

Proveemos
soluciones que garantizan
La Seguridad

y el buen desempeño en su infraestructura de IT, on-premise y en la nube



Consultorias
tecnologías
Seguridad y riesgos

ICT



Engineering & Services



ANÁLISIS DE TRAFICO DE RED

Soluciones para NOC

✓ **Allegro Packets**
Network Multimeter

Con Allegro Packets Network Analyzer detectas los problemas de red con solo unos pocos Clicks

✓ **Netreo**

Monitorización y visibilidad completa y AIOps observe y automatice todo en la empresa en un único panel unificado, desde donde quiera que esté.

Soluciones Para seguridad y gestión de End Points

✓ 
CROWDSTRIKE

Ciberseguridad que previene las amenazas a mayor velocidad, mayor escala y mayor precisión de lo que es humanamente posible. Somos XDR.

✓ 
filewave

Con FileWave administra todos los diferentes dispositivos de la compañía. Cada miembro del personal de TI siente como si tuviese 10 asistentes que pueden alcanzar cualquier dispositivo en cualquier momento, sin importar dónde se encuentre.



Netreo™

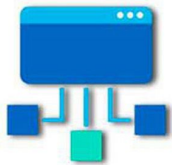
Monitorización y visibilidad completa y AIOps

Observe y automatice todo en la empresa en un único panel unificado, desde dondequiera que esté



OBSERVAR

Visibilidad completa de la infraestructura de TI, los sistemas, las aplicaciones y la experiencia del usuario, en un único panel de control personalizado.



ANALIZAR

El motor de AIOps de Netreo ofrece respuestas sencillas a partir de montañas de datos aprovechando más de 20 años de líneas de base y tendencias históricas.



ACTUAR

Netreo ofrece cuadros de mando (dashboards) en tiempo real, automatizaciones dinámicas y una integración extensible de Gestión de Servicios de TI (ITSM) para que pueda centrarse en tomar medidas inteligentes.

MONITOREO Y GESTIÓN

DE INFRAESTRUCTURA DE TI PARA CUALQUIER INDUSTRIA

Sector Financiero/Banca

La forma en que los bancos y las instituciones financieras prestan sus servicios está cambiando rápidamente. A medida que aumenta la lista de servicios digitales prestados por su institución, sus clientes esperan un tiempo de actividad y acceso a sus aplicaciones del 100%. ¿Cómo va a satisfacer las expectativas de los clientes?

Venta Al Por Menor

Las operaciones de TI tienen un papel estratégico a la hora de proporcionar una experiencia excepcional al cliente en el comercio minorista. Para maximizar el tiempo de actividad y el rendimiento de las aplicaciones y la infraestructura, desde el comercio electrónico hasta los sistemas de punto de venta, es necesario disponer de información procesable en todo el entorno de TI.

Sanidad/Salud

Con la implantación de las historias clínicas electrónicas y otros sistemas de información sanitaria, se ha producido un crecimiento explosivo de la cantidad de datos capturados por las organizaciones proveedoras. ¿Cómo va a mantener su organización sanitaria las operaciones de TI?



GTB Technologies
Data Protection that Works™



IDENTIFIQUE, COMPRENDA, SUPERVISE, CONTROLE Y PROTEJA LOS DATOS CONFIDENCIALES CON EL NUEVO ESTÁNDAR EN SEGURIDAD Y PROTECCIÓN DE DATOS

La plataforma GTB Data Security that Works™ mejora y moderniza las capacidades y funciones de Data Discovery y Data Classification, detectando de manera precisa y automática los intentos de violación de datos al mismo tiempo que brinda una respuesta automática independientemente donde se encuentren los datos (locales, remotos, en nube)

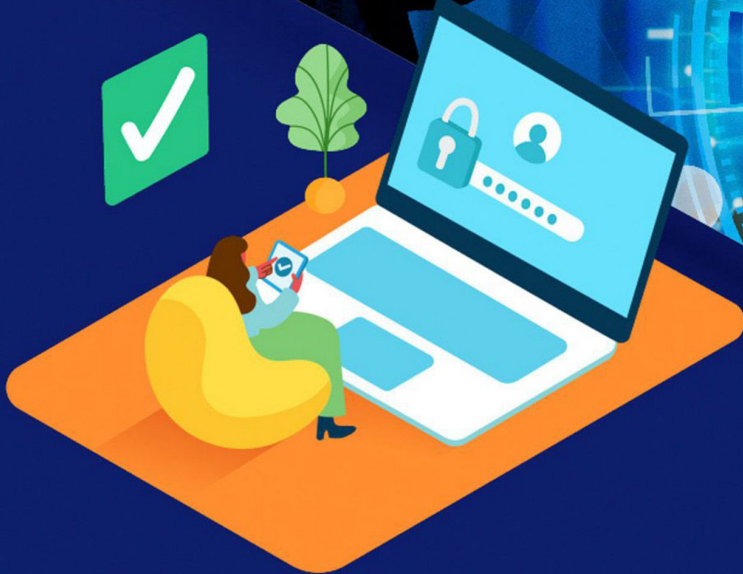
PREVENCIÓN DE PÉRDIDA DE DATOS (DLP) INTELIGENTE, INTELIGENTE Y PRECISO

En tiempo real y preciso, un cortafuegos inverso consciente del contenido inspecciona, clasifica y analiza TODAS las transmisiones de datos entrantes y salientes en tiempo real. TODOS los canales y TODOS los tipos de datos, estructurados y/o no estructurados, incluida la detección OCR y la nube (AWS, Azure, Google). Incluye correo electrónico DLP.





