



RevBits

Detecta. Rechaza. Derrota.

Las Cyber Amenazas son constantes.

Protégase contra ellas con las soluciones de Cyberseguridad de RevBits.



Lo que entregamos a nuestros clientes

- **Cobertura exhaustiva:** Cinco soluciones robustas que cubren la mayoría de necesidades de ciberseguridad para organizaciones de cualquier tamaño.
- **Innovación:** Soluciones reforzadas con patentes, administradas a través de un dashboard unificado que minimiza el número de proveedores, entregando inteligencia experta y accionable que mitiga el creciente panorama de amenazas.
- **Opciones de despliegue:** Sin importar el ambiente de instalación, SaaS, On-premises, Nube híbrida, o Air-Gap, nuestras soluciones se ajustan a los requerimientos de instalación.
- **Elección:** Empoderar a los clientes para configurar la compra de soluciones que cumplen con sus necesidades.



Privileged Access Management de RevBits

- Clientes nativos en todas las plataformas más usadas: Oracle, SSQL, PostgreSQL, Cassandra, MySQL
- Capacidad creciente de gestión de administración de identidades nativas
- Arquitectura de Jump Server para seguridad de servidores mejorada



RevBits Endpoint Security & EDR

- ICSA Labs de Verizon, 100% de detección, 0 falsos positivos
- Motor de detección de Exploits avanzado
- Control total de endpoints a través del más robusto módulo de EDR disponible



Tecnología de Engaño de RevBits

- Despliega Honeyports basadas en servidores reales que aparecen auténticas para el atacante
- Lanza múltiples honeypots con una instancia de MV
- Despliegue automático de data señuelo y credenciales para dirigir a los atacantes a los honeypots



Seguridad de Email de RevBits

- Seguridad de Email – SEG y agente de análisis de Endpoints para cada cuenta de correo de usuario
- Protección sofisticada de suplantación de página
- Capacidad automática de DMARC/DKIM/SPF



Zero Trust Network de RevBits

- Portal seguro que permite a los usuarios conectarse de forma segura a los activos de red
- En 24 regiones de nube geográficamente distribuidas alrededor del mundo, soportando los servidores proxy de ZTN de RevBits
- Capacidad de SWG para proteger a los usuarios y la organización de los peligros de internet



RevBits

Diseño innovador, fortalecido por patentes para nuestros clientes



Privileged Access Management de RevBits

- Sistema empresarial de llaves y gestión de contraseñas (US10666644B2)
- Almacenamiento en sesión de navegador como almacenamiento de llaves privadas en un esquema de cifrado de llaves públicas (US10579542B2)



Seguridad de Endpoints y EDR de RevBits

- Sistemas y métodos para prevenir la ejecución de código de kernel de Windows o drivers (US10055572B1)



Seguridad de Email de RevBits

- Sistema y método para detectar Emails de phishing (US10574696B2)
- System and method for page impersonation detection in phishing attacks (US20210176275A1)



Zero Trust Network de RevBits

- Sistema y método para proveer una red de zero-trust network (US11240242B1)



Plataforma de Cyber Inteligencia de RevBits



Cuatro verdades duras de Cyberseguridad

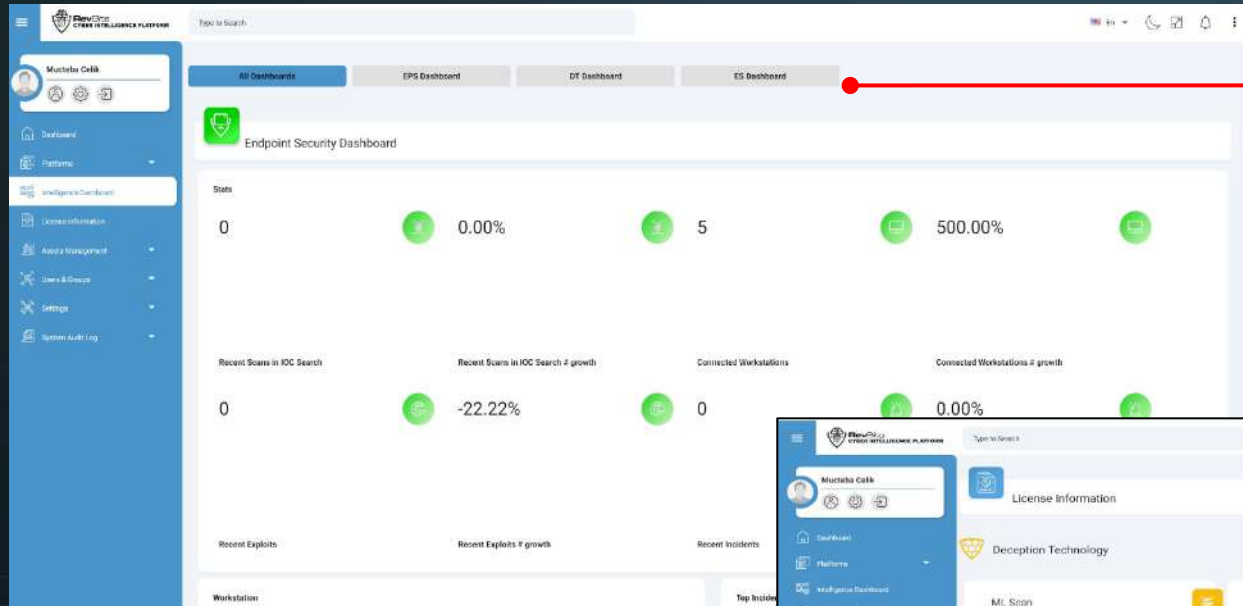
1. El esfuerzo de administrar múltiples herramientas de seguridad requiere mucho tiempo.
2. La falta de inteligencia compartida a través de múltiples soluciones, resulta en una oportunidad perdida para una defensa proactiva de amenazas divergentes.
3. Gestionar múltiples proveedores puede arruinar los presupuestos, dejando grietas en cobertura.
4. Productos separados pueden crear grietas de cobertura.

