ABSOLUTE®

Impulsando más allá de la Innovación

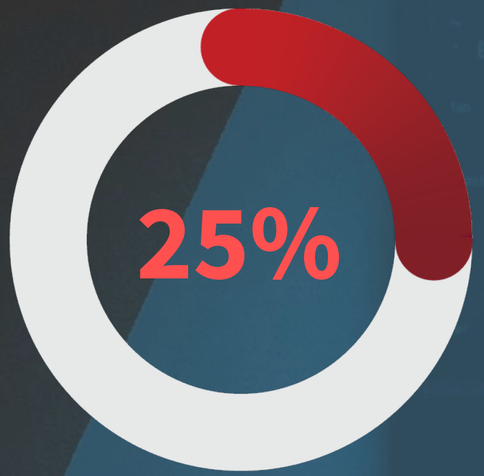
Polo Sánchez //Sales Director NOLA Region
Absolute LATAM

“Soy optimista y sé que todavía puedo ganar”

– Tadej Pogacar

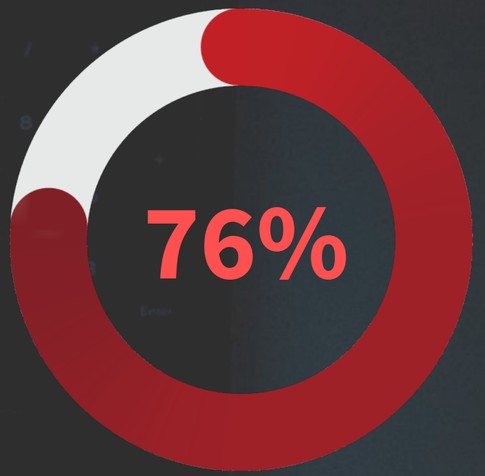
El talón de Aquiles: Dispositivos y el Acceso a la red

El 68 % de las organizaciones sufrieron un ataque de dispositivos exitoso en los últimos 12 meses[1].



de los dispositivos tenían controles de seguridad poco saludables[2]

de las organizaciones han visto evidencia de dispositivos comprometidos que se utilizan para acceder a los datos de la empresa[3]