GTB Technologies
Data Protection that Works™



PROTECTOR ENDPOINT, DLP, UBA, ITM CON OCR Y HUELLAS DACTILARES

Certificación OPSWAT. ¡FUERA DE LAS INSTALACIONES, detección de huellas dactilares en tiempo real para datos en uso! Ninguna otra solución puede. Correo electrónico DLP, clasificador de datos, control inalámbrico, OCR, SSL sin proxy, POS, redes sociales, correo electrónico, aplicaciones como BOX, Dropbox y más.

DESCUBRIMIENTO DE DATOS, CLASIFICACIÓN, MARCA DE AGUA, OCR. EN TIEMPO REAL, AUTOMÁTICAMENTE

Certificación OPSWAT. Descubra, localice, identifique, clasifique e inventaria con precisión: sus datos críticos, incluidos Exchange, PST/OST, NAS, SharePoint, archivos compartidos, almacenamiento local, almacenamiento en la nube (Google, BOX, Dropbox, OneDrive...), incluida la detección OCR.

GESTIÓN DE DERECHOS DIGITALES CON CONSCIENCIA DEL CONTENIDO

Control de acceso integral a datos confidenciales para usuarios internos y externos. El sistema controla automáticamente 4 Ws QUIÉN puede acceder a la información, QUÉ pueden hacer los destinatarios con la información, CUÁNDO puede acceder cada usuario a la información y DÓNDE se puede utilizar la información.



GTB Technologies
Data Protection that Works™



SEGURIDAD EN LA NUBE Y CONTROL DE APLICACIONES

Controle los datos desde y hacia una mirada de fuentes: computadoras portátiles, intercambios de bases de datos, todos los servicios e infraestructuras en la nube, como AWS, Amazon Cloud, Azure, Box, Dropbox, Evernote, Google Cloud, Google Docs, Google Drive, Office 365, OneDrive, Salesforce, Skype for Business y más para Shadow IT (BYOX). CASB de GTB con un toque

AUDITOR DE ARCHIVOS Y BASES DE DATOS

Certificación OPSWAT. Descubra, localice, identifique, clasifique e inventaria con precisión: sus datos críticos, incluidos Exchange, PST/OST, NAS, SharePoint, archivos compartidos, almacenamiento local, almacenamiento en la nube (Google, BOX, Dropbox, OneDrive...), incluida la detección OCR.

🏆 **GANADOR 2022 Mejor proveedor de soluciones DLP**

🏆 **GANADOR 2021 Mejor empresa de ciberseguridad**

📌 **VIRTUAL ZERO FALSOS NEGATIVOS Y POSITIVOS...
CUMPLIMIENTO UNIVERSAL DE POLÍTICAS**

censornet.

SECURITY TRANSFORMED A SINGLE CLOUD PLATFORM

Our world class cyber security platform provides full spectrum threat protection for your organization, integrating email and web security, CASB and MFA, enabling the Autonomous Security Engine to take you beyond alert driven security and into real-time automated attack prevention.

At Censornet we believe that security should work automatically, and enable businesses to achieve more without threats or complications. By making security simple, Censornet allows you to run your business safe in the knowledge that your protected every step of the way.



**100% cloud-based,
ultra-modern,
unparalleled email
protection**

Advanced email security providing comprehensive protection against all email threats.



**Lightning fast
protection for users
no matter where
they are**

Unrivalled web security offering protection from all web-related threats including web-borne malware, and offensive or inappropriate content.



**Visibility and
protection at every
stage of an attack**

Integrated with web security, CASB allows you to discover, analyze, secure and manage user interaction with cloud apps for complete protection



**powered by
IntelliTrust. So
much more than
password protection**

An additional layer of protection to user accounts eliminating account compromise and identity related threats.



AUTONOMOUS SECURITY ENGINE

**Cyber security that's faster, smarter, safer than
humanly possible**

Automated alerts don't stop attacks. Censornet's ASE takes automatic real-time action to protect against threats and prevent attacks, around the clock, with minimal to zero human input.

Enabling traditionally silo'd products to share and react to security events, whilst leveraging world-class threat intelligence, ASE prevents attacks before they enter the kill chain.



censornet.

A SINGLE CLOUD PLATFORM

Censornet's cloud security platform integrates email and web security, Cloud Access Security Broker (CASB) and adaptive Multi-Factor Authentication (MFA) - activate the Autonomous Security Engine (ASE) and take your business beyond alert driven security and into real-time automated attack prevention.

