ABSOLUTE SOFTWARE

¿Es posible una realidad híbrida realmente segura?

Juan Carlos Marín B.
Sales Engineering Lead
Absolute LATAM
Septiembre 2022

2º Jornada 2022 CIBERSEGURIDAD
19 - 23 de septiembre - Universidad de Guadalajara

cudi

CSIRT CUDI

UNIVERSIDAD DE GUADALAJARA

La seguridad informática hoy…No es Segura…

$173B

Gasto esperado en Seguridad de TI y gestion del riesgo de información en 2022[1]

78%

De los Líderes de TI y seguridad no tienen confianza en la postura de seguridad de sus organizaciones[2]

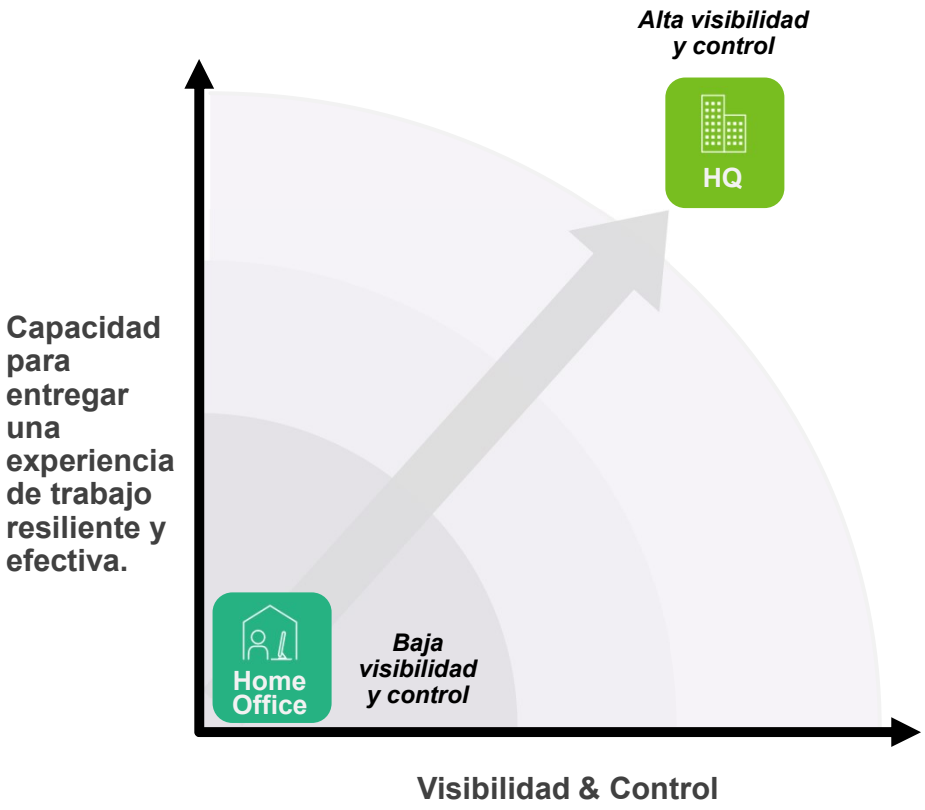
Estamos enfrentados a la necesidad de lograr una seguridad informática eficaz

[1] *Gartner, Forecast: Information Security and Risk Management, Worldwide, 2020 - 2026, 2Q22 Update*
[2] *IDG, Cybersecurity at a Crossroads: The Insights 2021 Report*

…y las cosas no están mas fáciles en esta era del trabajo desde cualquier parte

El Dilema actual: Visibilidad y Control

Nos enfrentamos a interrupciones, riesgos y costos in-crescendo



2 horas a la semana de tiempo productivo por empleado se está perdiendo por interrupciones. [1]
Recupere esas horas productivas con Absolute.

55% de los tickets de mesa de ayuda hoy están relacionados con los dispositivos de usuario final.[2]
Reduzca esos tiquetes con Absolute.

$25 millones de dólares es el costo promedio de las interrupciones en la tecnología movil en una compañía promedio de 10,000 personas en USA.[3]
Minimice esos costos con Absolute.

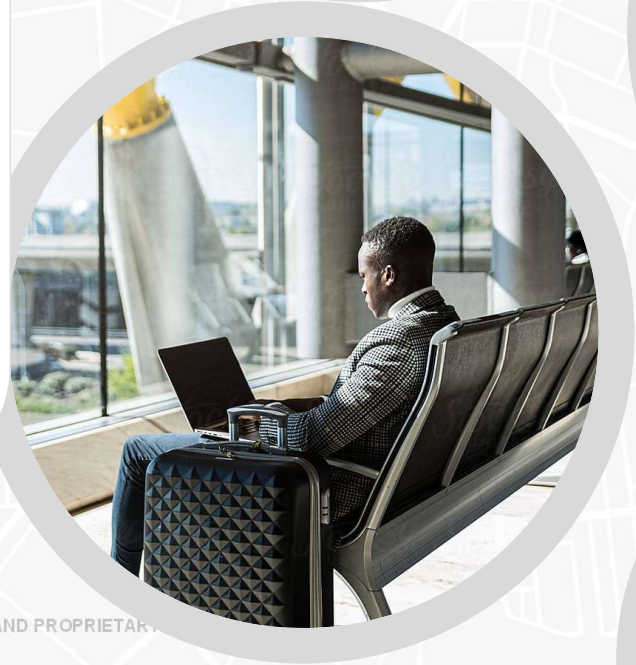
$3.86 millones fue el costo promedio de los data breach corporativos en 2020.[4]
Asegure que su seguridad de red y de dispositivo está operando correctamente, con Absolute.

/ABSOLUTE®

[1] *Robert Half Technology, Wasted Workday: Employees Lose Over Two Weeks Each Year Due to IT-Related Issues*
[2] *Vanson Bourne, The New Digital Workplace: Employee Experiences with Universal Remote Working Since COVID, 2020*
[3] *Vanson Bourne, The Experience 2020 Report: Digital Employee Experience Today, 2020*
[4] *IBM, Cost of a Data Breach Report, 2020*

Misión

Hacer del trabajo remoto, desde cualquier parte, un trabajo confiable que se pueda lograr con la máxima seguridad sin comprometer la productividad.



Esto es/ABSOLUTE®

When Insights Matters

- 240 unique endpoint data points
- 174 unique network data points
- 300M monthly application health scans

Asegurando Máxima Seguridad Sin comprometer Productividad

SECURE ENDPOINT

Seguridad moderna que fortalice de una manera única sus defensas, reduce el riesgo y automáticamente, mantiene saludable su stack de seguridad.

SECURE ACCESS

La única solución ZTNA que optimiza el desempeño de la red, potenciada por una mayor riqueza de datos

¿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.

ABSOLUTE®

Absolute – Secure EndPoint

La única plataforma de defensa indeleble en 500 M+ Dispositivos

Embebido en el firmware de fábrica desde 2005, hoy en día lo incluyen 28 PC OEMs

500M+ Dispositivos

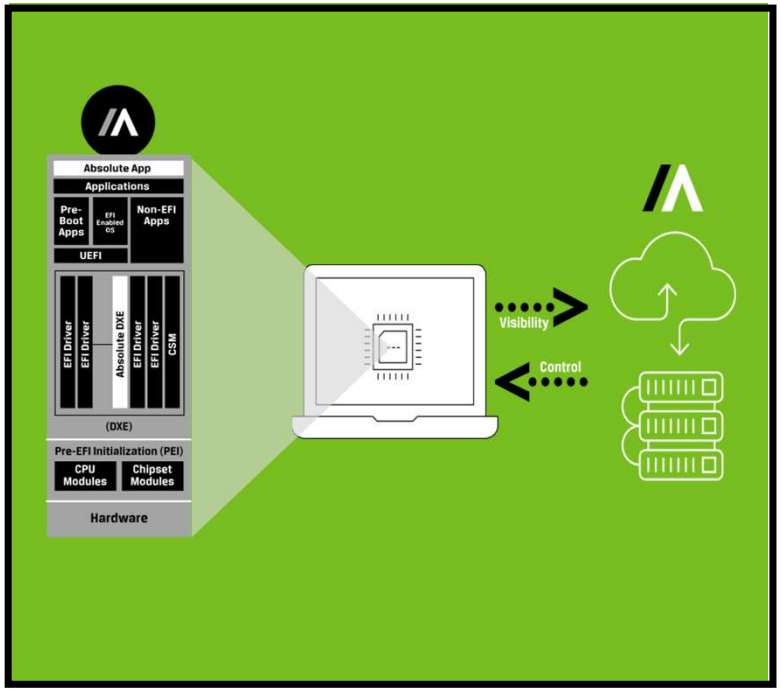
Fácilmente activable en desktops, laptops, MacOS, Chromebooks

Una conexión indeleble e irrompible desde el HW asegura visibilidad del endpoint, inteligencia y resiliencia

Basado en la nube
No se requiere infraestructura

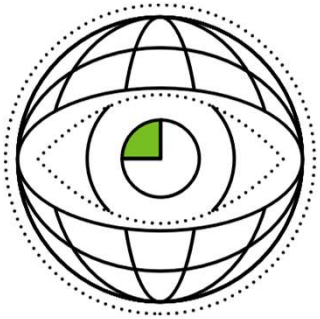
Visibilidad única desde la BIOS

Gestión de dispositivos desde la BIOS
habilitando congelados, borrados, ubicación y control



Absolute Ecosystem

Persistence, es una tecnología patentada embebida en **500+ millones PCs** que ofrece una conexión permanente dando visibilidad y control, y la capacidad de resistir cualquier ataque, **retornando a su estado original** de seguridad y eficacia.



