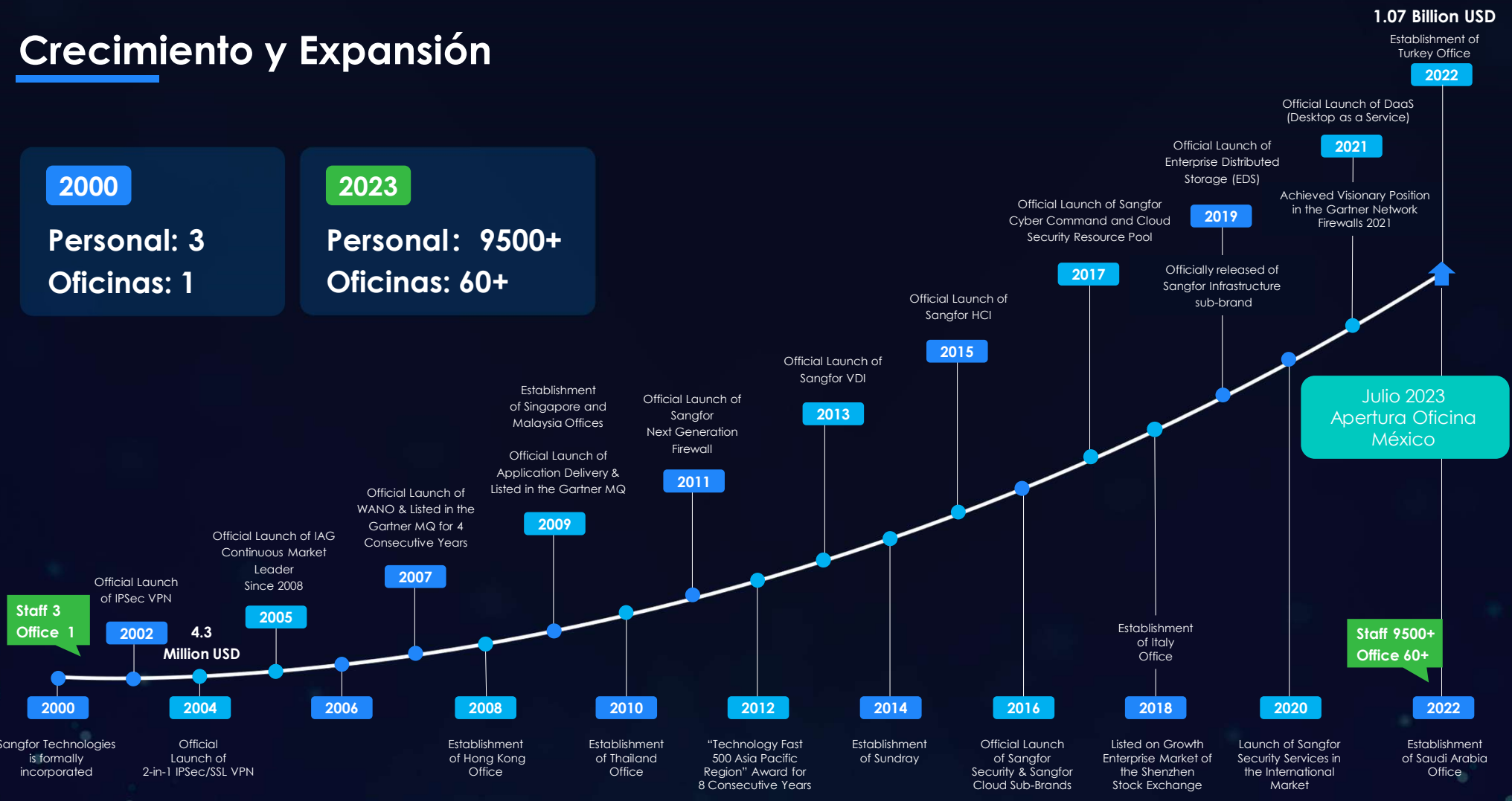
Crecimiento y Expansión

2000

Personal: 3
Oficinas: 1

2023

Personal: 9500+
Oficinas: 60+



División empresarial

SANGFOR

SANGFOR

Sangfor Security

Seguridad de clase mundial para empresas

Sangfor Cloud

Plataforma para aplicaciónes con seguridad y disponibilidad

Sangfor IT Infrastructure

Infraestructura de nube para la transformación digital

Sundray

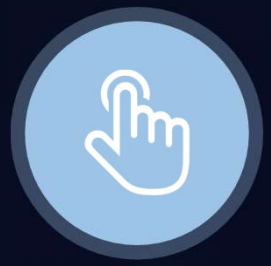
Redes corporativas GE, WiFi, & IoT

Objetivo del Desarrollo tecnológico

Simple

Estable & Velóz

Seguro



Accesible

Portafoilio de Productos, Soluciones, y Servicios

SANGFOR

Productos de Ciberseguridad

- Sangfor NGAF
- Endpoint Secure
- Sangfor IAG
- Cyber Command

Servicios de Seguridad Avanzados

- Incident Response
- TIARA
- Cyber Guardian (Next-Gen MDR)

Soluciones de Negocio

- Simplify SecOps
- Anti-Ransomware
- Continuous Threat Detection
- SD-WAN
- Secure Internet Access
- Proxy Avoidance

Soluciones de Nube con Seguirad

- Hyper-Converged Infrastructure (HCI/VDI)
- XDDR 2.0
- VM Backup/DR aSTOR
- Managed Cloud Services (MCS)
- Sangfor Access Secure (SASE)

IA x Humano

El Futuro de la Ciberseguridad con Sangfor

Protección Integral Extremo a Extremo

SANGFOR

Internet

Perímetro

NGAF/NSF

- NGFW con Inteligencia Artificial / TI
- Web Application Firewall
- SOC Lite Integrado
- Módulo de Engaño (Honeypot)
- Protección L2-L7
- App, IPS, AV, URL, BWM, LLB, SDWAN
- 4 Modos de operación simultánea: VW, L2, L3, TAP

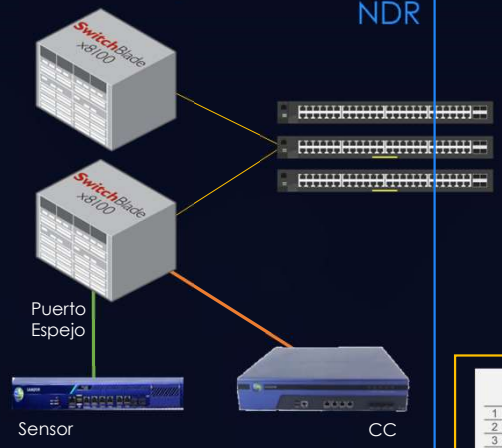
Internet

IAG

- Control Web vía Proxy
- Acceso seguro a internet
- Multi-Autenticación de usuarios
- Anti-Proxy Apps
- DLP para aplicaciones Web
- Reportes de uso web granulares

Red Interna

Cyber Command NDR



- Detección basada en IA y ML
- Múltiples fuentes de información, puerto espejo y eventos de terceros
- Respuesta automática o manual
- Integración con marcas de terceros

Firewall: paloalto, SOPHOS, FORTINET, Check Point, CISCO, WatchGuard, H3C, Hillstone, HUAWEI

Endpoint: Bitdefender, SOPHOS, TREND MICRO, Symantec, vmware Carbon Black

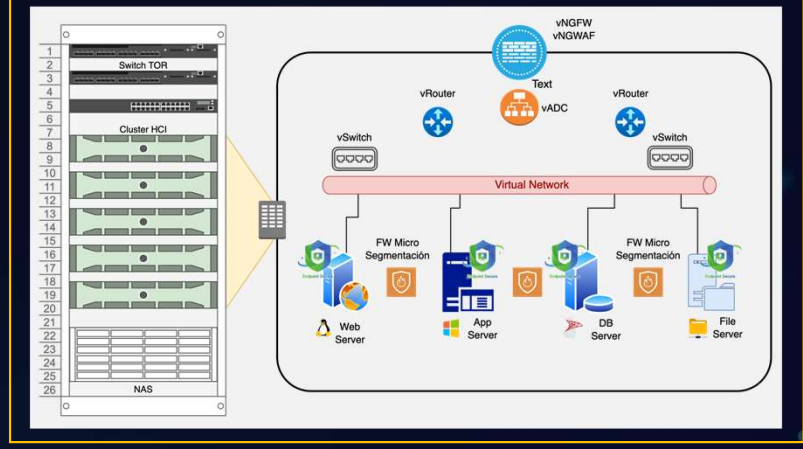
Endpoint Secure

EDR

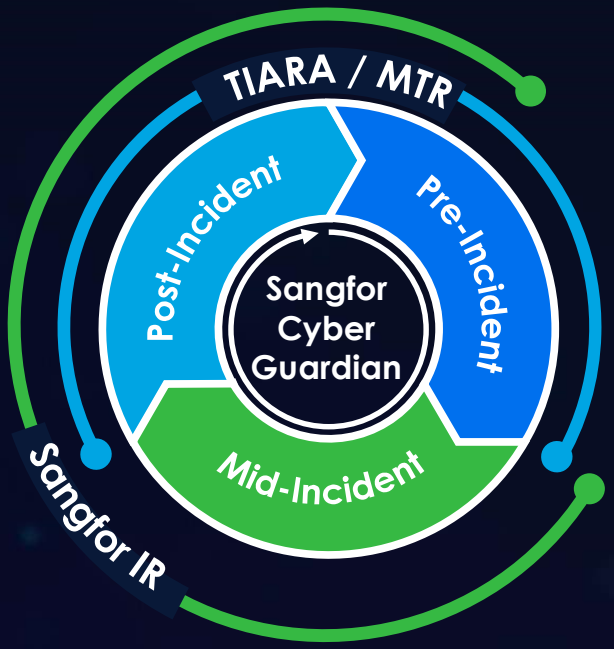
- Vulnerabilidades
- Parches de seguridad
- Postura de seguridad
- Anti Ransomware

Hyperconvergencia

HCI/VDI



Servicios de seguridad de Sangfor



Sangfor Cyber Guardian MDR Services

Servicio de detección y respuesta gestionado 24x7 que aprovecha la inteligencia humana y artificial para ayudar a las organizaciones a detectar y responder a las amenazas de seguridad

Sangfor MTR

Evaluación continua de la postura de la red centrada en descubrir amenazas aprovechando la tecnología Sangfor NDR.

Sangfor TIARA

Evaluación de la postura de red basada en tecnología para determinar la eficacia y la preparación contra incidentes de seguridad.

Sangfor IR

Asistencia experta en la investigación de incidentes de seguridad y proporcionar recomendaciones de corrección.

MDR - Managed Detection and Response
TIARA - Threat Identification, Analysis, and Risk assessment
MTR - Managed Threat Response
IR - Incident Response

Soluciones de Seguridad Sangfor

Ransomware + IR

- Integración entre NGAF y Endpoint Secure
- Protección excepcional vs ransomware
- Contención automática de amenzas
- Servicio de respuesta a incidentes

XDDR + MDR

- Detección oportuna de ataques internos
- Investigación y cacería de amenazas
- Mapeo de ataques al MITRE ATT&CK
- Respuesta automatizada
- Simplificación de operaciones de seguridad
- Evaluación de riesgo y reportes de incidentes

Acceso Seguro a Internet

- Autenticación unificada
- Control de App, URL, & SaaS
- Descubrimiento y bloqueo de Shadow IT
- Anti-proxy
- Anti-virus

SD-WAN Seguro

- Aprovisionamiento sin contacto (zero-touch)
- Conexión segura de múltiples sitios
- Control de acceso Interno & Internet
- Ruteo inteligente con agregación de enlaces
- Administración, Visibilidad & Operación centralizada

SANGFOR

Sangfor NGAF/NSF

www.sangfor.com

Sangfor Technologies Inc.

NGAF - Next Generation Firewall & Web Application Firewall
NSF – Network Secure Firewall

Agenda

SANGFOR

01 Network Secure Challenges

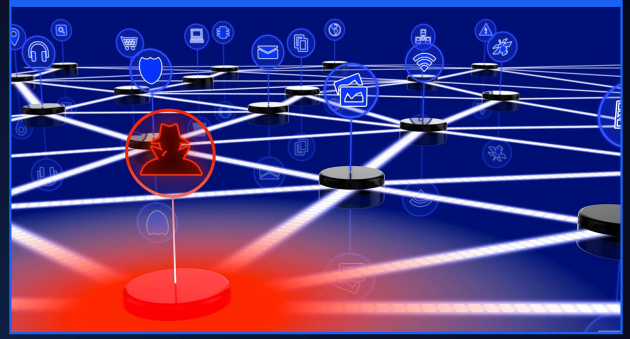
02 What's New in Sangfor Network Secure

03 Use Cases & Best Practice

04 Takeaways

Nuevos desafíos para mantener las redes seguras

Amplia superficie de ataque



- Dispositivos de TI/IoT/OT no gestionados
- Configuraciones incorrectas
- Vulnerabilidades
- Amenazas en sitios remotos desprotegidos

Atacantes sofisticados

- Ciberataque como servicio (CaaS)
- Más de 450.000 nuevos programas maliciosos al día
- IA armada para apuntar a sistemas de alto valor y entregar malware personalizadas

Falta de experiencia en seguridad

- Según ISC2, el 70% de las organizaciones no cuentan con suficiente personal de ciberseguridad para responder de forma rápida y precisa a las amenazas de seguridad
- El 95% de los ciberataques se deben a errores humanos

Enfoque de los desafíos de seguridad

SANGFOR

Protección estática/rígida	→	Protecciones más inteligentes, inteligentes y completas
		Tecnología AI/ML/TI
		Protección IoT/OT
		Proteja el perímetro de SD-WAN
Requiere habilidad para operar	→	Funcionamiento sin esfuerzo
		Interfaz y panel de control intuitivo
		Alarma de vulnerabilidad
		Detección de errores humanos
Protección en silos	→	Arquitecturas Integradas
		Integración con Endpoint
		Integración con el servicio (MDR)
		Integración con las nubes