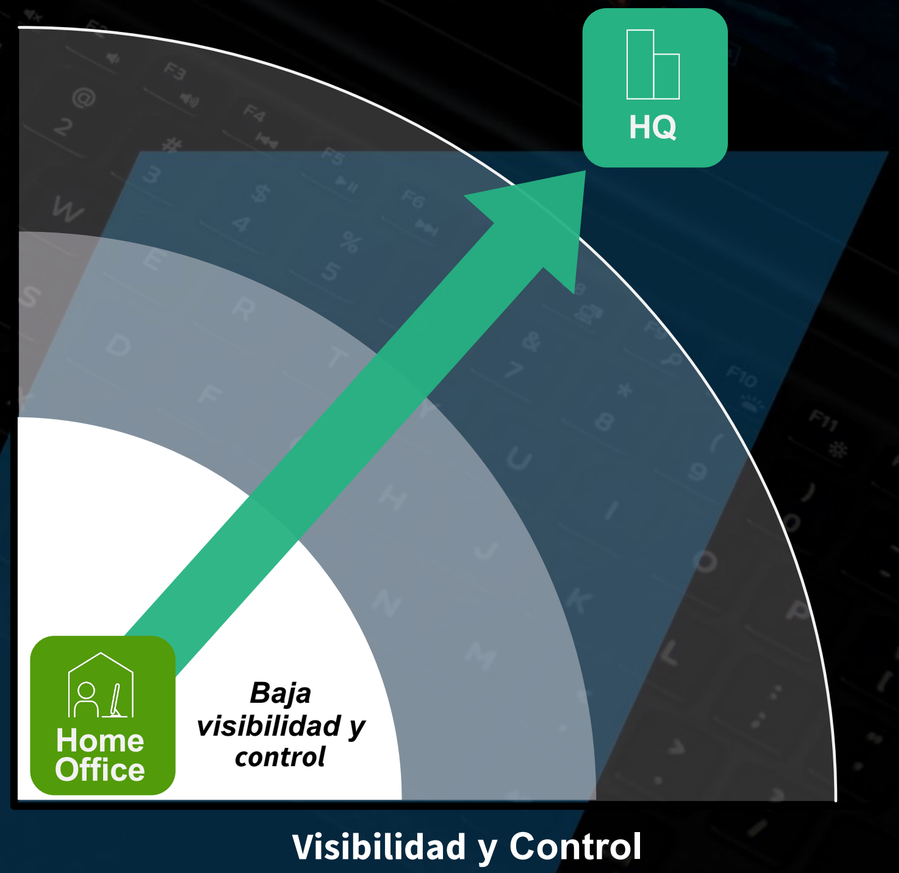


de las organizaciones piensa que los riesgos de seguridad son mayores cuando los empleados trabajan desde casa[4]

[1]Ponemon Institute, 2020 Estado del riesgo de seguridad de endpoints
[2]Absolute, Informe de riesgo del dispositivo de 2021
[3]HP Wolff Security, Informe de puntos ciegos y líneas borrosas de 2021
[4] sapioInvestigación, experiencias y actitudes hacia una fuerza laboral post-COVID, junio de 2021

Resiliencia = **Visibilidad y Control**

Sin esta fórmula aumentan las interrupciones, los riesgos y los costos.



Actualmente se pierden **2 horas semanales** de tiempo productivo por empleado debido a las interrupciones.[1]
Recupere esas horas productivas con Absolute.

El **55% de todos los tickets del helpdesk** están relacionados con los dispositivos endpoint.[2]
Reduzca esos tickets con Absolute.

$25 millones es el costo promedio de las interrupciones de la tecnología móvil en una empresa media de 10.000 personas.[3]
Minimice esos costos con Absolute.

$3,86 millones fue el costo medio de una brecha de datos corporativa en 2020.[4]
Asegúrese de que sus controles de seguridad de los dispositivos endpoint y de la red estén siempre presentes con Absolute.

[1] Robert Half Technology, Día de Trabajo Desperdiciado: Los empleados pierden más de dos semanas al año por problemas relacionados con TI [2] Vanson Bourne, El Nuevo Lugar de Trabajo Digital: Experiencias de los empleados con el trabajo a distancia universal desde COVID, 2020 [3] Vanson Bourne, Reporte de Experiencia 2020: La experiencia digital del empleado hoy, 2020 [4] IBM, Reporte sobre el Coste de una Brecha de Datos, 2020

Desafíos en las organizaciones

LOGRAR EFICIENCIA/ PRODUCTIVIDAD OPERACIONAL

- Tiempo de inactividad/interrupción del servicio
- Poca visibilidad de las fallas
- Problemas de conectividad de las aplicaciones
- Mala adopción de herramientas
- Herramientas superpuestas

MITIGAR EL RIESGO Y ASEGURAR EL CUMPLIMIENTO DE REGULACIONES

- Demostrar el cumplimiento normativo
- Deterioro de la aplicación de dispositivos
- Visibilidad y control de dispositivos fuera de la red
- Capacidades superpuestas
- Incidentes de seguridad (por ejemplo, ransomware)

HABILITAR EL NEGOCIO

- Usuarios finales frustados
- Ineficiencias en los procesos
- TI/Helpdesk en la sombra
- Falta de visibilidad en los sistemas
- Bajo rendimiento de la aplicación

Qué nos hace únicos

Tecnología Persistence®
IMBORRABLE, AUTOCURATIVA E IMPENETRABLE incorporada desde la fábrica
en el firmware de la mayoría de los dispositivos.

Al activar **Persistence** obtiene:

- Control absoluto y visibilidad completa de todos sus dispositivos.
- Consola basada en la nube, para mantener el control, investigar amenazas, y responder ante incidentes.
- Información actualizada en tiempo real.
- Aplicación de medidas de seguridad remota.

