# Cytomic, seguridad avanzada para la gran empresa



# Cytomic, seguridad avanzada para la gran empresa

**Cytomic no sólo es la nueva unidad de negocio de Panda Security para el mercado de seguridad más avanzado, es una arquitectura, una plataforma y unos servicios gestionados que quieren llevar la seguridad automatizada a un nuevo nivel. Cytomic es la apertura al mundo de Panda Security enfocada al segmento Enterprise.**

cytomicmodel.com

Hace unos meses, Cytomic se vestía de largo. Llegaba como la gran apuesta de Panda Security para redefinir la seguridad empresarial, para dar respuesta a ciberamenazas más sofisticadas y cubrir las necesidades de seguridad más avanzadas en organizaciones con una madurez mucho mayor. Llegaba con una oferta de soluciones y servicios basada en la nube, y dos paradigmas: la analítica de datos a escala, Security Data Analytics; y un modelo de comunidad que enriquece la inteligencia de amenazas.

Cytomic cuenta con una oferta de soluciones y servicios gestionados coherente, basada en una única plataforma nativa en la nube y unificada, que cubre el proceso completo de protección, detección y respuesta a incidentes en el endpoint. Esta gestión unificada es clave para los responsables de seguridad y analistas de los Security Operations Center (SOC), que a menudo tienen que enfrentarse a demasiadas tareas y herramientas de seguridad.

La plataforma Cytomic además ofrece una interfaz, basada en estándares de la industria (RestAPI y conectores con el SIEM) que permite automatizar

y acelerar la detección y la respuesta a incidentes entre las diferentes tecnologías de seguridad con las que los SOCs trabajan, facilitando el intercambio de datos y procesos a través de infraestructura conectada

La propuesta de valor de Cytomic se basa en la aplicación de dos componentes claves que se integran y colaboran estrechamente entre sí. Por un lado, un agente ligero que conserva la capacidad de detección y prevención en el endpoint, optimizando los recursos. Además, es capaz de tomar medidas preventivas y de respuesta de forma autónoma. El agente monitoriza toda la actividad en los puestos de trabajo y servidores, recopilando todos los eventos que se producen en los dispositivos y los envía a la plataforma Cytomic, sobre la cual delega las

Cytomic Orion acelera y simplifica el proceso de búsqueda, investigación y respuesta ante amenazas que ya están en la red corporativa

## Orion, el arma secreta de Cytomic

**Orion es la clave de la plataforma Cytomic. Es la que habilita la investigación, imprescindible para detectar y detener las amenazas. Orión está diseñada enteramente en y para ejecutarse en la nube en una arquitectura multitenant, lo que permite almacenar y procesar datos de forma masiva siguiendo los principios de extensibilidad y flexibilidad virtualmente ilimitado.**

Cytomic Orion acelera y simplifica el proceso de búsqueda, investigación y respuesta ante amenazas que ya están en la red corporativa. Cytomic Orion correlaciona más de un billón de eventos por semana en tiempo real, detectando actividad anormal mediante Inteligencia Artificial y técnicas búsqueda de patrones de comportamiento. Además, enriquece automáticamente los datos recogidos con inteligencia de amenazas, propia y de terceros, como TTPs, motivaciones, atribuciones, etc. Como resultado de este análisis se generan alertas de comportamientos sospechoso, priorizadas y con información de inteligencia de amenaza y contexto, que permite un triaje agilizado.

Cytomic Orion también proporciona herramientas de exploración y hunting sobre el conjunto completo y enriquecido de eventos en los últimos 365 días. Entre las herramientas de exploración, Cytomic Orion proporciona un conjunto de consultas predefinidas que descubren las técnicas y procedimientos de ataque en retrospectivo, con margen suficiente para descubrir cómo entró y que movimientos realizó, ya que los atacantes permanecen sin ser descubierto, de media, 200 días.

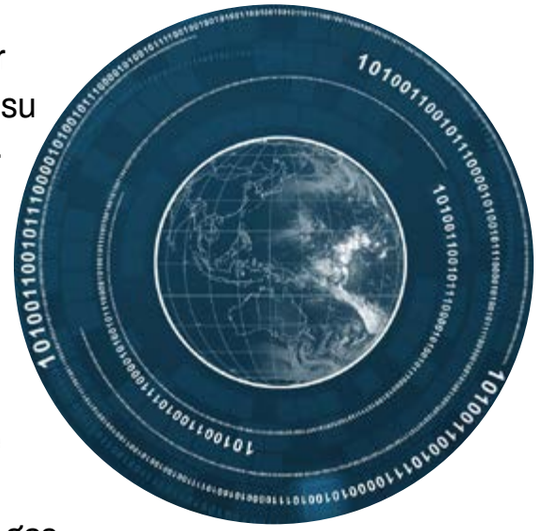
Por último, Cytomic Orion permite realizar acciones de contención y remediación en los endpoints, como aislar o abrir una shell remoto como la que realizar un conjunto de operaciones sobre el sistema.