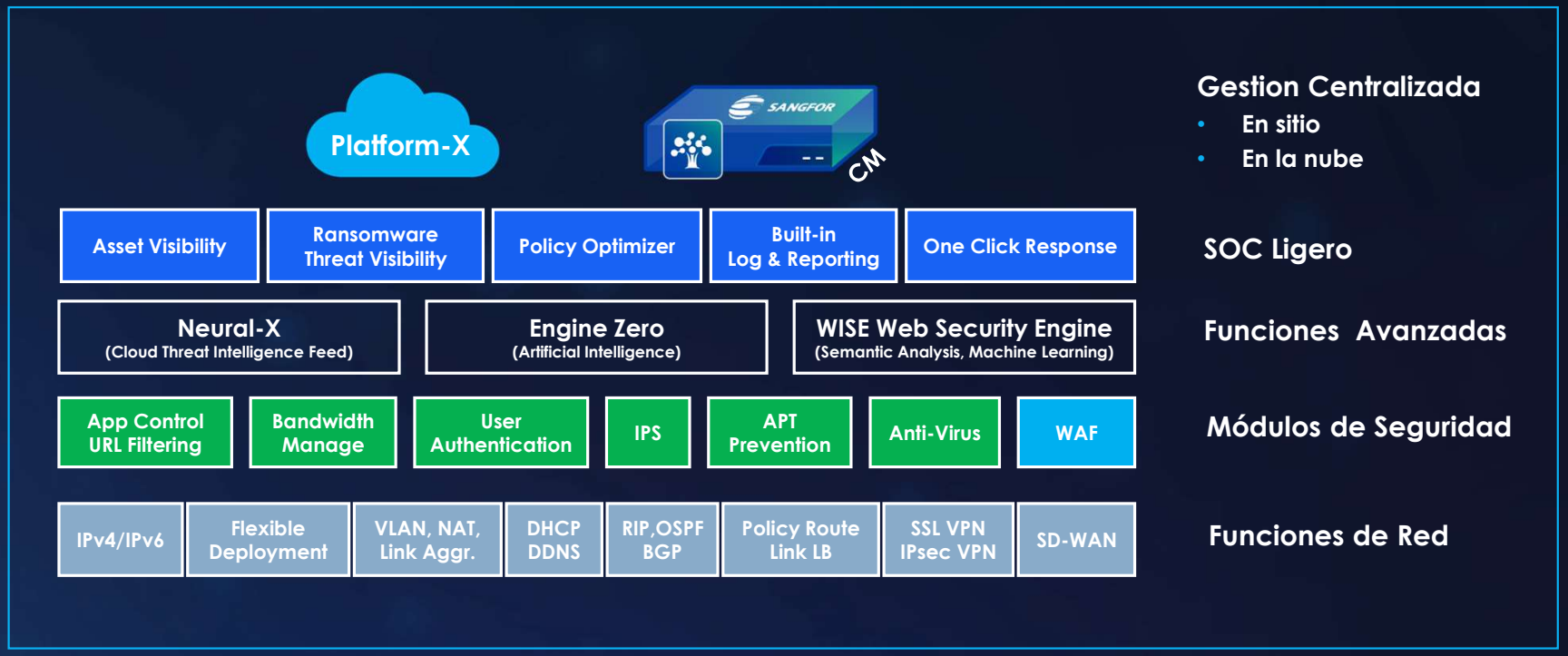
? ¿Es posible abarcar todos los enfoques en una solución?

NGFW + NGWAF + SOC Lite con IA

Protección complete y efectiva de L2 a L7

- Intrusion Prevention System
- Application Control & URL Filtering
- NG Web Application Firewall
- APT Prevention
- Engine Zero AI Malware Inspection
- Neural-X Cloud TI
- Bandwidth Management
- SOC Lite, Log & Reporting
- Seamless Integration with Sangfor XDDR
- Routing, NAT, IPv4/IPv6, SSL VPN, IPsec VPN, Link LB

Características principales de Sangfor NGAF



Gartner Magic Quadrant for Network Firewalls 2022

- **8** años consecutives en el CMG para Firewalls de Red
- **2** años consecutives como Visionary

Evaluaciones de efectividad y desempeño

SANGFOR

Seguridad de Clase Mundial sin Desfalcos

2021: Mejores evaluados
Categoría AAA

2023: Mejores evaluados
Categoría Recommended

**CyberRatings did not conduct an Enterprise Firewalls test in 2022*

SANGFOR

Sangfor Network Secure:
Reinventando el Firewall

www.sangfor.com

Sangfor Technologies Inc.

Introducing Sangfor Network Secure Firewall

SANGFOR

Evolución

NGAF → **Network Secure**

Hereda lo destacado del NGAF

- Engine Zero, Neural-X, NGWAF.
- SoC Ligero
- XDDR 2.0 Framework

Más seguridad e innovación

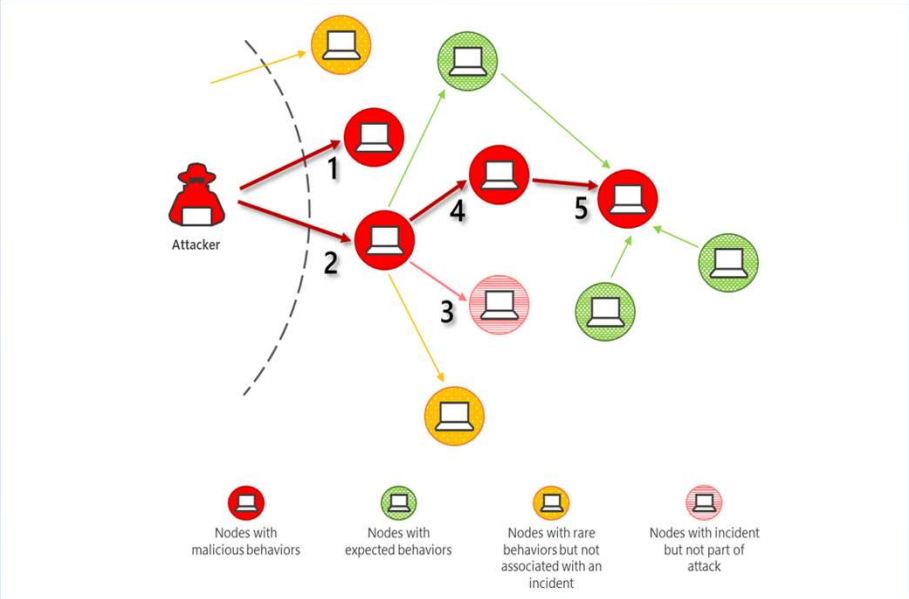
- 1º NGFW con engaño en la nube
- Seguridad IoT/OT
- SD-WAN segura

Arquitectura para el futuro

- Nuevo hardware y mayor rendimiento
- Experiencia más estable
- Se adapta a redes complejas

Innovación tecnológica:
Engaño en la nube en el cortafuegos

Problema: Responder a los ataques y movimiento lateral

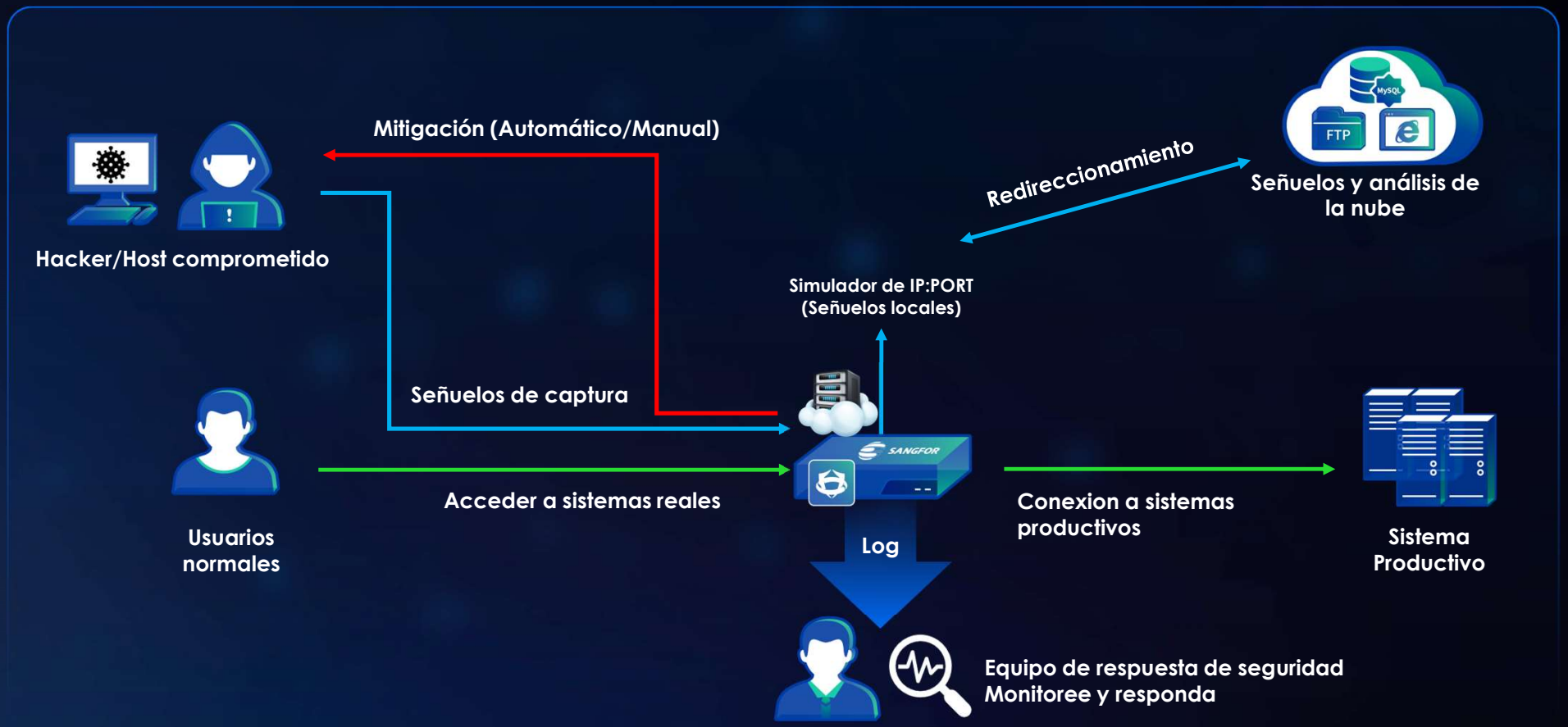


- El movimiento lateral es un método común para penetrar en los sistemas de una red
- Los ataques comienzan a comprometer las máquinas menos sensibles/seguras y llegan a invadir los sistemas centrales

Formas comunes de protección	Dificultades
Implementar la segmentación, el control de la comunicación lateral	Requiere políticas complejas y, posiblemente, más inversión
Mejore la gestión de credenciales y utilice MFA	Requiere una sólida formación en materia de seguridad, que puede no ser lo suficientemente eficaz, ya que la fuga de credenciales está creciendo.
Utilice herramientas avanzadas de monitoreo y análisis de red para detectar y responder al movimiento lateral	Alta inversión, difícil de configurar, requiere experiencia para operar

Complejo, de alto costo, requiere mucho tiempo y requiere una experiencia significativa

Defensa proactiva con Sangfor Network Secure



Extremadamente fácil de configurar

3 Pasos, 5 minutos de configuración

Valores de protección claves

El ÚNICO NGFW en el mundo con tecnología de engaño incorporada

Confundir a los atacantes

Despliega señuelos para confundir a los atacantes de los objetivos, ganando tiempo para proteger los activos

Localice la fuente

El motor de análisis basado en la nube identifica el origen del ataque

Identificar al atacante

Construya la huella digital del atacante basada en el análisis del comportamiento del atacante para bloquear nuevos ataques (ubicación, redes sociales, etc.)

Detener la propagación lateral

La respuesta rápida y precisa impide que los hosts comprometidos ataquen a otros

Reduce la superficie de ataque de IoT/OT

Riesgo de seguridad del IoT/OT

Falta de visibilidad

Los dispositivos IoT operativos y de instalaciones son adquiridos por unidades de negocio y es posible que TI no esté al tanto de la implementación o el uso.

Vulnerabilidades inherentes

- Los dispositivos IoT tienen múltiples vulnerabilidades con poca o ninguna aplicación de parches.
- Las brechas de seguridad de la red pueden infectar fácilmente los dispositivos IoT.

Riesgos del soporte remoto

- Algunos dispositivos IoT/OT son soportados de forma remota por el proveedor.
- No se puede detectar tráfico malicioso dentro de la conexión remota.

