VECTOR
CYBERSECURITY.

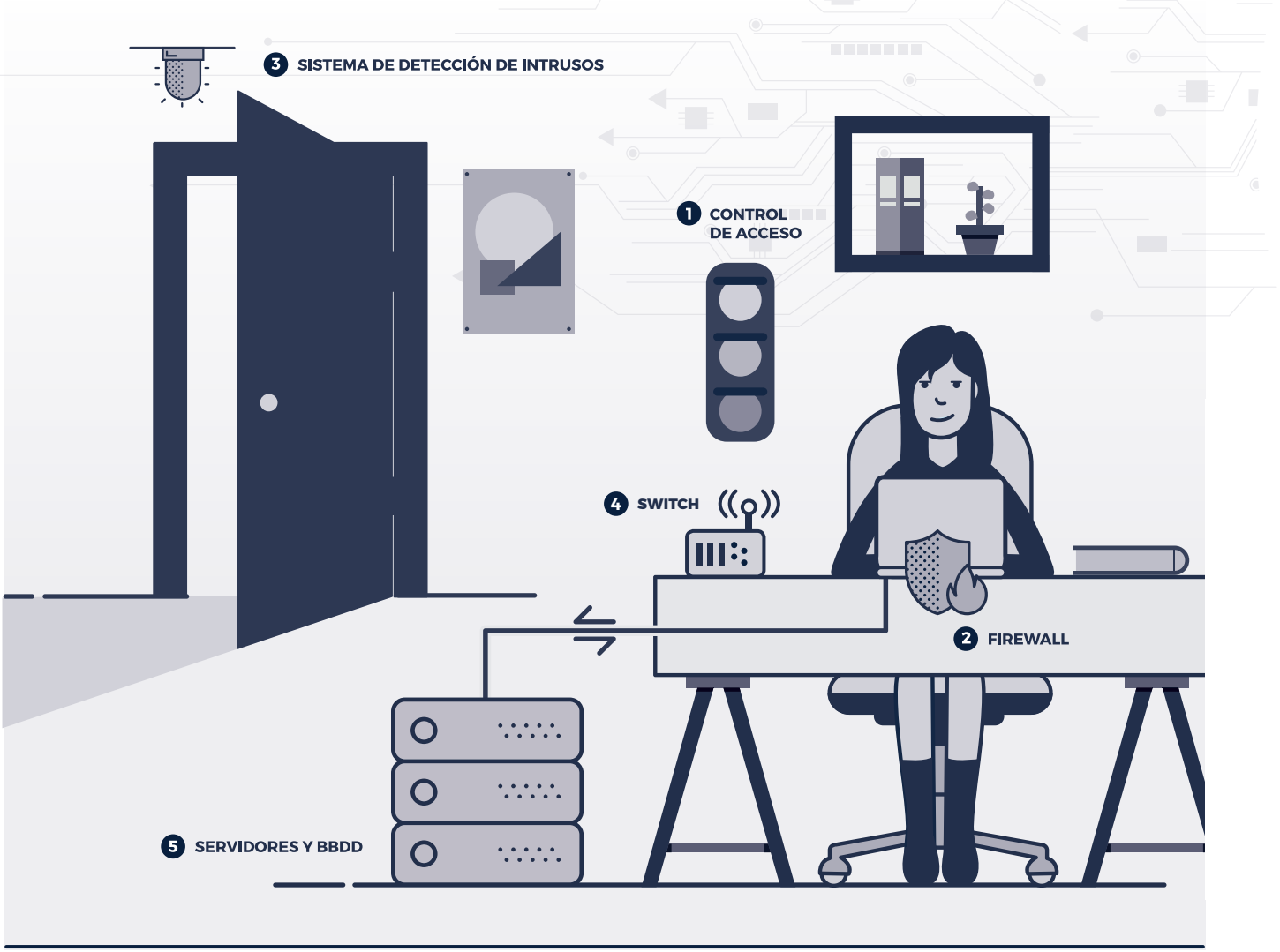
VECTOR.
ITCGROUP

# Vector Deep Surveillance

INFORMATION IS THE
NEW SECURITY PERIMETER

En el contexto tecnológico actual, se hace necesaria la correcta instrumentación, información y experiencia para combatir todos los ataques de ciberseguridad. Puede parecer simple, pero requiere una precisa organización y orquestación. Los equipos de seguridad deben trabajar con grandes cantidades de datos e información para tratar de identificar, responder y anticiparse a las amenazas reales. La mayoría de las organizaciones no tienen el tiempo, dinero y personal para el mantenimiento de un programa de ciberseguridad 24x7.

Con Vector Deep Surveillance se cubren las necesidades de identificar tanto comportamientos malignos (suplantación, malware, accesos no deseados, APT's) y de detección de fuga de datos (puerta trasera, bootnets, robo directo, shadow IT) para conseguir una vigilancia de las redes y del equipamiento del cliente de modo continuo que permita no sólo detectarlos, sino incluso predecirlos y prevenirlos.



## ¿EN QUÉ CONSISTE?

Vector Deep Surveillance ofrece una protección basada en la información de la red, mediante la recopilación de toda la información de los dispositivos, usuarios y redes del cliente, para posteriormente analizar en tiempo real su comportamiento, identificando patrones que puedan poner en riesgo la seguridad de la organización. Estos datos se enriquecen con la inclusión de información sobre amenazas provenientes de múltiples fuentes, de forma que sea posible anticipar la amenaza y neutralizarla.

Nuestra solución cuenta con un Anti-APT con inteligencia ampliada que se instala en los equipos del cliente con un IDS y un Sniffer para capturar la información de la red del cliente que nos permite hacer un perfilado en tiempo real de los dispositivos solicitando IPS (profiling y posturing), incluyendo también el acceso a repositorios de amenazas (IoCs), y con la tecnología necesaria para procesar y analizar toda la información recopilada, y actuar en caso de necesidad.

Vector Deep Surveillance incluye los servicios de consultoría de seguridad, donde realizamos una profunda investigación para determinar el nivel de madurez de la infraestructura del cliente, para analizar que implantación es la más óptima. Posteriormente se realiza la instalación y la configuración de todas las sondas, así como la de la infraestructura de VDS tanto en la red del cliente como en la nuestra. Una vez se pone en marcha, se ofrece el servicio de explotación del mismo basado en un SOC 24x7 para poder analizar y actuar en función de la información gestionada.

**Visibilidad constante del equipo y de la analítica Big Data en nuestros servicios Cloud:**

### PREVENCIÓN

Evita futuros ataques bloqueando aquellas aplicaciones que no sean goodware y utilizando tecnologías avanzadas anti-exploit.

### DETECCIÓN

Los ataques Zero-Day y los dirigidos serán bloqueados en tiempo real sin ficheros de firma.

### RESPUESTA

Información forense para investigar en profundidad cada intento de ataque.

### VISIBILIDAD

Trazabilidad y visibilidad de cada acción realizada por las aplicaciones en ejecución.

## FUNCIONALIDADES CLAVE

Detección de comportamientos malévolos:

- ✓ Suplantación, Malware, Infiltración de usuarios y dispositivos y APT's.

Detección de exfiltración de datos:

- ✓ Puerta trasera, Botnets y Shadow IT.

Vector Deep Surveillance:

- ✓ Monitorización del comportamiento del software (AD-EDR), del tráfico de red (IDS), y de accesos IPs (NAC).
- ✓ Correlación de eventos.
- ✓ Interprete IoC´s.
- ✓ Implantación de políticas de remediación.