nexica | econocom

NexicaCloud
Cybersecurity

SERVICIOS DE SEGURIDAD PERIMETRAL Y PROTECCIÓN DEL ENDPOINT

ÍNDICE

1 OPCIONES DE IMPLEMENTACIÓN

NEXT GENERATION FIREWALLS

OPCIONES DE IMPLEMENTACIÓN

NEXT GENERATION FIREWALLS – **CLÚSTER HA**

Solución de firewall de nueva generación (NGFW) con funciones avanzadas de seguridad (**Threat Prevention**, **URL Filtering**, **Wildfire**, **DNS Security**, **GlobalProtect**, etc.) para implementar en clúster de alta disponibilidad (2 unidades en HA). Dos opciones distintas de implementación mediante appliances dedicados gestionados íntegramente por nuestro equipo técnico:

Modelo PA-850

Rendimiento del cortafuegos: 2,2/2,1 Gb/s
Rendimiento de Threat Prevention: 1,0/1,2 Gb/s
Rendimiento de VPN Ipsec: 1,7 Gb/s
Nuevas sesiones por segundo: 13.100
Número máximo de sesiones: 192.000
Puertos: 6x 10/100/1000; 4x SFP; 4x SFP+
Almacenamiento interno: 240GB SSD
Fuente de alimentación redundante

Modelo PA-460

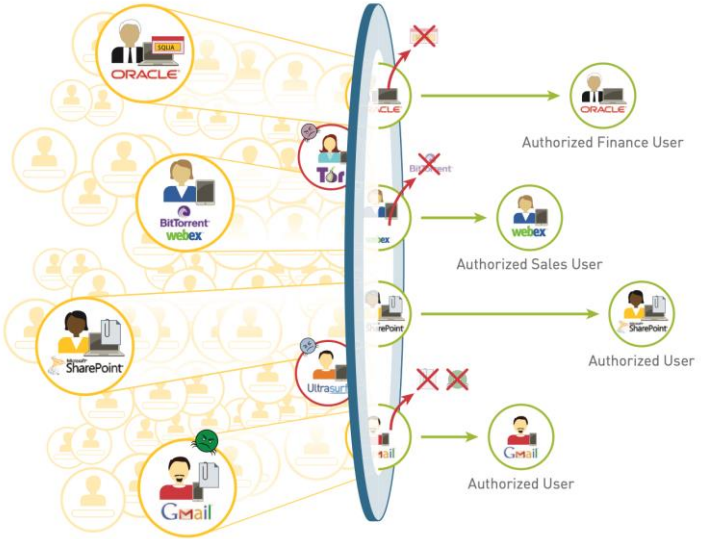
Rendimiento del cortafuegos: 5,2/4,7 Gb/s
Rendimiento de Threat Prevention: 2,4/2,6 Gb/s
Rendimiento de VPN Ipsec: 3,1 Gb/s
Nuevas sesiones por segundo: 74.000
Número máximo de sesiones: 400.000
Puertos: 8x 10/100/1000;
Almacenamiento interno: 128GB eMMC
Fuente de alimentación simple

2 SEGURIDAD PERIMETRAL

FUNCIONALIDADES AVANZADAS

SEGURIDAD PERIMETRAL

FUNCIONALIDADES AVANZADAS – **SEGURIDAD EN EL ACCESO DE USUARIOS Y APLICACIONES**



Control de Aplicaciones

Protección basada en identificación de aplicaciones analizando la comunicación, clasificándolas independientemente del puerto, protocolo, tipo de cifrado o la técnica utilizada para evitar la detección y poder aplicar reglas específicas de seguridad. A diferencia de los firewalls de capa 3/4, NGFW aplica directamente el control de aplicación junto con otros controles de Capa 7 como el control de usuarios.

Control de Usuarios

Vinculación de las aplicaciones con los usuarios, realizando la integración con grupos de directorios (como Active Directory y LDAP) para implementar políticas de protección coherentes por grupos de usuarios o usuarios particulares, independientemente de la ubicación del usuario o del dispositivo utilizado.

SEGURIDAD PERIMETRAL

FUNCIONALIDADES AVANZADAS – **SEGURIDAD EN LA NAVEGACIÓN & CONTROL EN EL ENVÍO Y RECEPCIÓN DE DATOS**

Inspección del trafico cifrado SSL / SSH

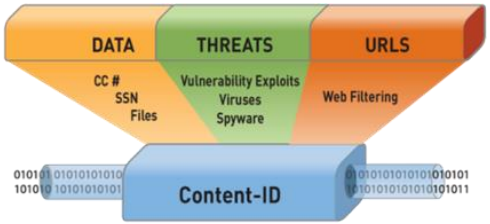
El uso de comunicaciones cifradas impide con métodos clásicos analizar el contenido de páginas y ficheros hasta que son descargados, y esto supone una ventaja para los desarrolladores de malware. Mediante la inspección del tráfico SSL/SSH, un sistema intermedio y confiable descifra el contenido y protege las comunicaciones cifradas incluso a nivel perimetral.

Control y filtrado en la navegación Web

Control de acceso a cualquier URL y aplicación de filtros basados en categorías personalizadas mantenidas por el usuario. Protege a los usuarios mediante la prevención automática de ataques basados en la web, incluidos los que utilizan phishing, C2 y kits de explotación. Las URL se clasifican en categorías benignas o maliciosas que puede incorporar fácilmente en la política de firewall para un control total del tráfico web.