Controles de seguridad tradicionales de IoT

Opción 1

Endurecimiento del firmware con SDK o actualizaciones

- Necesita soporte de proveedores
- Parche no disponible
- Complejo y lento
- No puede garantizar la seguridad

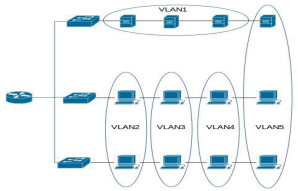
Opción 2

NAC o una solución similar a NAC

- Centrado únicamente en el control de nivel de acceso
- No se pueden proteger los dispositivos comprometidos

Opción 3

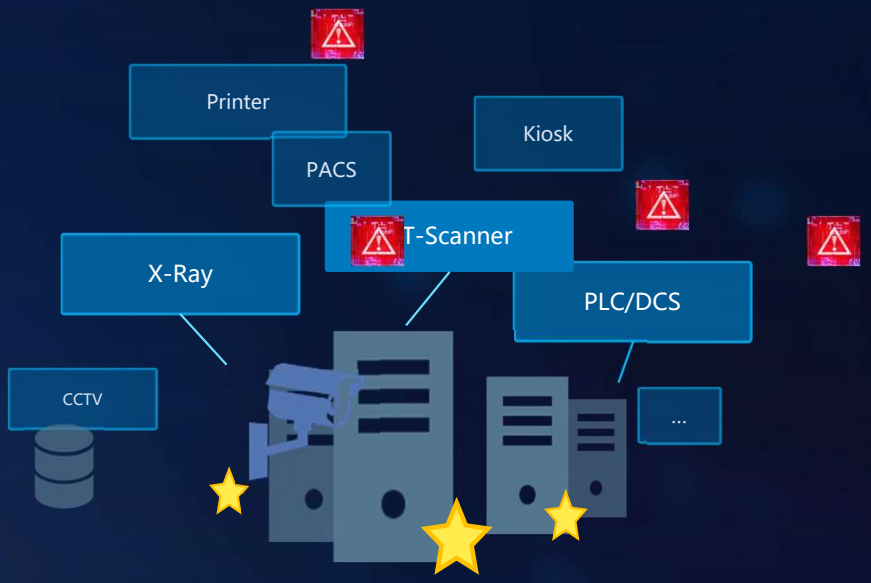
Segmentación de la red



- Gran carga de trabajo para planificar e implementar
- Alto costo y largo plazo
- Todavía no resuelve el problema de los dispositivos comprometidos

Sangfor Network Secure con protección IoT/OT

Detección y control inteligente de dispositivos IoT



- ✓ **Identifique los dispositivos IoT y cree una lista de activos.**
- ✓ **Base de datos de firma de huellas dactilares IoT integrada.**
- ✓ **Detener el acceso no autorizado a la red de dispositivos IoT**

Detenga los ataques contra los dispositivos IoT

Ataques de fuerza bruta

Detectar contraseña débil
Vulnerabilidad de OWASP

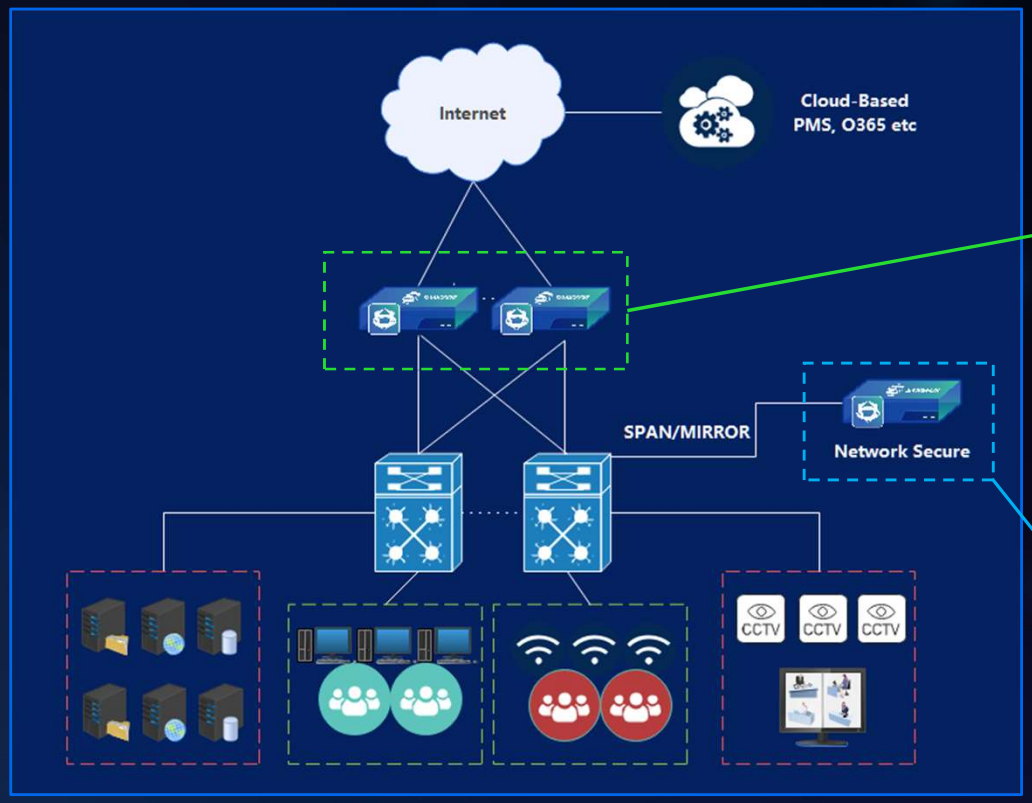
Comportamientos maliciosos
Comunicación C&C

Firmas IPS de IoT dedicadas

Auditar los protocolos de OT

(OPCDA, s7, s7-plus, MODBUS, IEC104, profinetIO, DNP3, CIP, etc.)

Protección IoT/OT fácil de poner en marcha



Implementación de Network Secure como puerta de enlace

- Identificación de los activos de IoT
- Filtrar virus, detener C2, prevención de intrusiones
- Tecnología de engaño para proteger el IoT

Implementación de Network Secure como modo de bypass/supervisión

- El switch central refleja el tráfico en Network Secure para su detección y auditoría
- Network Secure puede enviar el restablecimiento de TCP para finalizar las comunicaciones
- Sin impacto en la red existente

SD-WAN segura e integración con SASE

Ventajas / Desventajas de SD-WAN

SANGFOR

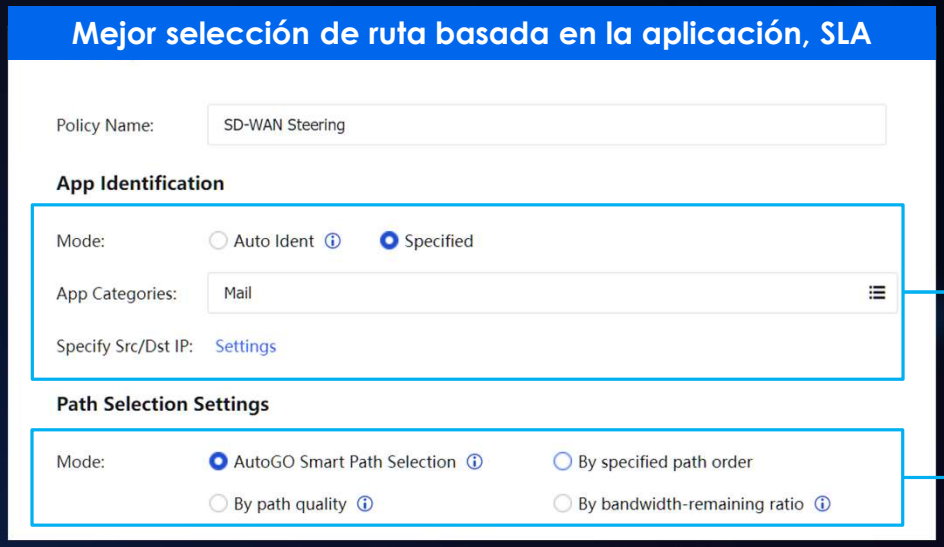
- ✓ Mejor velocidad con un menor coste total de propiedad
- ✓ Agilidad empresarial
- ✓ Gestión simplificada

- ⚠ Falta de control de seguridad
- ⚠ Comportamiento del usuario no administrado
- ⚠ Inversión en dispositivos en ROBO

Arquitectura SD-WAN segura de Sangfor

Dirección y optimización inteligente del tráfico SD-WAN

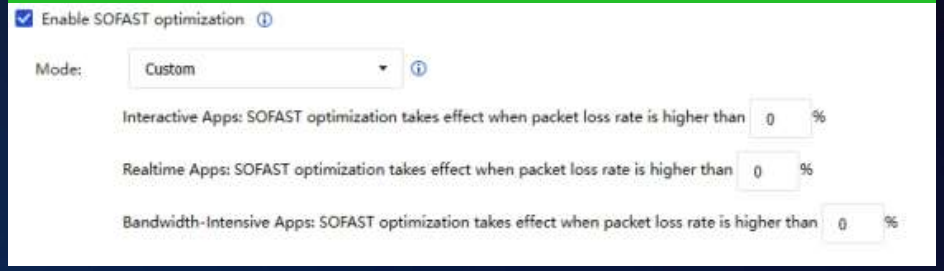
Mejor selección de ruta basada en la aplicación, SLA



Dirigir el tráfico por aplicación, dirección IP

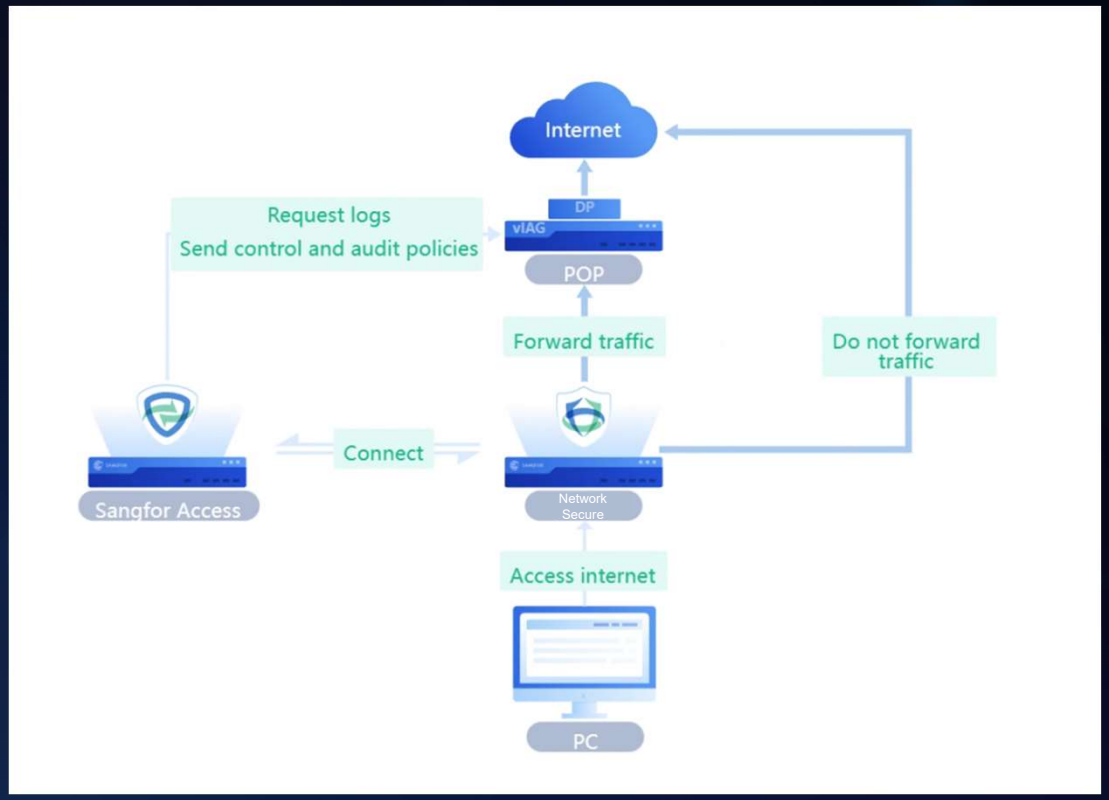
La mejor selección de ruta incluye en función de la naturaleza de la aplicación, el ancho de banda y el SLA de enlace (fluctuación, latencia, pérdida de paquetes)

Optimizar enlaces inestables



Mejore el rendimiento de 2 a 5 veces en entornos de alta pérdida de paquetes

Network Secure Integrates with Access Secure



Security flexibility for businesses

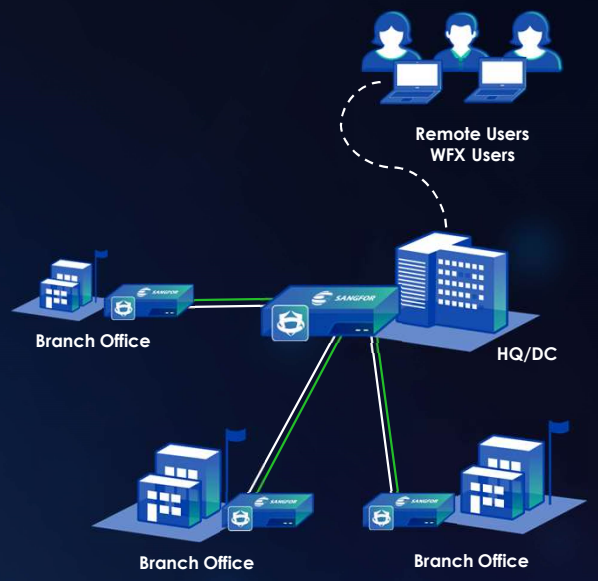
- ✓ Branch Site: local security
- ✓ ROBO: Sangfor Access Secure

Optimize traffic on demand

- ✓ HQ-Branch: Local links + best path selection
- ✓ SaaS/IaaS/Cloud: Sangfor Access Secure
- ✓ Over Country connection: Sangfor Access Secure

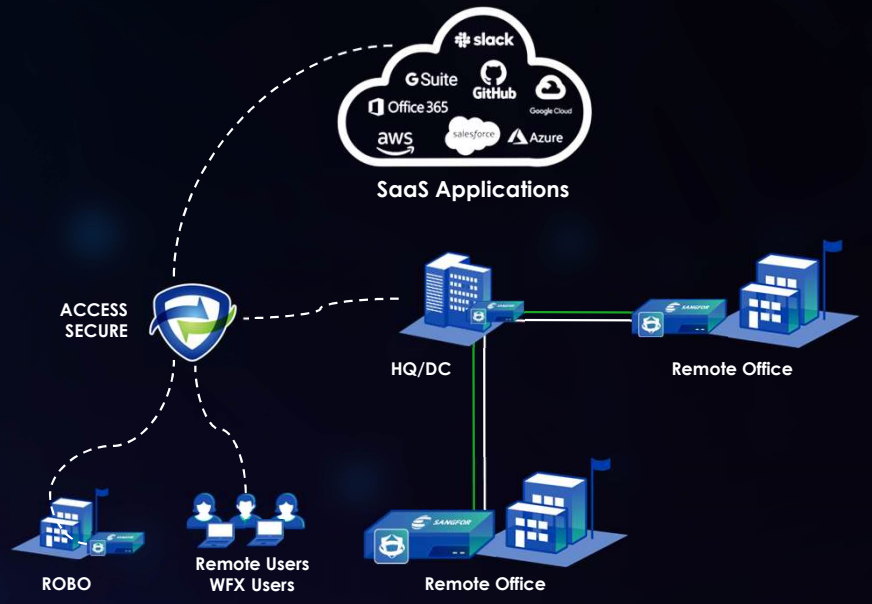
Casos de uso típicos

Caso de implementación tradicional



1. Conexión de sucursal a HQ/DC a través de MPLS, VPN
2. El usuario remoto se conecta a la sede central a través de SSL VPN

Aplicación SaaS y WFX



1. Las sucursales se conectan a la sede central / DC a través de MPLS, VPN
2. El usuario remoto, el agente de uso del sitio ROBO o la puerta de enlace se conectan a Sangfor Access Secure, utilizan el poder de SASE para proporcionar control de seguridad y optimización de acceso.