Cuatro grandes ventajas de la plataforma de Cyber Inteligencia de RevBits

1. La PCI de RevBits convierte la teoría de Detección y Respuesta Extendida en realidad.
2. La PCI de RevBits ofrece protección superior al compartir inteligencia de amenazas de múltiples módulos de seguridad y mejora el tiempo de respuesta a las amenazas.
3. La PCI de RevBits reduce los costos totales de implementación y libera presupuesto para otros proyectos.
4. La PCI de RevBits acaba con el efecto de productos dispersos y cierra las brechas de Cyberseguridad.

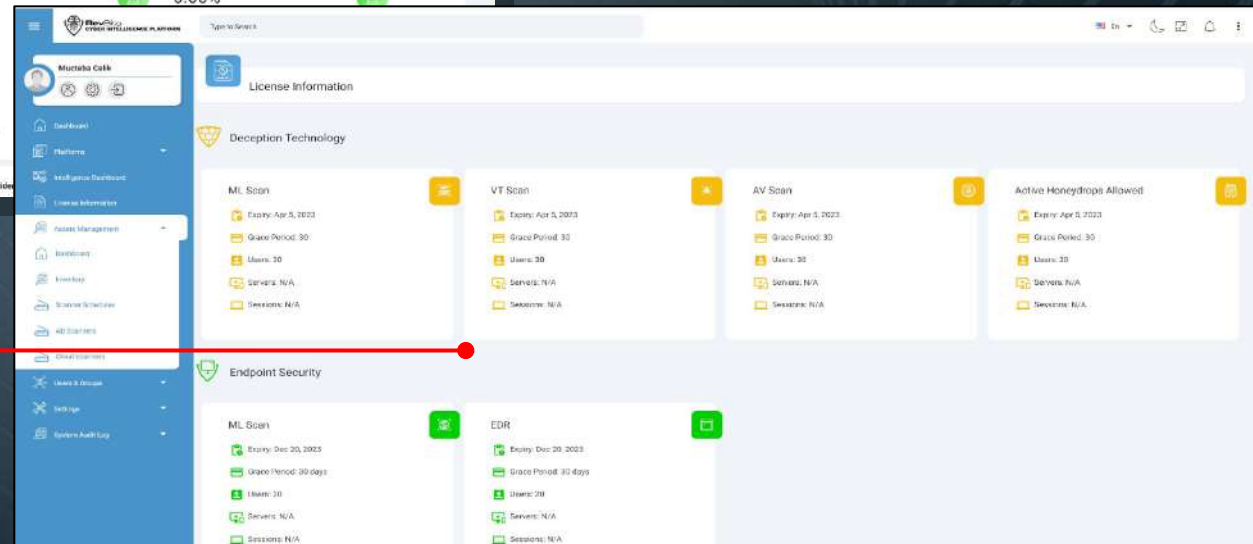


Plataforma de Cyber Inteligencia de RevBits



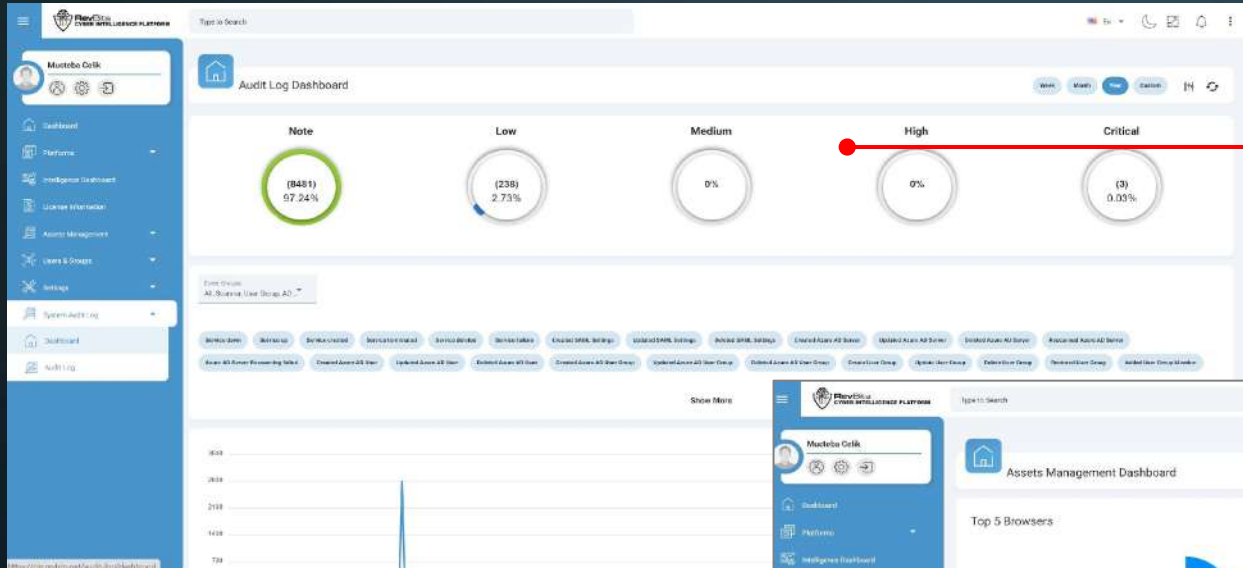
Cree un dashboard unificado que reporte inteligencia vital desde las soluciones de RevBits activas

Mantenga una conciencia situacional rápida acerca del estado de la licencia y las soluciones activas

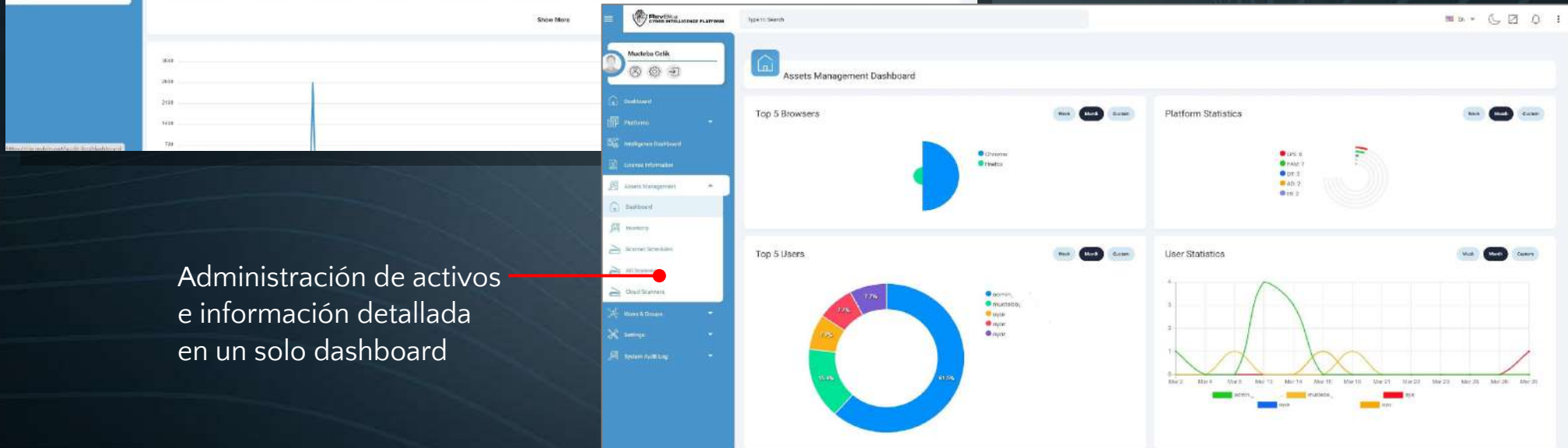




Plataforma de Cyber Inteligencia de RevBits



Todos los datos de registro reportados, pueden ser visualizados en una sola ubicación y se integra fácilmente con los más populares SIEM