Una de las ventajas de Cytomic Orion es que utiliza los Jupyter Notebooks, una tecnología lleva tiempo utilizándose en investigaciones médicas mediante código dinámicos que facilita las investigaciones. De las alertas de actividad sospechosa o de las exploraciones de hunting, se automatiza la investigación con las plantillas predefinidas o propietarias en Jupyter Notebooks, o el análisis de detalle en la consola de Investigación o bien una combinación de ambas.

## Cytomic, seguridad avanzada para la gran empresa

tareas de cálculo. Este agente ligero es único para todas las soluciones, módulos y servicios de Cytomic, lo que permite a los clientes evolucionar su programa de seguridad añadiendo nuevos módulos o servicios gestionados sin necesidad de ningún despliegue adicional.

El segundo gran componente es la plataforma de Cytomic en sí, o Cytomic Platform, una plataforma nativa cloud en la que reside toda la inteligencia, capaz de almacenar y procesar grandes volúmenes de información, como atributos estáticos, dinámicos, telemetría de comportamiento y threat Intelligence y procesarlos en tiempo real con algoritmos de Inteligencia artificial con el objetivo de bloquear automáticamente comportamientos maliciosos en los endpoints o descubrir aquellos sospechosos que requieren una investigación detallada antes de decidir si nos encontramos ante un atacante, para proceder a la mayor velocidad posible a su contención y erradicación en la red.



Esta gran plataforma en la nube aglutina un conjunto de tecnologías que colaboran entre sí para ofrecer dos servicios totalmente gestionados y transparentes para el cliente: El primero de ellos es el denominado “Zero-Trust App Service”, que determina automáticamente y en tiempo real la naturaleza de los procesos y binarios, clasificándolos en maliciosos o confiables, permitiendo su ejecución o no en función de ello. Este servicio acaba drásticamente con el malware de cualquier tipo, ya sea conocido o desconocido, incluido los devastadores ransomware. El otro servicio integrado es el Threat Hunting, que está orientado a encontrar nuevos patrones de comportamiento malicioso más allá de aplicaciones malware y desarrollar mecanismos de protección en el endpoint. Este nivel de servicio es la base que permite el bloqueo de atacantes que evaden los mecanismos de protección mediante el uso inapropiado de herramientas administrativas, ya existentes en el parque del cliente, los denominados ataque en base a técnicas “living-off-the-land”.

El servicio de Threat Hunting trasversal a todos nuestros clientes, es potenciado y especializado a cada cliente que así lo necesite, mediante la sus-

**‘DAMOS UNA RESPUESTA A LA PREVENCIÓN, DETECCIÓN, CAZA Y REMEDIACIÓN’ (MARÍA CAMPOS, CYTOMIC)**

**CLICAR PARA VER EL VÍDEO**

# Cytomic, seguridad avanzada para la gran empresa

Cytomic cuenta con una oferta de soluciones y servicios gestionados coherente, basada en una única plataforma nativa en la nube y unificada, que cubre el proceso completo de protección, detección y respuesta a incidentes en el endpoint

cripción a niveles superiores de servicios de Threat Hunting, que tanto el equipo de ciberseguridad de Cytomic como los partners certificados de la compañía ofrecen a los clientes.

**Soluciones**

El portfolio de soluciones y servicios de Cytomic cubre los escenarios de seguridad avanzada en el endpoint, además de otras áreas funcionales cercanas a la seguridad. Durante este primer año de vida la compañía ha realizado un esfuerzo de estructuración de la oferta permitiendo al cliente ir avanzando según sus necesidades y nivel de madurez.

Destacar que la plataforma Cytomic ha sido diseñada bajo el enfoque “API-first”, orientado a la extensibilidad e interoperabilidad con los otros procesos, sistemas y aplicaciones que ya disponga el cliente y los Partners. Se ha trabajado en abrir cada vez más las opciones disponibles para ser parte del ecosistema ya existente en SOCs y CSIRTs, mediante la integración con SIEMs, plataforma de intercambio de Threat Intelligence, sistemas de Ticketing o incluso las nuevas plataformas de Orquestación y automatización de la detección y la respuesta (SOARs).