SANGFOR

Actualización de la experiencia de operación de seguridad

Integración mejorada entre Firewall y Endpoint Secure

NGAF

Un clic para terminar procesos maliciosos

Network Secure

La inteligencia de amenazas a través de IP + AgentID facilita la identificación del cliente real en el entorno DHCP

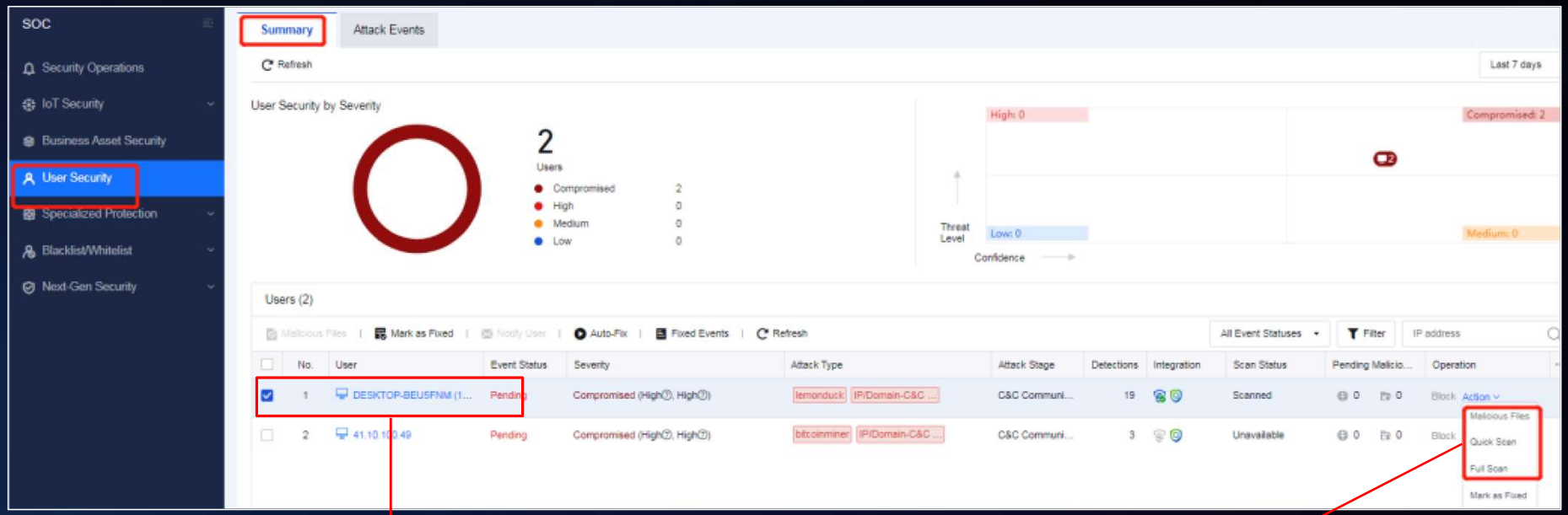
Un clic para iniciar el escaneo completo/rápido del disco

Un clic para finalizar un proceso malicioso

Seguimiento y respuesta en el End Point

SANGFOR

Descubrir amenaza → **Localice la fuente** → **Mitigación inmediata** → **Limpie las amenazas restantes**



Mostrar el ID del agente junto con la dirección IP

Inicie "Escaneo rápido", "Escaneo completo"

Punto débil: políticas de control de acceso complejas

Política N: XXXXX

Directiva 6: Directiva temporal para la solución de problemas

Política 5: Finanzas quiere acceder a xxxx durante unos días

Política 4: El equipo del sistema solicita abrir xxxx

Directiva 3: Permitir el servicio xxxxx

Directiva 2: Permitir la aplicación xxxx

Política 1: Denegar todo

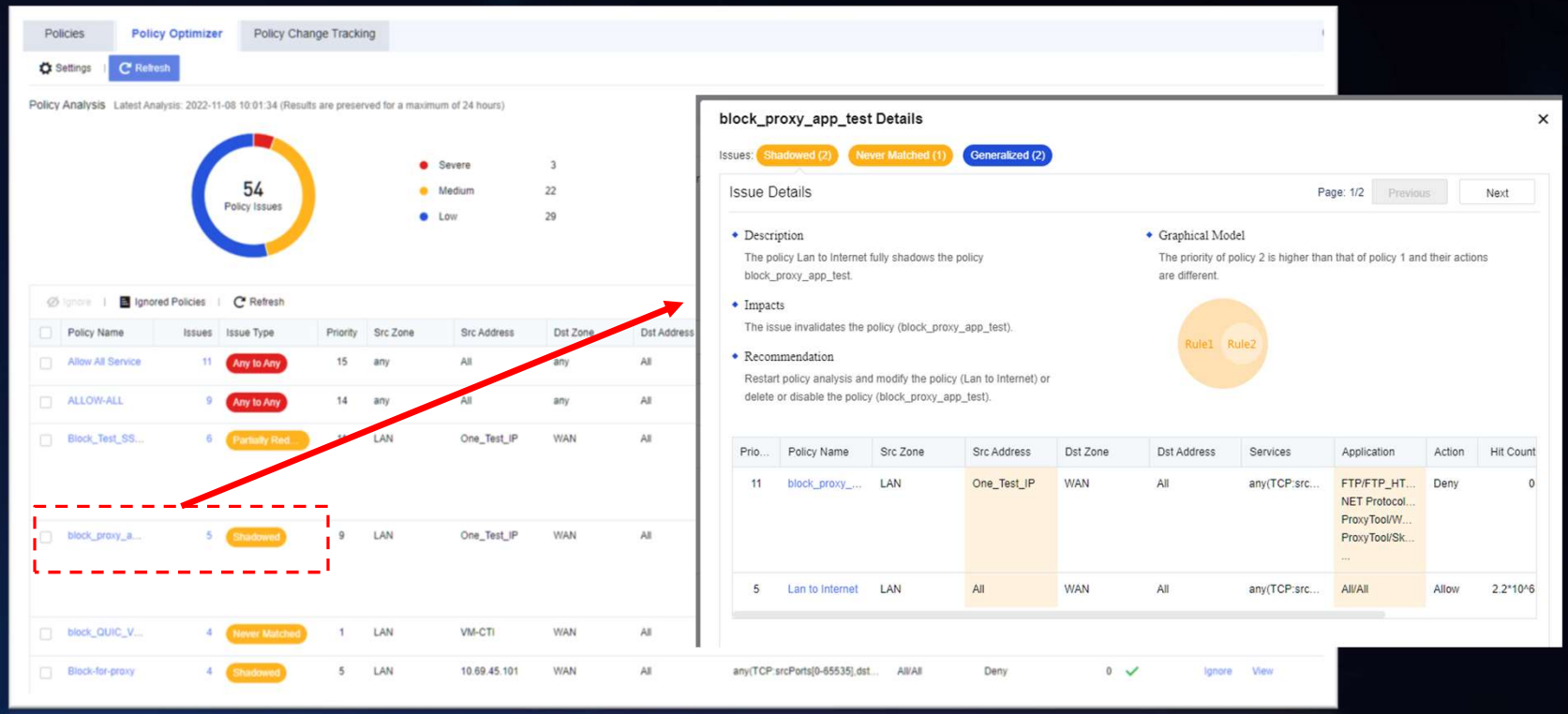
Políticas de control cada vez más complejas

1. Solicitudes de políticas de seguridad aleatorias
2. Configuraciones incorrectas
3. Políticas temporales que no se eliminan a tiempo
4. Tomar el control de un firewall del administrador anterior
5. Con el tiempo, termina con cientos de políticas que son difíciles de entender y administrar

SOC Lite | Optimización de políticas sin esfuerzo

SANGFOR

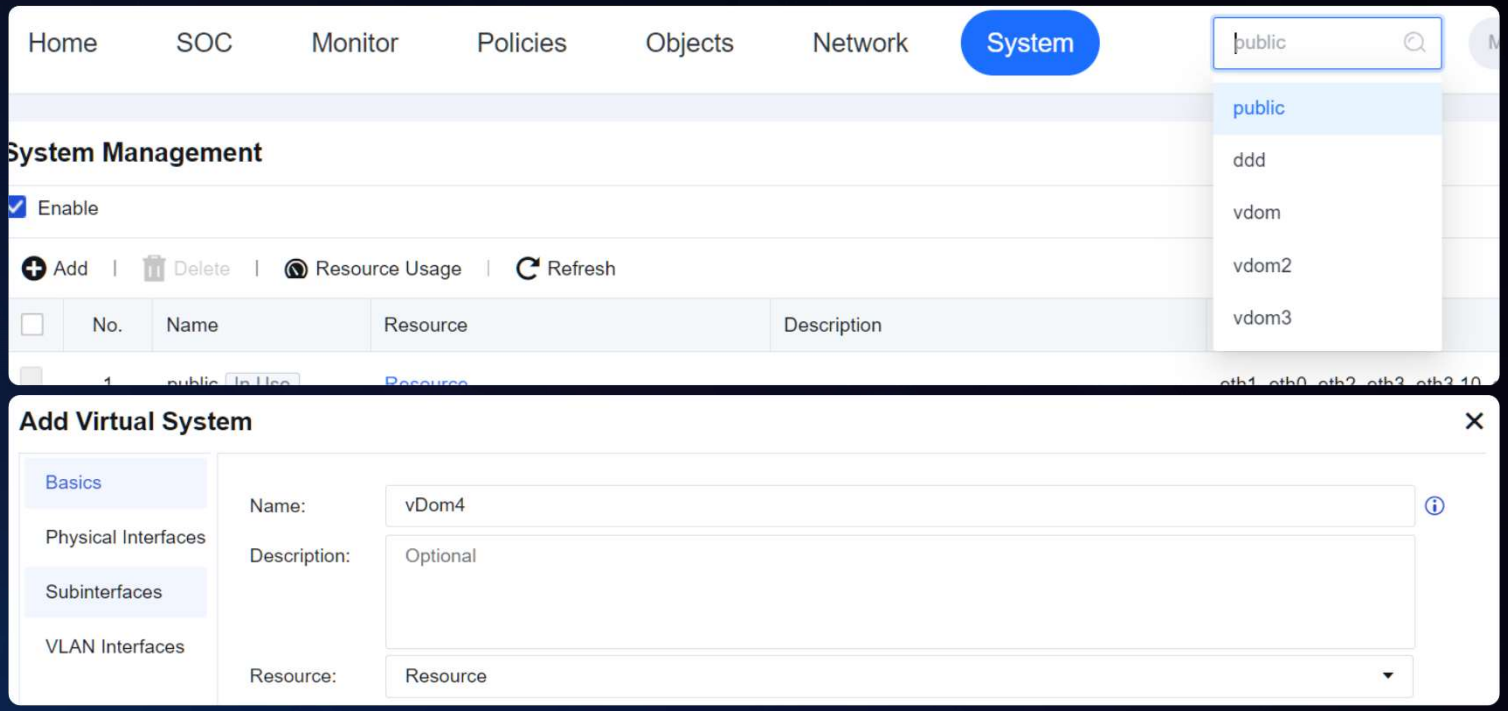
Identifique duplicaciones, conflictos y errores de configuración en miles de políticas con un solo clic



Compatibilidad con dominios virtuales

La compatibilidad con dominios virtuales permite al administrador definir varias instancias virtuales en un solo dispositivo.

Cada instancia de dominio virtual incluye un panel de administración dedicado, interfaces, etc.



Mejora de la alta disponibilidad

Support BFD

- Mecanismo de conmutación por error más confiable

Cambio mejorado

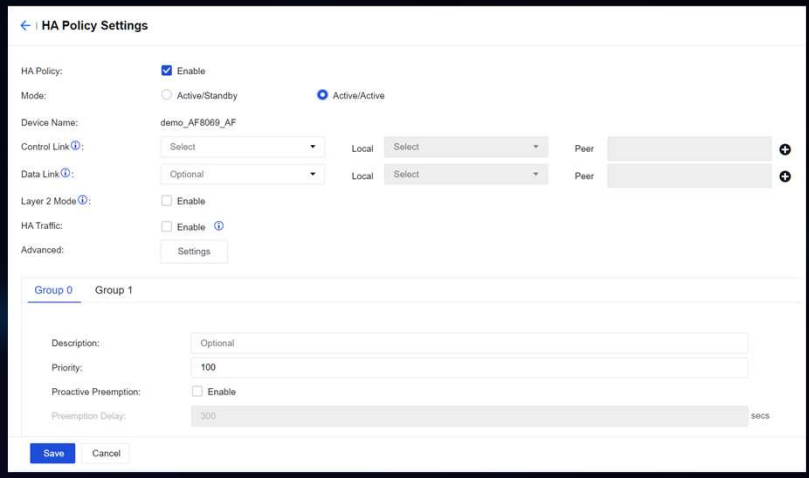
- Conmutación sin pérdida de paquetes

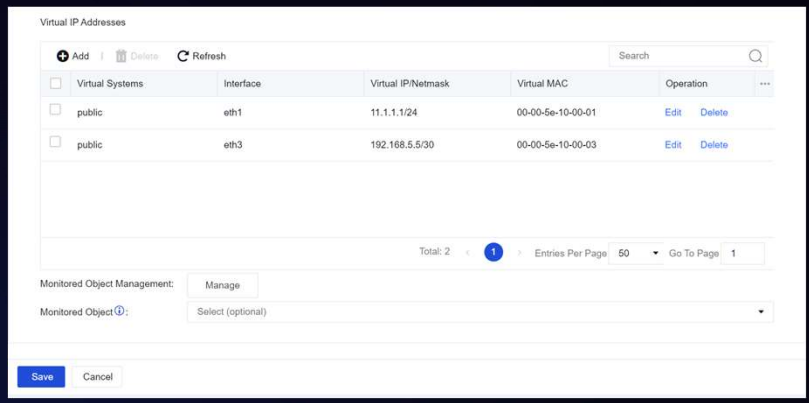
Actualización en línea

- La actualización de la versión principal no requiere la reconfiguración de alta disponibilidad

Admite múltiples modos de alta disponibilidad

- A-A en modo puente con soporte de enrutamiento asimétrico
- A-A en modo router con soporte de enrutamiento asimétrico





SANGFOR

¿Preguntas?