Administración de activos e información detallada en un solo dashboard

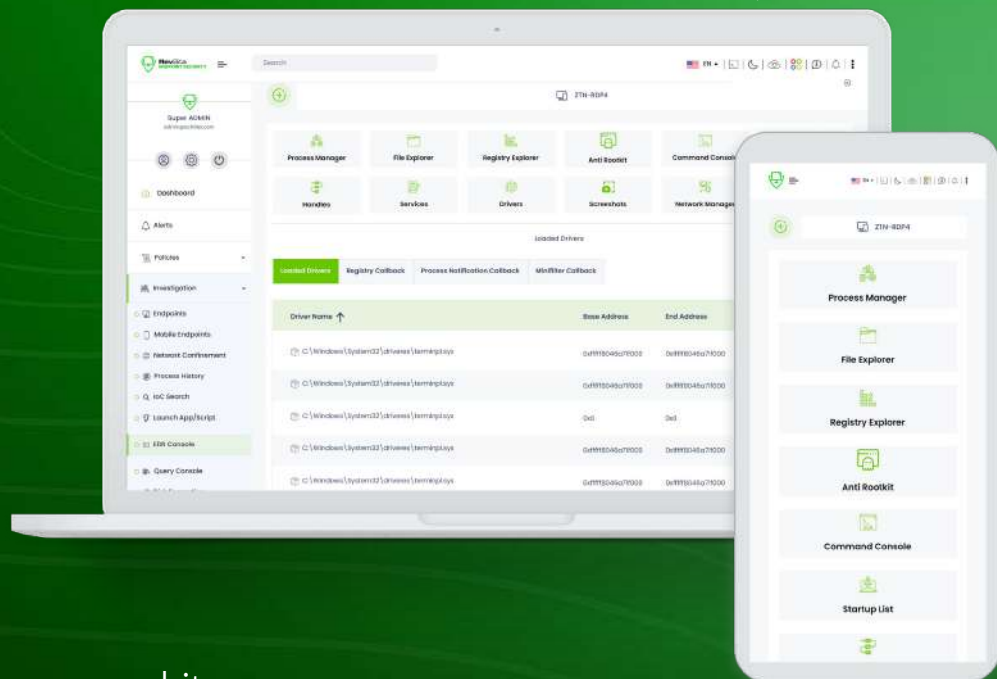


Seguridad de Endpoints y EDR de RevBits



Respuesta de Endpoints que entrega mitigación robusta y análisis forense

- Análisis de tres fases (Comportamiento, Firma, Machine Learning)
- Capacidad de control profundo de alta para dispositivos USB
- Motor de detección de Exploit avanzado
- Alineado al marco de MITRE ATT&CK
- Certificación de Verizon ICSA Labs, 100% Detección, cero falsos positivos



Seguridad de Endpoints que ofrece 100% de detección

- Patente de USA de protección de ataques de rootkit a nivel de kernel
- Control remoto de endpoints que cubre, administración de procesos, explorador de registro y acceso a nivel de kernel
- Control de análisis Forense en demanda o programado
- Confinamiento inmediato del Endpoint cuando se requiera
- Construcción de políticas granular que incluye:
 - * Drivers aprobados en lista blanca (controla ataques de BYOVD)
 - * Políticas de control de USB profundas



Plataforma de Cyber Inteligencia de RevBits

Seguridad de Endpoints de RevBits – Todas las bases de detección cubiertas



Análisis de Hash –
búsqueda en Google
con un click, listas
negras/blancas y
búsqueda en los
Endpoints de la red
Árbol de
ejecución de
procesos

Grid Line: C:\Users\RevBits\Temp\RevBitsMain_Main_Executable.exe

User: REVBITSEPS\RevBitsDemo

Packer: Microsoft Visual C++ 6

MDS: 3654CBFA69F10C23E4C70BDF3D158

SHA1: 19BF019FC0BF44828378F008332430A090871274

SHA256: 10279770ADC331D0903D0E91E714D395A1242161F4DAE093436CE37FFDCAF6

ML Score: 92.11%

Machine Learning Score: 92.11%

Process: RevBitsMain_Executable.exe

Name: RevBitsMain_Executable.exe

Path: C:\Users\RevBits\Temp\RevBitsMain_Main_Executable.exe

Grid Line: C:\Users\RevBits\Temp\RevBitsMain_Main_Executable.exe

Type: EXE

Line: REVBITSEPS\RevBitsDemo

Packer: Microsoft Visual C++ 6

MDS: SHA1 SHA256

MDS: 3654CBFA69F10C23E4C70BDF3D158

Scoring de Machine learning

Búsqueda de firmas

Process Activities

Indicator View | Timeline View | Attack Tactics

All | Malicious | Suspicious

Malicious

Software Information Retrieval

Credential harvesting (1/24)

Indicator: Malicious

Access: Read

Action: Credential harvesting

Type: Misc - Memory

Target: -

Value: -

Description: The application attempted to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear password, from the operating system and software. Credentials can then be used to perform lateral movement and access restricted information. The attempt was detected and blocked by RevBits EPS.

