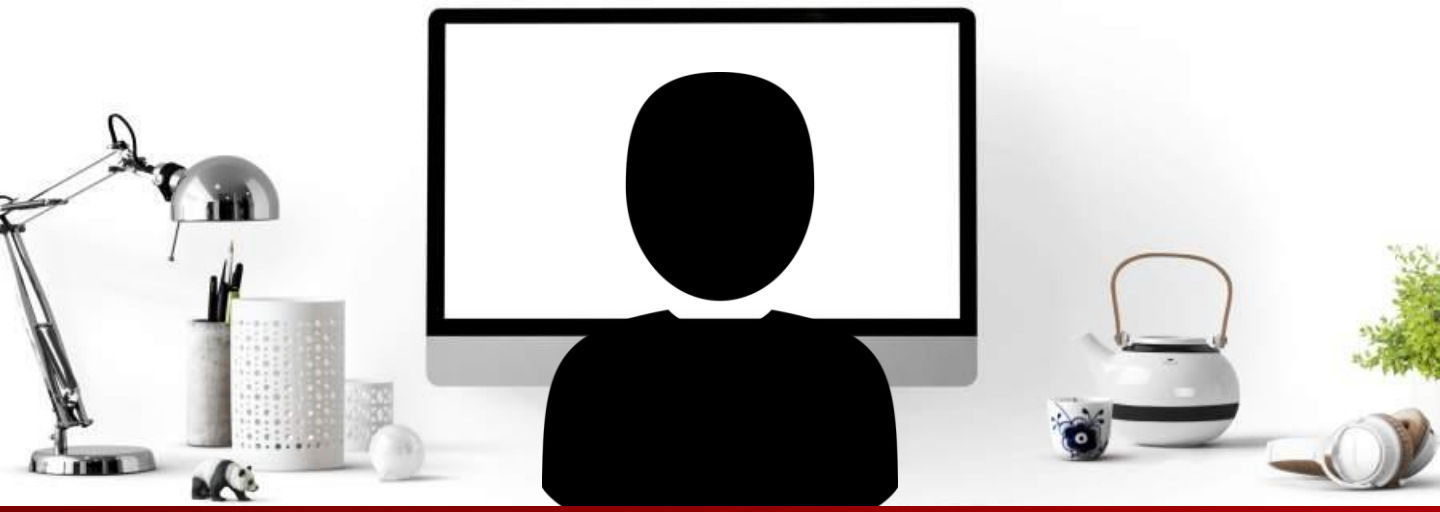
SISAP
Sistemas Aplicativos

/Sisap | @Sisap_Latam | @Sisap_Latam | /Sisap

Guatemala · El Salvador · Honduras · Nicaragua · Costa Rica · Panamá · República Dominicana



Home Office Security

Endpoint Protection

Endpoint Monitoring

Endpoint Support

SOPHOS INTERCEPT X

novacoast novaSOC

SISAP
Sistemas Aplicativos

Teletrabajo & BYOD
Una ventaja y una problemática

El teletrabajo se ha convertido en el principal reto de las organizaciones cuando se hace necesario habilitar a los usuarios, accesos a los recursos de la empresa para mantener la continuidad del negocio. Sin embargo, esto puede representar una amenaza a la seguridad de la información.

De acuerdo a NIST (National Institute for Standards and Technology) en la publicación especial de 800-46r2 sobre la seguridad en el teletrabajo menciona:

'Todos los componentes de teletrabajo […], incluidos los dispositivos desde los cuales se conectan los usuarios deberán ser asegurados contra amenazas esperadas, tomando en cuenta que entre las mayores preocupaciones de seguridad están: el uso de redes inseguras, conexión de dispositivos infectados en las redes usadas para el teletrabajo y todo esto representando una amenaza a los recursos de la organización que son accedidos desde los dispositivos de los usuarios en su hogar o bien desde otras localidades.'

Amenazas del entorno de teletrabajo & BYOD

Dentro de las principales amenazas en el entorno del Teletrabajo encontramos las siguientes:

- **Virus:** Diseñado para esparcirse de host a host y con la habilidad de replicarse. Representa una amenaza común cuando se le da acceso a los recursos de la organización a empleados que utilizarán su propia computadora para trabajar en forma remota.