LANIX
Microsoft
Panasonic
SAMSUNG
Prestigio
XPLORE TECHNOLOGIES
hp
Motion
FUJITSU
TOSHIBA
ASUS
DELL
PCsmart try the future
Getac
inforlandia
intel
GAMMATECH
Lenovo
acer

Firmware Partners

phoenix technologies
insyde
American Megatrends

Absolute | Cómo funciona la persistencia

Visibilidad y Control completamente confiable, basada en el Firmware

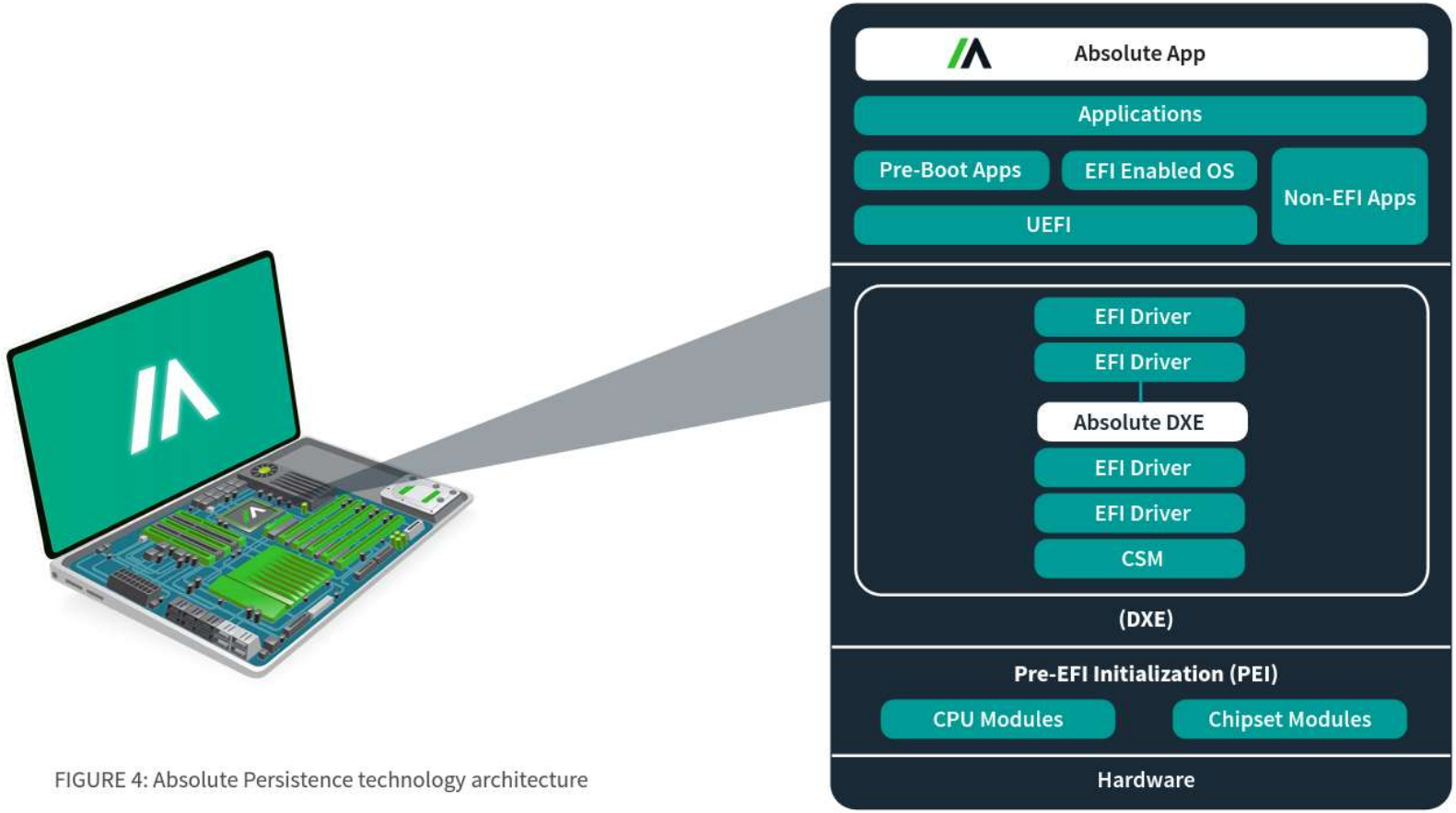
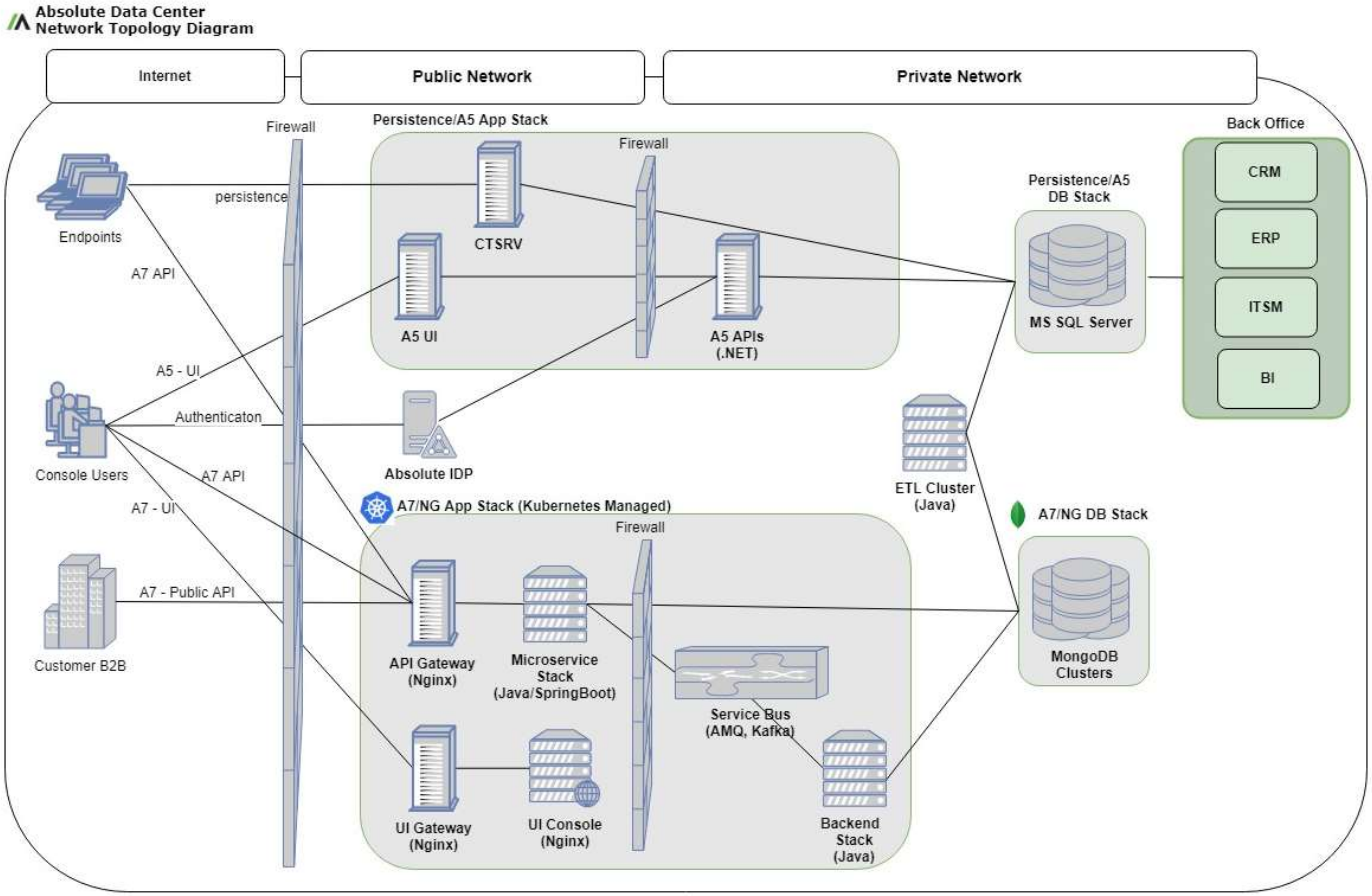