ASE enables traditionally silo'd services to share and react to security events and state data whilst leveraging world class threat intelligence - delivering security outcomes, instead of events and alerts, to already overwhelmed security teams.

E.
EMAIL

W.
WEB

C.
CASB

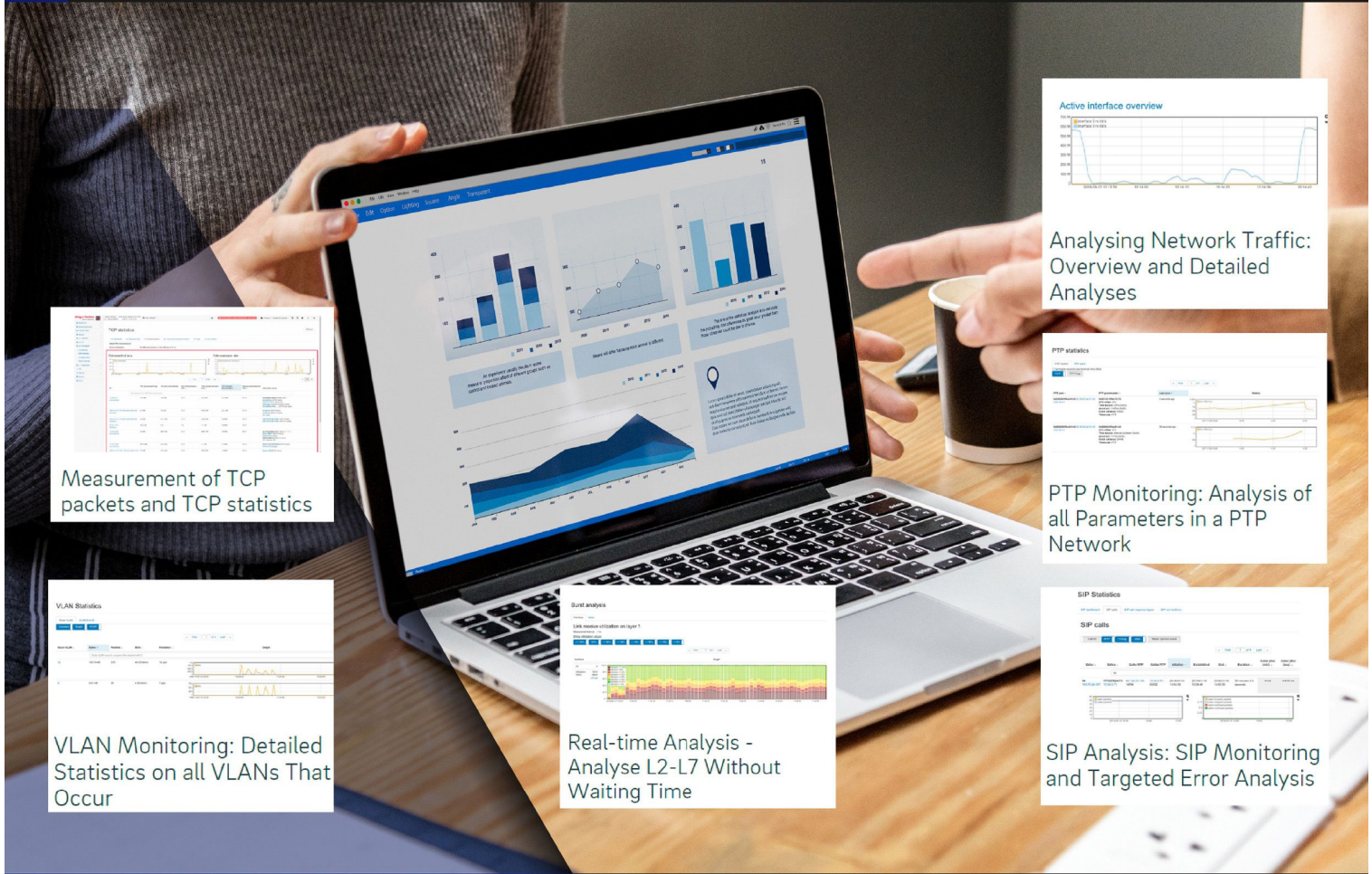
M.
MFA

ASE

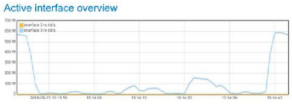
AUTONOMOUS SECURITY ENGINE

SECURITY TRANSFORMED



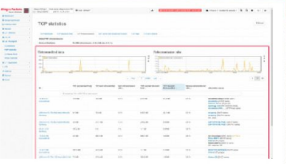


Active interface overview




Analysing Network Traffic: Overview and Detailed Analyses

TCP statistics




Measurement of TCP packets and TCP statistics

PTP statistics




PTP Monitoring: Analysis of all Parameters in a PTP Network

VLAN Statistics



VLAN Monitoring: Detailed Statistics on all VLANs That Occur

Real-time analysis



Real-time Analysis - Analyse L2-L7 Without Waiting Time

SIP Statistics



SIP Analysis: SIP Monitoring and Targeted Error Analysis

Monitorize en Tiempo Real de la Capa 2 a la capa 7 hasta 100 Gbit/s

Allegro Packets

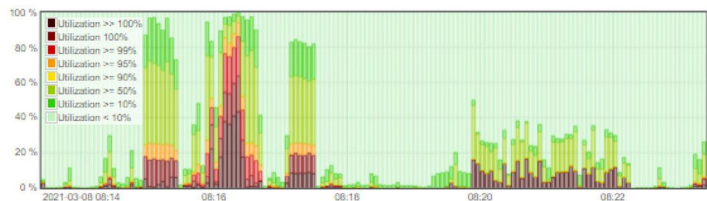
Network Multimeter

TE IMAGINAS
PODER ENCONTRAR
LOS PROBLEMAS
DE RED EN POCOS
SEGUNDOS?

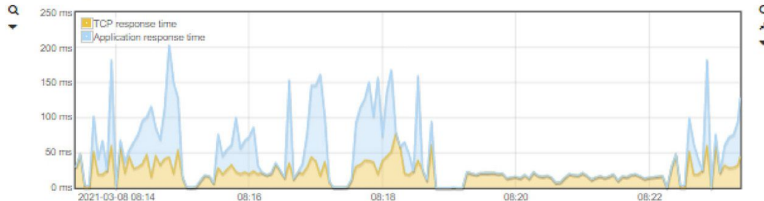
Con Allegro Packets Network Analyzer
detectas los problemas de red
con solo unos pocos Clicks

Análisis En tiempo Real con Fácil y Rápido Retrospectivo PCAP

