Forescout

Threat Detection and Response

FORESCOUT

Forescout
Threat Detection and Response

450 veces más eficiencia en los SOC gracias a una mejor detección y mitigación de amenazas reales

Los equipos de los centros de operaciones de seguridad (SOC, por sus siglas en inglés) reciben cada día una avalancha de alertas incompletas e imprecisas, en las que falta importante información de contexto. Muchos de ellas son falsas alarmas. Como consecuencia, los analistas pasan por alto amenazas críticas o necesitan más tiempo para examinarlas y mitigarlas, lo cual eleva el riesgo de vulneraciones de la seguridad. Un SOC típico recibe 11.000 alertas al día o 450 por hora[1]; la mayoría de ellas son poco fiables o incluso una «alarma ciega».

Con Forescout® Threat Detection and Response, esta cantidad se reduce a una detección por hora, concreta y que requiere una actuación o, dicho de otro modo, a amenazas probables que los empleados del SOC realmente tienen que examinar.[2]

Vista general de la solución

Basándose en datos telemétricos y logs, Forescout Threat Detection and Response genera alertas de alta fiabilidad frente a amenazas probables que el SOC debe evaluar de forma concreta.
La solución automatiza la detección, búsqueda, evaluación y resolución de amenazas sofisticadas para todos los dispositivos conectados. En este proceso incluye IT, OT/ICS, IoT e IoMT y abarca el campus, el centro de computación, la nube y los bordes (Edge). Forescout Threat Detection and Response reúne tecnologías y funciones de SOC imprescindibles en una plataforma unificada y nativa en la nube. El equipo puede ver toda la información a través de una única consola y tomar medidas de inmediato.

Forescout Threat Detection and Response utiliza datos de la totalidad del entorno corporativo, teniendo en cuenta los dispositivos tanto administrados como no administrados (sin agente).

Forescout Threat Detection and Response genera detecciones evaluables, a partir de datos telemétricos y protocolos, 450 veces más efectivas que las del típico SOC.

Con Forescout Threat Detection and Response

VS

SOC típico

*** Detección: una amenaza probable, que los empleados del SOC tienen que examinar manualmente**

Basado en datos agregados recabados a lo largo de un periodo de un año (dic. 2021-2022) y procedentes de 30 grandes empresas distintas de diferentes sectores.

11.000 alertas al día = 450 alertas por hora.
Fuente: The 2020 State of Security Operations, Forrester Consulting

La cantidad exacta que un SOC recibe depende de muchos factores, entre ellos, el número, el tipo y la ubicación de los controles de seguridad, la compenetración de estos controles (lo cual, a su vez, depende de la capacidad de los analistas, de la tolerancia al riesgo y del know-how), el número de empleados/dispositivos y el sector.

Ventajas empresariales

Reduce el riesgo empresarial

FForescout Threat Detection and Response disminuye el riesgo y el alcance de ataques exitosos o fallos de datos y filtra prácticamente todo el «ruido de fondo de datos». Esto permite a los equipos del SOC detectar, examinar y mitigar las más diversas y sofisticadas amenazas en todo el entorno corporativo con mayor rapidez y precisión.

De este modo, Forescout Threat Detection and Response contribuye a evitar las interrupciones y los costes empresariales que podría conllevar el éxito de un ataque o una vulneración de la seguridad.

Optimiza los procesos de seguridad

Forescout Threat Detection and Response enriquece automáticamente datos importantes, los normaliza y correlaciona indicadores para generar una cantidad pequeña de detecciones altamente fiables, que de verdad tienen que ser examinadas por una analista. La solución simplifica y acelera complejos procesos de examen y threat hunting (caza amenazas) mediante información más completa y precisa y datos contextualizados; y todo ello a través de un consola unificada, que se puede integrar con otras soluciones de Forescout, así como con SIEM, sistemas de gestión de casos y soluciones de respuesta de otros proveedores.

Forescout Threat Detection and Response ofrece paneles de control (dashboards) preconfigurados y adaptados e informes con indicadores (KPI) específicos para analistas/respondedores de incidentes, técnicos, directores de SOC, encargados de cumplimiento, gestores de riesgo y directivos. Esto mejora la visión de conjunto de las amenazas a lo largo de todo el ciclo de vida y permite al equipo del SOC dedicar más tiempo a tareas de seguridad más valiosas.

Reduce los costes

La solución disminuye las tareas del SOC en los siguientes aspectos:

- Adquisición de licencias y administración de varias soluciones aisladas para el SOC, por ejemplo, lagos de datos; soluciones para análisis de seguridad; orquestación de seguridad, Automation and Response (SOAR); User and Entity Behaviour Analytics (UEBA); y plataformas de inteligencia de amenazas.
- Almacenamiento de registros
- Burnout de los analistas, fluctuación, contratación y formación de los empleados
- Soporte para nuevas fuentes de datos
- Creación y adaptación de reglas