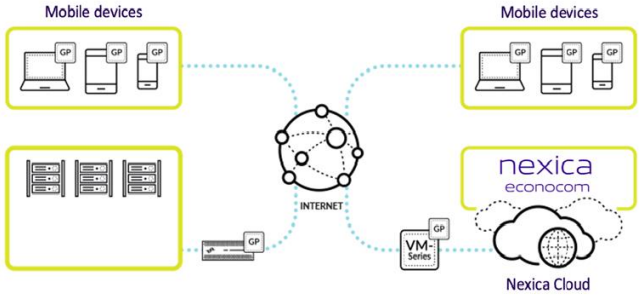
Control en el envío de datos confidenciales

incluidos los números de la tarjeta de crédito y Seguridad Social, revisando el contenido de la aplicación o los archivos adjuntos y sus metadatos. Controla la transferencia de archivos de cada aplicación lo que permite evitar transferencias de archivos o información entrante o saliente no deseado.



SEGURIDAD PERIMETRAL

FUNCIONALIDADES AVANZADAS – **SEGURIDAD EN LOS USUARIOS MÓVILES (GLOBALPROTECT)**



Acceso seguro tanto a aplicaciones empresariales internas como en la nube

desde equipos portátiles, tabletas y teléfonos inteligentes. Permite controlar el acceso y hacer cumplir las políticas para sitios web y aplicaciones, incluidas las aplicaciones SaaS.

Control de la configuración del equipo o dispositivo del usuario

Comprueba el dispositivo del usuario para obtener información de la configuración y crea un perfil que se comparte con el Firewall. El Firewall utiliza esta información para comprobar que cumple las políticas establecidas permitiendo solo el acceso cuando el dispositivo está configurado y protegido correctamente.

Métodos de autenticación

Admite los métodos de autenticación: Kerberos, RADIUS, LDAP, certificados de cliente, base de datos de usuarios local y **MFA (Multi-Factor Authentication)**. Una vez que GlobalProtect autentica al usuario, proporciona inmediatamente al Firewall una asignación de dirección de usuario <-> IP para que la utilice la tecnología User-ID.

Identificación de equipos o dispositivos peligrosos

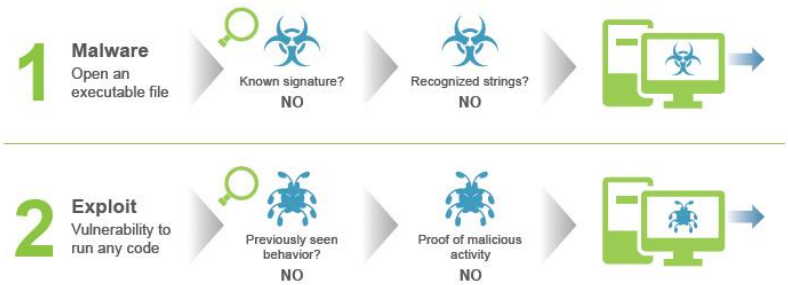
Refuerza la seguridad identificando equipos comprometidos y poniéndolos en cuarentena. Al realizar una comprobación de la configuración del dispositivo desde el que se realiza la conexión puede identificar posibles riesgos y restringir su acceso a la red, así como evitar que infecte a otros usuarios y dispositivos.

SEGURIDAD PERIMETRAL

FUNCIONALIDADES AVANZADAS – **THREAT PREVENTION**

Intrusion Prevention System (IPS)

Bloquea exploits de vulnerabilidades, desbordamientos de búfer, escaneos de puertos, bloqueo de paquetes no válidos o mal formados, desfragmentación de IP y reensamblaje de paquetes TCP. Las protecciones IPS se basan en la coincidencia de firmas y la detección de anomalías, con la capacidad de importar y aplicar automáticamente firmas y reglas. Las firmas basadas en vulnerabilidades se actualizan continuamente y protegen contra una variedad de exploits en segundos con inteligencia de amenazas del servicio de prevención de malware **WildFire**.



Anti-Malware

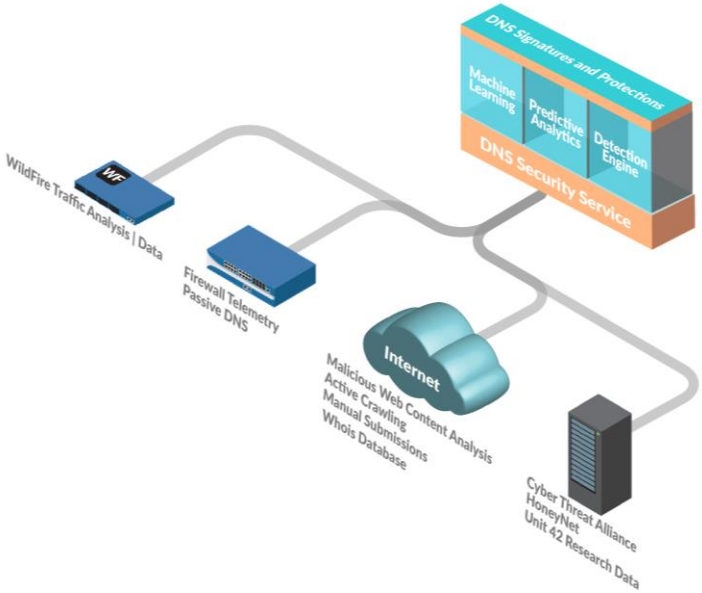
Sistema que bloquea en tiempo real, detectando malware conocido, así como variaciones desconocidas. IPS y antimalware abordan múltiples vectores de amenazas de manera combinada para garantizar la detección en todos los casos.

Anti-Spyware

Detiene las comunicaciones salientes maliciosas derivadas de infecciones de malware, analiza las consultas de DNS e identifica los patrones generados por bots. Esto detecta a los usuarios infectados, evita las descargas infecciosas y la fuga de datos de la organización.

SEGURIDAD PERIMETRAL

FUNCIONALIDADES AVANZADAS – **DNS SECURITY**



Detección y bloqueo de dominios maliciosos

Prevención automáticamente decenas de millones de dominios maliciosos identificados con análisis en tiempo real e inteligencia de amenazas global en continuo crecimiento. Puede predecir y detener dominios maliciosos y malware basado en algoritmos de generación de dominios. Protección ilimitada para dominios maliciosos con una base de datos basada en la nube siempre actualizada.