27 años de Experiencia en
Seguridad de la información

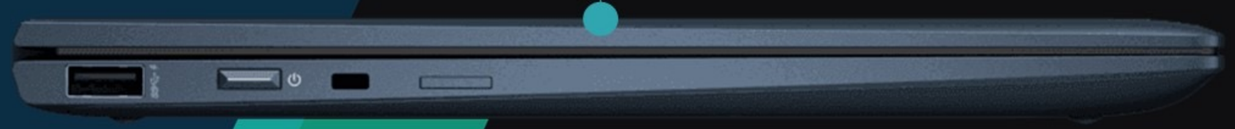
Integrado en el Firmware en **500M+** de dispositivos

13K+ de clientes en todo el mundo

140+ patentes

15M+ de dispositivos endpoints activos

ABSOLUTE®



Entregando **Seguridad** Resiliencia, Autosanación y Seguridad

SECURE ENDPOINT

La única solución de seguridad integrada de fabrica en el firmware de más de 600 millones de dispositivos.

SECURE ACCESS

La única tecnología de acceso seguro que se autorrepara activamente y optimiza la experiencia del usuario final.

Secure Endpoint:

Casos de Uso

CASOS TÁCTICOS

- Informa el estado del dispositivo, configuraciones, HW y SW
- Descubre la presencia de datos confidenciales en dispositivos
- Mantiene persistente la postura de seguridad y la experiencia del usuario
- Optimiza el consumo de licencias de software con informes sobre el estado y uso de aplicaciones

CASOS ESTRATÉGICOS

- Gestiona el movimiento de los dispositivos con la geolocalización
- Consulta acerca de dispositivos no encriptados, con USB conectada ó en ubicación no autorizada
- Evalúa el complimiento de la implementación de parches y actualizaciones de aplicaciones
- Provee métricas de uso de suscripciones SAAS y de uso de la web