Burst analysis



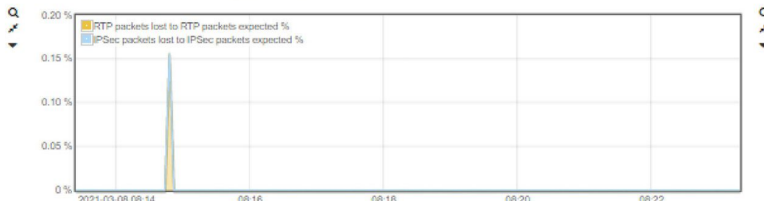
Response time TCP / Application



Jitter RTP / Profinet



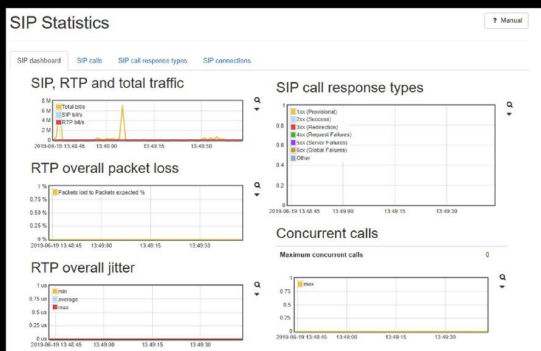
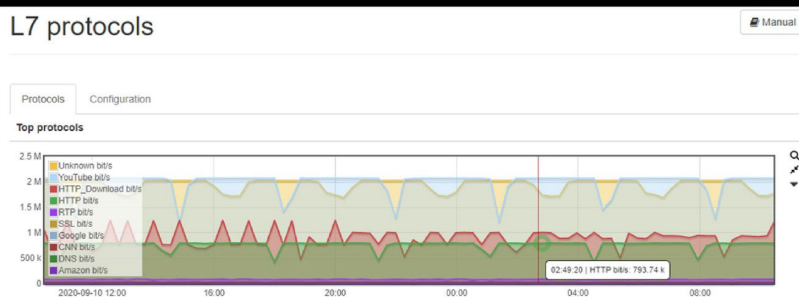
Packet loss RTP / IPSec / Profinet



Soluciones para Monitorización de RED Allegro Packets

Localizar y resolver eventos de red en cuestión de minutos para infraestructuras Físicas y Virtualizadas, Cobre y Fibra, desde 1Gbps hasta 100Gbps.

Detección de problemas en minutos, Tráfico de Aplicaciones, VoIP, Redes Industriales ,

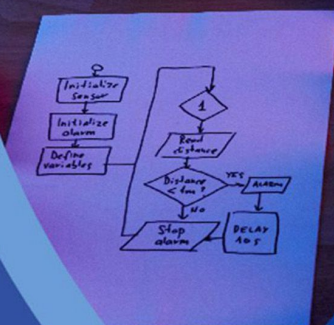


Principales diferenciales de Allegro-Packets

- Amplia gama de dispositivos, desde unidades ultra portátiles de 2G a unidades de montaje en rack de 100G.
- Todas las estadística están almacenadas en RAM: (esto hace que el análisis sea muy rápido inclusive para velocidades de 100Gbps)
- Fácil y rápido retrospectivo PCAP
- Mismo software en todos los dispositivos.
- El software todo en uno incluye todas las funciones (sin cargos adicionales por módulos como las estadísticas de VoIP).
- Análisis de capa 2 - 7.
- Medida de retardo real de las aplicaciones (path measurement)
- Precios atractivos y competitivos con otras soluciones.
- Remote packet processing
- Desarrollado 100% En Alemania

Cada 11 segundos 1 empresa es víctima de un delito cibernético.