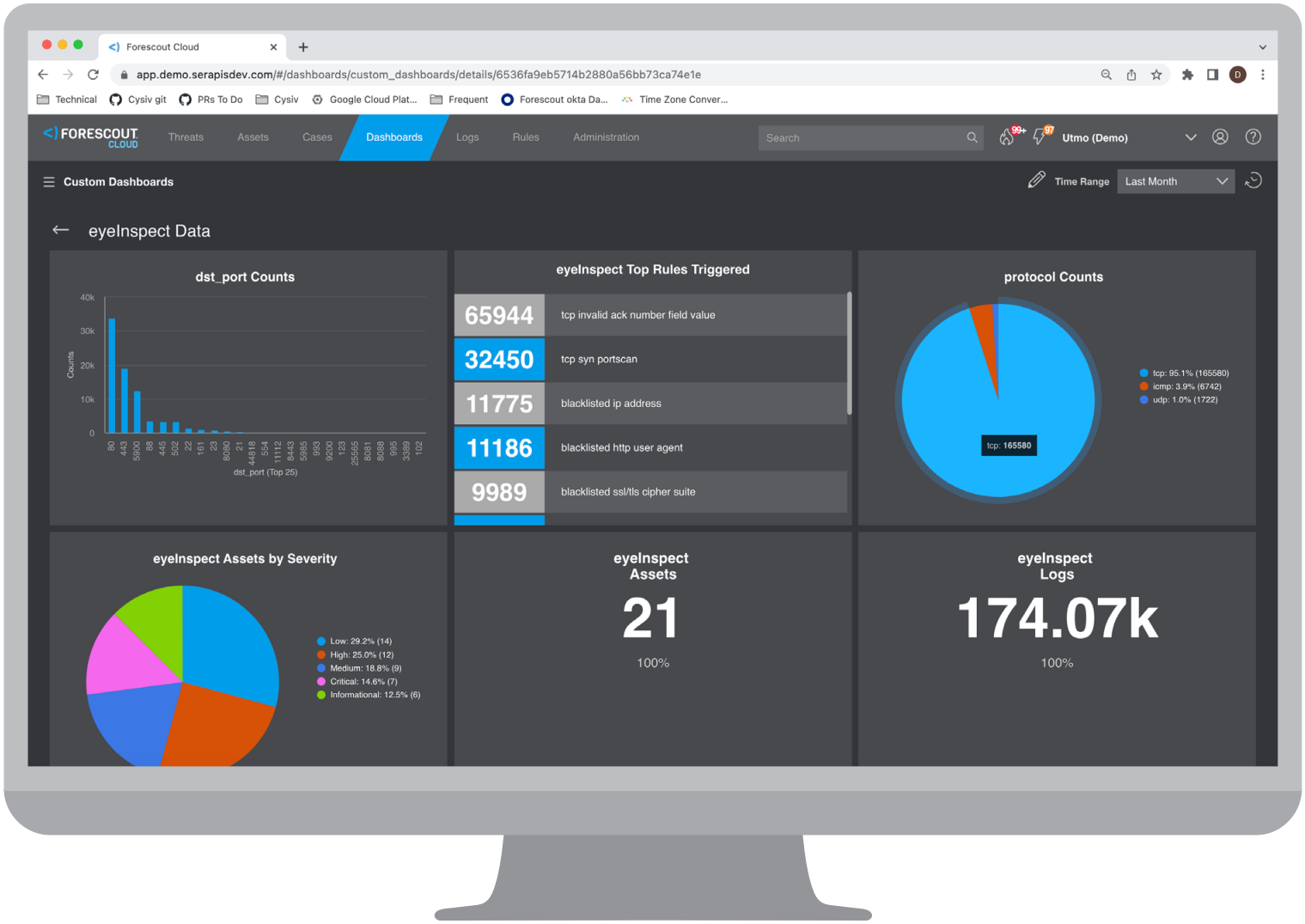
Simplifica el cumplimiento normativo

Las diversas opciones de almacenamiento tibio y frío, la detección automática de amenazas y la inteligencia de amenazas favorecen el cumplimiento de las disposiciones y los estándares relevantes. A su vez, ayudan a cerrar los posibles agujeros entre el momento en el que se percibe la vulneración de la seguridad o la avería y el momento en que se responde.

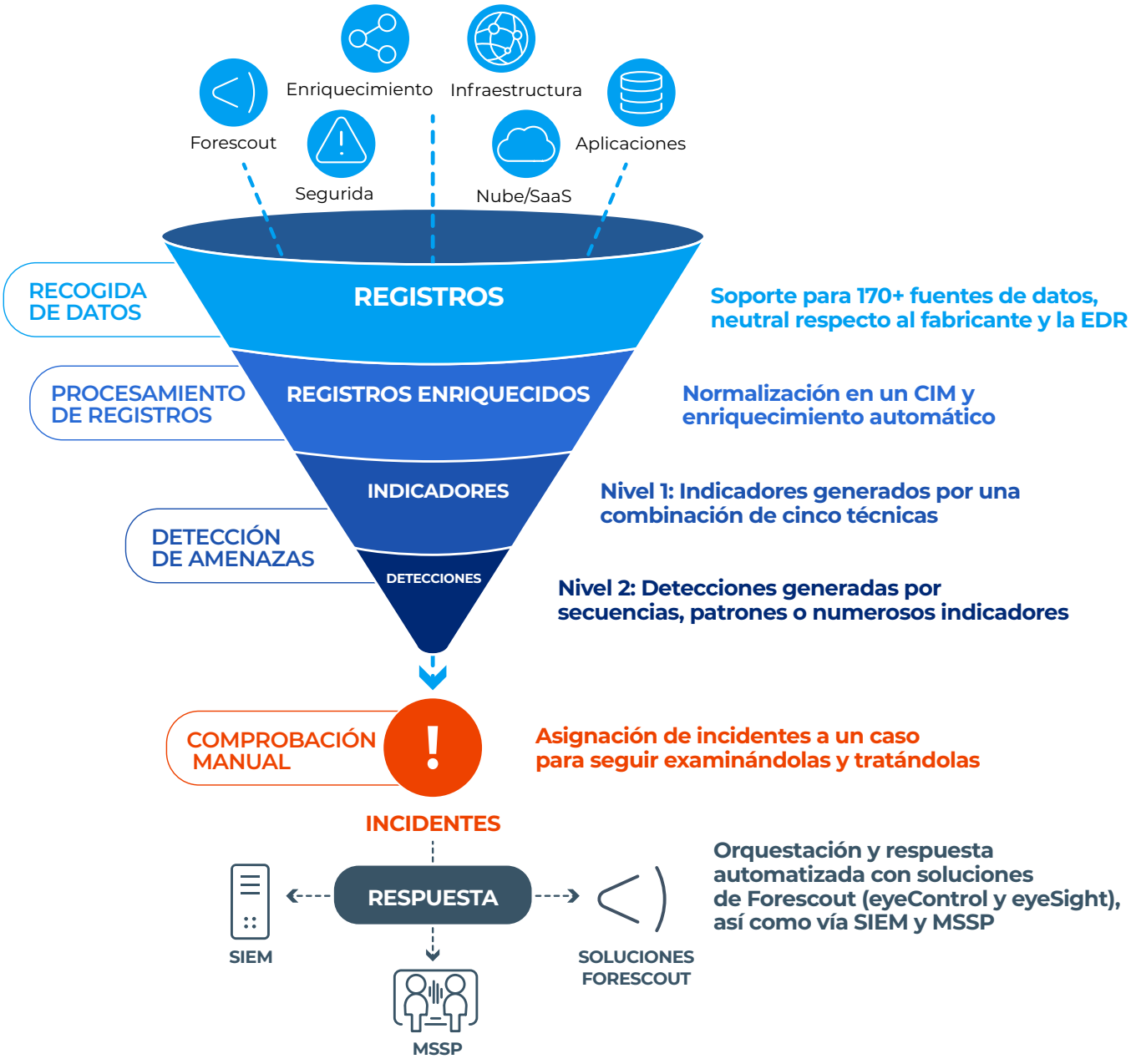
Utiliza productos de seguridad ya presentes

Forescout Threat Detection and Response aumenta la utilidad de las demás funciones de Forescout, así como las de sus sensores de red, de terminales y de seguridad en la nube y de sus puntos de aplicación, sean del fabricante que sean. Con Forescout Threat Detection and Response no tiene que implementar ningún nuevo software o hardware de un flbriclnte específico.