Application Health Status - IT Dashboard

Summary of application report and repair status on devices

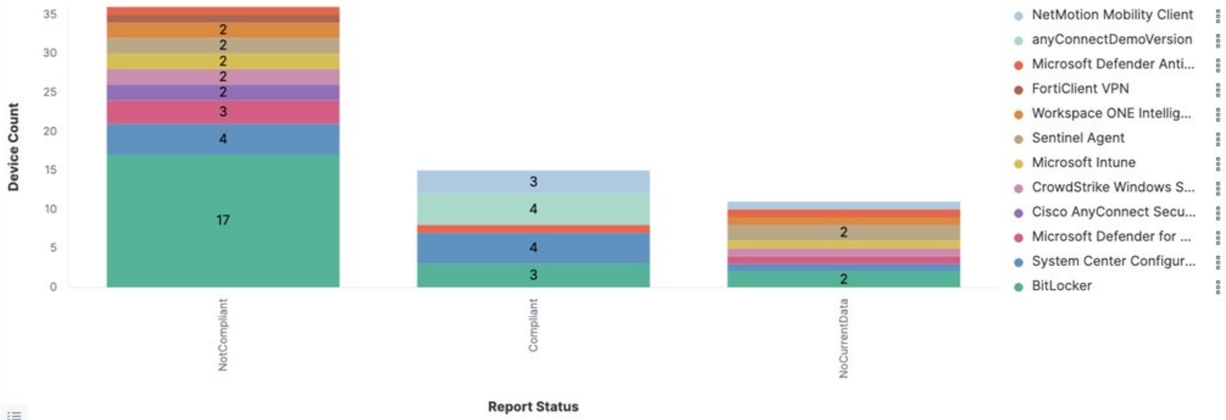
Learn more about this dashboard

Participating Device Count

25

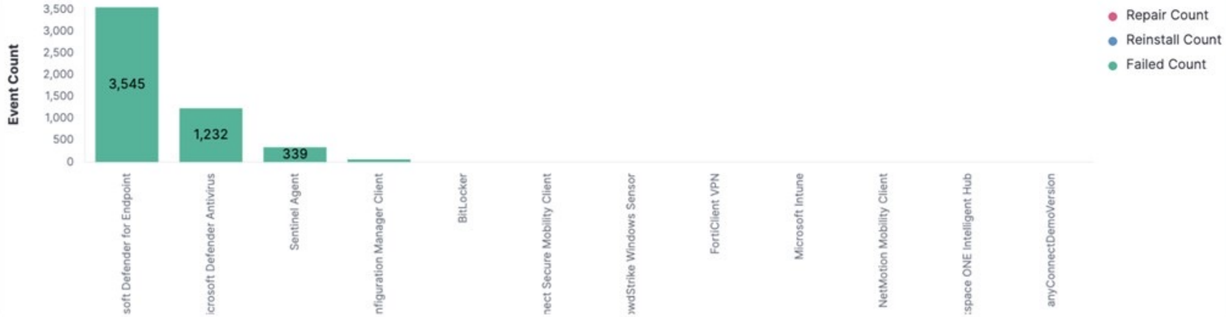
Participating Device Count

Application Health Status

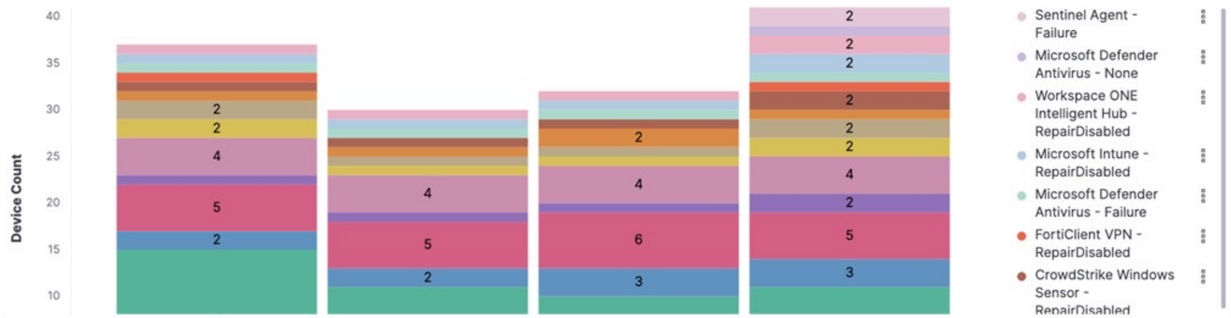


Compliance Status

Report and Repair Event Count



Application Repair/Reinstall Status



Secure Endpoint:
Enfocado en los Dispositivos

INTELIGENCIA DE ACTIVOS

- Dashboards sobre la plataforma de dispositivos.
- Acceso en tiempo real a históricos y métricas de seguridad.
- Métricas de las actualizaciones del SO y de software
- Indicadores de uso de las aplicaciones.
- Geolocalización (5 tecnologías incorporadas).
- Patrones de comportamiento de los usuarios.
- Descubrimiento de datos sensibles.

RANSOMWARE RESPONSE

- Evaluación de la salud de los dispositivos.
- Integración de medidas preventivas para un posible ataque.
- Reduce el área de ataque.
- Provee asistencia en la recuperación de dispositivos en caso de un ataque.

BIBLIOTECA DE APLICACIONES PERSISTENTES

- Persistencia a 60+ aplicaciones críticas en nuestra biblioteca.
- Permite al instalador persistente alojar el entorno de la nube de Absolute.
- Aumento de la adopción de nuevas aplicaciones criticas y su despliegue.