Demo:

https://demo.sangfor.com:444/

SANGFOR

Cyber Command

Intelligent Network Detection and Response Platform

¿Qué es NDR?

SANGFOR

N – Network
D – Detection
R - Response

Categoría tecnológica para clasificar equipos que NO usan detección con Firmas.
- Inteligencia Artificial
- Machine learning / Deep learning
- Analítica de comportamiento

Para detector actividad maliciosa y sospechosa en la Red, y Responder a las Cyber-Amenazas.

¿Por qué es importante NDR?

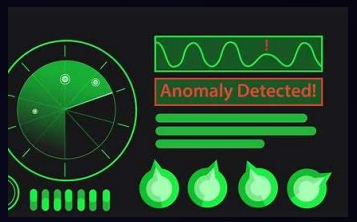
SANGFOR

Seguridad tradicional Insuficiente

- Enfoque en la prevención 80% a 99% de las amenazas - CyberRatings
- 0-Day, APT, sobre pasan la seguridad tradicional - > 450K variantes diarias
- No contempla plan de respuesta a incidentes
- La seguridad es ineficaz: MTTI y MTTR altos > 300 días
- Visibilidad limitada en el perímetro
- La superficie de ataque interna es enorme

Ataque de IA
vs
Defensa de IA

Los ataques cibernéticos impulsados por IA no se pueden defender sin asistencia de detección y prevención de IA



La visibilidad y la respuesta integrales son imprescindibles

Detección (tráfico espejo, registros de seguridad, IOC, BIOC) - Disminuye el MTTI

Respuesta (búsqueda de amenazas, bloqueo, cuarentena, copia de seguridad) - Disminuye el MTTR

¿Por qué Sangfor Cyber Command?

SANGFOR

Fuentes de datos eficaces y amplias

Sistemas de Seguridad

Dispositivos de usuario

TAP de red

Lago de información CC

SIEM

Radar

ArcSight

splunk>

Forward events

Sofisticada Detección y visibilidad

AI+ML

Detection

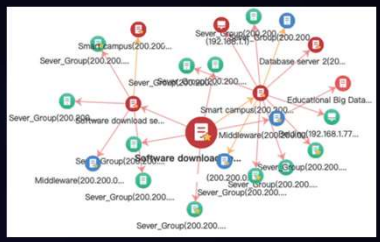
Engine zero	AI
UEBA	NTA
TI	Endpoint Secure
NGAF	Others

Comprehensive Visibility

Simplifique la caza de amenazas

Threat Hunting

- Attack chain analysis
- Contextual verification
- Attack sorting | Attack Path
- Security incident alert



MITRE ATT&CK

Respuesta eficaz más rápida

Response

- Block open ports
- Scan for other malware
- Quarantine | Stop processes
- Shut down C&C Connections

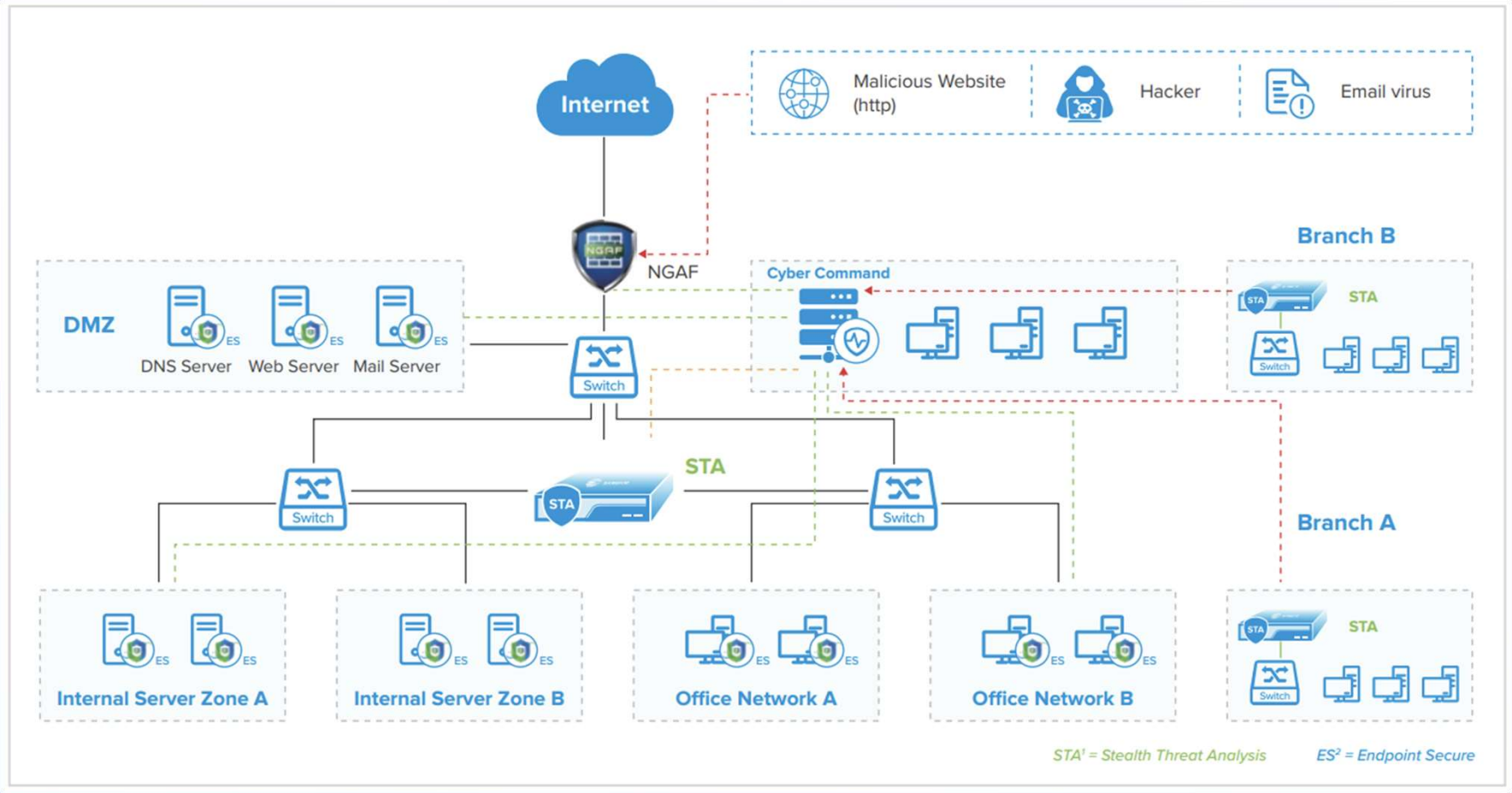
Firewall

paloalto NETWORKS · SOPHOS · FORTINET · Check Point · CISCO · WatchGuard · H3C · Hillstone NETWORKS · HUAWEI

Endpoint

Bitdefender · Windows Defender ATP · SOPHOS · TREND MICRO · Symantec · vmware Plan

Arquitectura de implementación



SANGFOR

¿Preguntas?

Demo:

https://demo.sangfor.com:8443/

SANGFOR

Endpoint Secure

The Future of Endpoint Security

www.sangfor.com

Sangfor Technologies Inc.

¿Qué hace el antivirus tradicional?

Los bomberos están cansados de lidiar con el fuego en todas partes
Basado en la característica, incapacidad para las variedades

450K Archivos únicos todos los días

AV-TEST registra una media de más de 450.000 nuevas variantes de malware y aplicaciones potencialmente no deseadas (PUA) cada día

Promedio **99.5%** Tasa de detección

Si no es 100% exitoso, algo PASARÁ

450K * (100%-99.5%) = **2250**

Potential new missed files every day

-- AVTest.org AVatlas

Enfoque ideal para proteger los endpoints

Pre-Attack

Medidas para detectar y prevenir que sucedan cosas malas

During-Attack

- Enfrente eficazmente las amenazas de mutación rápida.
- Detener la propagación de las amenazas

Post-Attack

- Habilitar la búsqueda de amenazas
- Respuesta de bucle cerrado por sinergia con otros componentes.

Resumen de la solución endpoints de Sangfor

- Gestión de activos
- Vulnerabilidad y parche
- Comprobación de línea base

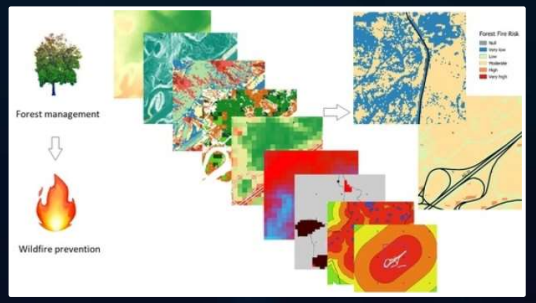
Pre-ataque

Prevenir es major que curar

- Detección de múltiples motores
- Microsegmentación
- Detener la propagación y explotar

Durante el ataque

Activamente y en profundidad contra las amenazas



- Búsqueda de toda la red
- Trazabilidad de amenazas
- Testificación

Después del ataque

A través de sinergia e integración

Protecting End-of-Support Windows Systems

Windows XP, Win7, Windows 2003, Windows 2008 , CentOS…

Más opciones para el endurecimiento del sistema

Aplicación de parches de vulnerabilidad

- ✓ Detección de vulnerabilidades
- ✓ Instalación oficial programada del parche
- ✓ Reinicio del sistema para habilitar el parche (recordatorio de reinicio)

Reduce la administración de parches

Mejora regular del sistema

Parcheo en caliente

- ✓ Corregir vulnerabilidad en la codificación de memoria (tiempo de ejecución)
- ✓ Impacto menor en el rendimiento
- ✓ No es necesario reiniciar para surtir efecto

Detenga las vulnerabilidades de día cero

Reduce number of reboots

Sin ralentización de los sistemas

Proteger el sistema EoS

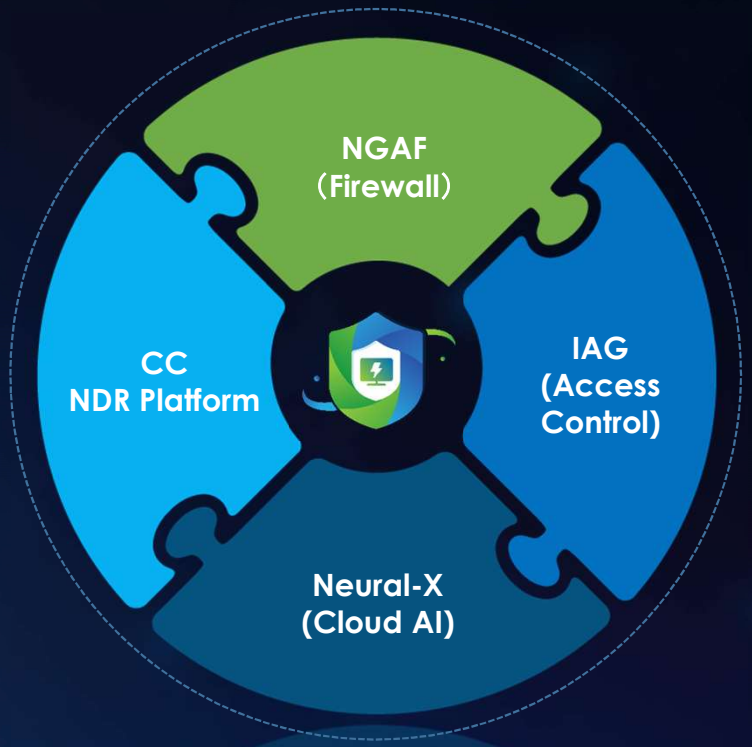
Eliminación de malware mediante múltiples motores

- Base de datos de malware completa y de alta calidad
- Familia de malware ADN
- Identificación de huellas dactilares
- Múltiples algoritmos expertos refinan la identificación ideal
- Las reglas de IA + identifican la respuesta óptima a las amenazas conocidas

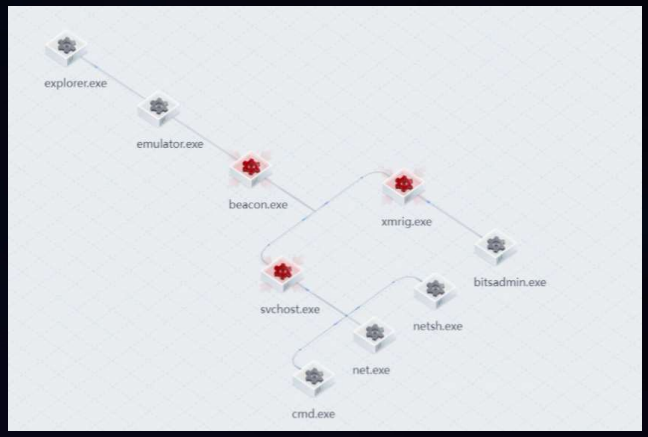
Alta detección, Disminución de Falsos

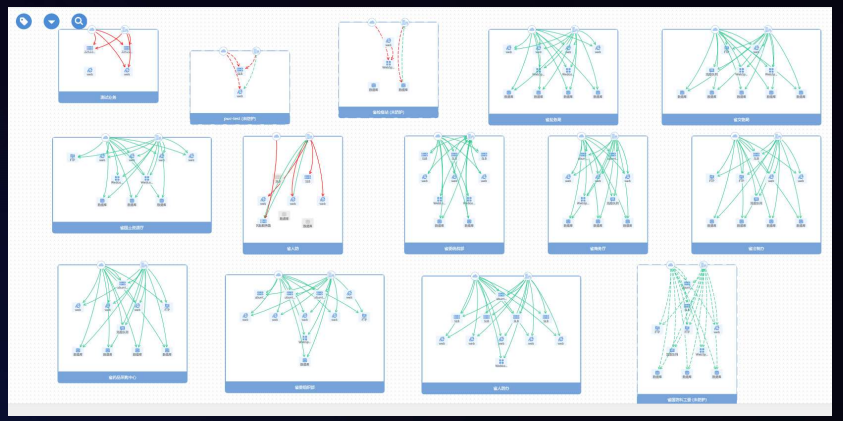
- Modelos de IA Aprendizaje continuo en Cloud Engine
- Mecanismos de aprendizaje de actualización automática iterativa rápida

Cadena de detección muy integrada



Endpoint / Network / Perimeter / Cloud
Del mismo proveedor





Seguridad avanzada para pequeñas y medianas empresas

- Operación y mantenimiento de seguridad simplificados
- Protección integral contra ransomware
- Anti – Proxy
- Microsegmentación de red
- Administración en la nube / local

TCO

Buy NGAF free 30 ES !