Attack ID: T1003.001

Created At: Sep 29 2021, 11:47:20

General

Attempted DLL Hijacking

Indicator: Malicious

Action: Create

Diagnóstico de análisis de comportamiento



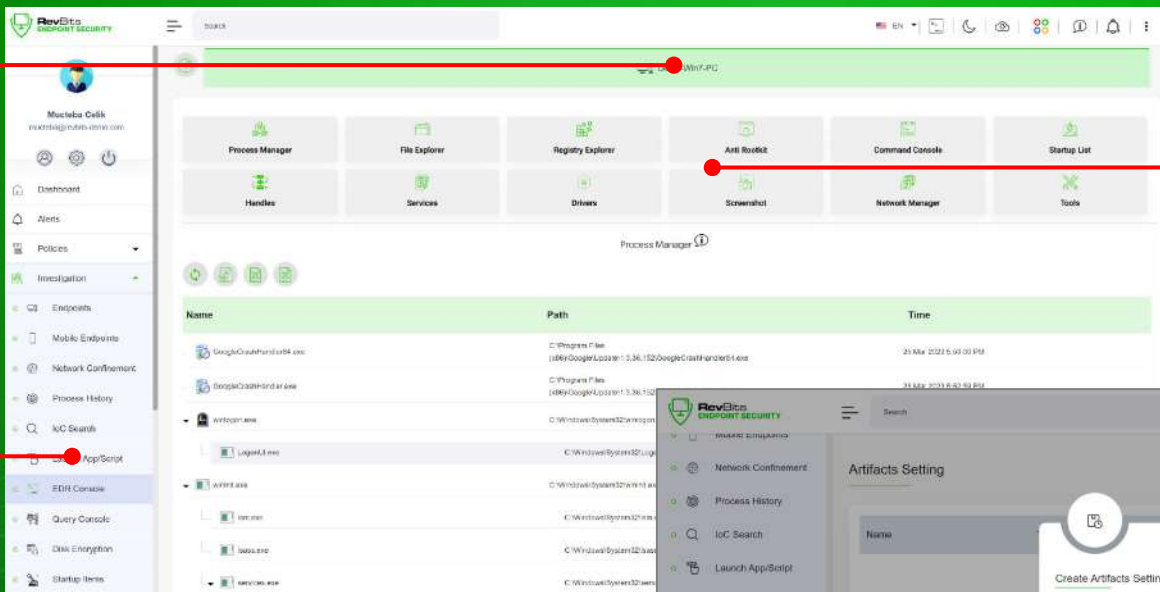
Plataforma de Cyber Inteligencia de RevBits

Control remoto completo de estaciones de trabajo, mitigación y protección

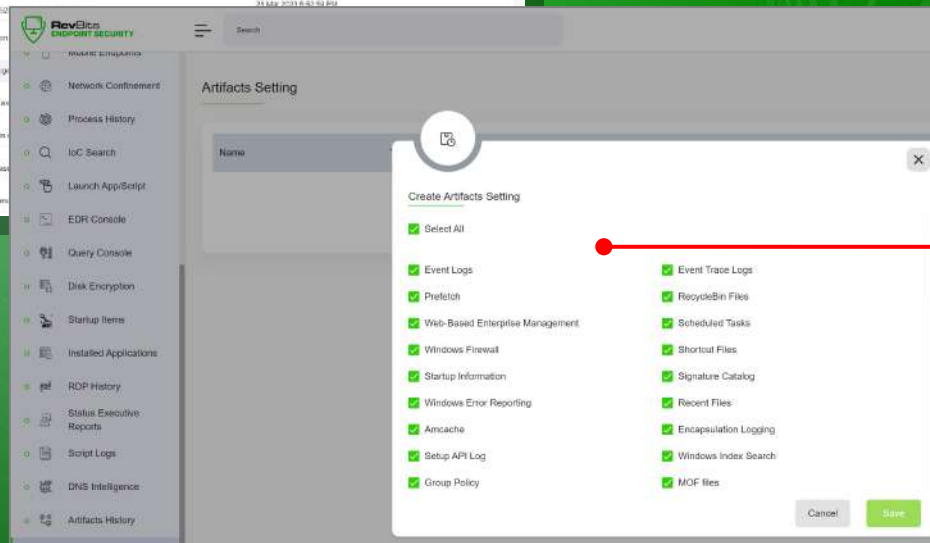


Múltiples sesiones de EDR a través de múltiples Endpoints pueden ser lanzadas al mismo tiempo

Menú de investigación profundo de cerca de 15 opciones de interacción de Endpoints



Control completo de Endpoints al interior de la consola de EDR de la mayoría de procesos de máquina con un solo click