Métricas y datos de proceso importantes para controlar mejor el rendimiento del SOC



Cuadros de mando e informes preconfigurados y adaptables basados en personal aportan KPI relevantes para distintos grupos objetivo, entre ellos analistas/respondedores de incidentes, técnicos, directores de SOC, directores de cumplimiento, gestores de riesgo o directivos.


Forescout
Enriquecimiento
Infraestructura
Aplicaciones
Segurida
Nube/SaaS
RECOGIDA DE DATOS
REGISTROS
Soporte para 170+ fuentes de datos, neutral respecto al fabricante y la EDR
PROCESAMIENTO DE REGISTROS
REGISTROS ENRIQUECIDOS
Normalización en un CIM y enriquecimiento automático
DETECCIÓN DE AMENAZAS
INDICADORES
Nivel 1: Indicadores generados por una combinación de cinco técnicas
DETECCIONES
Nivel 2: Detecciones generadas por secuencias, patrones o numerosos indicadores
COMPROBACIÓN MANUAL
!
Asignación de incidentes a un caso para seguir examinándolas y tratándolas
INCIDENTES
RESPUESTA
SIEM
SOLUCIONES FORESCOUT
MSSP
Orquestación y respuesta automatizada con soluciones de Forescout (eyeControl y eyeSight), así como vía SIEM y MSSP

Por qué Forescout

Junto con otras soluciones de Forescout, Forescout Threat Detection and Response ofrece una combinación única de recogida de datos neutral respecto al fabricante y la EDR, una detección 450 veces mejor, un amplio espectro de respuesta y una minimación de riesgos proactiva; y todo ello por un precio asequible y calculable.

Recogida de datos neutral respecto al fabricante y la EDR

- Compatible con los productos y soluciones en los que ya haya invertido
- Puede recoger datos de cualquier dispositivo administrado o no administrado (IT, OT/ICS, IoT, IoMT)
- Garantiza una detección de amenazas más exhaustiva, potente, flexible y efectiva

Detección 450 veces mejor

- Una pipeline de datos ultramoderna requiere un modelo de información común (CIM, por sus siglas en inglés) para poder normalizar los datos recogidos y enriquecerlos automáticamente con información del usuario, IP asignada, datos de geolocalización e información sobre activos críticos
- Un motor de dos pasos para la detección de amenazas utiliza una combinación de 5 técnicas con el fin de reducir el ruido de datos y de aumentar la fiabilidad

Respuestas exhaustivas

- Herramientas de examen potentes
- Integraciones nativas con soluciones de gestión de casos
- Respuestas automatizadas con soluciones de Forescout, que abarcan todos los dispositivos administrados y no administrados

Minimización de riesgos proactiva

- La integración con otras soluciones de Forescout reduce la superficie de ataque y rebaja el peligro de que un dispositivo comprometido o no conforme con las normas se conecte a la red
- Vigilancia continua de todos los activos conectados con ayuda de directrices de acceso dinámicas

Fijación de precios sencilla, calculable y asequible

- Sin tasas adicionales cuando se transfieren más registros a Forescout Threat Detection and Response; fomentando una mejor detección
- Las tasas de licencia se basan en el número total de dispositivos finales (dirección IP/MAC) de su empresa
- El precio incluye diferentes opciones de almacenamiento tibio y frío para satisfacer sus exigencias empresariales

Características esenciales

Forescout Threat Detection and Response reúne tecnologías y funciones de SOC imprescindibles en una única consola unificada y nativa en la nube.

Recogida de datos

Soporte nativo de datos de Forescout eyeSight, eyeInspect y Medical Device Security y de más de 170 fuentes de datos neutrales en cuanto al fabricante y la EDR, incluyendo:

- **Seguridad:** Cortafuegos, IDS/IPS de la red, EDR, plataformas para protección de terminales (EPP, por sus siglas en inglés), seguridad de servidores, de carga de trabajo y de contenedores, proxies web y seguridad de correo electrónico
- **Infraestructura:** Seguridad de Windows, autenticación de AD, IAM, DHCP, DNS, Cloud Audit-Trails y metadatos de red
- **Enriquecimiento:** Identidades (LDAP), inventarización y clasificación de activos, gestión de configuración, resultados de escáneres de puntos débiles, inteligenck de amenazas (indicadores de compromisos, IOC)
- **Aplicaciones:** Bases de datos, ERP, CRM y API
- **Nube/SaaS:** AWS, Microsoft Azure, Google Cloud, Microsoft 365, Google Workspace y todas las demás aplicaciones SaaS

Onboarding de datos

Le ayuda a extraer la mayor cantidad de conocimientos de sus casos de aplicación más importantes. Los ingenieros de datos de Forescout apoyan a su equipo a la hora de planificar y priorizar las fuentes de datos que se deben vincular. A continuación, ayudan a configurar la pipeline de datos y se aseguran de que sus datos sean analizados sintácticamente, depurados, normalizados y enriquecidos.