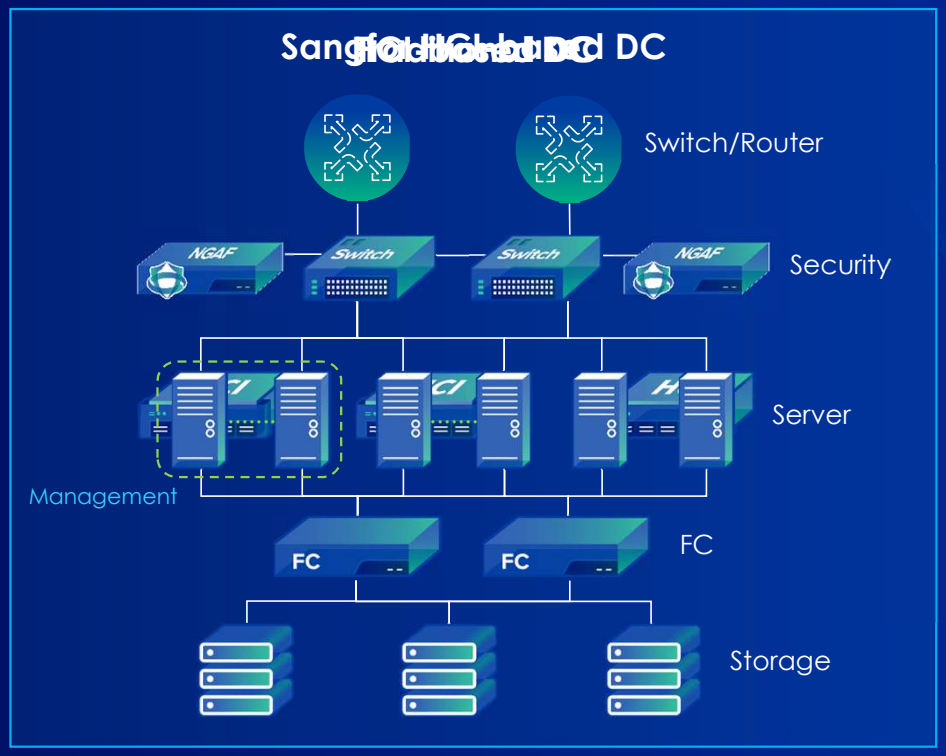
* Bundle Ultimate

SANGFOR | SANGFOR HCI

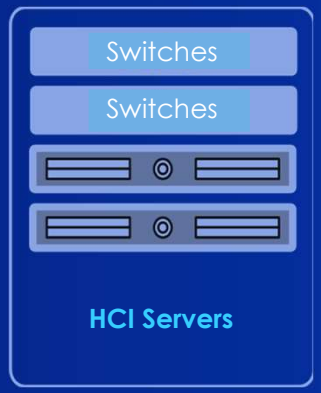
Sangfor Hyper-Converged Infrastructure

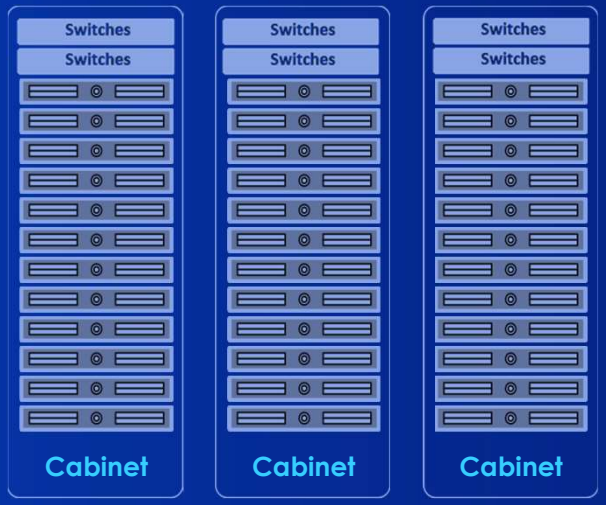
The Best Building Block for Your Future-Proof IT

Sangfor HCI Consolida el Centro de Datos



Escalabilidad sencilla

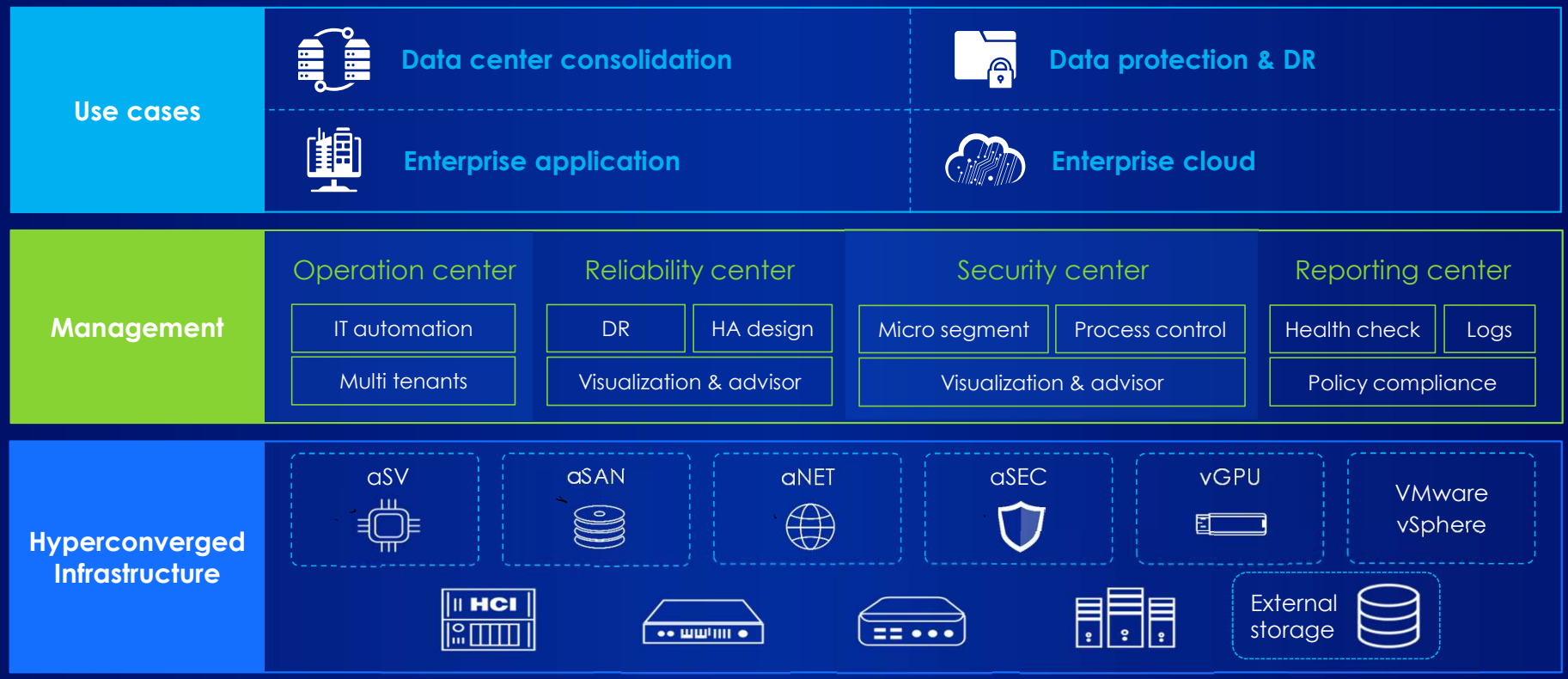




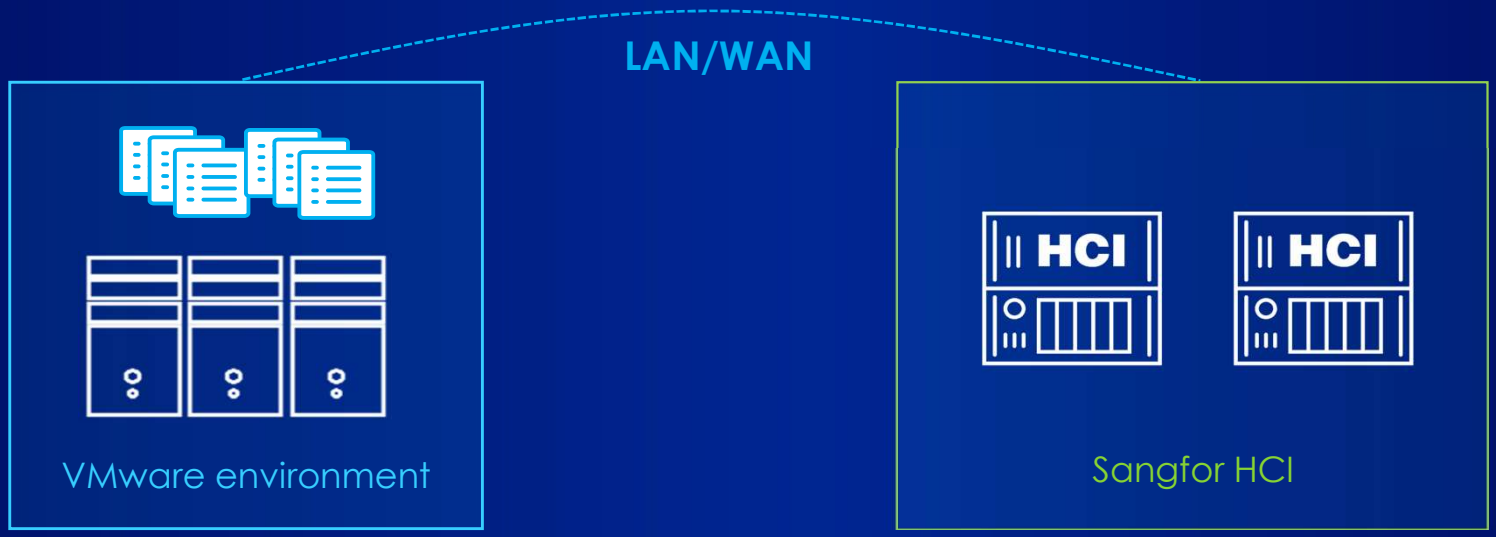
- Pre-inversión 3-5 años de anticipación
- Migración de datos para expansión
- Cuello de botella de rendimiento

- Comience con solo 2 nodos, hasta 64
- Expansión sin tiempo de inactividad
- Sin limitación de capacidad