FIGURE 4: Absolute Persistence technology architecture

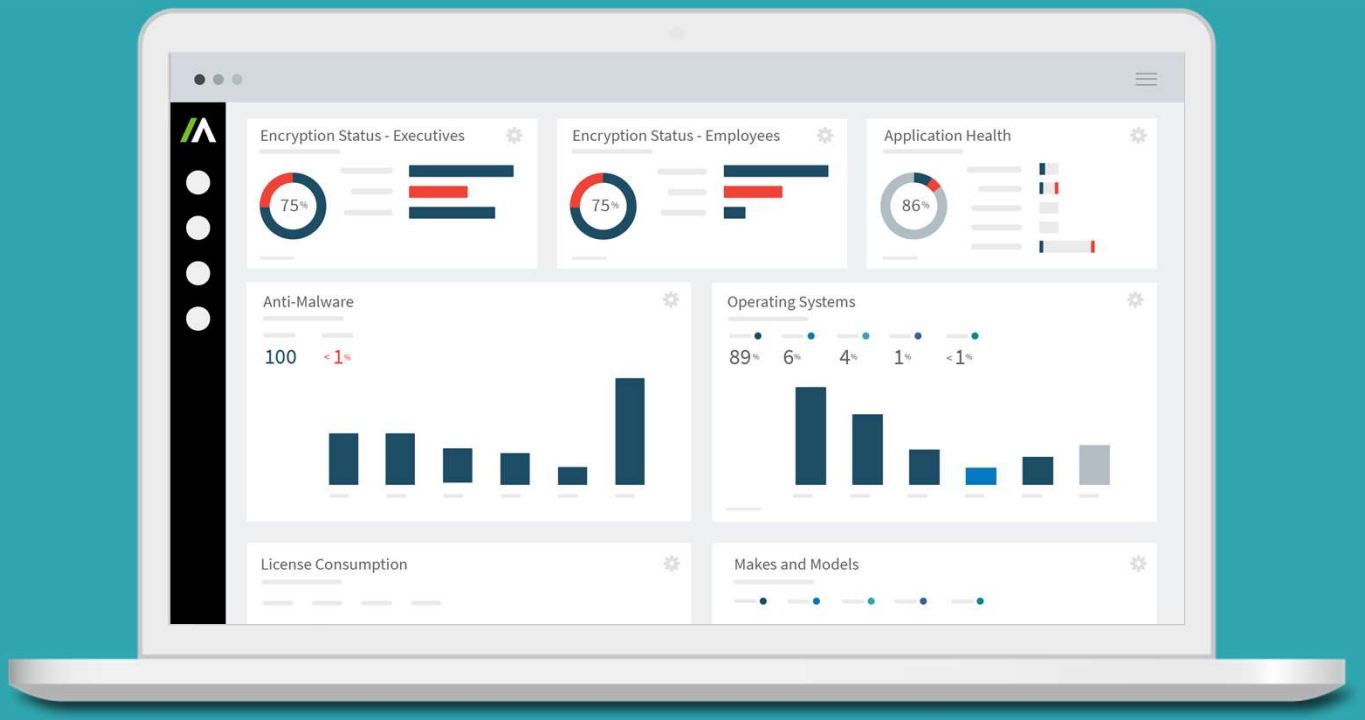
+25 OEMs

Network Topology



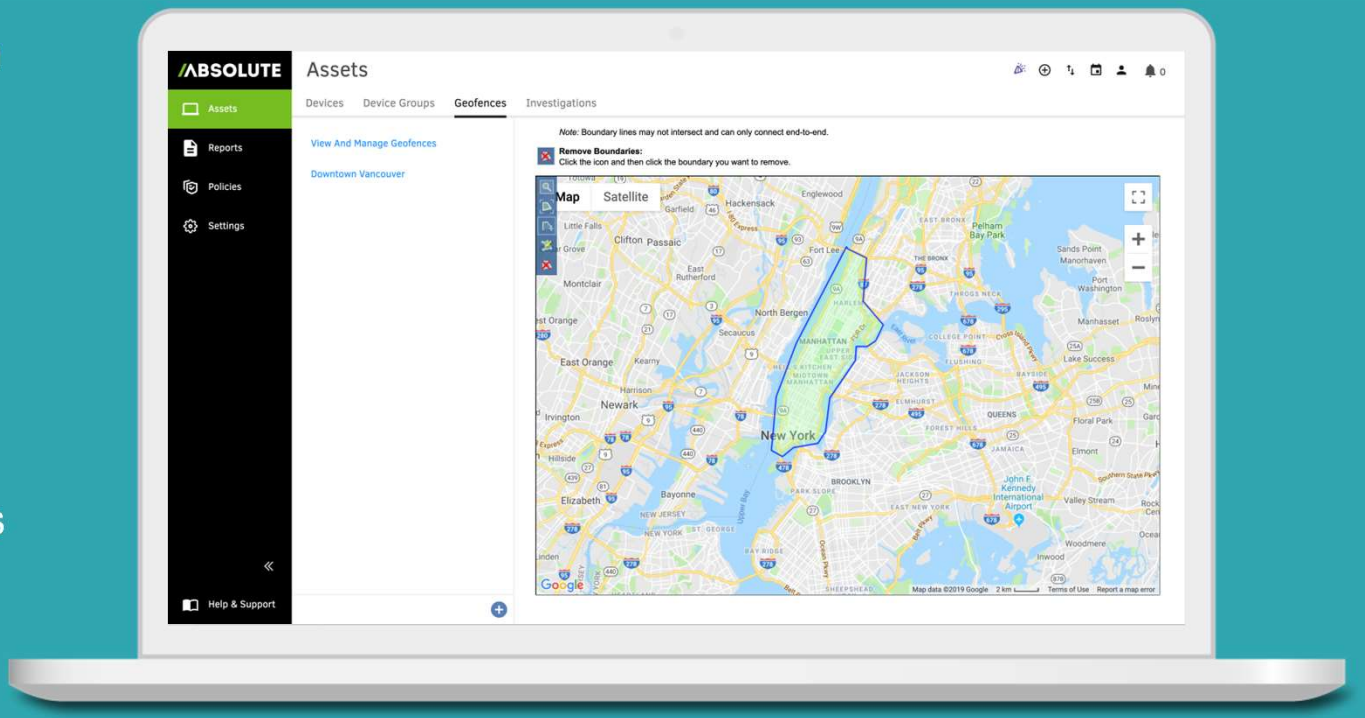
Postura de Seguridad

- Reporte la postura de seguridad crítica de todos los dispositivos.
- Sea proactivido en elementos críticos contra el Malware como la encripción de sus dispositivos y la salud de sus aplicaciones en el dispositivo
- Monitoree el status de sus herramientas de seguridad