Bloqueo de túneles DNS

Emplea análisis de aprendizaje automático para detectar rápidamente C2 o el robo de datos mediante el uso de túneles de DNS.

Inteligencia frente a las amenazas sobre DNS

Proporciona una visión de las amenazas a través de los informes, aportando una visibilidad completa del tráfico de DNS. Las capacidades de análisis de DNS permiten optimizar la seguridad, diseñar políticas y remediar rápidamente los eventos de seguridad.

SEGURIDAD PERIMETRAL

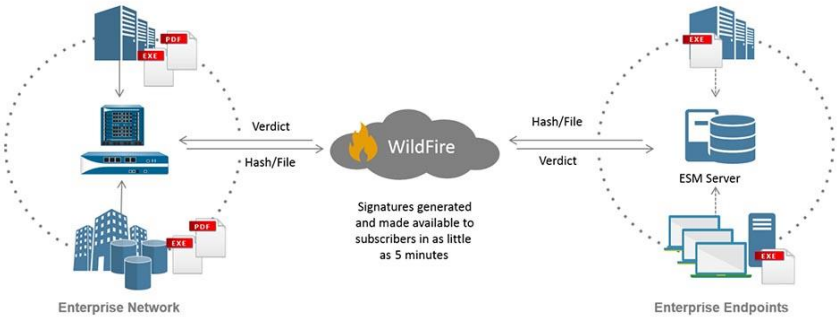
FUNCIONALIDADES AVANZADAS – **WILDFIRE SERVICE**

Detección y protección contra amenazas desconocidas

Servicio ofrecido desde la nube de Palo Alto que identifica amenazas desconocidas gracias a los datos compartidos de la comunidad de análisis de malware empresarial que incluye amenazas enviadas desde redes, terminales, nubes y clientes. WildFire utiliza motores de análisis como el aprendizaje automático para detener los ataques avanzados de amenazas desconocidas.

Prevención en línea basado en aprendizaje automático

Incluye un motor en línea basado en aprendizaje automático impulsado por modelos de amenazas continuamente perfeccionados en la nube. Esta capacidad sin firma evita el contenido malicioso (por ejemplo, archivos ejecutables portátiles y ataques peligrosos sin archivos derivados de PowerShell) completamente en línea.



Análisis de comportamiento de archivos

Análisis de comportamiento que ayuda a comprender cómo funciona el malware recién descubierto. Los registros permiten identificar rápidamente a los usuarios infectados e investigar posibles infracciones con visibilidad de los eventos de amenazas desconocidas.

Ejecución integral de archivos sospechosos

Ejecuta en la nube los archivos sospechosos utilizando múltiples versiones de aplicaciones y sistemas operativos simultáneamente para comprender completamente el alcance de una amenaza. Este sistema evita que un archivo malicioso pueda considerarse benigno simplemente porque el sistema operativo de destino o la versión de la aplicación no se especificaron en la imagen dorada.

FIREWALL PERIMETRAL

FUNCIONALIDADES AVANZADAS – **COMPARATIVA CISCO FIREPOWER VS. PALO ALTO NGFW**

Palo Alto	Cisco	Comentario
Next-Generation Firewall	Firepower Threat Defense Meraki MX IOS Zone-Based Firewall	Todas las opciones de Cisco están totalmente desconectadas y ninguna se acerca a las capacidades y la seguridad de Palo Alto Networks.
App-ID	OpenAppID (for FTD) NBAR/NBAR2 (for IOS) Stealthwatch App Detector Meraki App Detector	Con Cisco, la aplicación identificada depende del dispositivo, sin una única fuente de verdad.
Threat Prevention	IPS (Snort engine)	Con Palo Alto se pueden manejar firmas de Snort e ir más allá de Cisco al tener automatización y API.
WildFire	Advanced Malware Protection (AMP)	AMP también está en EndPoint, correo electrónico, web, etc .; todos escanean el tráfico de forma diferente; ninguna fuente unificada.
URL Filtering	SenderBase (Umbrella) BrightCloud (Meraki) BrightCloud (FTD 6.4 and below) Talos (FTD 6.5 and above)	Cisco utiliza una combinación de dos bases de datos diferentes, sin una única fuente de verdad.

Característica	Palo Alto	Cisco
Machine-Learning inline NGFW	Si	No
Rendimiento predecible con todas las firmas de prevención de amenazas gracias a la arquitectura de Single-Pass	Si	No
Envío automático de todos los tipos de archivos admitidos para el análisis de malware	Si	No
Soporte de sistema operativo para análisis de malware	Windows, Linux, macOS, Android	Windows
Bare metal malware analysis	Si	No
Multi-factor Authentication	Si	No
Capacidades SD-WAN	Si	No

3 SEGURIDAD EN LOS ENDPOINT

CORTEX XDR

CORTEX™
BY PALO ALTO NETWORKS

SEGURIDAD EN LOS ENDPOINT

CORTEX XDR

La seguridad en los sistemas se enfrenta a una enorme variedad de amenazas, desde ransomware, ciberespionaje, ataques dirigidos y robo de información. Sin embargo, el mayor problema para el equipo de seguridad son las tareas repetitivas que deben realizar todos los días clasificando incidentes e intentando reducir un sinfín de alertas pendientes.

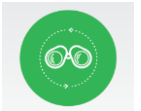
Cortex XDR aporta la ayuda necesaria para eliminar amenazas y simplificar las operaciones.

Threat Prevention

La prevención avanzada permite detener más del 99% de los ataques en tiempo real sin necesidad de verificación manual. Aporta una prevención coherente y coordinada en todos los sistemas y dispositivos.