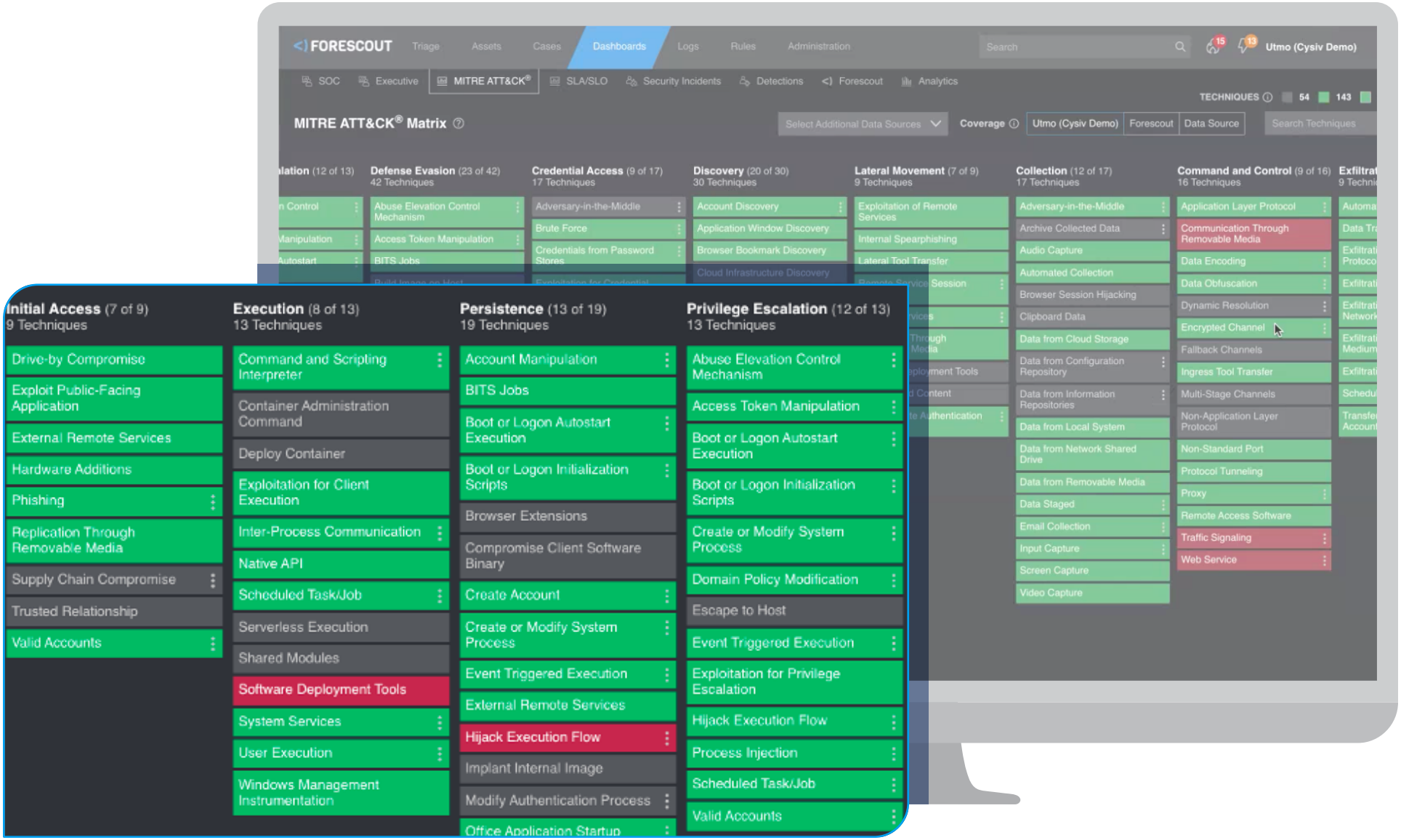
Pipeline de datos avanzada

Administra los datos que, procedentes de fuentes de toda la empresa, se introducen en el motor altamente desarrollado para la detección de amenazas de acuerdo con estrictos principios de las ciencias de datos. Primero, Forescout Threat Detection and Response impone un modelo de información común (CIM) para normalizar los datos recogidos. A continuación, la solución enriqueces estos datos automáticamente con la dirección IP, datos de geolocalización, características ADObject, datos de configuración y otros datos contextuales para proporcionar el contexto de seguridad necesario. Esto maximiza la extracción de conocimientos y acelera la correlación y la caza de amenazas (Threat Hunting) entre numerosas fuentes de datos. Y, por último, se aplica un proceso de extracción, transformación y carga (ETL, por sus siglas en inglés) que permite un análisis de datos más rápido, más estable y más eficiente que los procesos ELT convencionales (extracción, carga y transformación).

Integración del marco ATT&CK® de MITRE

El marco ATT&CK de MITRE hace un seguimiento de las tácticas y técnicas de los ciberataques a lo largo de todo el ciclo de vida del ataque. Forescout Threat Detection and Response está integrado con este marco, lo cual le permite ver de inmediato qué fuentes de datos se deberían registrar para abarcar TTP (Tácticas, Técnicas y Procedimientos) específicos o una extensa variedad de TTP. Podrá descubrir potenciales puntos ciegos, que los atacantes podrían aprovechar, y establecer qué fuentes de datos adicionales podrían mejorar la cobertura.

La integración con el marco ATT&CK de MITRE ayuda a descubrir potenciales puntos ciegos y encontrar maneras de mejorar la detección de amenazas añadiendo más fuentes de datos.



Detección de amenazas altamente desarrollada

Ejemplos de amenazas que se pueden detectar con Forescout Threat Detection and Response

- Mal uso de aplicaciones
- Ataques de fuerza bruta
- Ataques de desbordamiento de búfer
- Escaneo de activos en la nube
- Configuraciones erróneas en servicios de nube
- Nube: Acceso no autorizado
- Nube: Detección de memorias no seguras
- Conexión de comando y control
- Infracciones de cumplimiento
- Cross Site Scripting
- Criptominado
- Extracción de datos
- Accesos a archivos fallidos
- Acceso no autorizado a recursos
- Amenazas internas
- Movimientos laterales
- Malware/brotes de malware
- Escáneres de red
- Desciframiento de contraseñas
- Ataques de phishing
- Escáneres de puertos y vulnerabilidades
- Ransomware
- SQL Injection
- Comportamiento sospechoso
- Acceso no autorizado a sistemas
- Cambio no autorizado de reglas de cortafuegos
- Reinicios de servicios no autorizados
- Creación de servicios/procesos no autorizada
- Aprovechamiento de vulnerabilidades
- Configuración errónea de aplicaciones web
- Ataques a aplicaciones web (todos los ataques web de capa 7)
- Brote de gusanos/virus

Lago de datos basado en la nube

Lago de datos altamente escalable, desarrollado especialmente e indexado con almacenamiento de datos por niveles (tibio, frío) y rápida búsqueda de texto completo. La solución permite un almacenamiento de protocolos a corto plazo, eficiente en cuanto a los costes, y opcionalmente a largo plazo (de 7 días a 1 año+), y administración de datos brutos telemétricos o datos enriquecidos. De este modo se fomenta de forma óptima la satisfacción de las exigencias de seguridad y cumplimiento.