¿Podrías ser el próximo?



QUE PUEDE HACER GRADIENT CYBER POR USTED?

Identificar, proteger, responder y recuperar.

Cuando se trata de ciberseguridad, los equipos de TI más pequeños tienen el trabajo más difícil que existe. Eso es porque debe ocuparse de todo lo relacionado con TI, además de administrar la seguridad.

Con demasiada frecuencia, no hay nadie en tu equipo dedicado a la seguridad, e incluso si lo hay, los malos no se desconectan y tu persona de seguridad no puede trabajar las 24 horas del día, los 7 días de la semana.

La elección parece ser: hacerlo solo, o intentar obtener el presupuesto para más herramientas de ciberseguridad.

¡Ya no!

SIMPLIFY CIBERSECURITY

PROXIMA GENERACIÓN DE OPERACIONES DE SEGURIDAD

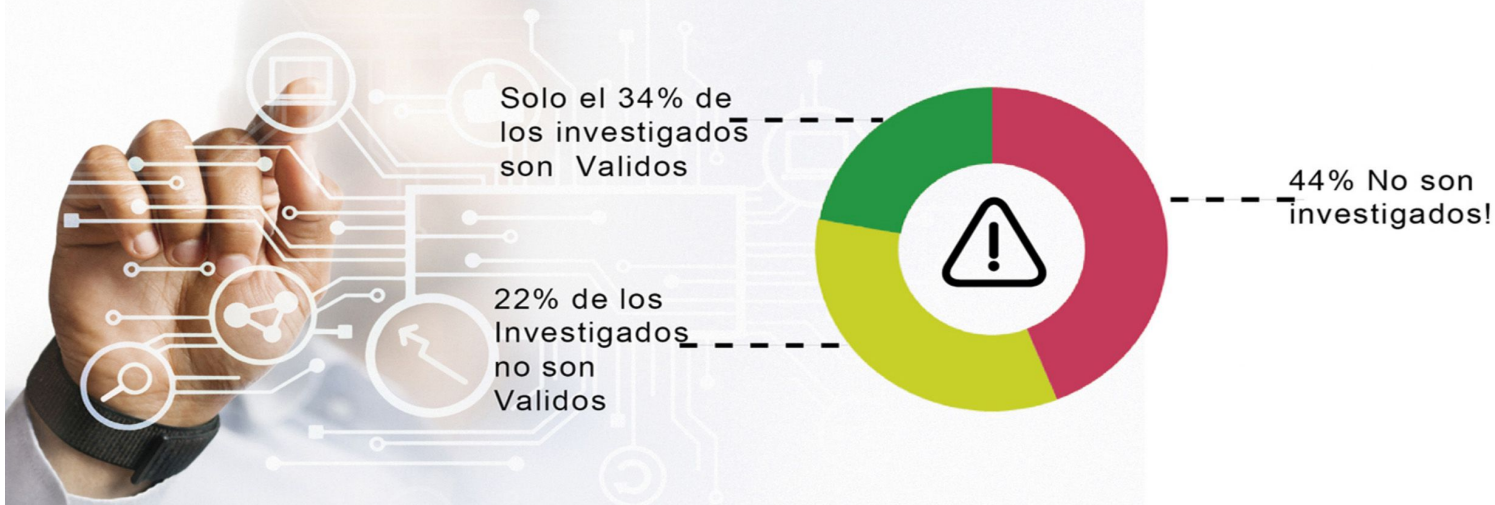
Gradient le ayuda a :

- ✓ Gestionar el riesgo
- ✓ Proteger su imagen y salvaguardar su balance final
- ✓ Simplificar y ampliar su capacidad de gestión de la ciberseguridad

Gestión automatizada de riesgos y amenazas impulsada por inteligencia artificial con mayor experiencia cibernética humana

PROBLEMA: DEMASIADA POTENCIALES AMENAZAS

Miles de Security Logs y Eventos cada día.



ENORME EXPOSICION AL RIESGO!

UNA PLATAFORMA

Gradient es el unico en entregar todas estas funciones en una unica plataforma

NTA – Network Traffic Analysis

SIEM – Security Information Event Management

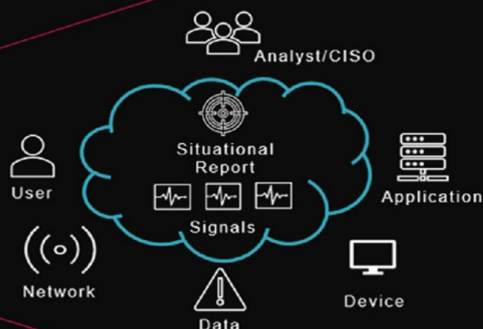
TI – Threat Intelligence

Gradient.