Biblioteca de App Persistence

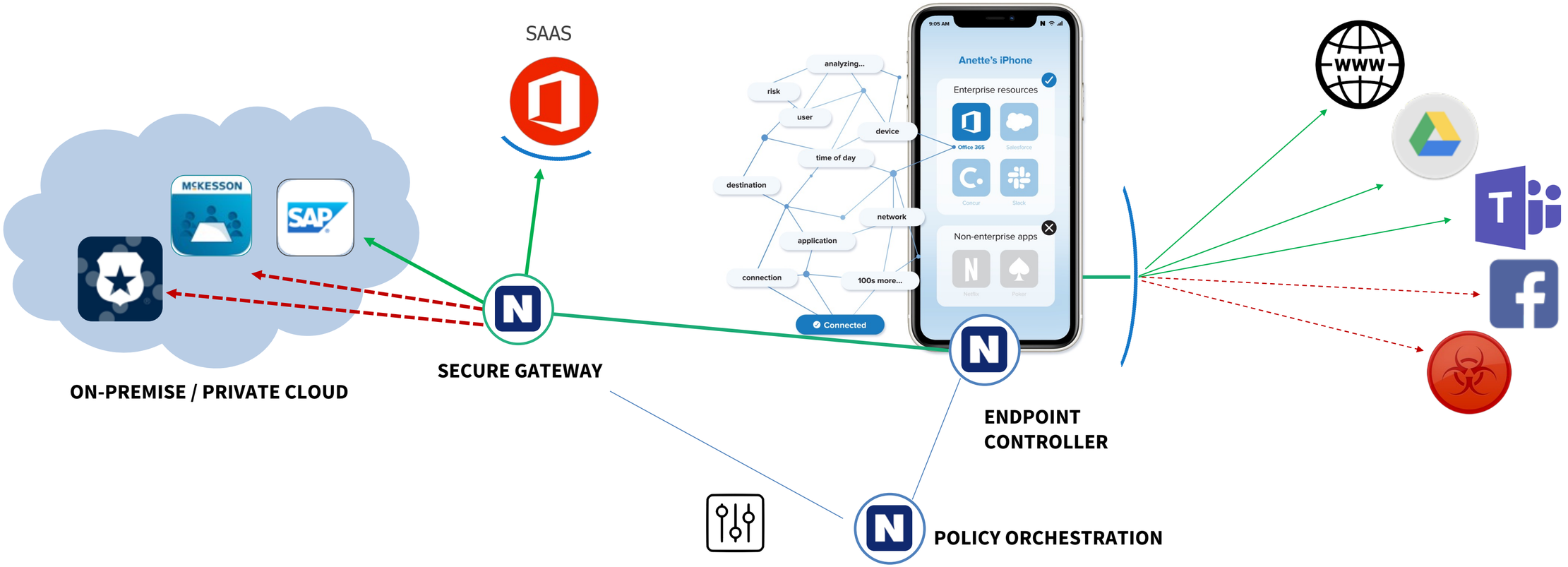
Zero Trust Network Access

Gartner®

“Productos y servicios que crean un límite de acceso lógico basado en la identidad y **el contexto** *desde el cual se genera la conexión. Las aplicaciones y los recursos están ocultos del descubrimiento y el acceso está restringido a través de un agente de confianza minimizando el* **movimiento lateral** *a otras partes de la red.*

ZTNA *elimina la* ***confianza implícita excesiva*** *que a menudo acompaña a otras formas de acceso a las aplicaciones, como la VPN tradicional”*

Beyond ZTNA – Only Absolute



Secure Access:

Casos de Uso

CASOS TÁCTICOS

Persistencia, Resiliencia y Escalabilidad de la Red

- **Gateway de Web Segura (VPN)**
- **Aislamiento del Navegador**
- **Inspección y Filtrado de Contenidos**

Monitorear métricas de las aplicaciones y la geolocalización

Analizar patrones de uso y evaluación del ROI

CASOS ESTRATÉGICOS

Evaluar los estados de configuración y el impacto de la conectividad de la red

Comprender el uso de la red e identifica el estado de conectividad

- **Conectores de Aplicaciones**
- **Monitoreo de Datos**
- **Protección de Perdida de Datos DLP**

Network Health

Network connectivity issues detected and reported by Mobility. "Connections persisted" are networking issues mitigated by Mobility.

Time: Month to date

Refresh interval: None

Hide Filters

Last updated: 08/08/2022 - 15:36:24

Connections persisted

32,568

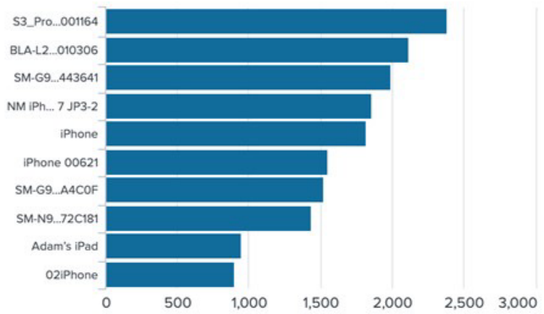
<1m ago

Trends

0

Last hour

Connections persisted (counts by device)