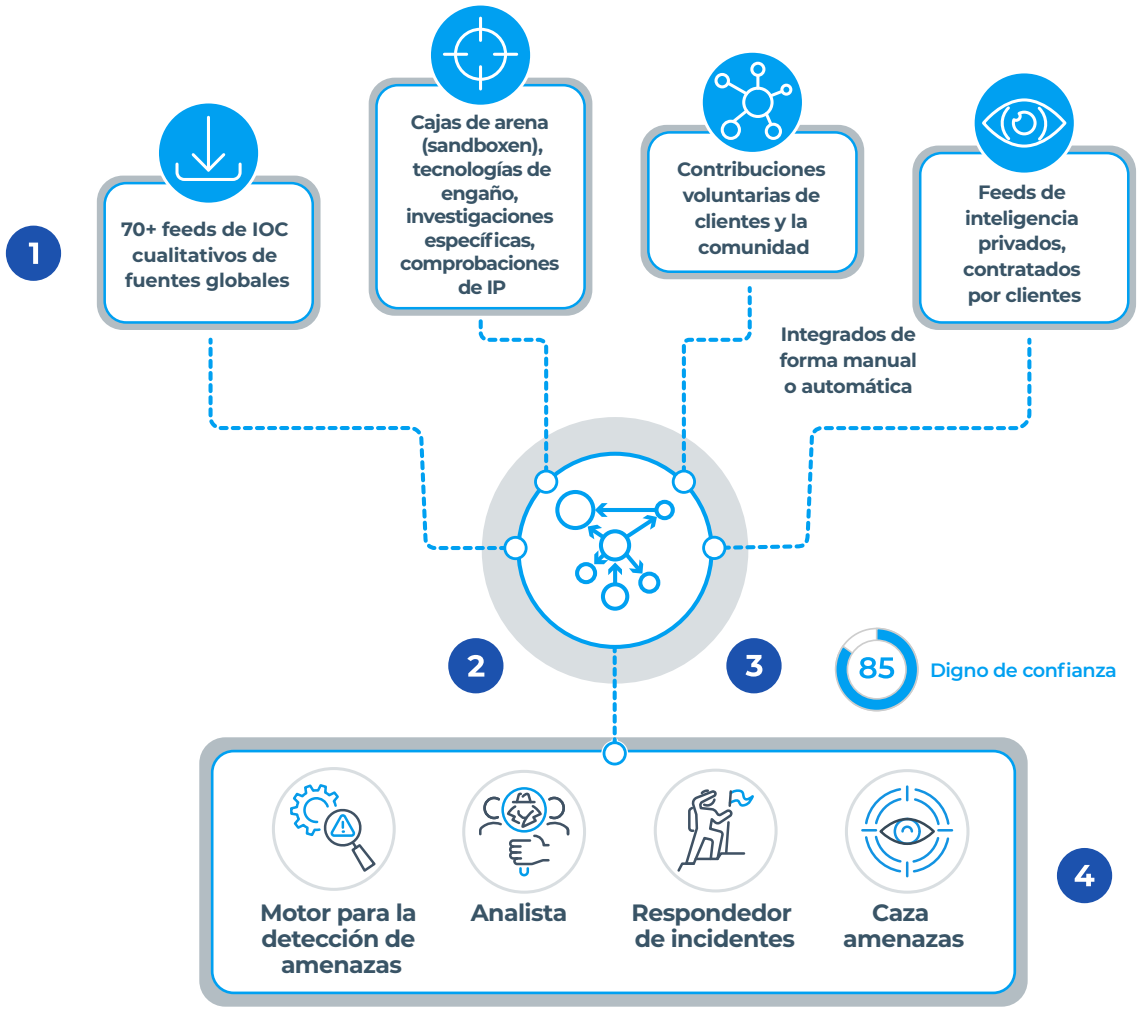
Reglas de detección

La solución ofrece más de 1500 reglas y modelos de detección, comprobadas y aplicables de inmediato, para sus fuentes de datos. Las reglas se han probado con datos productivos para asegurarse de que son efectivas y ofrecen valor añadido desde el primer día. Además, las reglas de detección definidas por el usuario le ofrecen la posibilidad de crear, en una interfaz de usuario dirigida, reglas de estado, detección e indicadores, rápidas y flexibles, para sus exigencias específicas.

Motor para la detección de amenazas

El motor de dos niveles para la detección de amenazas utiliza cinco técnicas de detección para identificar automáticamente y con gran fiabilidad amenazas reales que tienen que ser examinadas y al mismo tiempo filtrar y descartar falsos positivos («ruido»):