- **Malware:** Software malicioso diseñado para ganar acceso a la computadora sin conocimiento del usuario. Si esta computadora tiene acceso a recursos de la empresa en forma remota, esto podría ser fácilmente explotable para comprometer datos de la organización.

- **Exploits:** Son utilizados para comprometer la integridad, disponibilidad y confidencialidad de los servicios.

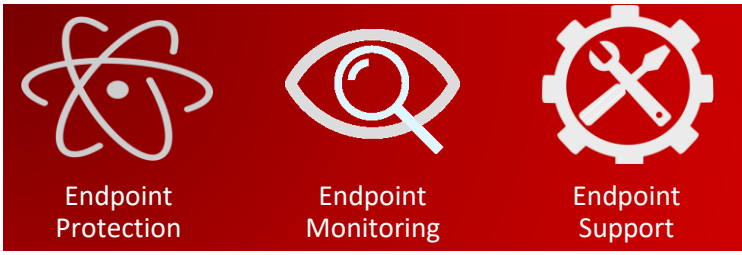
- **Ransomware:** Son programas maliciosos diseñados para secuestrar los datos del usuario. Cuando se permite el teletrabajo desde dispositivos que no necesariamente son de la empresa, existe una gran probabilidad que datos sensibles de la organización residan en estos y este tipo de amenazas también podría afectar la seguridad de la información sensible.

- **Falta de control y visibilidad:** Teniendo una cantidad considerable de dispositivos conectados desde distintas redes que no pertenecen a la empresa, se vuelve una tarea casi imposible controlar la seguridad de estos y además, contar con la visibilidad necesaria para anticipar incidentes de ciberseguridad.

Seguridad para el teletrabajo y BYOD

Componentes de nuestra solución

- Sophos Intercept X Advanced
- Sophos Central
- NovaSOC Endpoint
- SISAP Security Operation Center



Sophos Intercept X Advanced

Utiliza un completo enfoque de defensa exhaustiva a la protección para endpoints, en lugar de simplemente depender de una técnica de seguridad principal. Hace una combinación de técnicas base (tradicionales) y modernas (next-generation) con el objetivo de proteger contra virus, malware y exploits.

NovaSOC Endpoint

Es una herramienta para monitoreo, alerta y respuesta en el endpoint que provee de información relevante a los analistas de SOC que están monitorizándola. Entre sus características están:

- ***Endpoint Monitoring*** permite detectar vulnerabilidades conocidas y actividad sospechosa.
- ***Automated Incident Reporting*** sube bitácoras en forma instantánea a la nube, permitiendo la remediación rápida por parte de los analistas del SOC.
- ***Detailed Analytics*** provee reportes de incidentes, identifica debilidades, mejora los tiempos de respuesta y el flujo de trabajo desde un portal y tablero de control.
- ***Non-invasive*** usa un proceso en segundo plano, fácil de integrar con los servicios existentes.
- ***100% Inspection*** de los archivos y del tráfico.

Sophos Central para Control y Visibilidad

Intercept X está integrado en Sophos Central, es una consola basada en la nube para gestionar los productos de Sophos. No hay que preparar servidores; basta con iniciar sesión para descargar el agente y configurar todas sus políticas desde un único sitio.

SISAP Security Operation Center

SISAP cuenta con un SOC que se encarga del monitoreo y gestión de las herramientas de seguridad para garantizar vigilancia, detección y respuesta ante eventos de ciberseguridad.

- ***Monitoreo 24x7x365*** con tres niveles de analistas cubriendo de monitoreo para detectar eventos, incidentes y reaccionar a alertas de ciberseguridad.
- ***Gestión de seguridad*** permite descansar en la experiencia de los analistas de SISAP para altas, bajas y/o cambios en configuraciones que permiten mantener afinada la solución para que esta funcione de forma correcta.
- ***Soporte*** provee asistencia ante eventos de ciberseguridad o bien, sobre las soluciones implementadas en el endpoint para asegurar que estos están protegidos siempre.