- Vista Centralizada
- Visibilidad mas amplia
- Ruido reducido
- Cumplimiento mas facil
- Mayor efficiency

EUBA - End User Behavior Analysis

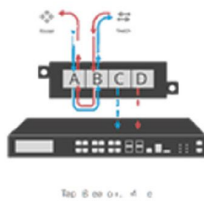
SOAR – Security Operations & Automated Response



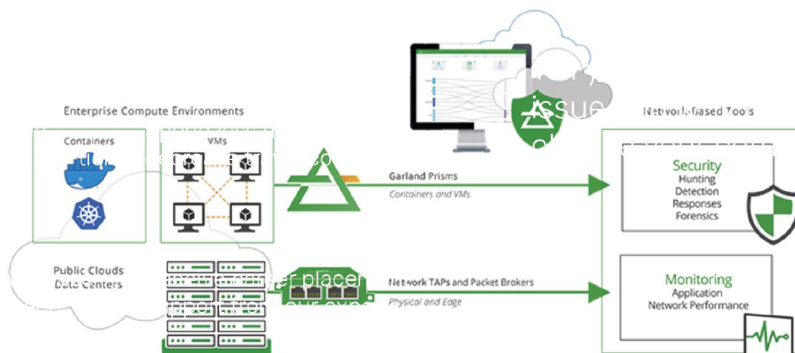


SOLUCIONES PARA MONITORIZACIÓN DE RED

ENTORNOS FISICOS NETWORK TAPS NETWORK PACKET
BROKERS INLINE BYPASS



ENTORNOS VIRTUALES Y EN LA NUBE GARLAND PRISMS



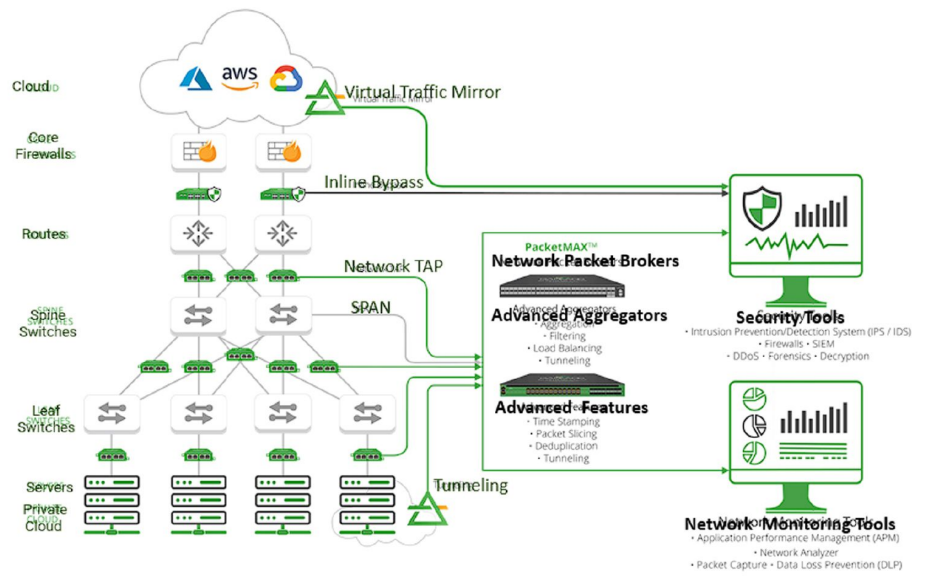


VISIBILIDAD DE PAQUETES EN CUALQUIER ENTORNO

INFRAESTRUCRA EN LA NUBE

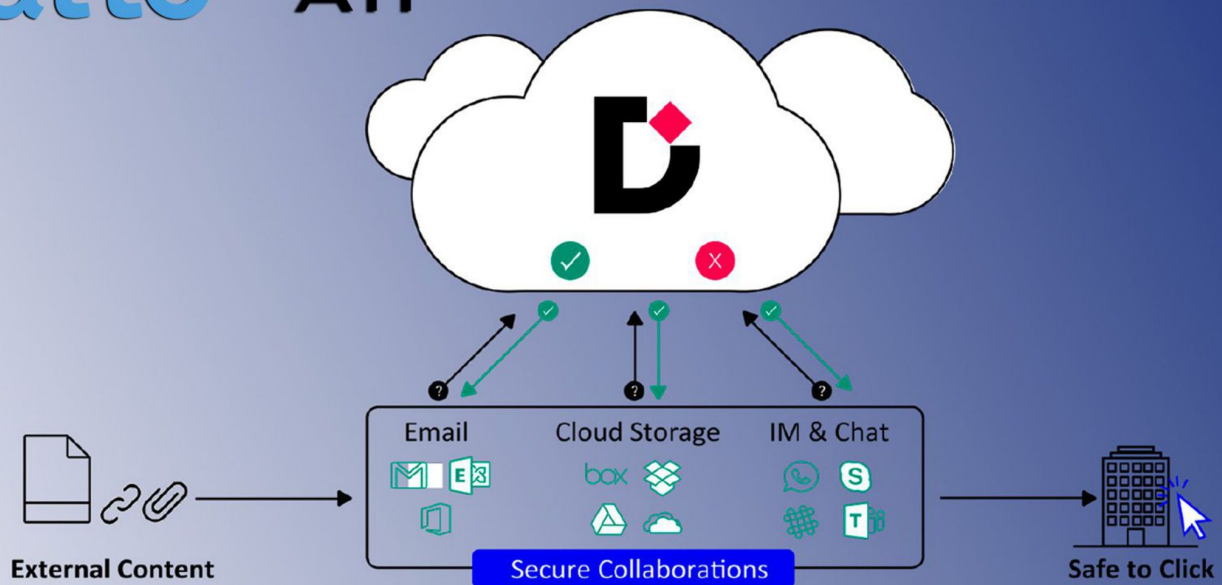
INFRAESTRUC TURA FISICA

INFRAESTRUCTURA VIRTULIZADA



datto

ATP



BitDam hace que todos los canales sean seguros al hacer click.

datto

Asegura el contenido en todos los canales de colaboración empresarial: servicios de correo electrónico de cualquier proveedor, almacenamiento en la nube y servicio de intercambio de archivos, mensajería instantánea y más, todo en un solo lugar.



Email

Proteja Microsoft Exchange, Microsoft Office 365, G-Suite o cualquier otro servicio de correo electrónico para resguardar sus empleados de correos electrónicos maliciosos.



Almacenamiento en la nube y uso compartido de archivos

Proteja Microsoft OneDrive, Sharepoint, Google Drive, Dropbox, Box o cualquier otra unidad en la nube, para garantizar que los usuarios finales.



Chat y mensajería instantánea

Convierta su mensajería instantánea empresarial en una zona segura con BitDam para Slack, Skype, Teams, Zoom y otras plataformas de chat.



BREACHES STOP HERE

CLOUD-DELIVERED
ENDPOINT PROTECTION