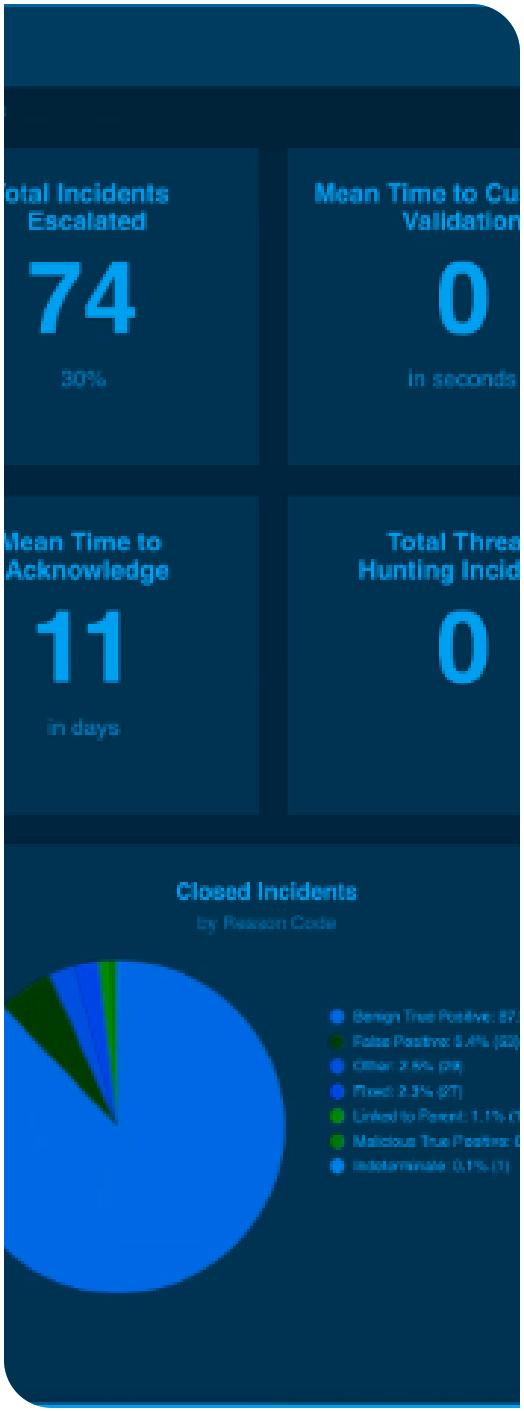
- **Signaturas:** Comparación de características de objetos con un objeto malicioso conocido para detectar amenazas en datos telemétricos, por ejemplo, malware o ransomware, que no se puede eliminar.
- **UEBA:** Busca comportamientos atípicos que se corresponden con muestras digitales, huellas, comportamientos humanos o de red conocidos como maliciosos. Ejemplos: Un empleado de Venta descarga miles de conjuntos de datos de su sistema CRM; actividades insuales fuera del horario de trabajo habitual; beaconing; cambio de ubicación irrealista de un usuario.
- **Estadísticas y valores atípicos:** Identificación de actividades inhabituales con ayuda de técnicas como clusterización, agrupación, apilado, determinación de líneas bases y desviaciones, detección de valores atípicos y regresión logística. Ejemplos: Caída de fuentes de protocolos, ataques de denegación de servicio.
- **Algoritmos:** Utilización de técnicas de IA y AA contextuales, como el aprendizaje supervisado/no supervisado o aprendizaje profundo, para detectar actividades inusuales o maliciosas o predecir ataques. Ejemplos: Identificación de rutas de procesos o algoritmos de generación de dominios (DGA, por sus siglas en inglés).
- **Inteligencia de amenazas:** Uso de más de 70 fuentes de ciberinteligencia para, por ejemplo, buscar puertas traseras y tráfico de comando y control o personas, que accedan a páginas de phishing maliciosas.



Inteligencia de amenazas

Indicadores de Compromiso (IoC, por sus siglas en inglés) de más de 70 fuentes cualitativas, entre ellas, Vedere Labs, el equipo de expertos global de Forescout. Estos IOC se clasifican, endurecen y evalúan para extraer conocimientos valiosos, que se involucran automáticamente en el proceso de detección, búsqueda y examen de amenazas. Los equipos tienen acceso a informes de amenazas detallados de investigadores de Forescout, que elaboran perfiles de atacantes y amenazas peligrosos. Mediante un sistema de intercambio integrado, interno de la comunidad, y un procedimiento «opt-in» se pueden intercambiar datos IOC anonimizados también entre los miembros de la comunidad, incluyendo ISAC específicos del sector.

1. Forescout recopila datos IOC de un amplio abanico de fuentes fiables.
2. Los conocimientos extraídos de los IOC se correlacionan con una base de datos orientada a grafos que contiene dominios, URL y direcciones IPv4 y Ipv6 «conocidos como maliciosos»
3. A cada IOC se le asigna dinámicamente un valor de confianza, basado en una valoración de la calidad de la fuente.
4. Esta información IOC clasificada según la fiabilidad que se le otorga es utilizada a continuación por el motor para la detección de amenazas y por los equipos SOC de los clientes para acelerar y mejorar el examen y la detección de amenazas.



UEBA

Los análisis basados en el comportamiento sirven para detectar cambios de comportamiento o actividades significativos, que no son habituales en una empresa. A lo largo de tiempo se van creando perfiles y comportamientos estándares para los usuarios y dispositivos anfitriones (host). Cada actividad que se desvíe de las líneas basales estándares se clasificará como sospechosa.

Paneles de control e informes

Cuadros de mando preconfigurados y adaptables basados en el personal aportan KPI relevantes para distintos puestos, entre ellos analistas/respondedores de incidentes, técnicos, directores de SOC, directores de cumplimiento, gestores de riesgo o directivos. Mediante la distribución proactiva de informes y/o métricas se suministra información importante tanto a los empleados encargados de los procesos en el SOC como a los miembros del equipo directivo.

SOAR

Orquesta, con gestión de fallos integrada y notificaciones, todo el proceso del SOC, desde la detección, pasando por el examen, hasta la respuesta. Forescout Threat Detection and Response automatiza los procesos de seguridad mediante el enriquecimiento, por ejemplo, con datos de ubicación IP, información sobre usuarios y activos y correlación con numerosas fuentes de información. La solución utiliza Forescout eyeSight y eyeControl para los procesos automatizados de dirección y respuesta, en los que se puede involucrar a cualquier dispositivo administrado y no administrado (no compatible con agentes) de una empresa. Gracias a la integración con Palo Alto Cortex XSOAR y otras soluciones SOAR, puede seguir usando también su SOAR existente.

Nativo en la nube

No requiere implementación; cada dos semanas se ponen a disposición nuevas funciones, correcciones y reglas sin transición.

Integración en SIEM

Las verdaderas amenazas establecidas por Forescout Threat Detection and Response se pueden incorporar al SIEM existente para la orquestación y la respuesta centralizada de incidentes.

Actualización continua de software y contenidos

A intervalos de dos semanas se ponen a disposición nuevas características, funciones y soluciones de fallos, así como nuevas reglas y modelos de detección, sin que se produzcan perturbaciones ni se requiera asistencia por parte de la empresa.