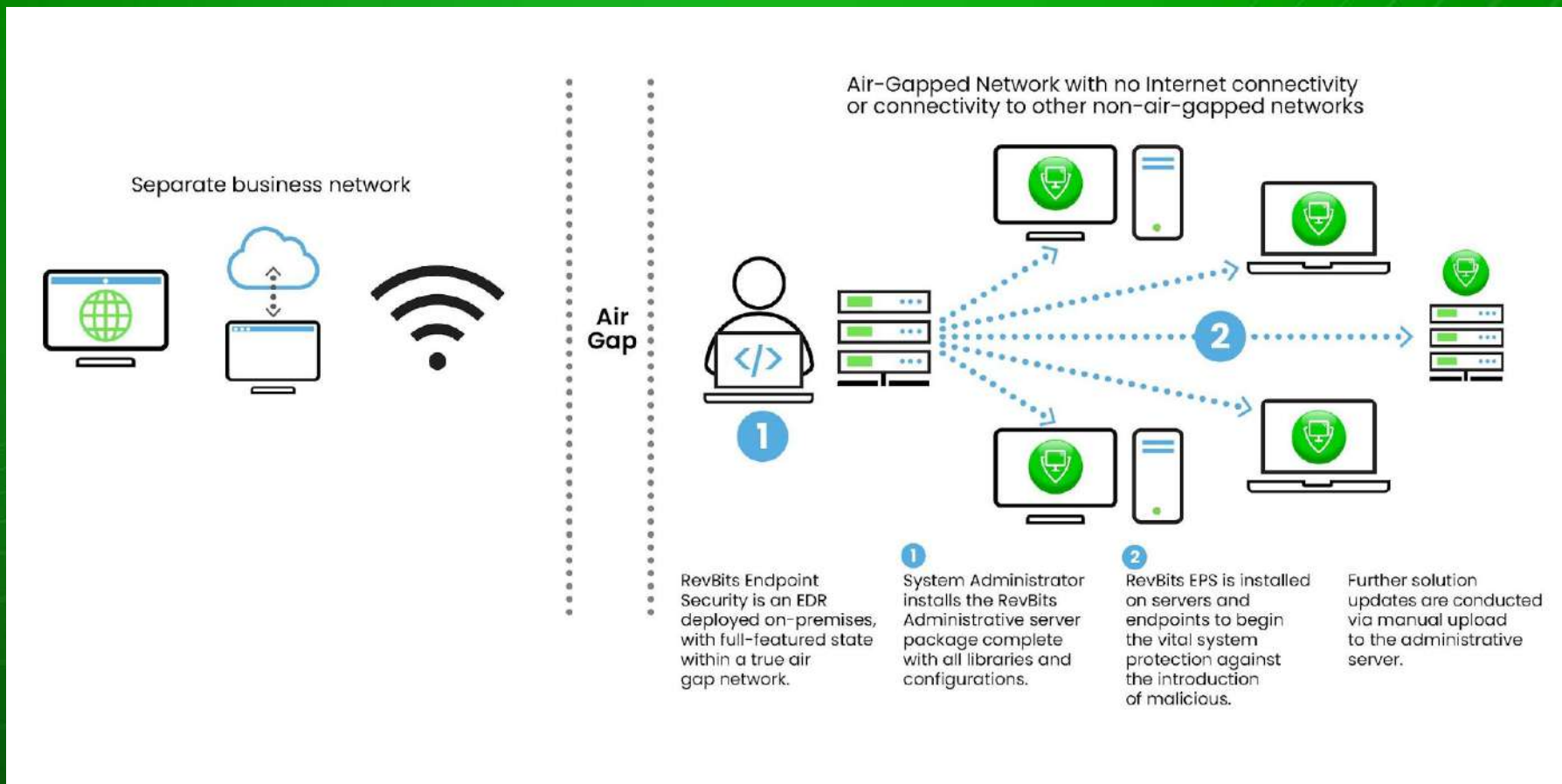


Recoge cerca de 70 "artifacts" en demanda o programados en los Endpoints



Plataforma de Cyber Inteligencia de RevBits

Arquitectura simple, aun en entornos de Air-Gap



Seguridad de Endpoints de RevBits y EDR puede ser desplegada como una solución On-premises, nube híbrida, SaaS, o Air-Gap

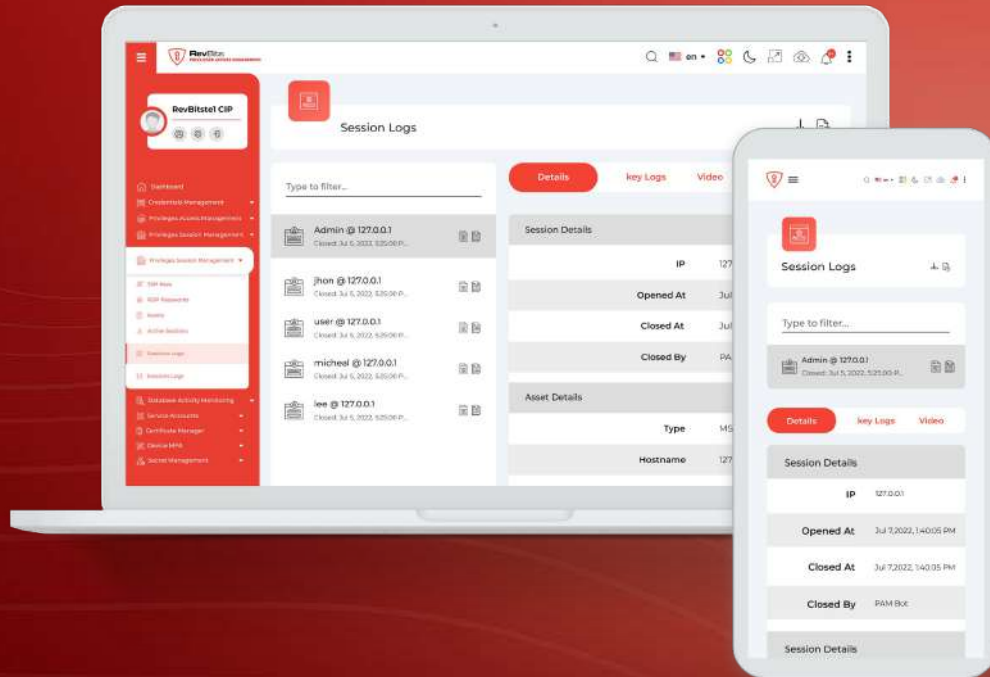


Privileged Access Management de RevBits



Extienda el acceso sin extender sus proveedores

1. Administración de sesión privilegiada
2. Administración de contraseñas
3. Administración de llaves
4. Administración de cuentas de servicios
5. CI/CD Integration
6. Administración de certificados