Geolocalización

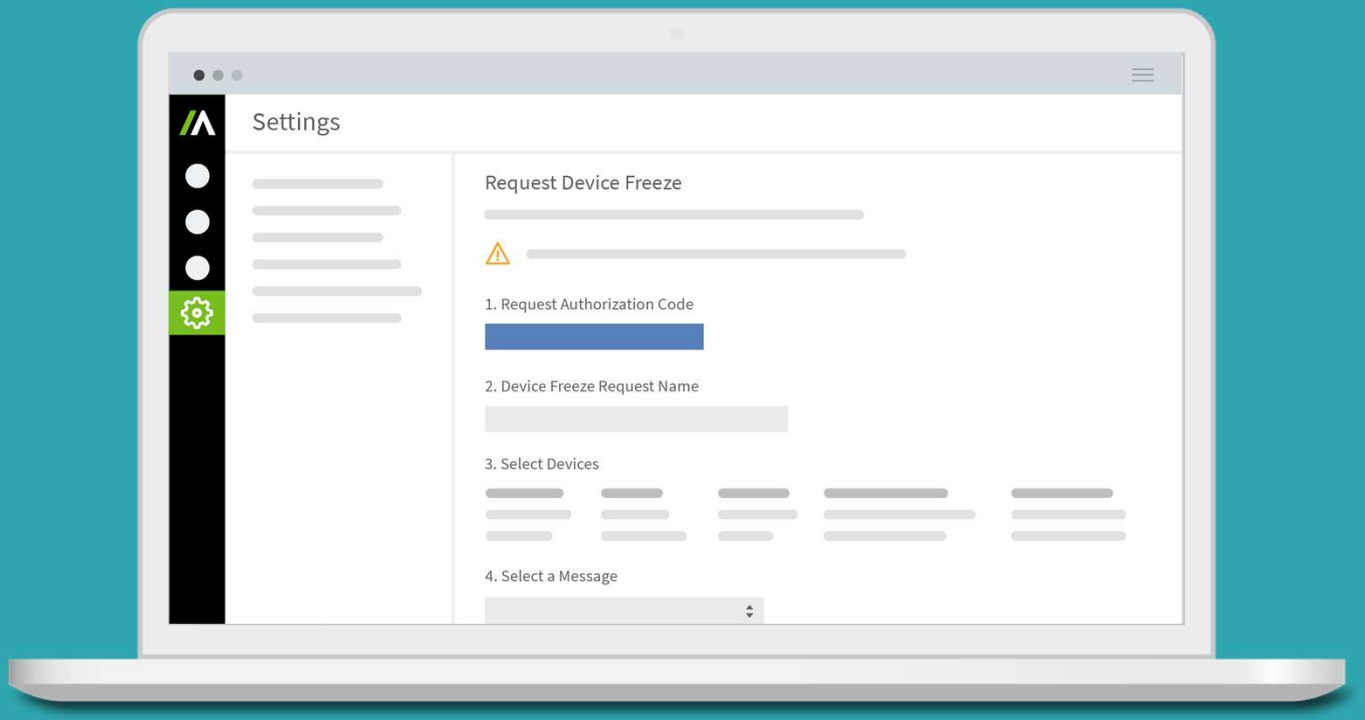
- Localice los dispostivos sin GPS usando Wifi-Triangulation
- Defina fronteras geográficas o geocercas para identificar riesgos en el movimiento de sus dispositivos.
- Controle 365 días del movimiento de sus dispositivos



Congelamiento de dispositivos

- **Proteja sus dispositivos fuera de control**

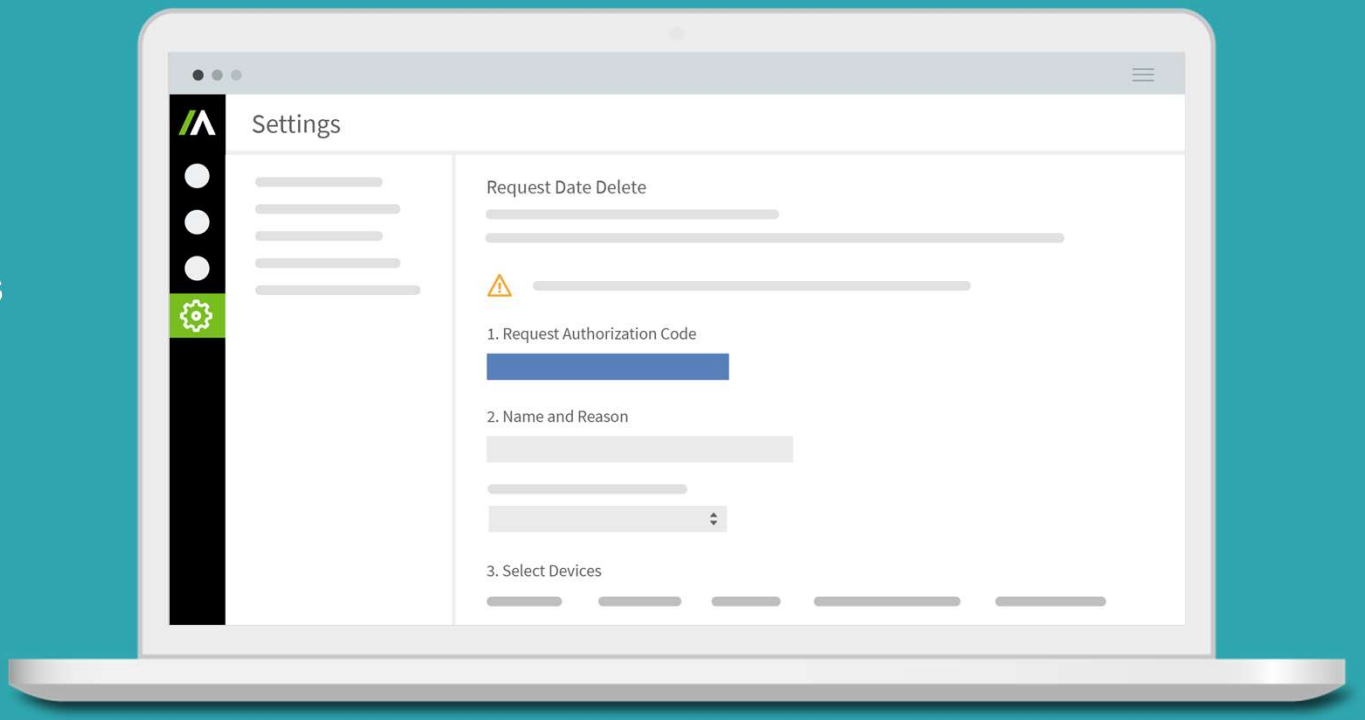
- Congele dispositivos perdidos o robados, configure timers que automáticamente bloqueen un dispositivo en caso de desconexión por mucho tiempo.



Borrado de dispositivos

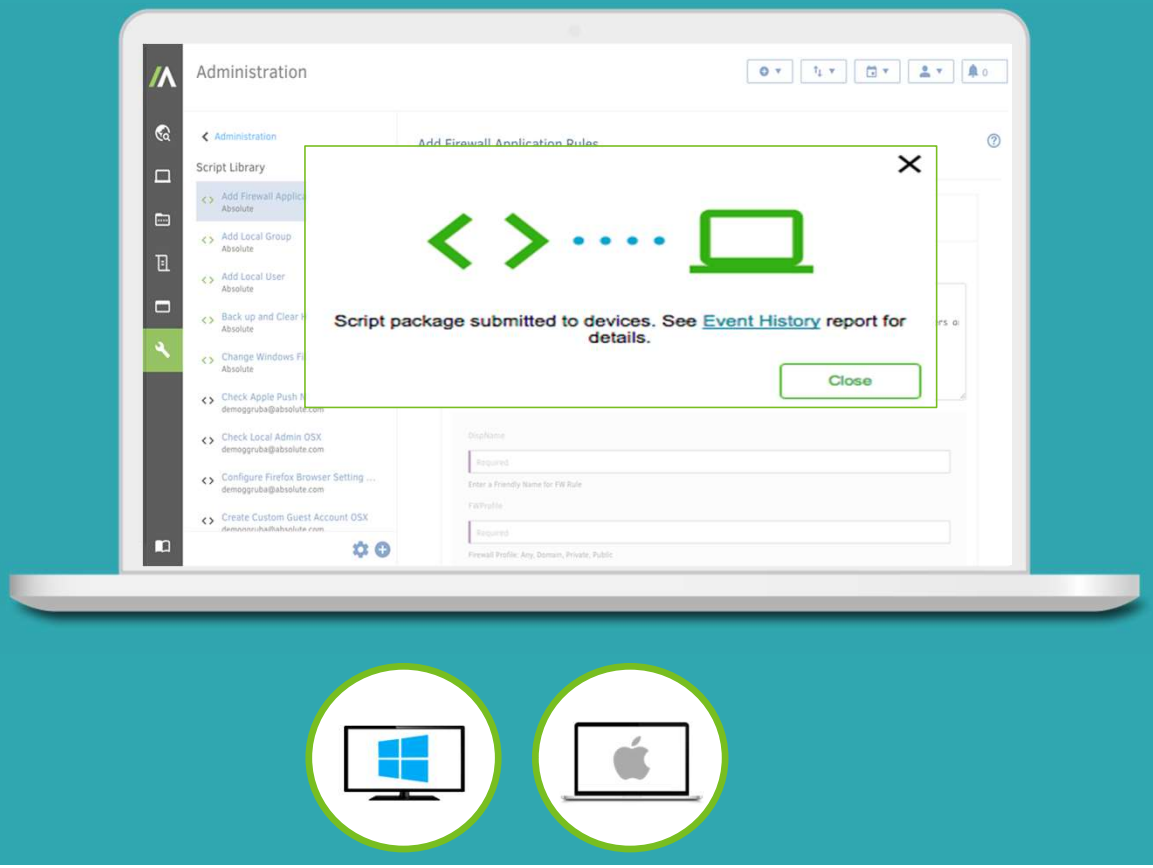
- Gane confianza y garantice cumplimiento de estándares de seguridad en dispositivos que salen de la organización.

- Selectivamente borre los datos de dispositivos en riesgo o ejecute borrados de fin del ciclo de vida de un dispositivo y genere certificados de cumplimiento.