IA y aprendizaje automático

La creciente cantidad de datos que se deben recopilar necesita de un aprendizaje y análisis automático para conocer las características de la organización, estableciendo unos patrones del comportamiento esperado para así poder detectar ataques avanzados.



Automatización

Para realizar una análisis y confirmar rápidamente un ataque, se necesitan alertas procesables con detalles de investigación aplicando comprensión para conocer fácilmente el origen de los ataques y que apliquen medida de manera automática.

SEGURIDAD EN LOS ENDPOINT

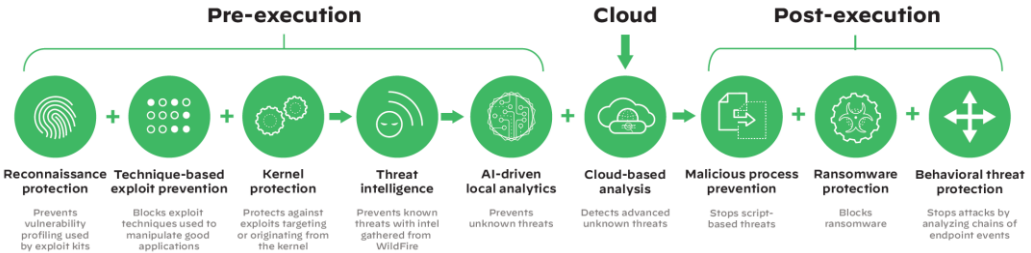
CORTEX XDR – **FUNCIONES DE PROTECCIÓN DEL ENDPOINT**

Administración segura de dispositivos USB

✓ El módulo de control de dispositivos incluido **permite proteger el acceso USB sin necesidad de instalar otro agente**. Se pueden asignar políticas basadas en el grupo de Active Directory y Unidad Organizativa, restringir el uso por tipo de dispositivo y asignar excepciones de política de solo lectura / escritura, por producto y por número de serie.

Protección de los datos del equipo mediante el firewall integrado y el cifrado de disco

✓ El firewall integrado en Cortex XDR **permite controlar las comunicaciones entrantes y salientes** en los equipos con Windows o macOS. Además, puede aplicar **cifrado BitLocker o FileVault en su EndPoint** mediante la creación de políticas y reglas de cifrado de disco.



Evita amenazas conocidas y desconocidas con una visibilidad completa

✓ **Detención de exploits, malware, ransomware y ataques sin archivos**. Impacto mínimo en el EndPoint; el agente Cortex XDR liviano bloquea los ataques y, al mismo tiempo, recopila datos de eventos.

✓ Conjunto de módulos de protección para **bloquear vulnerabilidades que conducen a infección de malware**: *Cada archivo es examinado por un motor de análisis local adaptable **impulsado por una IA** que siempre está aprendiendo a contrarrestar nuevas técnicas de ataque.*

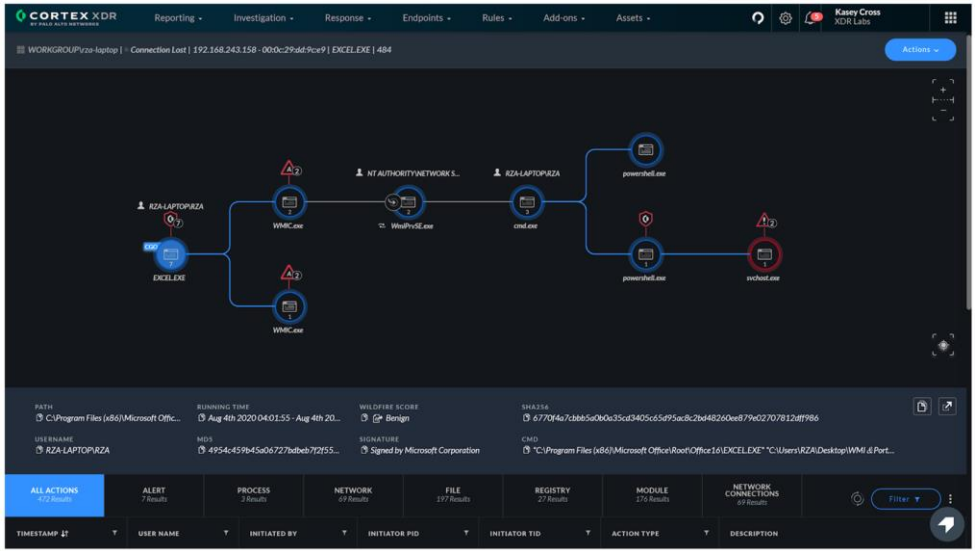
✓ **Integración con el servicio de prevención de malware WildFire** para analizar archivos sospechosos en la nube y coordinar la protección en todos los productos de seguridad.

✓ **Aislamiento del equipo de la red**, cuarentena, interrupción de procesos, eliminación de archivos, y lista negra de archivos.

✓ **Protección** frente al robo de credenciales.

✓ **Live Terminal** para conectarse directamente al equipo infectado.