CROWDSTRIKE FALCON: THE NEW STANDARD IN ENDPOINT PROTECTION

AUTOMATICALLY PREDICT AND PREVENT THREATS IN REAL TIME

The CrowdStrike Falcon® platform's single-lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph® database, CrowdStrike Falcon correlates trillions of endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

THE CROWDSTRIKE DIFFERENCE

SINGLE LIGHTWEIGHT AGENT

Provides frictionless deployment and stops all types of attacks while eliminating agent bloat and scheduled scans

CLOUD-NATIVE PLATFORM

Leverages the network effect of crowdsourced security data while eliminating the management burden of cumbersome on-premises solutions

PROPRIETARY THREAT GRAPH

Uses cloud-scale AI and rich contextual relationships from multiple telemetry sources in a massive distributed graph database that accurately predicts and prevents threats to stop breaches with no human interaction required

CROWDSTRIKE FALCON: REDEFINING SECURITY FOR THE CLOUD ERA

They said it was impossible to provide complete endpoint protection using a single lightweight agent with no impact on user performance.

CrowdStrike proved them wrong. With the revolutionary cloud-native CrowdStrike Falcon security platform, **it is possible to:**

Prevent both commodity and sophisticated attacks — whether they use malware or not, regardless of whether your endpoints are online or offline

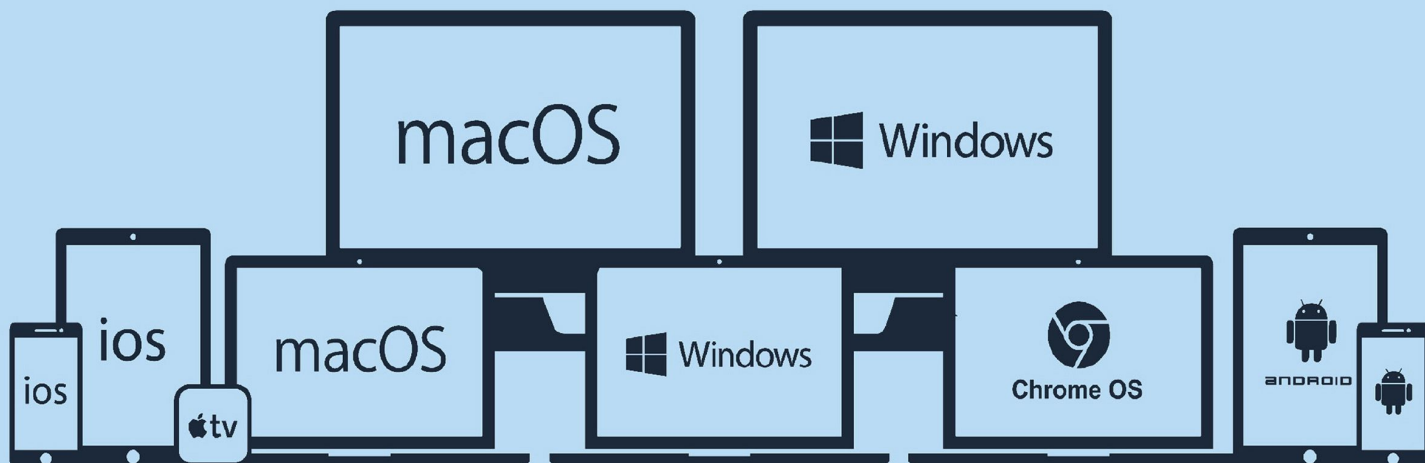
Gain real-time endpoint visibility and insight into applications and processes running anywhere in your environment, ensuring that nothing is missed and everything that requires a response gets one

