

# Advanced Reporting Tool

Convierte los datos en conclusiones de Seguridad y Gestión IT



El aumento del volumen de información de seguridad manejado impide a los departamentos de IT fijarse en los detalles importantes

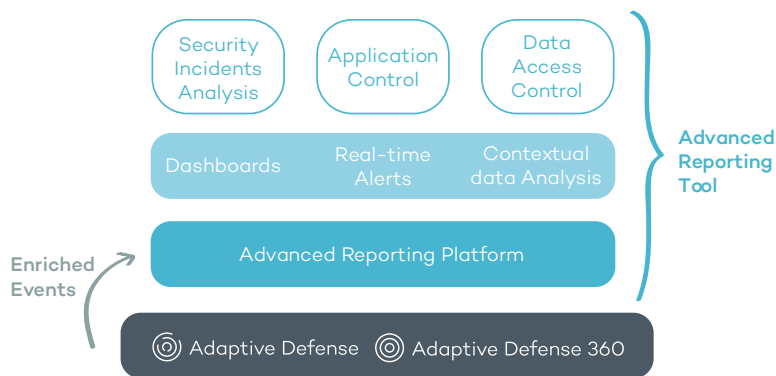
Esta información es utilizada para detectar problemas e infracciones de seguridad provocados tanto por elementos externos como por los Insiders de la compañía.

**Los departamentos de IT se encuentran desbordados:** el alto volumen de información gestionada, y la entrada en escena del malware de nueva generación hacen que **muchos detalles pasen inadvertidos o no sean registrados en absoluto**, comprometiendo la seguridad del todo el sistema.

## La solución: Adaptive Defense y Advanced Reporting Tool

**Advanced Reporting Platform** automatiza el almacenamiento y correlación de la información generada por la ejecución de procesos y su contexto, extraída por **Adaptive Defense** en el endpoint.

Gracias a esta información, **Advanced Reporting Tool** es capaz de generar inteligencia de seguridad de forma automática, y ofrecer herramientas que permitan tanto **localizar ataques y comportamientos extraños**, sea cual sea su origen, como **revelar el mal uso interno que se hace de los equipos y de la red corporativa**.



**Advanced Reporting Tool** proporciona las herramientas necesarias para obtener conclusiones fiables sobre la seguridad y la gestión IT de la empresa. Estas conclusiones son el inicio de un plan de actuación IT orientado a:

- › **Determinar el origen de las amenazas de seguridad** y aplicar mecanismos de resolución y políticas de seguridad que eviten futuros ataques.
- › **Implantar políticas más restrictivas de acceso a la información** crítica de la empresa.
- › **Controlar el mal uso de los recursos** que pueden afectar al negocio o al desempeño de los empleados
- › **Corregir los comportamientos de los empleados** no ajustados a las políticas de uso establecidas.

## Principales Beneficios



### 1. Buscar la información relevante

Q Maximizando la visibilidad de lo que sucede en todos los dispositivos e incrementando la eficiencia del departamento de IT.

Q Visualizando datos históricos para analizar los Indicadores de seguridad y de utilización de los recursos de la empresa.

Q Profundizando el detalle para localizar fácilmente dónde están los riesgos de seguridad o abusos en el uso de la infraestructura IT.

### 2. Diagnosticar el problema

🩺 Reduciendo el número de herramientas y conocimientos para comprender lo que sucede en los dispositivos y su relación con la seguridad y el uso de activos corporativos.

🩺 Extrayendo patrones de uso de los recursos y el comportamiento de los usuarios identificando su impacto en el negocio.

### 3. Ser alertado y alertar

🔔 Transformando las búsquedas de anomalías en alertas en tiempo real e informes.

🔔 Generando confianza en la empresa, detectando en el momento las anomalías de seguridad o de mal uso de los recursos corporativos.

### 4. Informar tanto horizontal como verticalmente

📄 Generando informes de detalle configurable que permiten un análisis metódico del nivel de seguridad de la empresa, del mal uso de los activos y de actividades anómalas de los usuarios

📄 Mostrando, el estado de indicadores claves de seguridad y su evolución en el tiempo, como consecuencia de las acciones correctivas tomadas.

## ANÁLISIS PREDEFINIDOS ADAPTABLES A LAS NECESIDADES DE LAS EMPRESAS

**Advanced Reporting Tool** incorpora paneles de control con Indicadores claves, búsquedas y alertas predeterminadas en 3 áreas específicas de actuación:

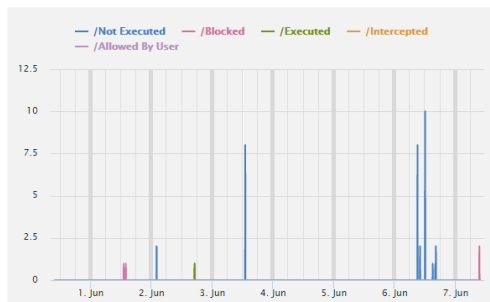
- Incidencias de seguridad.
- Acceso a la información crítica.
- Aplicaciones y recursos de red utilizados.