SEGURIDAD EN LOS ENDPOINT
CORTEX XDR – **ANÁLISIS DE EVENTOS**

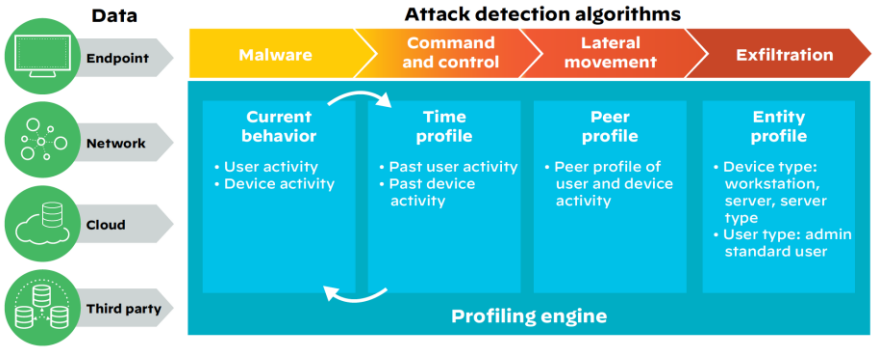


Análisis del origen del ataque o infección: El motor revisa continuamente miles de millones de eventos para identificar la cadena de eventos detrás de cada amenaza. Visualiza la secuencia del ataque hasta la causa raíz y proporciona detalles esenciales sobre cada elemento de la secuencia, lo que hace que los ataques complejos sean fáciles de entender. Permite ver instantáneamente qué procesos fueron responsables de las alertas de seguridad de la red o la nube.

Análisis de la línea de tiempo: una línea de tiempo forense de toda la actividad de ataque proporciona detalles procesables para las investigaciones de incidentes, lo que permite determinar el alcance, el impacto y los próximos pasos en segundos. Las alertas informativas mejoran el análisis de la línea de tiempo al identificar comportamientos sospechosos y hacer que los eventos complejos sean fáciles de entender.

SEGURIDAD EN LOS ENDPOINT

CORTEX XDR – **DESCUBRIMIENTO DE AMENAZAS EVASIVAS CON REGLAS PERSONALIZADAS**



Mediante el uso de reglas personalizas se puede identificar amenazas exclusivas de su entorno, permitiendo activar alertas contra IOCs (*Indicadores de Compromisos*) conocidas y detectar también combinaciones complejas de comportamientos para exponer tácticas, técnicas y procedimientos (TTP) de atacantes específicos.

Como resultado, permite cerrar brechas de seguridad y obtener visibilidad de la actividad potencialmente maliciosa. Las reglas personalizadas pueden identificar el uso indebido de sistemas y aplicaciones, así como detectar ataques de día cero que frustran las técnicas de evasión, lo que garantiza que pueda descubrir amenazas incluso si un adversario manipula nombres de malware, hashes o direcciones IP.

El equipo de seguridad puede definir reglas basadas en docenas de parámetros diferentes, incluida información de proceso, archivo, red o registro. Más de 200 reglas predefinidas detectan una amplia gama de amenazas listas para usar, incluida la persistencia, la manipulación, la escalada de privilegios y el movimiento lateral.

SEGURIDAD EN LOS ENDPOINT

CORTEX XDR – **DATOS INSPECCIONADOS POR CORTEX XDR**

Cortex XDR analiza metadatos a nivel de protocolo en registros de tráfico, registros de aplicaciones, registros de amenazas recopilados por los firewalls, datos de los EndPoint Cortex XDR y datos de terceros. Al crear un perfil basado en cientos de dimensiones de comportamiento, incluida la frecuencia de las conexiones, la fuente y el destino del tráfico, y los protocolos utilizados, Cortex XDR puede conocer el comportamiento esperado de los usuarios y dispositivos.

Datos a nivel de sesión

- ✓ IP origen, IP destino, puerto origen y puerto destino
- ✓ Bytes enviados y recibidos
- ✓ Duración de la conexión
- ✓ Registros de aplicaciones con datos a nivel de transacción en DNS, HTTP, DHCP, RPC, ARP, ICMP, etc..
- ✓ Detalles de la aplicación con la tecnología de App-ID

Datos del usuario

- ✓ Usuario que inició sesión
- ✓ Usuario típico de una máquina
- ✓ Usuario que crea el proceso que inició la comunicación
- ✓ Grupo de usuarios y unidad organizativa del Directorio
- ✓ Eventos de autenticación de registros de eventos de Okta, Azure Active Directory, PingOne, PingFederate, Kerberos y Windows

Datos en la nube

- ✓ Prisma Access y VM-Series
- ✓ Google Cloud y Google Kubernetes® Engine
- ✓ Amazon CloudWatch y AWS CloudTrail

Datos del EndPoint

- ✓ Creación, eliminación y actualización de archivos
- ✓ Archivo hash
- ✓ Ruta de archivo
- ✓ Nombre del proceso
- ✓ Cambio de registro
- ✓ Argumentos CLI, llamadas RPC e inyección de código
- ✓ Eventos de hardware, como USB
- ✓ Manipulación del registro de eventos
- ✓ Alertas de seguridad del agente Cortex XDR
- ✓ Veredicto de malware WildFire

Datos del host

- ✓ Nombre de host
- ✓ Dirección MAC
- ✓ Sistema operativo

SEGURIDAD EN LOS ENDPOINT

CORTEX XDR – **FUNCIONES Y CAPACIDADES DE DETECCIÓN E INVESTIGACIÓN**

Funciones y capacidades	
✓ Agrupación automatizada de datos de la red, el endpoint y la nube procedentes de Palo Alto Networks y de terceros	✓ Análisis de comportamiento basado en aprendizaje automático
✓ Procesamiento de alertas y logs de terceros de cualquier origen con la información de red necesaria	✓ Reglas personalizadas para detectar tácticas, técnicas y procedimientos
✓ Datos de logs de terceros desde cortafuegos Check Point, Fortinet y Cisco ASA	✓ Análisis de la causa original de las alertas
✓ Prevención de malware basada en la nube con WildFire	✓ Análisis de la cronología de las alertas
✓ Detección de ataques de malware y sin archivos	✓ Motor de incidentes unificado
✓ Detección de ataques dirigidos, personal interno malicioso y comportamientos peligrosos de los usuarios	✓ Análisis de repercusión posterior a los incidentes
✓ Análisis del tráfico de red (NTA) y análisis de comporta miento de usuarios (UBA)	✓ Paneles y elaboración de informes
✓ Detección y respuesta en el endpoint (EDR)	✓ Búsqueda de indicadores de riesgo e inteligencia sobre amenazas
✓ Integración nativa con Cortex XSOAR para la orquestación, la automatización y la respuesta	✓ Búsqueda de amenazas
✓ Servicio Managed Threat Hunting de Cortex XDR	✓ Respuesta a incidentes y recuperación