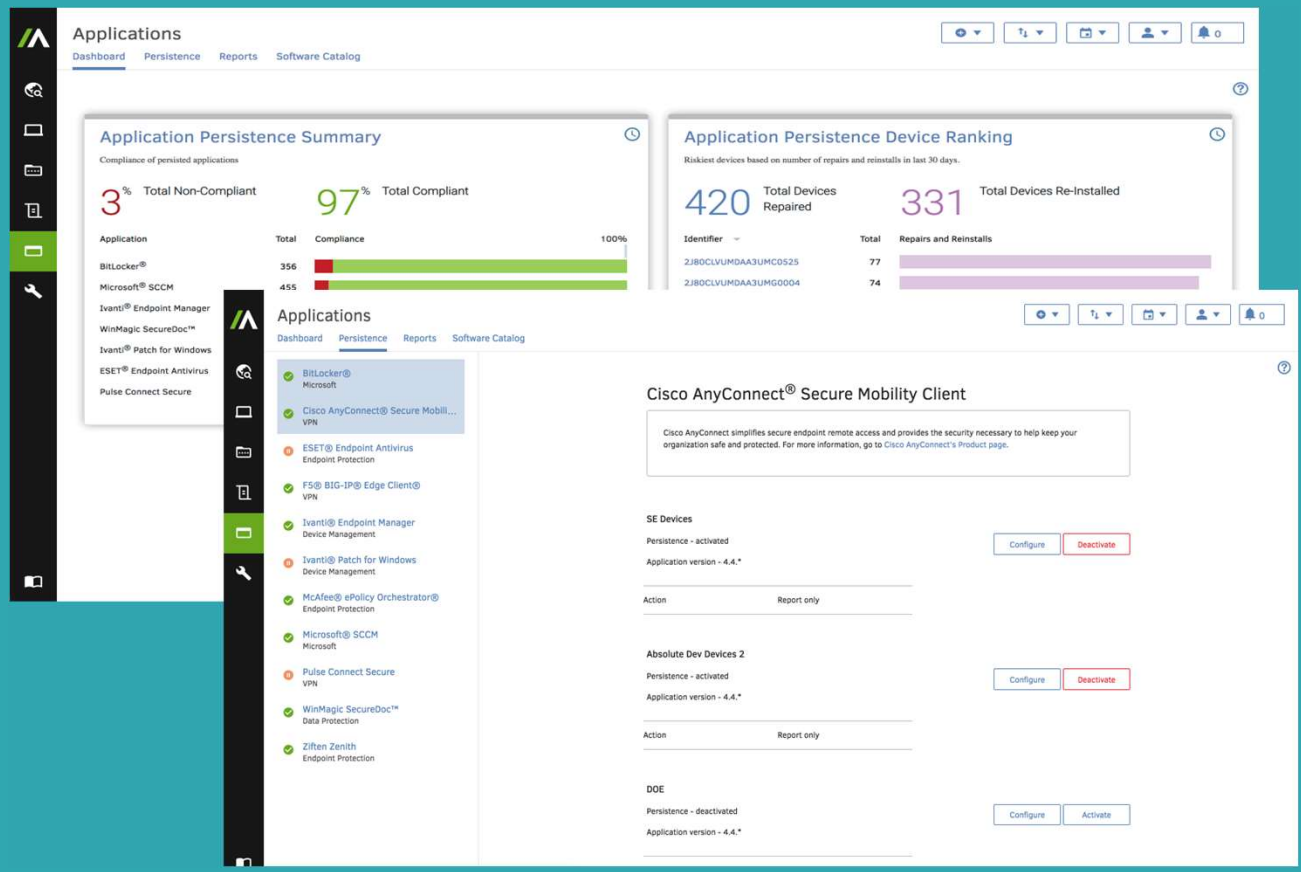
Absolute Reach

- PowerShell & BASH Scripting
- Conexión única y Segura a cada dispositivo
- Garantía de envío y ejecución de scripts en el dispositivo, aun si está fuera de red.
- No se requiere infraestructura adicional
- Corra los scripts en uno o varios dispositivos, basado en criterios de selección.
- Librería preconstruída por Absolute, disponible para nuestros clientes.
- Arme sus propios scripts y automatice tareas repetitivas de administración



Persistencia de Aplicaciones

- Valide el status y automáticamente repare aplicaciones de su stack de seguridad.
- Persista cualquier app de su portafolio – incluyendo custom apps
- Protejase contra la corrupción de aplicaciones
- Asegurese que las aplicaciones y versiones correctas están en todos los dispositivos



Absolute | Application Persistence Ecosystem

1. **Endpoint Protection**
   - Next-Gen Endpoint Security (AV/AM)
   - Endpoint Detection and Response (EDR)

2. **Endpoint Management**
   - Unified Endpoint Management (UEM)
   - Vulnerability and Patch Management
   - Remote Desktop Management

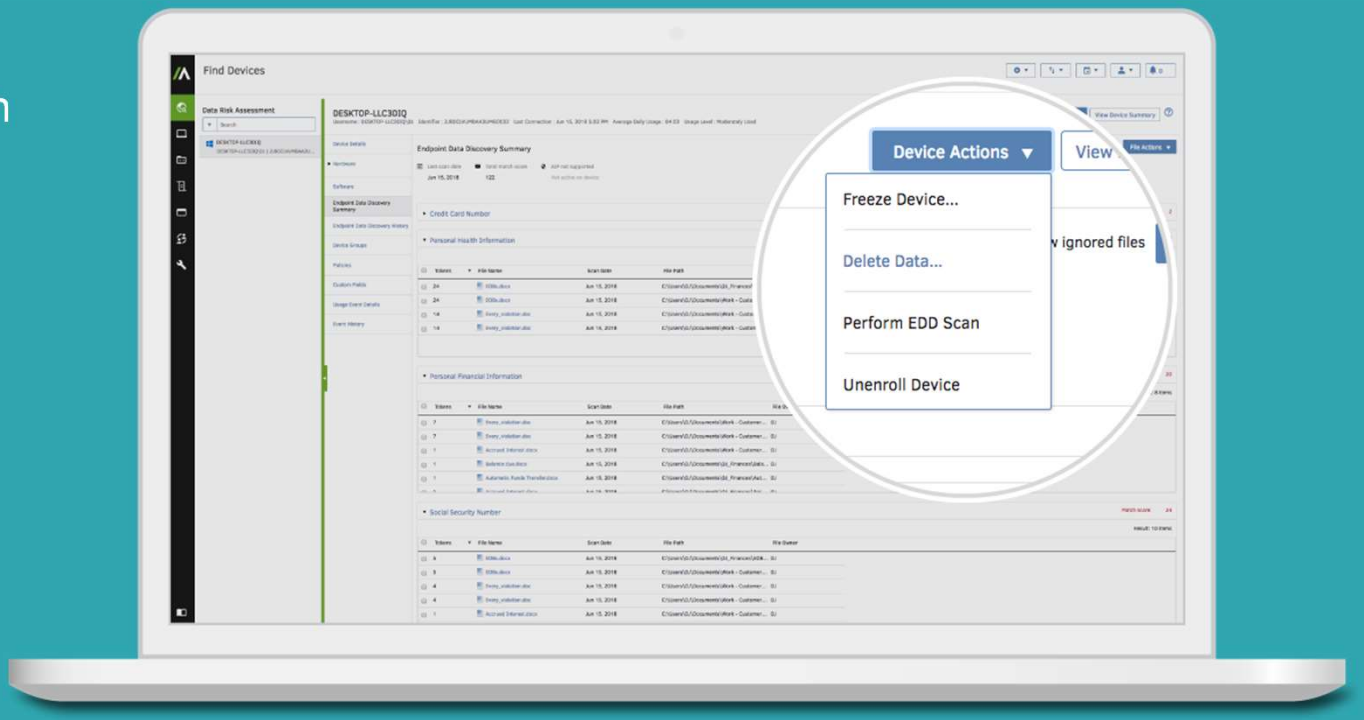
3. **Network Security**
   - Virtual Private Network (VPN)
   - Cloud Access Security Broker (CASB)
   - Zero Trust Network Access (ZTNA)

4. **Data Protection**
   - Full Disk and File Encryption
   - Data Loss Prevention (DLP)