Arquitectura de soluciones HCI de Sangfor

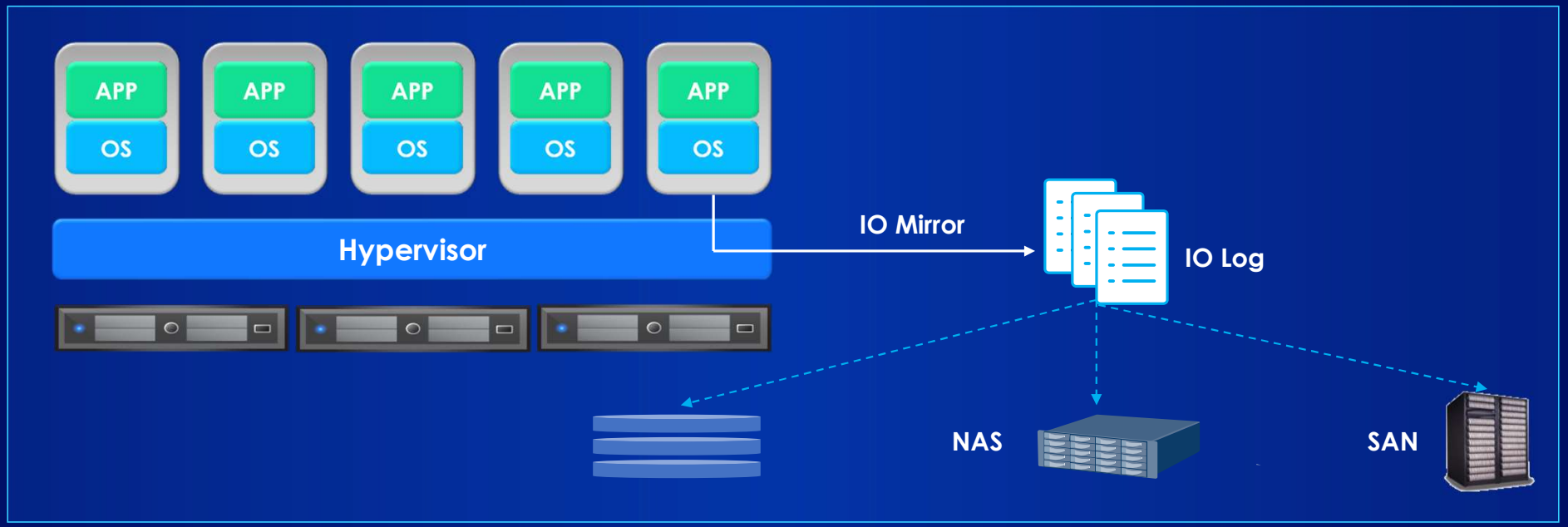


Administración y copia de seguridad integradas de VMware



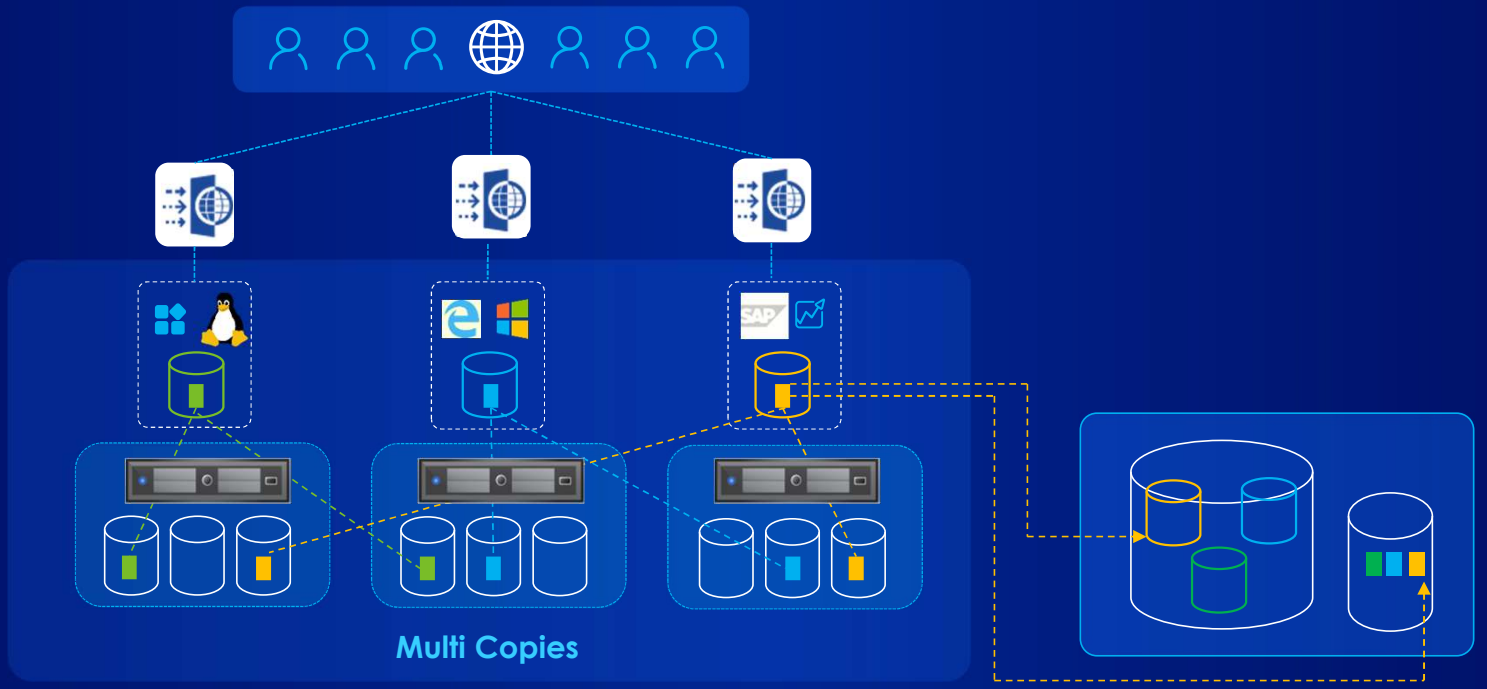
- Administración del ciclo de vida integrada de VMware
- Migración bidireccional
- Copia de seguridad integrada de VMware a Sangfor y recuperación instantánea
- Compatibilidad con VMware vSphere 7.0

CDP: Protección Continua de Datos



- Copia de seguridad de datos avanzada integrada
- RPO≈0. RTO≤5 Min

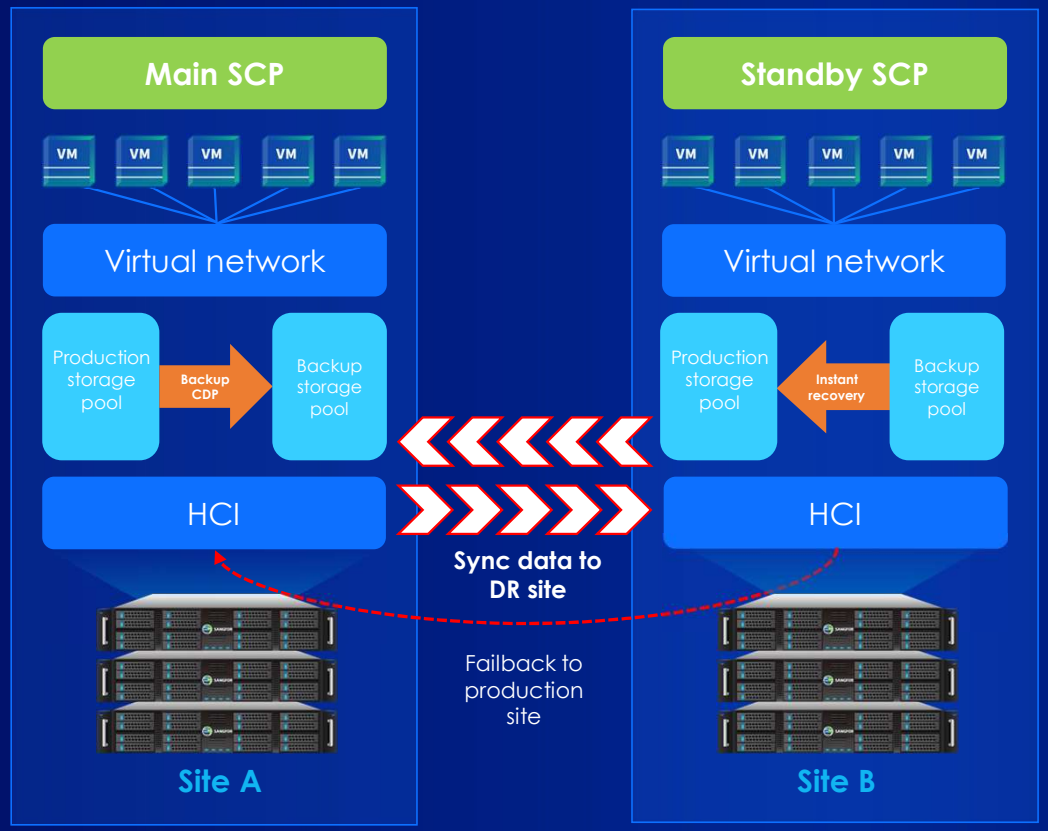
Copias múltiples y copia de seguridad incorporada



- Punto único de falla
- Se requiere software de copia de seguridad adicional

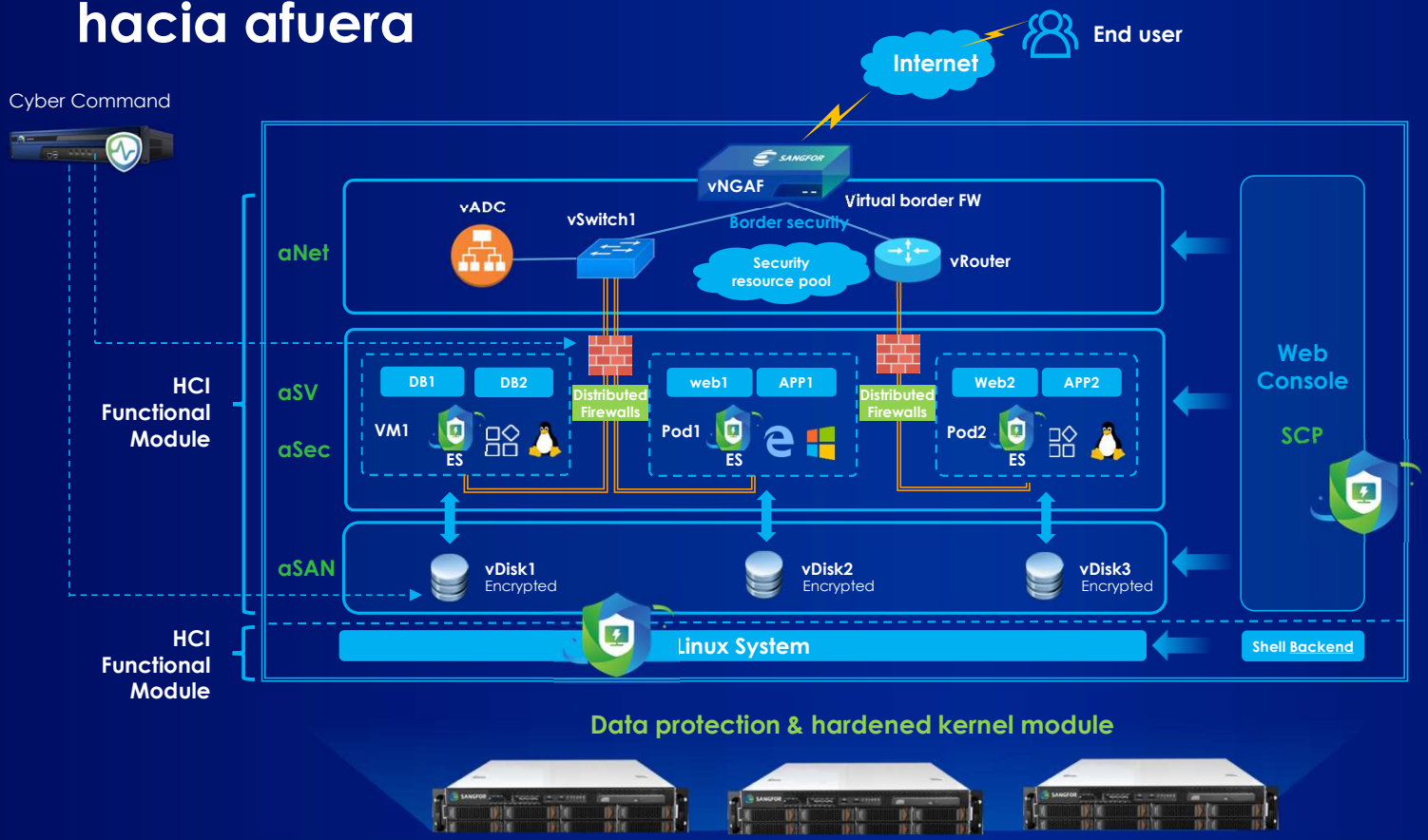
- Diseño inherente de múltiples copias
- Función de copia de seguridad incorporada con RPO = 1 hora

Recuperación ante desastres activo-pasivo o activo-activo



- Integrado y fácil de usar
- Backup local + replicación remota
- Almacenamiento activo-activo
- RPO flexibles, mín. 1s
- 0 pérdida de datos
- Fácil de implementar y administrar

Seguridad y escalabilidad maximizadas, de adentro hacia afuera



Plataforma en la nube

- Multinube, Multiinquilino, Fiabilidad empresarial

Seguridad de red

- vAF: Norte-Sur
- FW distribuido: Este-Oeste
- Microsegmentación

Seguridad de endpoints

- Escáner de vulnerabilidades
- EDR

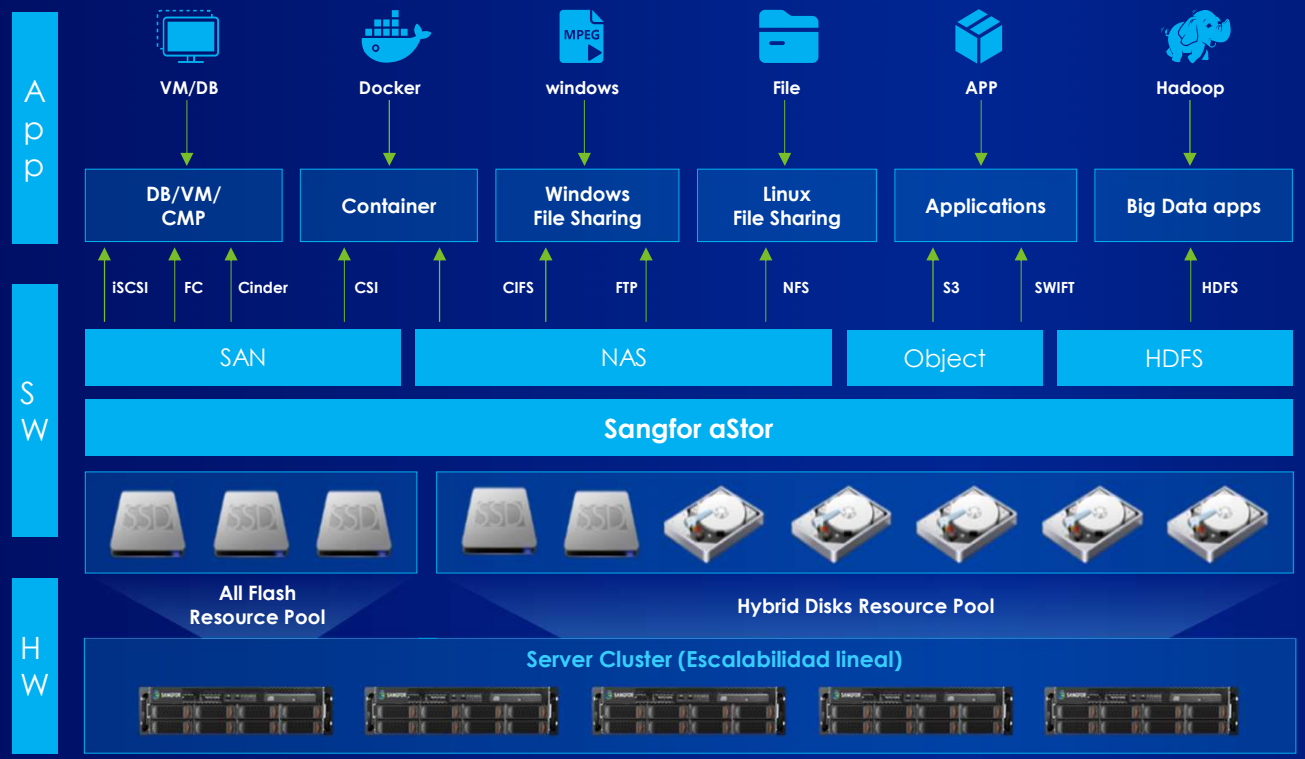
Seguridad de los datos

- Cifrado de disco
- HA, copias de seguridad/instantáneas

Seguridad del kernel

- WAF/IPS integrado

Sangfor aStor - Almacenamiento distribuido empresarial



Alta capacidad

Adecuado para la demanda de Big Data y HPC, proporciona múltiples protocolos de almacenamiento al mismo tiempo.
Puede tener almacenamiento de bloques, archivos y objetos al mismo tiempo.