SEGURIDAD EN LOS ENDPOINT

COMPARATIVA ENTRE CORTEX XDR PREVENT Y XDR PRO

Feature	Cortex XDR Prevent	Cortex XDR Pro per Endpoint	Cortex XDR Pro per TB
Log storage	• Minimum of 200 endpoints • 30 day log retention	• Minimum of 200 endpoints • 30 day log retention	Minimum 5TB log storage
Cortex XDR Add-on Licenses Add-on licenses are required on top of a Cortex XDR license			
Host Insights, including: • Host Inventory • Vulnerability Assessment • File Search and Destroy	–	✓ Without the add-on license, Host Insights is available with Cortex XDR Pro per Endpoint for a 1-month trial period.	–
Endpoint Prevention Features			
Endpoint management	✓	✓	–
Device control	✓	✓	–
Host firewall	✓	✓	–
Disk encryption	✓	✓	–
Response Actions			
Live Terminal	✓	✓	–
Endpoint isolation	✓	✓	–
External dynamic list (EDL)	–	✓	✓
Script execution	–	✓	–
Remediation analysis	–	✓	–
Incident Scoring Rules	–	✓	✓
Featured Alert Fields	–	✓	✓
Widget Library	–	✓	✓

Feature	Cortex XDR Prevent	Cortex XDR Pro per Endpoint	Cortex XDR Pro per TB
Analysis			
Analytics	–	✓	✓
Alert and Log Ingestion			
Cortex XDR agent alerts	✓	✓	–
Enhanced data collection for EDR and other Pro features	–	✓	–
Other alerts (from Palo Alto Networks and third-party sources)	–	✓ (API)	✓
Other logs (from Palo Alto Networks and third-party sources)	–	–	✓
Integrations			
Threat intelligence (AutoFocus, VirusTotal)	✓	✓	✓
Outbound integration and notification	✓ + agent audit logs	✓ + agent audit logs	✓

Feature	Cortex XDR Prevent	Cortex XDR Pro per Endpoint	Cortex XDR Pro per TB
forwarding (Slack, Syslog)			
Broker VM			
Agent Proxy	✓	✓	✓
Syslog Collector			✓
Network Mapper		✓	✓
Pathfinder		✓	✓
Windows Event Collector			✓
MSSP			
MSSP (requires additional MSSP license)	✓	✓	✓
Managed Threat Hunting (requires an additional Managed Threat Hunting License)	–	✓ + a minimum of 500 endpoints	–

SEGURIDAD EN LOS ENDPOINT

CORTEX XDR – **SISTEMAS OPERATIVOS SOPORTADOS**

Sistema Operativo	Versión / Distribución
Windows	7, 8.1, 10, Server 2008 R2 SP1, Server 2012, Server 2016, Server 2019
Linux	CentOS 6 / 7 / 8, Debian 8 / 9 / 10, OpenSuse Leap 15.1, Oracle 6 / 7 / 8, Read Hat Enterprise 6 / 7 / 8, Suse Linux Enterprise 11 SP4 / 12 / 15 SPO / 15 SP1 / 15 SP2, Ubuntu Server 12 / 14 / 16 / 18 / 20
Mac	OS X 10.13 / 10.14 / 10.15 / 11.0
Android	6 / 7 / 8 / 9 / 10

https://docs.paloaltonetworks.com/compatibility-matrix/cortex-xdr/where-can-i-install-the-cortex-xdr-agent.html

4 SERVICIOS DE SEGURIDAD

GESTIÓN DE LA DISPONIBILIDAD Y LA CONFIGURACIÓN

nexica Services

SERVICIOS DE SEGURIDAD

FIREWALL PERIMETRAL - **GESTIÓN DE LA DISPONIBILIDAD Y LA CONFIGURACION**

1. Gestión de políticas

Gestión de las **políticas en base a la aplicaciones utilizadas y detección del uso de nuevas aplicaciones** por parte de los usuarios. En base a la monitorización e informes mensuales, se crearán las políticas para securizar las nuevas aplicaciones que puedan aparecer.

2. Gestión de usuarios

Creación y mantenimiento de los **grupos de usuarios para poder obtener una seguridad granular** para cada departamento o grupo, pudiendo establecer a que redes, aplicaciones y navegación Web deben poder acceder.

3. Control de la navegación web

Gestión de la navegación Web utilizando las herramientas de URL **Filtering y DNS Security** para asegurar que la navegación de los usuarios es confiable y evitar infecciones desde sitios maliciosos.

4. VPN Mobile y VPN Site-to-Site

Gestión de los **requerimientos de acceso mediante Global Protect para los equipos de usuarios** cumpliendo con unos mínimos de versiones de sistema operativo, antivirus y configuración para confirmar la seguridad local del usuario. Creación de las VPN necesarias para la interconexión con sedes del cliente y aplicación de las políticas para restringir el acceso únicamente a los servicios internos requeridos.

5. Gestión del IPS

Configuración y mantenimiento del servicio IPS para comprobar la correcta actualización de firmas, así como la comprobación de su aplicación en el acceso a las aplicaciones internas.

6. Gestión del Anti-Malware

Comprobación de las actualizaciones y las alertas generadas sobre infecciones detectadas y realizar las actuaciones y cambios necesarios para proteger los servicios que hayan sido sensibles de ser atacados.

7. Gestión de Logs

Todos los logs recibidos de los Firewalls **son almacenados durante un periodo de 6 meses** para poder analizar una situación de ataque, realizando un **estudio en el tiempo** sobre todo lo sucedido en los últimos días, semanas o meses.