Las búsquedas y alertas a de información clave pueden ser adaptadas a las necesidades específicas de cada empresa.

## INFORMACIÓN DE INCIDENCIAS DE SEGURIDAD

Generación de inteligencia de seguridad, procesando y relacionando los eventos generados en intentos de intrusión.

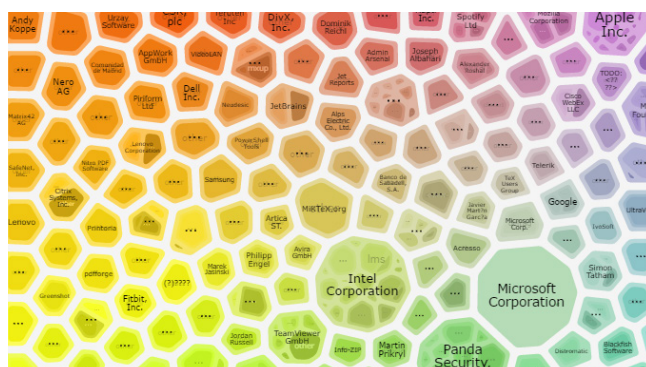
- Calendario anual con el malware y PUPs detectado.
- Equipos con más intentos de infección y tipo de malware detectado.
- Estado de la ejecución del malware en los equipos de la red.
- Localización de equipos que usan aplicaciones con vulnerabilidades conocidas



## REDUCCIÓN DE COSTES

Descubrimiento de patrones de uso de los recursos informáticos por parte de los usuarios para el desarrollo y aplicación de políticas que produzcan ahorros de costes.

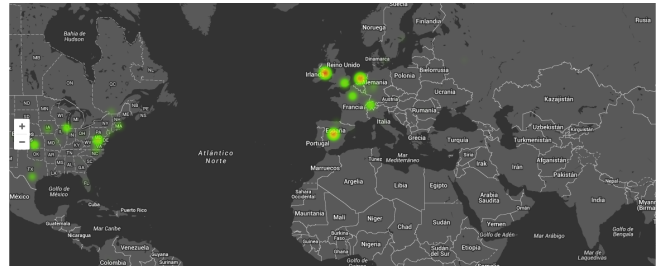
- Aplicaciones corporativas y no corporativas ejecutadas en el parque informático.
- Licencias de Office usadas frente a contratadas.
- Aplicaciones con mayor consumo del ancho de banda.
- Aplicaciones vulnerables ejecutadas o instaladas en el parque que puedan ser origen de infecciones y tengan un impacto en la producción y costes derivados de resolución.



## CONTROL DE ACCESO A LOS DATOS DE LA EMPRESA

Muestra el acceso a ficheros con información confidencial y su circulación en la red

- Países de mayor tráfico intercambiado con la red del cliente.
- Ficheros más accedidos por los usuarios y ejecutados con mayor frecuencia.
- Localiza qué usuarios han accedido a determinados equipos de la red.
- Calendario anual de datos enviados.



## ALERTAS EN TIEMPO REAL

Creación de alertas tomando como base eventos que pueden identificar una brecha de seguridad o una violación de las políticas de gestión de datos de la empresa:

- Alertas predefinidas que identifican situaciones de peligro.
- Creación de alertas personalizadas en base a consultas creadas por el usuario.
- 7 métodos de entrega (en consola, email, JSON, Service Desk, Jira, Pushover, PagerDuty)

## SERVICIO BIG DATA ALOJADO EN LA NUBE, FLEXIBLE Y CONFIGURABLE

- Adaptado a las necesidades del administrador de red, tanto en espacio de almacenamiento como en ejecución de búsquedas sobre los datos históricos.
- Puesta en marcha instantánea, sin cambios en la red del cliente ni instalación de infraestructura adicional.
- Entorno configurable a la medida de las necesidades del departamento de IT.

### REQUISITOS TÉCNICOS

Navegador compatible certificado (otros pueden funcionar):

- Mozilla Firefox.
- Google Chrome.

Conexión a internet y comunicación segura a través del puerto 443.

Resolución mínima 1280x1024, recomendada 1920x1080.

Compatible con:

- Adaptive Defense
- Adaptive Defense 360