PAM desarrollado para entregar control y seguridad de los servidores

- Administrador para flujos de dada de altas
- Arquitectura de Jump Server para seguridad real de los activos
- Integra y administra servidores de nube
- Integración completa con SIEM
- Seguridad de sesiones de conexión a través de grabación de video y entradas de teclado
- Verdadera arquitectura de un click a través de una amplia variedad de clientes nativos para la mayoría de protocolos de lenguajes de servidores



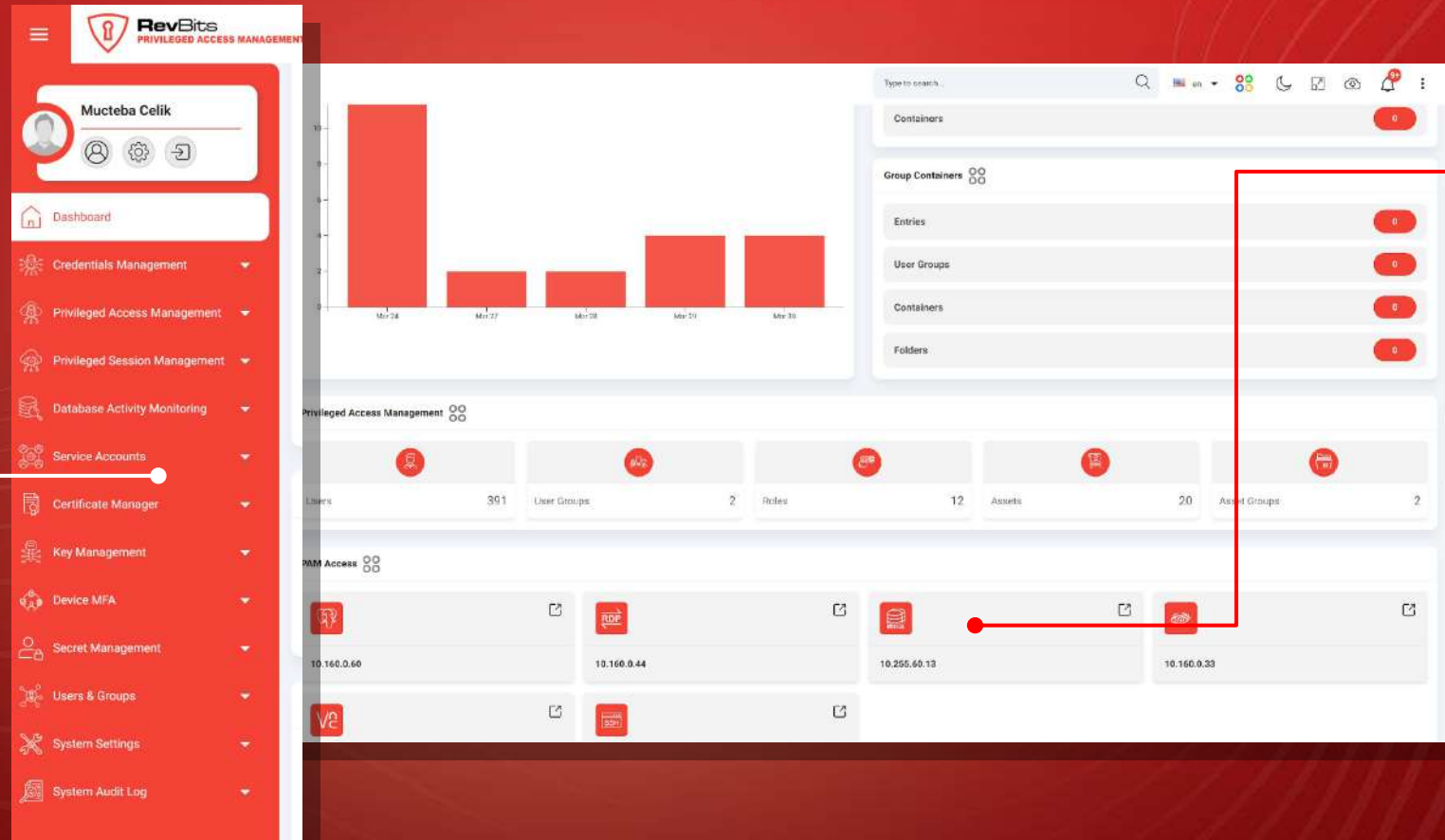
Privileged Access Management de RevBits

Extienda el acceso sin extender sus proveedores - Las herramientas que quiere y necesita



PAM de RevBits continúa expandiéndose junto con sus necesidades de administración de acceso.