8. Generación de informes

Informes **mensuales** de las **aplicaciones mas utilizadas**, usuarios, navegación y con **recomendaciones de seguridad en base al trafico detectado**. Se realizará un control de las nuevas aplicaciones que han aparecido para determinar si se tiene que permitir el acceso y en caso afirmativo, establecer que funciones de dichas aplicaciones se deben permitir.

SERVICIOS DE SEGURIDAD

ENDPOINT CORTEX XDR - **GESTIÓN DE LA DISPONIBILIDAD Y LA CONFIGURACION**

Gestión

- ✓ **Verificación diaria de que los servidores reciben las actualizaciones de seguridad**. En caso de no ser así, se tratará automáticamente desde soporte para realizar las acciones pertinentes sobre el servidor. En caso de ser necesario un reinicio del servicio, se consensuará con el cliente el horario adecuado para realizarlo.
- ✓ **Envío de reporte diario con los equipos y dispositivos de usuario que no se han actualizado** para que el cliente tenga constancia de los equipos que no se mantienen conectados a la plataforma Cortex XDR y que no reciben por tanto las actualizaciones de seguridad.
- ✓ Envío de **informe mensual con las detecciones registradas y el estado de la plataforma a nivel de actualizaciones** tanto de servidores como de equipos de usuarios.
- ✓ **Registro de alertas** (*hasta 30 días*)

Soporte 24x7 ante alertas

- ✓ Se considerará una alerta todo incidente referente a una **infección** sobre cualquier de los **servidores virtuales** que puedan poner en riesgo la continuidad del negocio de la empresa y que **requieran asistencia por parte del personal técnico**.

Se atenderán las incidencias que estén dentro del siguiente alcance:

Infección

La infección de cualquiera de los servidores virtuales de la plataforma del cliente que haya sido detectada por Cortex XDR y que no haya podido eliminar de manera automática o, que requiera reinicio del servidor para que Cortex XDR pueda aplicar las acciones de remediación necesarias.

Problemas derivados de la instalación del agente Cortex XDR

Se consideran problemas derivados de la instalación del producto cuando el agente provoque alguna afectación en el funcionamiento o rendimiento del servicio.

5 SERVICIOS DE SEGURIDAD

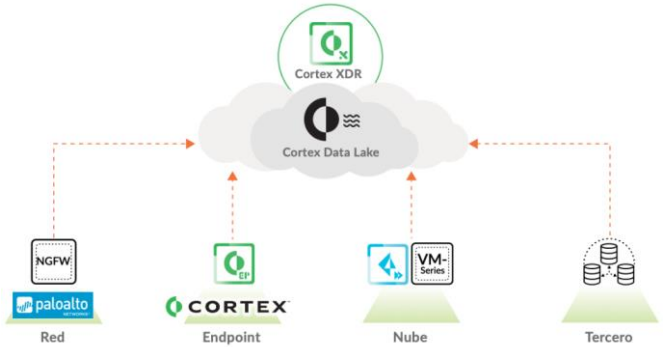
GESTIÓN DE LA SEGURIDAD

nexica Services

SERVICIOS DE SEGURIDAD

ENDPOINT CORTEX XDR - **GESTIÓN DE LA SEGURIDAD**

El agente **Cortex XDR PRO** y la solución **Cortex Data Lake** nos permite disponer de un análisis de datos sea cual sea su procedencia, ofreciendo una visibilidad mas amplia para una mejor detección y aplicando inteligencia en la cadena de eventos o cadena de causalidad. El **envio de eventos desde la seguridad perimetral y los dispositivos permite correlar la información para poder averiguar el origen y cronograma de una amenaza**.



Funcionalidades y Servicios

- ✓ **Investigación y análisis de alertas de seguridad procedentes del Firewall y en los EndPoint** utilizando la herramienta Cortex XDR y XDR Data Lake, que aportan una visión de conjunto y permiten obtener una trazabilidad completa del ataque o infección.
- ✓ Definición de las **acciones de remediación** y **realización de los procedimientos de resolución** para el personal de soporte 24x7. (*No se incluye en el servicio la resolución de incidencias, este servicio se realizará contra bolsa de horas*).
- ✓ Envío de **informe mensual con las alertas registradas y las acciones de remediación.**
- ✓ **Gestión de reglas IOC** (*Indicators of Compromise*) y **BIOC** (*Behavioral Based Indicators of Compromise*) para detectar comportamientos anómalos con acciones de remediación automáticas, permitiendo ser más rápidos en la resolución de un incidente.
- ✓ **Sincronización de Cortex XDR con Active Directory** para tener visibilidad por usuarios y grupos en el análisis e investigación de amenazas.
- ✓ **Monitorización** de las conexiones de usuario mediante **GlobalProtect**.

6 PROPUESTA ECONÓMICA

INFRAESTRUCTURA Y SERVICIOS PROFESIONALES

Consorci Administració Oberta de Catalunya

PROPUESTA ECONÓMICA - CONCEPTOS PAGO ÚNICO

Elementos de Infraestructura – Firewall Perimetral

Dos opciones:
1.- Bundle Firewalls PA-850
2.- Bundle Firewalls PA-460

Descripció equipament	Qt	Preu Unitari	Preu Total
Palo Alto, model PA850, que inclou:	**2**	6.942,94	**13.885,88**
Threat prevention subscription	**2**	2.510,59	**5.021,18**
WildFire subscription	**2**	2.510,59	**5.021,18**
Advanced URL Filtering	**2**	3.765,88	**7.531,76**
Premium support 2 years	**2**	4.016,94	**8.033,88**
Palo Alto, model PA460, que inclou:	**2**	4.021,60	**8.043,20**
Professional Subscription Bundle (Threat Prevention, Advanced URL Filtering, Wildfire, DNS Security	**2**	3.090,35	**6.180,71**
Premium support 2 years	**2**	1.718,59	**3.437,18**