Proactively hunt down advanced threat activity — faster and more effectively than ever before

Protect all workloads, from mobile devices to traditional endpoints running Windows, macOS and Linux, as well as cloud workloads, servers and containers in modern hybrid multi-cloud data centers

Eliminate the bloat and massive performance impact that comes with legacy antivirus solutions, replacing it all with a single lightweight agent built for speed

UNIFIED ENDPOINT MANAGEMENT (UEM) AND IT ASSEST MANAGEMENT (ITAM)



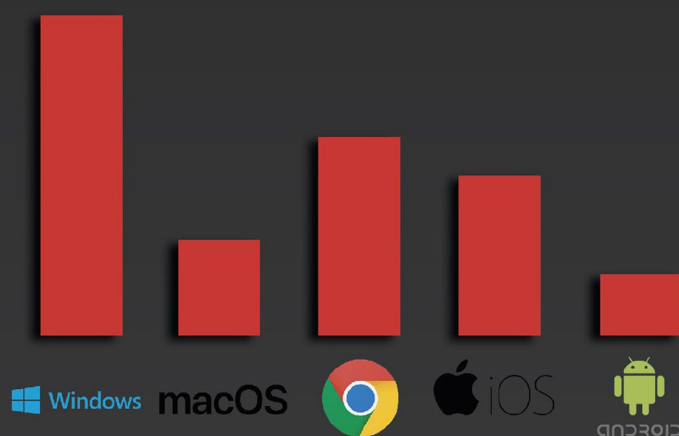
The better way to manage and enable users

filewave

ICT 
Engineering & Services

Los 5 principales desafíos que escuchamos de TI son...

1. ¡Necesito conectarme a todos los dispositivos fuera de mi red o dominio!
2. Necesito administrar un entorno de SO mixto y en crecimiento.
3. Necesito una forma de rastrear mis activos: dónde están ubicados, cómo están configurados y qué se instala en ellos.
4. Mi personal dedica demasiado tiempo a solucionar problemas y necesito una forma más sencilla de detectar y solucionar problemas ... fuera de la red.
5. Tenemos demasiadas herramientas de administración para implementar y configurar cada tipo de dispositivo diferente (Windows, macOS, iOS / tvOS, Android y Chrome)

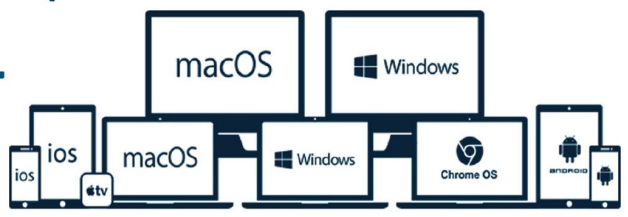


NO ES SUFICIENTE PERSONAL, NO SUFICIENTES HORAS AL DÍA

Con FileWave administrando todos nuestros diferentes dispositivos en todo el distrito, cada uno de nuestro personal de TI siente que tiene 10 asistentes que pueden tocar cualquier dispositivo en cualquier momento, sin importar dónde se encuentre.

UNIFIED ENDPOINT MANAGEMENT - Made Simple

SU KIT "UEM " ESENCIAL
MDM+EMM+ITAM
ALL-INCLUSIVE



Imaging/Provisioning

Remote Desktop

Gestion de Licencias

Strategic Integrations
(Hayes Software, Content Keeper...)

Distribución de software y aplicaciones

Rastreo de Dispositivos

Uso de software

Premier Partner

Kiosko de Autoservicio

Descubrimiento de Dispositivos

Self-Healing

Microsoft Partner

Gestión Parches

Gestión de Activos

Auto-Resuming Deployments

Premier Partner

android enterprise recommended
Clever

Aproveccionamiento

Proporcionar una experiencia de incorporación perfecta para los nuevos empleados con procesos personalizables que distribuyen y parchean el software, apoyan a los usuarios y más desde una herramienta conveniente

Gestión de parche

Reducir el riesgo de violación de la privacidad mediante la aplicación automática de los parches de seguridad necesarios, la agrupación automática de los dispositivos y la personalización de los informes.

Gestión de parche

Proporcione a los trabajadores remotos la capacidad de entregar software, aplicaciones y más desde cualquier lugar, mientras ahorra el valioso tiempo de su equipo de TI.

Gestión de activos de TI

Ahorre el tiempo y el presupuesto de su equipo de TI haciendo un seguimiento de los dispositivos perdidos, reduciendo las licencias de software desperdiciadas e identificando los dispositivos que necesitan ser reemplazados.