Network failures

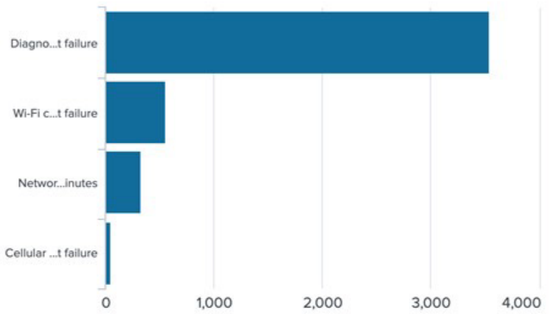
4,475

Trends

0

Last hour

Network failure types



Mobility disconnects

1,363

Trends

0

Last hour

Disconnect reasons

	Count	Reason
1	248	Manual disconnect
2	183	Authentication failed
3	165	Client-side disconnect.
4	86	Reconnection initiated by the mobility administrator.
5	66	Client established new connection from same device
6	64	Authentication mode or protocol is invalid. contact the mobility

Failed network diagnostic reports

3,539

Trends

0

Last hour

Failed reports - probable root causes

	Probable Root Cause	Count
1	HTTP send request failed.	1462
2	https://bwtestserver.netmotiondemo.com	630
3	ftp connection to upload server	322
4	S: drive is unavailable	298
5	Mobility is using an alternate network interface.	189
6	Web server responded but ping had data loss.	130

Secure Access:
Enfocado en la Conectividad

LA ÚNICA ZTNA CON

- Cliente Windows resiliente
- Infraestructura resiliente
- Políticas flexibles
- Inteligencia de red
- Reduce el movimiento lateral del software malicioso.
- Oculta las aplicaciones, minimizando la superficie de ataque.
- Reduce los costos de hosting
- Diagnóstico para las modernas redes 5G y redes Wi-Fi

INTELIGENCIA DE LA RED

- Visualización de las amenazas bloqueadas y sitios web maliciosos.
- GDPR: Configure la recopilación de datos dentro/fuera del túnel para dispositivos BYOD, CYOD y COPE.
- Aumento de la escalabilidad en 2x hasta para soportar grandes despliegues.

- Cliente de Windows e infraestructura persistente a prueba de manipulaciones.
- Diagnóstico para las modernas redes 5G y redes Wi-Fi.
- Políticas de ZTNA que aumenta la seguridad e impide el movimiento lateral.

Monitoreo de Datos:

La AI impulsa la seguridad avanzada

¿Cómo?:

- Recoge datos detallados de flujo y comportamiento fuera del firewall.
- Aplica algoritmos basados en Deep Learning e AI.
- Análisis de usuario, dispositivo y comportamiento (UEBA).
- Detecta cambios en el comportamiento y patrones de uso que son típicos de la actividad maliciosa:
  - ✓ Escaneo de detección de puertos
  - ✓ Cambios en el comportamiento de las aplicaciones y la navegación
  - ✓ Cambios en el uso de datos

- Detecte, alerte, informe y corrija con políticas en la nube y en los dispositivos.

Imagínese…

Seguridad de Datos Avanzada:

El **malware se desarma en la nube** antes de llegar a la aplicación, el navegador o el dispositivo.

¿Cómo?:

- Secure Access analiza dinámicamente el riesgo de cada destino.
- El tráfico de alto riesgo se dirige al gateway de Web Segura y al Navegador Web en el contenedor de la nube.
- DLP e Inspección de Contenidos. (en desarrollo)
- El sistema elimina el malware oculto en archivos adjuntos y sitios web.

Ejemplo:
Clientes de email basados en la web

PRINCIPIOS DE ZERO TRUST EN TODOS LOS NIVELES

Desde el firmware hasta la red

SECURE ENDPOINT

Evaluaciones de seguridad únicas que comienzan en el firmware

Visibilidad profunda de las aplicaciones y configuraciones de cada usuario

Una presencia resiliente en el dispositivo que permite la autorreparación

Información y controles sólidos para cualquier dispositivo en cualquier red

SECURE ACCESS

Preguntas

¡Gracias!

Polo Sánchez
Sales Director NOLA

PSanchez@absolute.com

ABSOLUTE® LATAM