5. **Others**

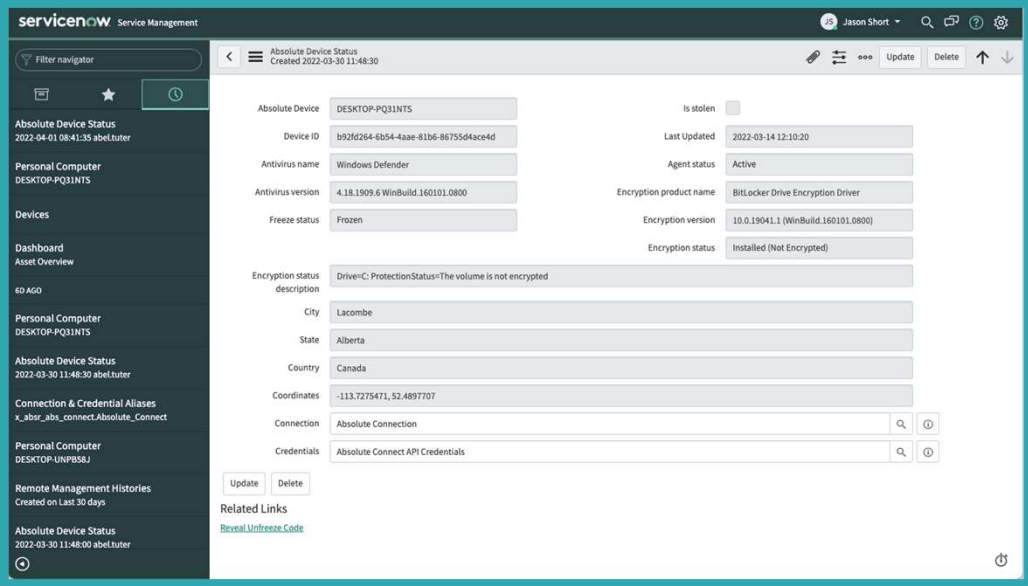
Endpoint Data Discovery

- Ayude a sus usuarios a mantener responsabilidad sobre los datos y a cumplir con las políticas de manejo de información sensible o confidencial.
- Identifique información en riesgo residiendo en los dispositivos
- Remotamente borre archivos específicos o ejecute un borrado seguro de sus dispositivos.



Integraciones

- Accese datos y tome acciones seguras sobre los dispositivos desde otras aplicaciones, via exportación de archivos o vía API.
- Conexión a través de una interface SIEM para control de eventos en los dispositivos
- Modulo de integración directa con ServiceNow



Preguntas ?

ABSOLUTE®

Absolute Secure Access

Seguridad Zero Trust enfocada en la red y en la nube

ABSOLUTE®

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"*

ABSOLUTE®

The remote access journey

"NetMotion by Absolute, gives businesses a software-defined perimeter solution that can grow with them as they evolve toward zero trust situations."

IDC

Full VPN

Tunnel everything

Primarily on-premise

VPN & ZTNA

Tunnel partially

Blend of cloud and on-prem

Full ZTNA

Tunnel rarely

Primarily cloud

ABSOLUTE

The Absolute Secure Access Solution

ABSOLUTE SECURE ACCESS PLATFORM

Zero-Trust Network Access (ZTNA)

- Real-time risk assessments
- Conditional access policy to safeguard enterprise resources
- Deep visibility and intelligent controls to protect users

Optimized performance, with a zero-trust security posture

ABSOLUTE INSIGHTS FOR NETWORK

- Unique & rich digital experience data
- Diagnostic engine to identify distributed worker's issues
- Customizable dashboards with analytics and remediation tools

Complete visibility of remote devices and employee experience

ABSOLUTE VPN

- High performance mobile VPN
- Software-based, enabling rapid scaling and flexible deployments
- Patented network optimizations and resiliency technologies

Context-aware policy enforcement for all endpoints on any network

Architecture

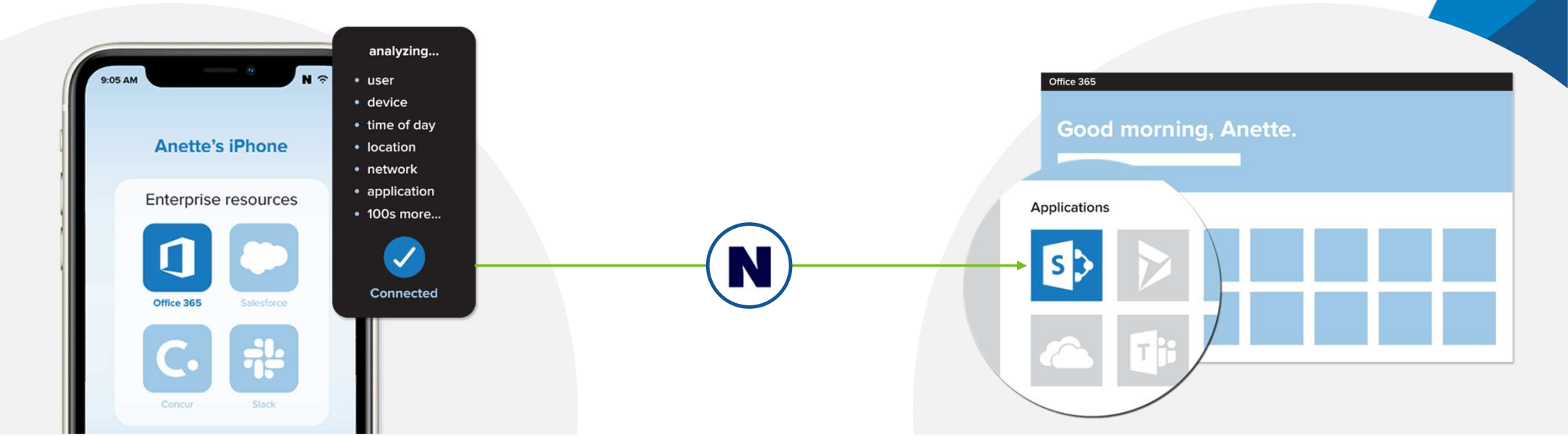
Gateway	Client	Administration

Absolute ZTNA

ABSOLUTE ZTNA

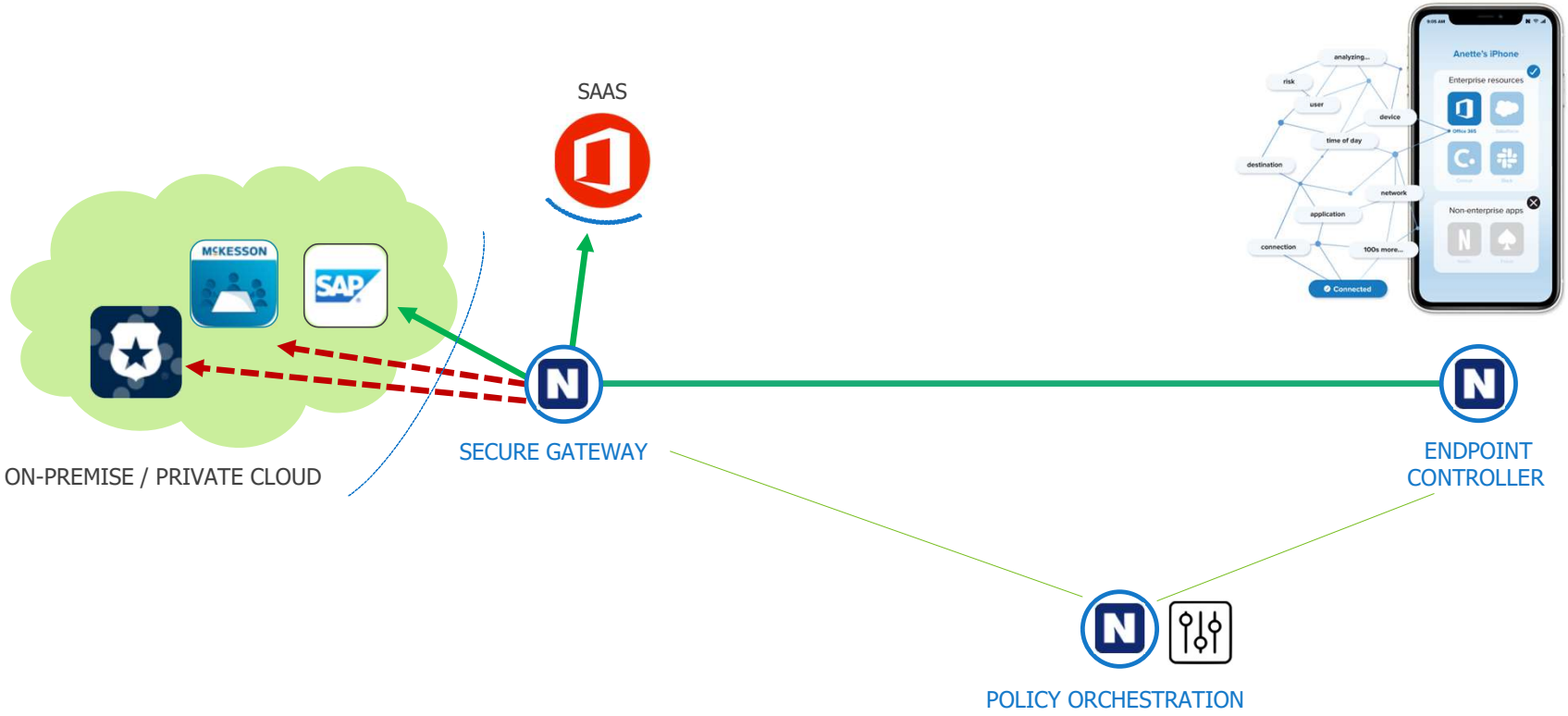
Context-aware protection for both your remote workers and your enterprise resources