Condiciones de la Oferta

- ✓ Los bundles indicados incluyen las subscripciones de seguridad “Threat Prevention”, “Wildfire”, “URL Filtering” y “GlobalProtect” por periodo de 2 años
- ✓ Los bundles indicados incluyen los soportes de fabricante “Premium Support” por periodo de 2 años.
- ✓ En caso de requerir ampliaciones o subscripciones de seguridad adicionales durante el periodo de contrato éstas estarán sujetas a un precio adicional
- ✓ Los precios indicados se facturarán en único pago al inicio del contrato
- ✓ Los precios indicados no incluyen IVA

PROPUESTA ECONÓMICA - CONCEPTOS PAGO RECURRENTE MENSUAL

Servicio Gestion de la Disponibilidad y la Configuración – Firewall Perimetral

Descripción – Servicios gestionados para Firewalls perimetrales	Cuota Unitaria	Unidades	Total Mensual
Servicio Gestión de la Disponibilidad y la Configuración (PA-850 o PA-460)	175,00 €	2	**350,00 €**
TOTAL			**350,00 €**

Condiciones de la Oferta

- ✓ Actividades descritas y especificadas en Apartado 4 (SERVICIOS DE SEGURIDAD – Firewall Perimetral. Gestión de la Disponibilidad y la Configuración)
- ✓ Los precios indicados se facturarán mensualmente durante el contrato del servicio
- ✓ Los precios indicados no incluyen IVA

PROPUESTA ECONÓMICA - SETUP IMPLANTACIÓN

Configuración y Puesta en Marcha – Firewall Perimetral

Descripción – Implantación y puesta en marcha del servicio	Coste	Cantidad	Total
Implantación solución Firewalls (PA-850 o PA-460) en Datacenter Nexica	2.643,75 €	1	**2.643,75 €**
TOTAL			**2.643,75 €**

Listado de tareas (ejecución en horario laboral: L a V de 9:00h a 18:00h)

- Instalación en clúster de los firewalls Palo Alto (unidades PA-850 o bien PA-460), incluyendo pruebas de fail-over y alta disponibilidad.
- Traspasar y adaptar configuración desde los Cisco ASA5516 a los Palo Alto (traspaso de reglas, políticas de red, usuarios locales, etc.)
- Realizar configuración de funcionalidades avanzadas:
    - Configuración de conexiones para usuarios en movilidad e integración mediante GlobalProtect
    - Configuración IPS/IDS con nivel de sensibilidad baja (para no provocar inicialmente falsos positivos)
    - Configuración servicios Antimalware (modo alert)
    - Configuración funcionalidades Threat Prevention (modo alert)
    - Configuración de filtros URL y DNS (modo alert)
    - Implementación de políticas anti-DDoS
- Configuración envío de alertas de antimalware y Threat Prevention al equipo de soporte de Nexica

Condiciones de la Oferta

- ✓ Servicios de implantación valorados exclusivamente para los firewalls en HA. La implantación de agentes Cortex XDR deberá contratarse a parte una vez se haya definido la modalidad y el alcance deseado.
- ✓ Los precios indicados se facturarán en único pago al inicio del contrato
- ✓ Los precios indicados no incluyen IVA

PROPUESTA ECONÓMICA - SERVICIOS OPCIONALES CORTEX XDR

Elementos de Infraestructura - Agentes Cortex XDR

Dos opciones:
1.- Cortex XDR Prevent
2.- Cortex XDR PRO + Data Lake (para la integración de logs con los Firewalls Perimetrales de Palo Alto)

Descripció equipament	Qt	Preu Unitari	Preu Total
Cortex XDR Prevent, includes 30 days of alerts retention and standard success	**220**	51,76	**11.387,20**
Cortex XDR Pro for 1 endpoint, includes 30 days of data retention and standard success	**220**	81,53	**17.936,60**
Cortex XDR Pro for 1 TB, includes 1TB of Cortex Data Lake and standard success	**5**	11.388,24	**56.941,18**

Condiciones de la Oferta

- ✓ Los agentes Cortex XDR incluyen suscripción a los servicios de Palo Alto por periodo de 2 años
- ✓ Los agentes Cortex XDR incluyen por defecto 30 días de retención de logs. Para ampliar dicho periodo deberá contratarse espacio adicional en Data Lake.
- ✓ En caso de requerir ampliaciones o subscripciones de seguridad adicionales durante el periodo de contrato éstas estarán sujetas a un precio adicional
- ✓ Los precios indicados se facturarán en único pago al inicio del contrato
- ✓ Los precios indicados no incluyen IVA

PROPUESTA ECONÓMICA - SERVICIOS OPCIONALES CORTEX XDR

Servicio Gestion de la Disponibilidad y la Configuración – Agentes Cortex XDR

Descripción – Servicios gestionados para Endpoints Cortex XDR	Cuota Unitaria	Unidades	Total Mensual
Servicio Gestión de la Disponibilidad y la Configuración (Cortex XDR)	812,50 €	1	**812,50 €**
TOTAL			**812,50 €**

Condiciones de la Oferta

- ✓ Actividades descritas y especificadas en Apartado 4 (SERVICIOS DE SEGURIDAD – Endpoint Cortex XDR. Gestión de la Disponibilidad y la Configuración)
- ✓ Los precios indicados se facturarán mensualmente durante el contrato del servicio
- ✓ Los precios indicados no incluyen IVA

Aprende a volar con nosotros

Algunos ya lo han hecho y están encantados de poder dedicarse a su negocio.

Contacta con nosotros y un equipo de asesores analizará tu situación sin ningún tipo de compromiso.

hola@nexica.com

900
800
296