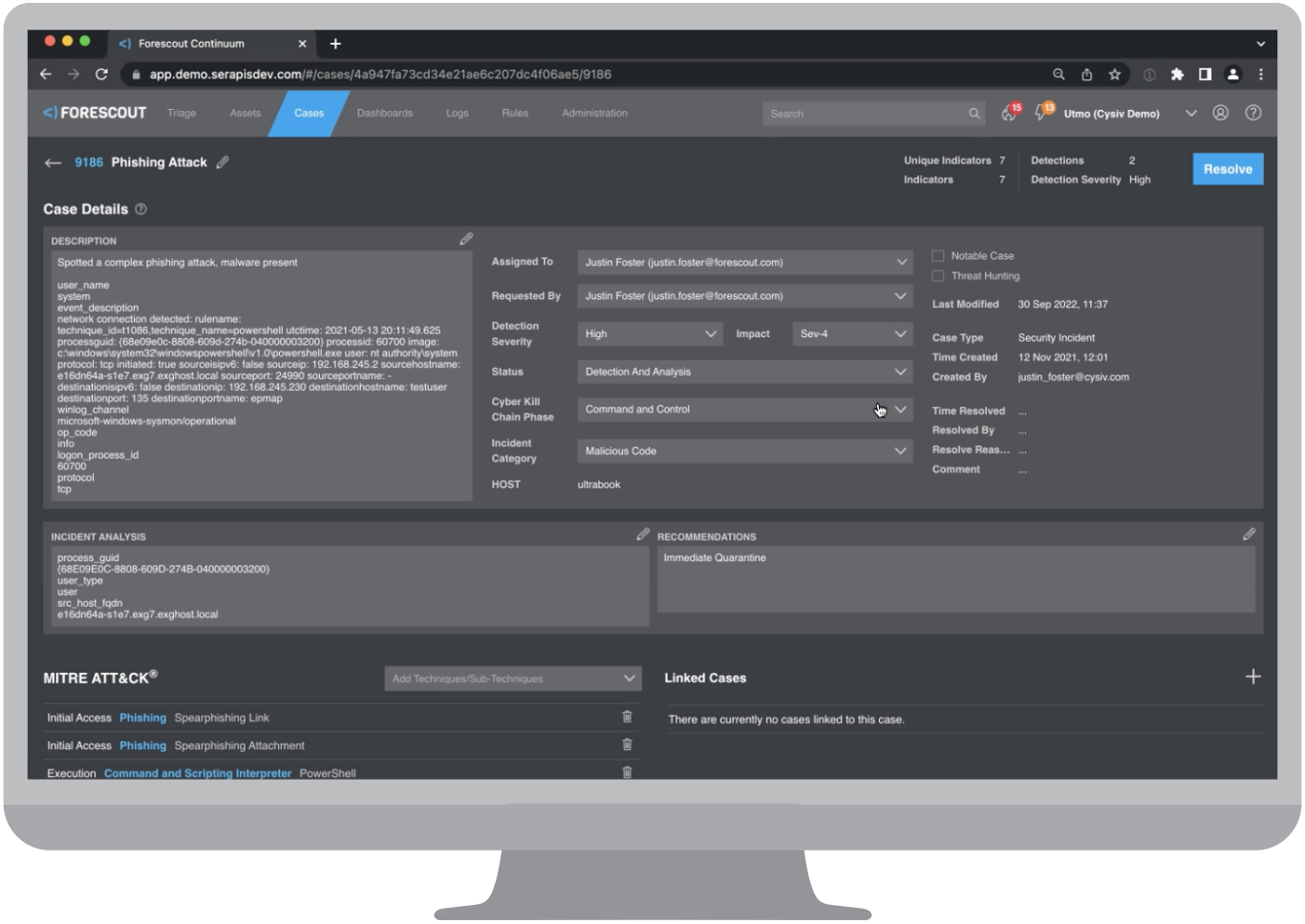
Arquitectura de tenencia múltiple

Puede crear de forma sencilla divisiones lógicas (tenedores o instancias), por ejemplo, basándose en países, sedes o áreas de negocio. También puede crear vistas agregadas y llevar a cabo consultas y análisis sobre múltiples instancias y unidades de negocio a la vez, hasta incluso a nivel global. Esto supone una ventaja especialmente para grandes empresas, multinacionales, MSSP y organizaciones con SOC regionales.

Arquitectura global unificada

Permite satisfacer sin problema las exigencias de cumplimiento normativo y de residencia de datos y apoya las medidas de seguridad regionales de forma asequible. Usted puede establecer en cuál de las 25 regiones de Norteamérica, Sudamérica, Europa y Asia-Pacífico se almacenan sus protocolos. Independientemente de ello, podrá ver y acceder a sus datos en todo momento desde todo el mundo.

La gestión de casos aporta detalles exhaustivos y permite exámenes y respuestas más rápidos y efectivos.