- Full visibility of device activity outside the corporate perimeter, from network status and application usage to categorization and risk profile of online activity.
- Conditional access to any online destination, with or without use of the VPN
- Continuous risk assessments for every single device in your fleet, using location, configuration, destination and dozens of other data points to power access policies.
- Protect your enterprise resources by restricting unsanctioned access, no matter where they are hosted

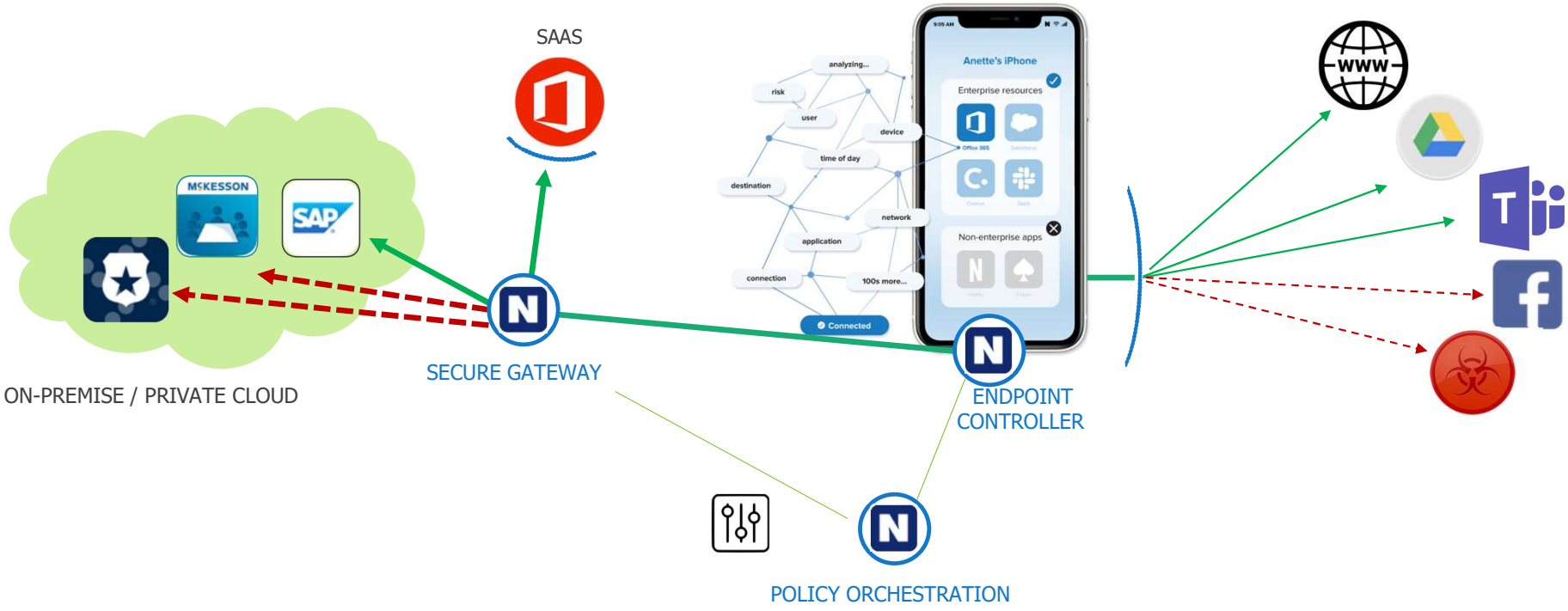


ABSOLUTE ZTNA | How It Works

Zero Trust Network Access



Beyond ZTNA


SAAS
ON-PREMISE / PRIVATE CLOUD
SECURE GATEWAY
ENDPOINT
CONTROLLER
POLICY ORCHESTRATION
Anette's iPhone
Enterprise resources
Non-enterprise apps
Connected
analyzing...
risk
user
device
time of day
destination
network
application
connection
100s more...
WWW

ABSOLUTE VPN

ABSOLUTE VPN | Remote access

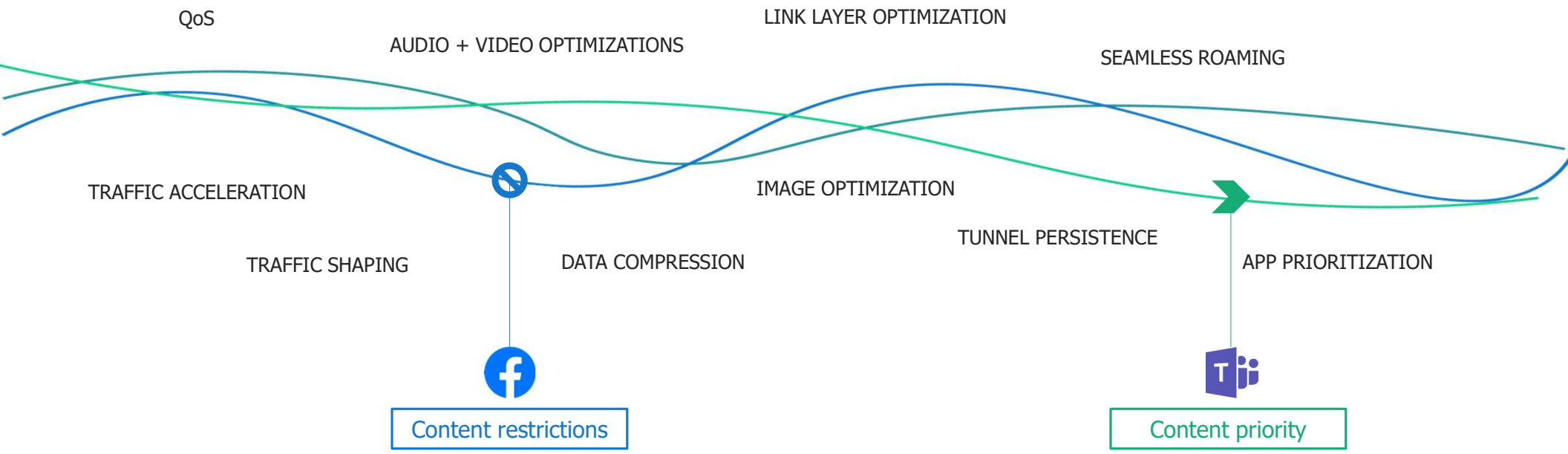
The only VPN on the market built specifically with Employee Experience in mind

- Actively improves the employee experience
- Unbreakable connectivity
- Tunnel and session persistence
- Video and audio optimizations

4G 5G

ABSOLUTE

ABSOLUTE Optimized SECURE Tunnel



ABSOLUTE INSIGHTS FOR NETWORK

NetMotion Experience Monitoring

Complete visibility of remote workers, with the deepest and most detailed analytics available for enterprise mobility

- Diagnostics on device, connectivity and network issues to empower helpdesk teams
- Rich analytics on network performance outside the corporate perimeter, from cellular to public WiFi
- Realtime geolocation dashboards
- Reputation and categorization of domains visited by remote workers

/ABSOLUTE®

Mobile IQ Dashboards

Default Dashboards

- Performance
- Threat Defense
- Cost Control
- Inventory
- System

- Device was unable to make a network connection for 5min or more
- A diagnostic report failure indicates one of a variety of networking issue
- Cellular connect failure occurs when a cellular adapter attempts to connect, but fails
- Wi-Fi connect failure occurs when a Wi-Fi adapter attempts to connect, but fails

/ABSOLUTE®

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

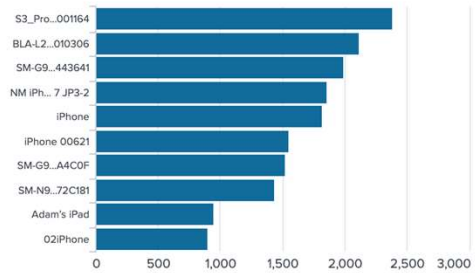
<1m ago

Trends

0 0

Last hour

Connections persisted (counts by device)



Network failures

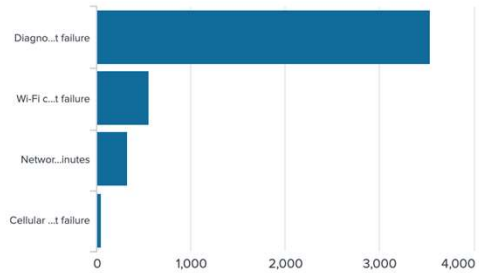
4,475

Trends

0 0

Last hour

Network failure types



Mobility disconnects

1,363

Trends

0 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 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

ABSOLUTE SECURE ACCESS – HOW IT WORKS

Mobility Architecture

Mobility Server

The Mobility server runs on Windows Server 2016 or 2019.
It manages network connections for mobile devices, and is the VPN termination point for all client connections.