Como no podía ser de otra forma todo empieza con el endpoint. Cytomic cuenta con una solución de protección avanzada para el punto final que trabaja previniendo ataques mediante la monitorización continua de la actividad en los endpoints, el servicios gestionado Zero-trust App Services y el

# Cytomic, seguridad avanzada para la gran empresa

Maria Campos, VP Cytomic

servicio de Threat Hunting integrado, tecnologías dinámicas antiexploit, detección de Indicadores de Ataque y de compromiso (IoAs, y IoCs), análisis de comportamiento y otras tecnologías de prevención más extendidas e igualmente válidas y necesarias como , filtrado de navegación web, control de dispositivos, firewall, IDS, etc…

Cytomic se aproxima a la protección del endpoint mediante capacidades muy robustas de EDR, monitorización de los endpoints, su telemetría enriquecida con inteligencia de amenazas y analítica de datos a escala. Esta es la base de las soluciones Cytomic EDR y Cytomic EPDR, e incluye las capacidades más tradicionales en la lucha contra los atacantes. Pero como bien es sabido por todos, no existe la seguridad absoluta, siempre habrá ciberatacantes y/o insiders que sean capaz de evadir la seguridad y acceder a los dispositivos, es por ese motivo que Cytomic ofrece una amplío abanico de opciones que se ajustan a la realidad de cada organización:

De esta forma, para aquellas organizaciones que no disponen de equipo de seguridad, Cytomic propone un conjunto de servicios gestionado de threat hunting, que detectarán aquellos atacantes que haciendo uso de herramientas administrativas, aprovechando errores de configuración, o utilizando técnicas avanzadas de evasión, estén generando un riesgo de seguridad para la organización. El servicio es ofrecido por nuestros partners certificados o por nuestro propio equipo de expertos de seguridad.

Por otro lado, y para aquellas organizaciones con un equipo de seguridad dedicado (SOCs) Cytomic pone a su disposición la plataforma utilizado por nuestros equipo de expertos en seguridad en forma de una solución completa que acelera el proceso de detección, investigación, contención y erradicación de atacantes en la red corporativa, la forma de entrega de la plataforma a estos SOCs y los equipos de Incident Response correspondiente es Cytomic Orion y la familia de soluciones: Cytomic Ionic y Cytomic Covalent (que incluyen Cytomic EDR o Cytomic EPDR respectivamente).

Por último, sabemos que los equipos de seguridad ya disponen de un stack tecnológico de seguridad en producción para implementar su propio plan de Incidente Response, es por ello que Cytomic ofrece un conjunto de conectores e interfaces es-

> El portfolio de soluciones y servicios de Cytomic cubre los escenarios de seguridad avanzada en el endpoint, además de otras áreas funcionales cercanas a la seguridad

# Cytomic, seguridad avanzada para la gran empresa

tándar (Mensajería y RestAPI) que permite la colaboración con otros elementos de seguridad para acelerar y aumentar la capacidad del ecosistema de seguridad de la organización.

Por último, el cliente también puede optar por módulos que facilita la reducción de su superficie de ataque con Cytomic Patch, Cytomic Encryption, Cytomic Data Watch y Cytomic Insights. El primero permite detectar vulnerabilidades de los sistemas operativos y cientos de aplicaciones habituales en entornos empresariales en tiempo real, proporcionando a la vez un mecanismo de parcheado centralizados desde la consola cloud de Cytomic Ionic y Cytomic Covalent.

Cytomic Insights es una herramienta de agregación de datos, reporting y generación de informes.

Cytomic Encryption permite gestionar de forma centralizada el cifrado de disco de los endpoints, almacenar y recuperar las claves de recuperación de BitLocker desde la consola cloud. Y Cytomic Data Watch monitoriza los ficheros en los dispositivos en búsqueda de datos personales y sensibles, permitiendo el borrado de ficheros desde la consola única de Cytomic para mitigar el riesgo.

Los módulos de control del dato ayudan a las empresas a hacer frente a GDPR. Con la aparición de nuevas amenazas cada día, el riesgo de no proteger adecuadamente los datos en los endpoints es cada vez más alto, aun así, según datos de Varonis, el 41% de las empresas tiene más de 1000 ficheros con datos confidenciales, incluidos números de tarjetas de crédito y datos sanitarios sin proteger e incluso la organización no es consciente de la presencia de esos datos en el endpoints.

*Cytomic ha llegado al mercado con una propuesta orientada a resolver la realidad de ciber riesgo en la que muchas organizaciones se encentran*

**Servicios**

Los clientes de Cytomic pueden hacer uso de toda la potencia de la solución Orion en su propio SOC si cuentan con un equipo capacitado para tal función. Pero, en el caso de no tener esos recursos, o de tenerlos externalizados y no interesar llevar a cabo esta función internamente, Cytomic se lo ofrece como servicios gestionados de seguridad, una parte muy importante del offering de la compañía.