Alta estabilidad

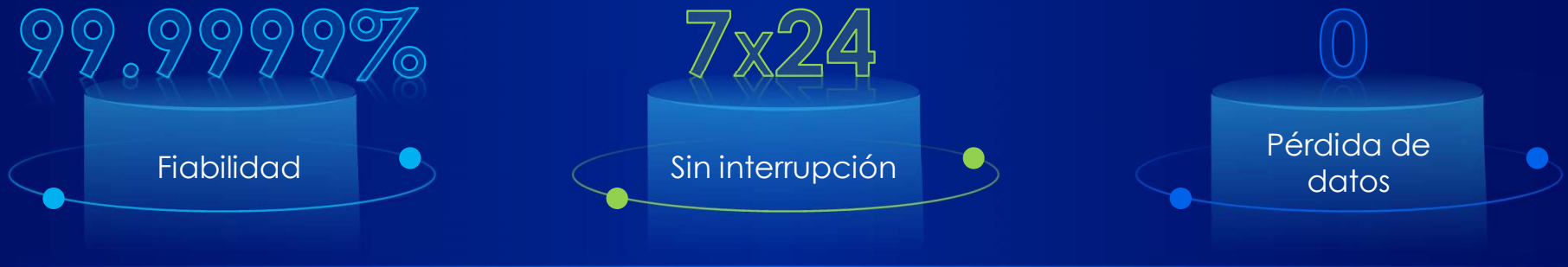
La arquitectura de protección de datos de 0 pérdida de información proporciona arquitecturas multiactivas para diferentes tipos de almacenamiento.

Alta seguridad

Las capacidades integradas de control de acceso convergen con las capacidades de seguridad de Sangfor

Arquitectura de protección de datos con 0 pérdida de datos

SANGFOR



Redefiniendo la fiabilidad: arquitectura de protección de datos de bucle cerrado

01 Protección proactiva

- Predicción de fallas de disco
- Detección de fallas del disco
- Redundancia multicopia
- Redundancia de código de borrado

02 Procesamiento automático

- Aislamiento automático de salud
- Conmutación automática de ruta IO
- Reconstrucción automática de datos dañados
- Reparación automática de datos diferenciales

03 Respuesta rápida

- Recuperación rápida de instantáneas y respaldos
- Recuperación multicéntrica
- Papelera de reciclaje de almacenamiento

Beneficios comerciales aportados por Sangfor HCI

Hasta **70%** en reducción de TCO

50% Reducción TTM

30% Alto Rendimiento

SANGFOR

Sangfor VDI Solution

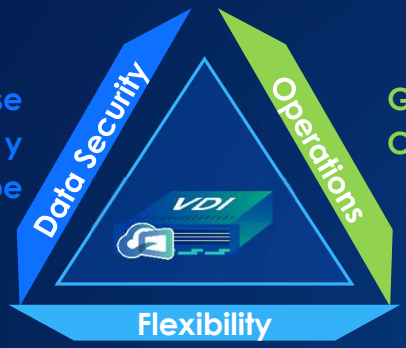
Seamless Experience, Secure and Efficient

www.sangfor.com

Sangfor Technologies

Infraestructura de escritorio virtual (VDI)

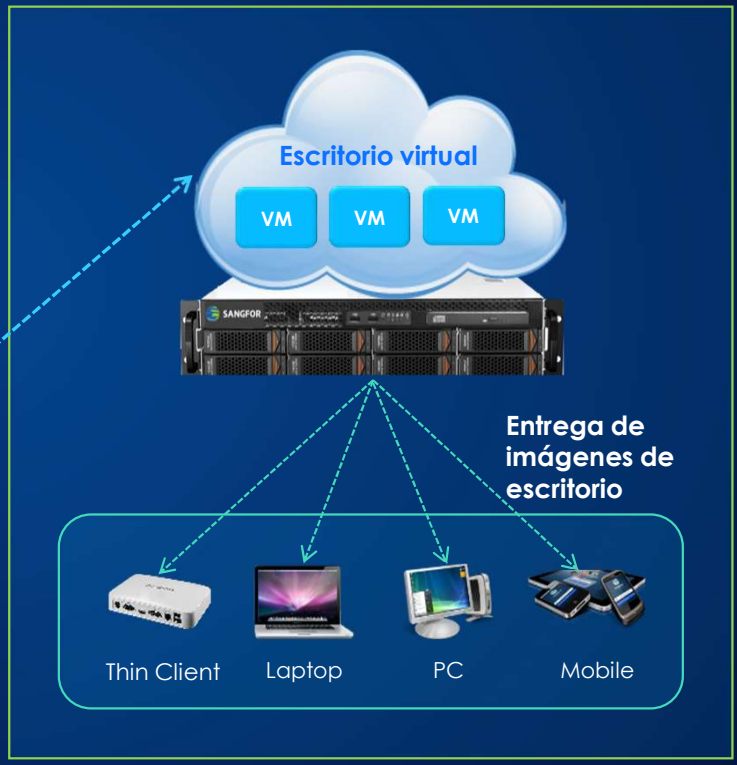
Los datos se almacenan y protegen en la nube



Gestion Centralizada

Escalabilidad/Flexibilidad WFA

El escritorio, las aplicaciones y los datos son Migrado a la nube (centro de datos)



Arquitectura VDI de Sangfor

Riesgos de seguridad de los PC tradicionales

Intrusión en la red

- Ransomware
- APT
- Trojan
- Sniffer

Error de disco
Pérdida de datos

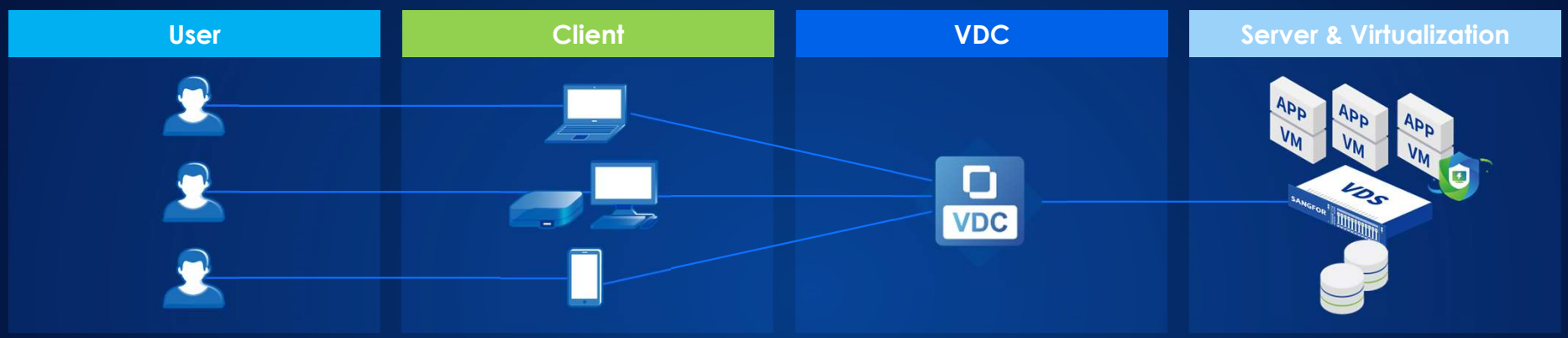
Fuga de datos por parte de los usuarios

- USB
- Export file
- Screenshot
- Send file

Sangfor VDI VS PC tradicional

Categoría	Sangfor VDI	Traditional PC
Implementación del espacio de trabajo	100 VMs in 5 Mins	2 Horas por PC
Expansión de usuarios	Implemente expansión lineal bajo demanda	Activos pesados, activos inactivos
Tasa de utilización del hardware	Pool Mode, High	Bajo
Interrupción del negocio	Creación en Minutos	4-8 Horas por año
Personal de TI	1 IT Engineer for 600-1000 Users	100 PCs per IT Engineer
Consumo de electricidad	Server: 600-1000W Thin Client: 20W	PC: 350W
Seguridad	Diseño de seguridad de extremo a extremo	PC + Third-party AV
Soporte de trabajo remoto	Escritorio virtual o aplicación, Seguro y suave	RDP, Experiencia de usuario insegura y deficiente

Diseño de seguridad de extremo a extremo



Seguridad para el comportamiento

- Marca de agua de pantalla
- Anti-captura de pantalla
- Auditoría de documentos exportados
- Control del portapapeles
- Lista blanca USB
- Lista blanca de aplicaciones
- Grabación de pantalla (3ros)

Seguridad de acceso

- Comprobación del entorno de endpoint
- Autenticación multifactor
- Ataque de fuerza bruta
- Inicio de sesión único (SSO)

Seguridad de red

- HTTPS Transmission
- Anti-Man-in-the-Middle Attack
- Anti-SWEET32 Birthday Attack
- Distributed Firewall

Seguridad integrada

- Múltiples copias de seguridad
- WAF incorporado
- Firma de disco
- Cifrado de disco

Seguridad integrada

- Sangfor Endpoint Secure

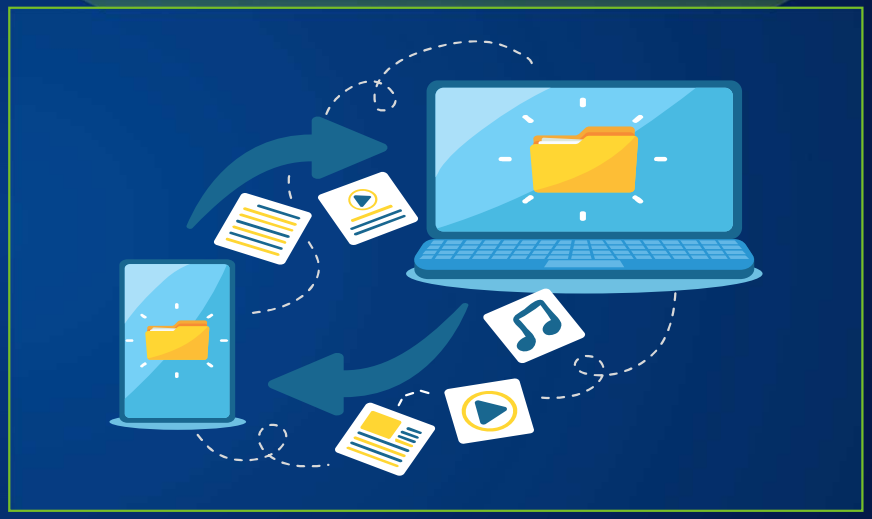
Gestión de aplicaciones y distribución de software

Descargar e instalar

Las aplicaciones solo provienen de contenedores de aplicaciones

- Mas eficientes
- Más seguras

Actualizar



La distribución de software no requiere actualizar la máquina virtual de plantilla

- No es necesario restaurar máquinas virtuales a la plantilla para actualizar las aplicaciones
- Actualice las aplicaciones más rápido

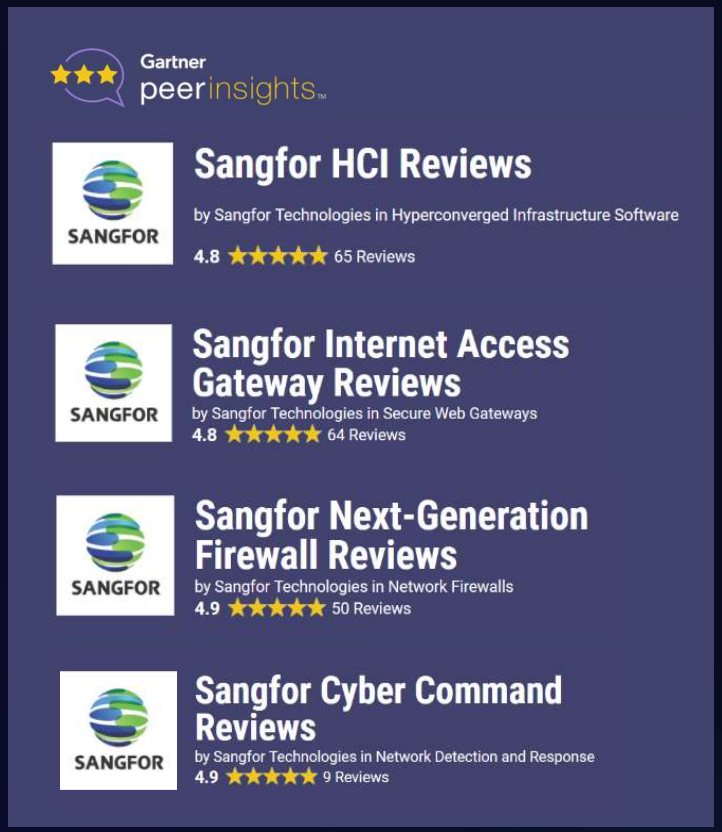
SANGFOR

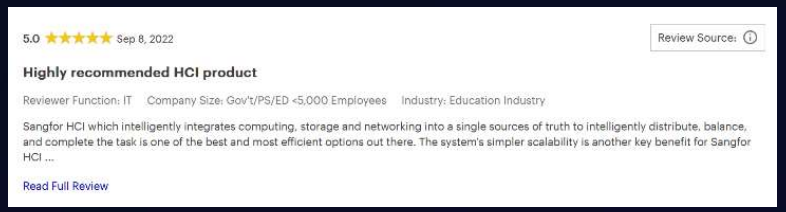
Resumen para llevar

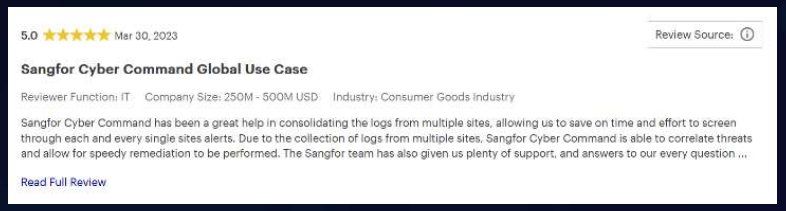
SANGFOR

Por qué Sangfor

Comentarios auténticos de los clientes







Gartner Recognition

Gartner

Magic Quadrant

- HCI
- IAG
- VPN
- WANO
- AD
- NGAF
- SSL VPN

Listed in the Gartner Peer Insights 'Voice of the Customer' Reports

NGFW	4.9 ★★★★★
HCI	4.8 ★★★★★
SWG	4.8 ★★★★★

Note: As of June 2021
Source: Gartner Peer Insights

Reconocimiento internacional y cooperación

100,000

Over 100,000 Customers Worldwide

Global Fortune 500, Government Institutions, SMEs, Banking & Finance,
Universities, Hospitals, ISPs, and More

Clientes de Sangfor Fortune Global 500


SANGFOR
Demo


SANGFOR
GRACIAS
Roberto Espinosa | Sr Sales Engineer México
roberto.andrews@sangfor.com
Sangfor Technologies México
SANGFOR
SANGFOR TECHNOLOGIES HEADQUARTERS
Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, Guangdong Province, P. R. China.
www.sangfor.com
Sangfor Technologies Inc.