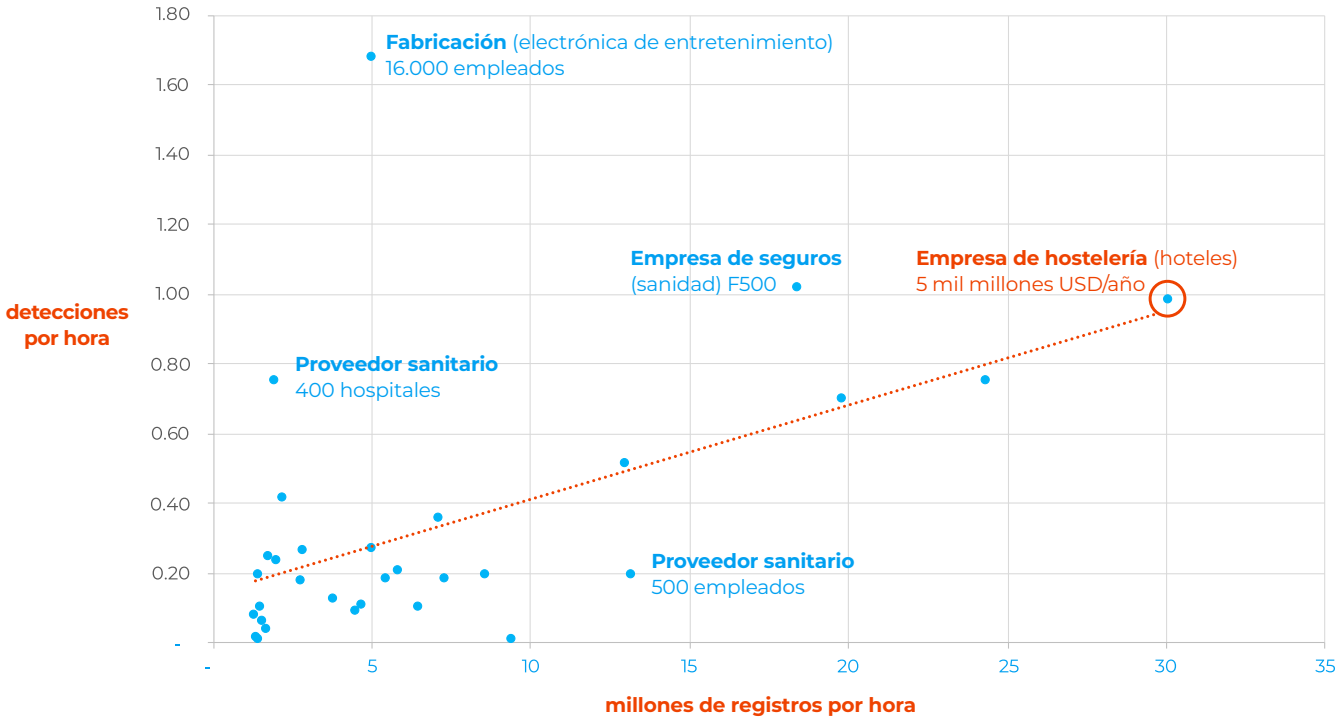


La solución es compatible con flujos de trabajo, una integración estrecha, transparencia y una comunicación y cooperación sin fisuras para el procesamiento de detecciones y la gestión de incidentes. Forescout Threat Detection and Response se basa en el NIST Incident Response Life Cycle y permite integraciones con ServiceNow, RSA Archer, Jira Software, ManageEngine ServiceDesk Plus, Palo Alto Cortex XSOAR, TheHive y ConnectWise.

Resultados

No importa si tiene millones, decenas de millones o cientos de millones de registros, Forescout Threat Detection and Response puede penetrar automática y rápidamente en la avalancha de datos para generar una cantidad muy pequeña de detecciones altamente fiables que requieren la intervención de analistas humanos.

El siguiente diagrama muestra los datos de 31 clientes durante el periodo de un año a partir del 15 de diciembre de 2021. Por ejemplo, una empresa hotelera con un volumen de venta anual de 5 mil millones podría reducir de media 30 millones de registros por hora a 0,98 detecciones que requieren acción por hora.



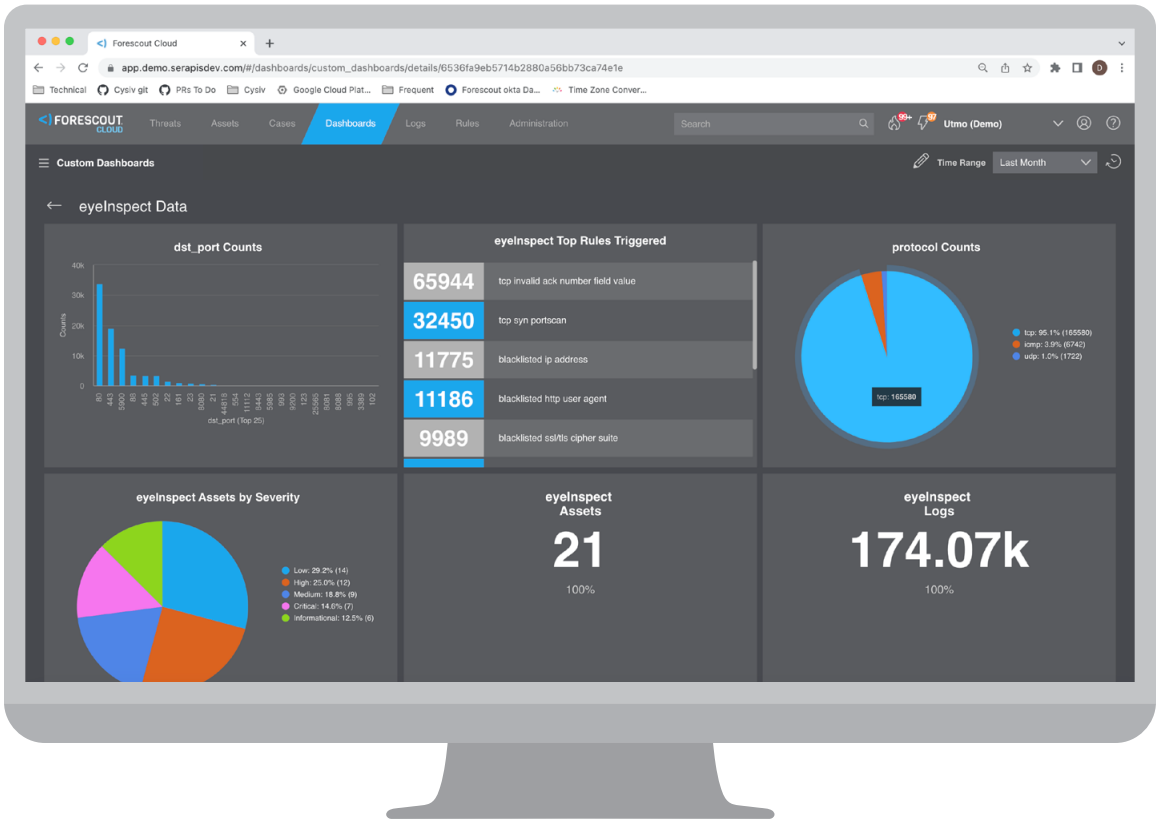
Notas:

- Están representadas empresas de diferentes tamaños y diversos sectores:
  - Construcción
  - Bienes de consumo
  - Empresas energéticas y de suministro
  - FinTech
  - Sanidad
  - Seguros
  - Producción
  - Minería
  - Editorial
  - Tecnología
  - Transporte/logística
- Los resultados individuales pueden variar y dependen de diferentes variables, como los casos de aplicación, selección de los protocolos, número total de protocolos y adaptación continua de reglas.

1 The State of Security Operations, Forrester, 2020
2 El punto final se refiere a cada dirección IP y MAC de un dispositivo de usuario, un dispositivo de infraestructura de red, un dispositivo no relacionado con un usuario o un componente de una infraestructura de red.

Forescout

Threat Detection and Response



VEA a FORESCOUT Threat Detection and Response EN ACCIÓN

forescout.com/xdr-demo-request

FORESCOUT

Forescout Technologies, Inc.

Gratuita (EE. UU.) 1-866-377-8771
Tel. (internac.) +1-408-213-3191
Asistencia +1-708-237-6591

Descubra más en Forescout.com

Forescout

Threat Detection and Response

FORESCOUT