Se parte de servicios profesionales muy básicos, como es Cytomic Bronze, que le dice al cliente, a través de notificaciones muy limpias y de informes mensuales qué se ha estado haciendo, qué se ha detectado y cómo se ha mejorado la postura de seguridad del cliente en un formato 8x5. Después se avanza hacia propuestas Gold y Diamond, de 24x7, con capacidades mucho más avanzadas, mayor

# Cytomic, seguridad avanzada para la gran empresa

detalle, conociendo el negocio del cliente y metiéndose en sus procesos.

Además de estos servicios profesionales, se ofrecen servicios de Threat Hunting. El objetivo es acompañar al cliente en el proceso de descubrimiento de amenazas en su red, su bloqueo y la respuesta necesaria para erradicar su presencia en su entorno productivo.

**El valor de Cytomic**

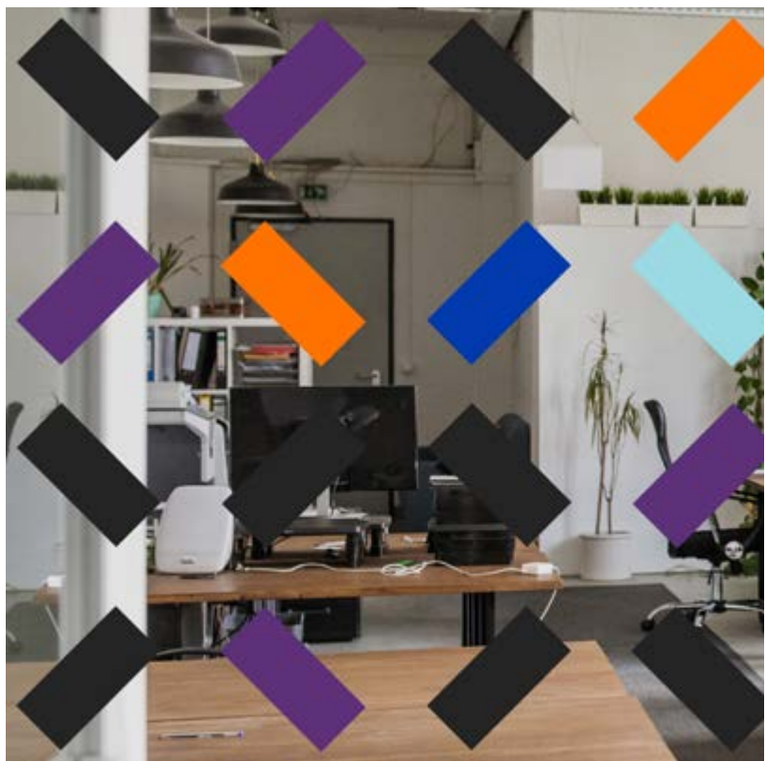
Cytomic ha llegado al mercado con una propuesta orientada a resolver la realidad de ciber riesgo en la que muchas organizaciones se encentran. Una realidad en la que el número, la profesionalización y la sofisticación de los atacantes obliga a fortalecer sus políticas de seguridad y desarrollar procesos específicos para prevenir, detectar, investigar, contener y erradicar ciberataques.

Porque el foco no debe centrarse en la posibilidad de ser atacado, sino en estar preparado para cuando eso ocurra. Por otro lado, la demanda de profesionales cualificados en seguridad es uno de los mayores desafíos que enfrenta la industria de la ciberseguridad hoy en día. Según la organización de seguridad de IT (ISC)² actualmente existen 2.93 millones de puestos sin cubrir en todo el mundo.

En esta realidad, Cytomic propone una plataforma única de prevención, detección y respuesta 100% nativa cloud, centrada en su amplia y probada experiencia en el endpoint. Sobre esta arquitectura se articula una oferta comercial extensible, flexible y adaptable, combinando soluciones y servicios integrados como parte de ella, servicios gestionados profesionales, para descargar a las organizaciones que así no necesiten, y herramientas que permiten la interoperatividad y automatización dentro del stack tecnológico desplegado ya en un SOC y/o CSIRT.