Warehouse

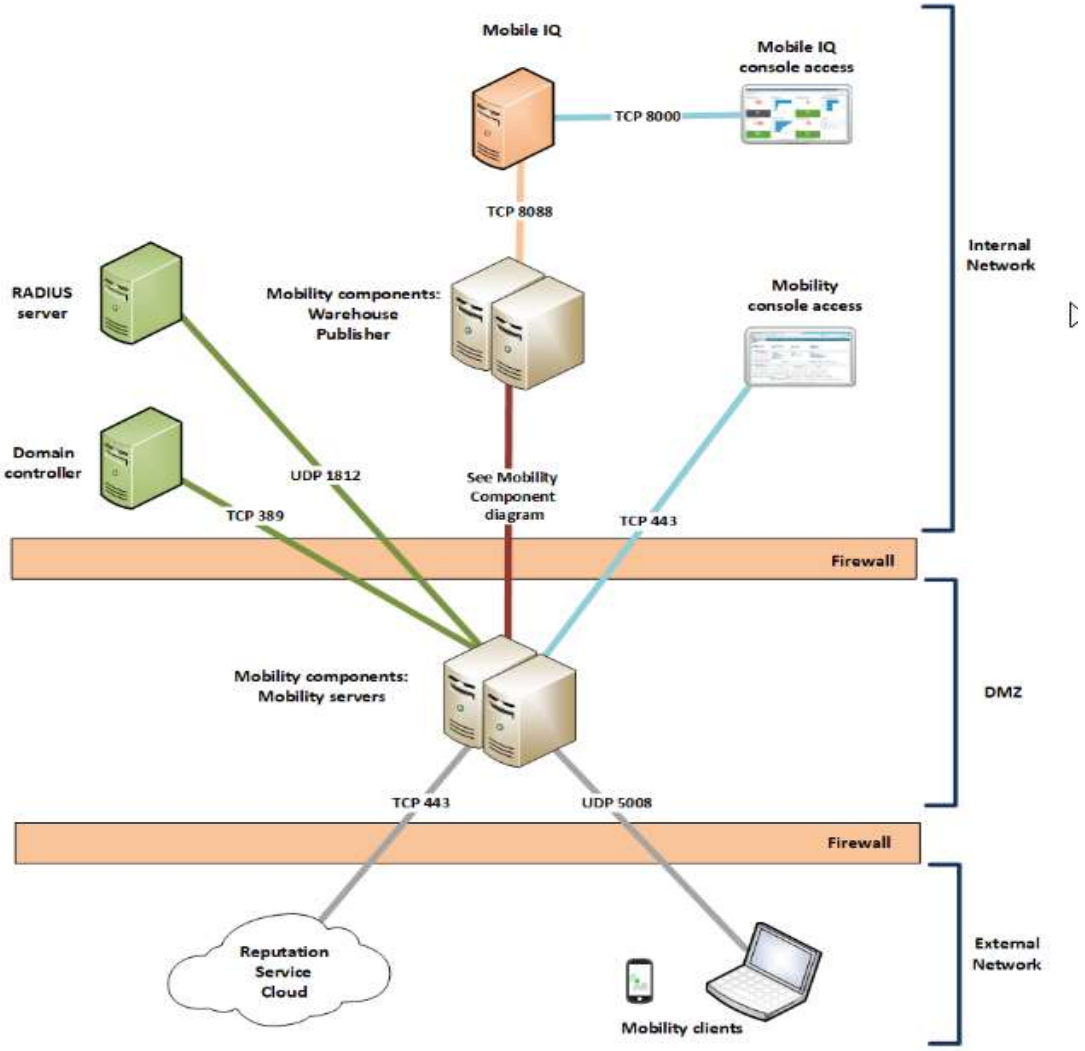
The Warehouse runs on Server 2016 or 2019 and is a directory that serves as the settings and management backbone for a Mobility server or pool of servers

Publisher and Reputation Service

The Publisher runs on Server 2016 or Windows Server 2019 and sends the data it gathers from mobile devices—running on Windows, macOS, iOS, or Android—to publisher targets that support syslog data sources, such as NetMotion Mobile IQ.

Mobility Clients

Enables mobile devices—running Windows, OS X, iPhone, iPad, or Android—to intercept all TCP/IP network activity and relay it to a Mobility server using the Mobility RPC protocol. It allows client-side application sessions to remain active when the device loses contact with the network. It also gathers data from the devices.

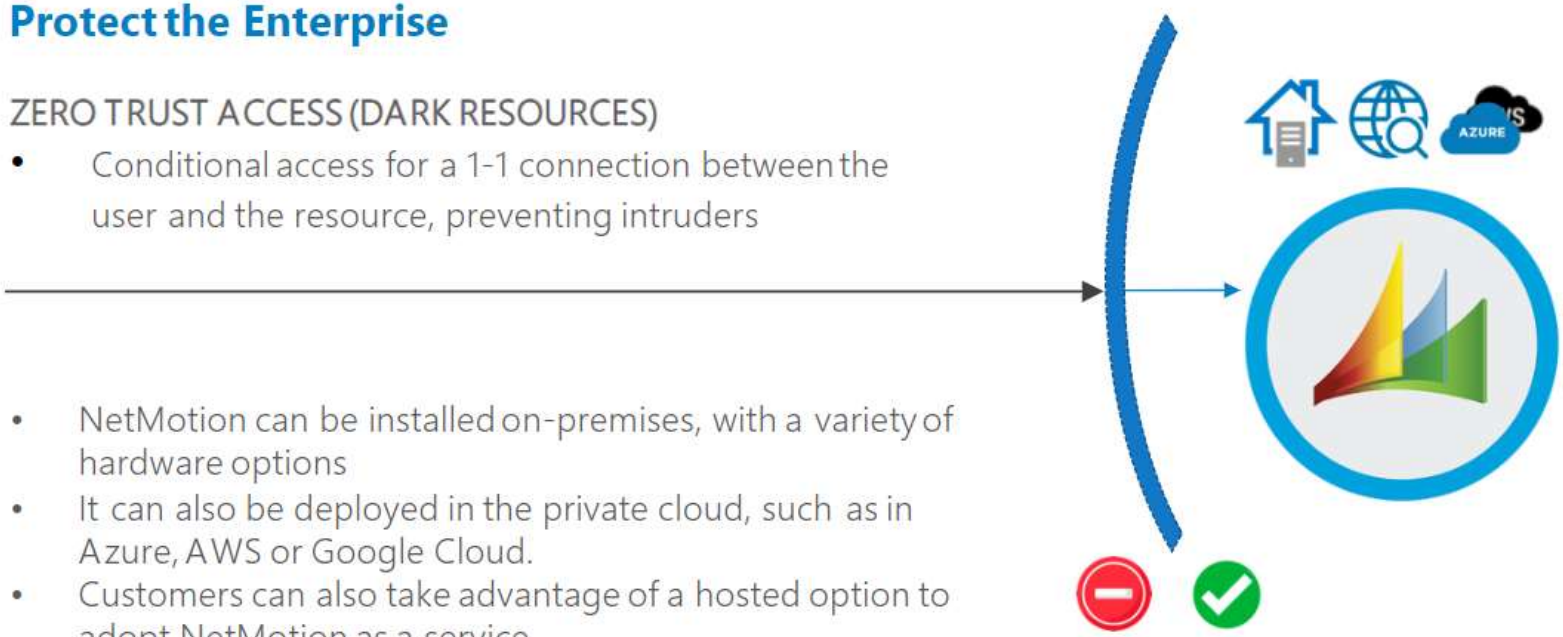


How It Works

Protect the Enterprise

ZERO TRUST ACCESS (DARK RESOURCES)

- Conditional access for a 1-1 connection between the user and the resource, preventing intruders



- NetMotion can be installed on-premises, with a variety of hardware options
- It can also be deployed in the private cloud, such as in Azure, AWS or Google Cloud.
- Customers can also take advantage of a hosted option to adopt NetMotion as a service

Preguntas ?

ABSOLUTE®