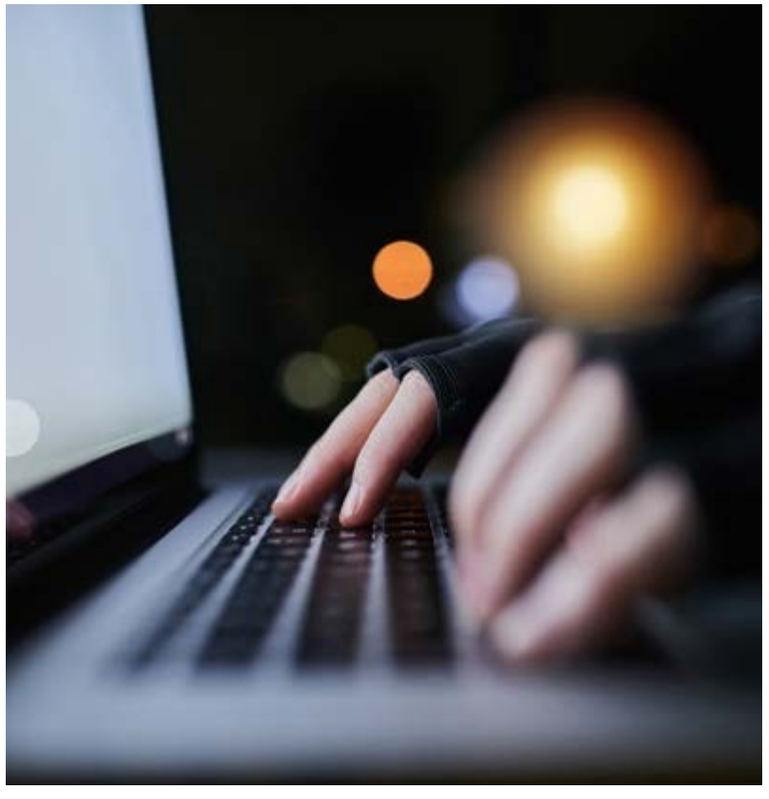
**¿Qué otros valores y ventajas aporta Cytomic?**

- **Una arquitectura única basada en la nube,** donde residen la telemetría a escala, los modelos y algoritmos de procesamiento y la inteligencia propia de amenazas.



# Cytomic, seguridad avanzada para la gran empresa

- **Filtrado automatizado de ataques basados en malware a través del servicio gestionado Zero-trust App Service,** incluido en todas las soluciones de seguridad endpoint, lo que permite al equipo centralizar sus esfuerzos en minimizar el tiempo de detección y respuesta y elevar automáticamente el nivel de madurez de seguridad de la organización.
- **Analítica de datos y la automatización a través de Cytomic Orion,** que pone a disposición de los equipos de seguridad Inteligencia de amenazas y herramientas de automatización tanto en la detección de comportamientos sospechosos, en el proceso de triaje e investigación y en la acción de contención y respuesta directa desde una única consola cloud.
- **La baja incidencia de falsos positivos** gracias a la identificación de patrones de comportamientos que alimentan y entrenan automáticamente lo modelos de IA, supervisados por un equipo de analistas de seguridad.
- **Mínimo impacto en el despliegue y puesta a marcha de las soluciones y los servicios al ser soluciones totalmente cloud.** Una vez que se despliega el único agente ligero, los niveles de seguridad y los módulos adicionales se activan desde la consola en la nube, sin importar el volumen de endpoints, sin importar el tipo, con un solo clic y en tiempo real.
- **Reducción de coste total de propiedad** ya que la plataforma, al estar basada en la nube elimina la necesidad de adquirir hardware o software, ni personal para su mantenimiento.
- **Plataforma abierta gracias a un amplio conjunto de APIs y conectores** que permite complementar y ampliar la infraestructura de seguridad existente del cliente, como SIEMs, la API de IoC, permite la consulta sobre el streaming de eventos y retrospectivo 365 días y las API de gestión, que permita a los clientes aprovechar aún más sus inversiones en seguridad.
- **La consolidación de productos y agentes.** Las soluciones Cytomic están integradas en una única plataforma desde la cual se activan capacidades, el conjunto es una consolidación de funcionalidades completas de prevención, detección y respuesta, así como de operativa IT y privacidad de datos.
- Además de soluciones, **Cytomic también ofrece servicios gestionados y proactivos de descubrimiento y caza de amenazas,** específicamente diseñados para aquellas organizaciones que requieren un alto nivel de madurez en seguridad pero que no disponen de un equipo propio de threat hunting.
- **Los servicios multiplican las capacidades del personal** existente en la organización, mejorando y amplificando su productividad.



## Enlaces de interés...

- cytomicmodel.com
- Cytomic, a la conquista del mercado enterprise con el Threat Hunting como propuesta diferencial
- Panda Security propone a las empresas un enfoque de seguridad proactivo y avanzado con Cytomic

in https://www.linkedin.com/company/cytomic/

t @Cytomic_