1. Siete módulos de administración de acceso en una solución
2. Simplifique dar de alta a los proveedores



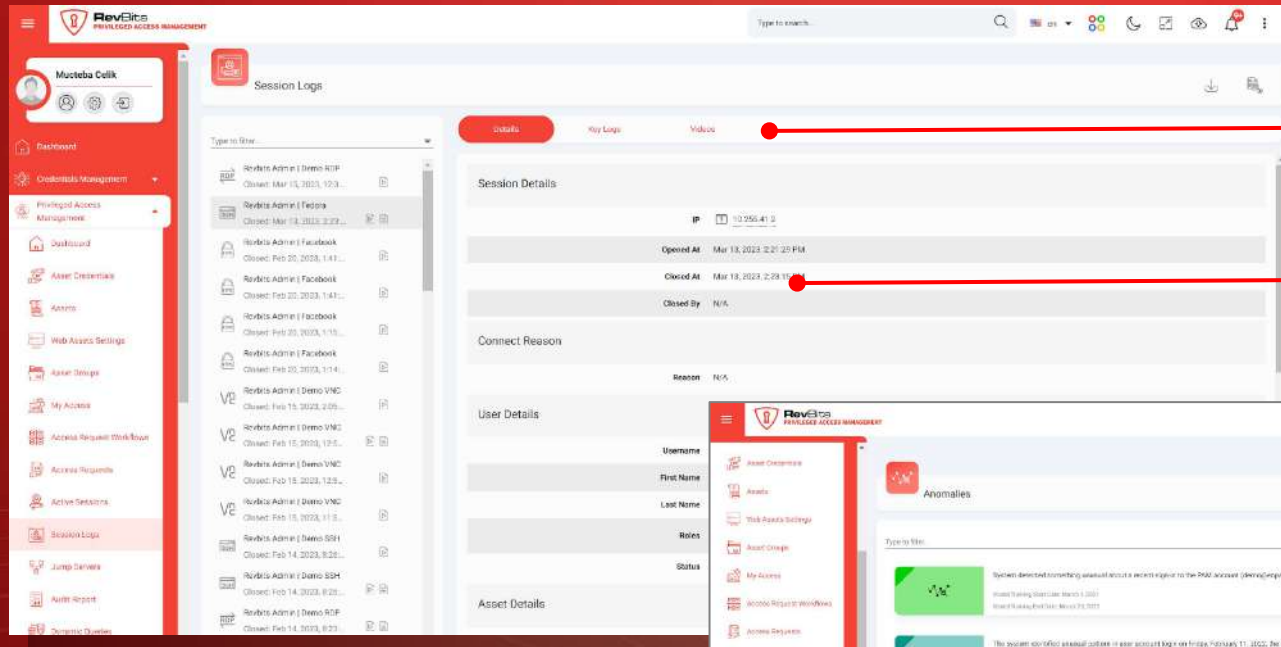
Arquitectura de cliente nativa significa:

1. Use las herramientas que quiere cuando quiera
2. Y el acceso está a un click



Privileged Access Management de RevBits

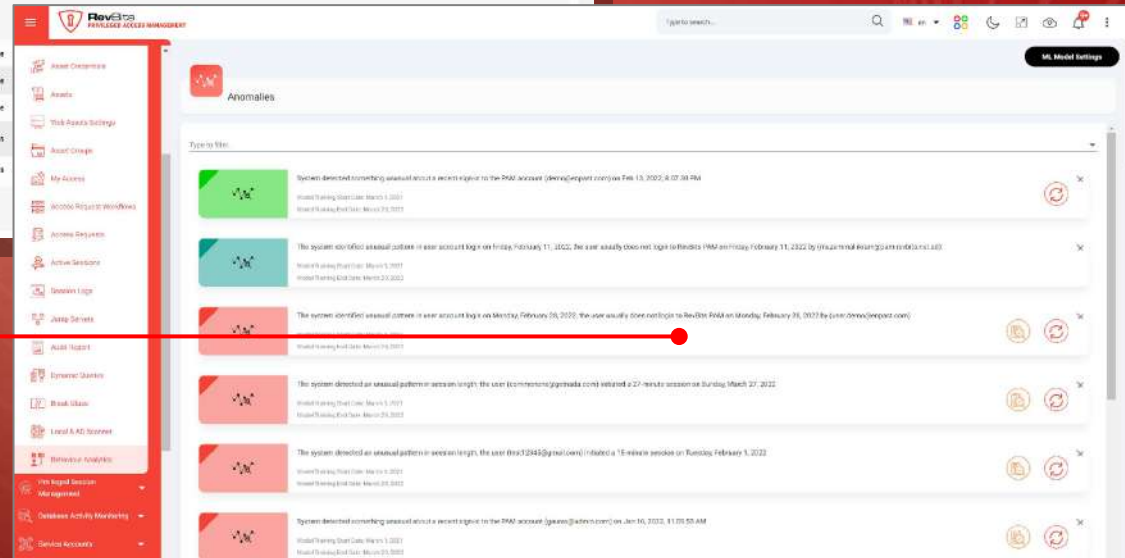
PAM real – Seguridad de servidor real



Monitoree las sesiones en tiempo real o cuando quiera a través de las grabaciones de video y entradas de teclado

Seguridad máxima de activos a través de arquitectura de Jump Server

Controle el abuso de los servidores a través del análisis de comportamientos anómalos





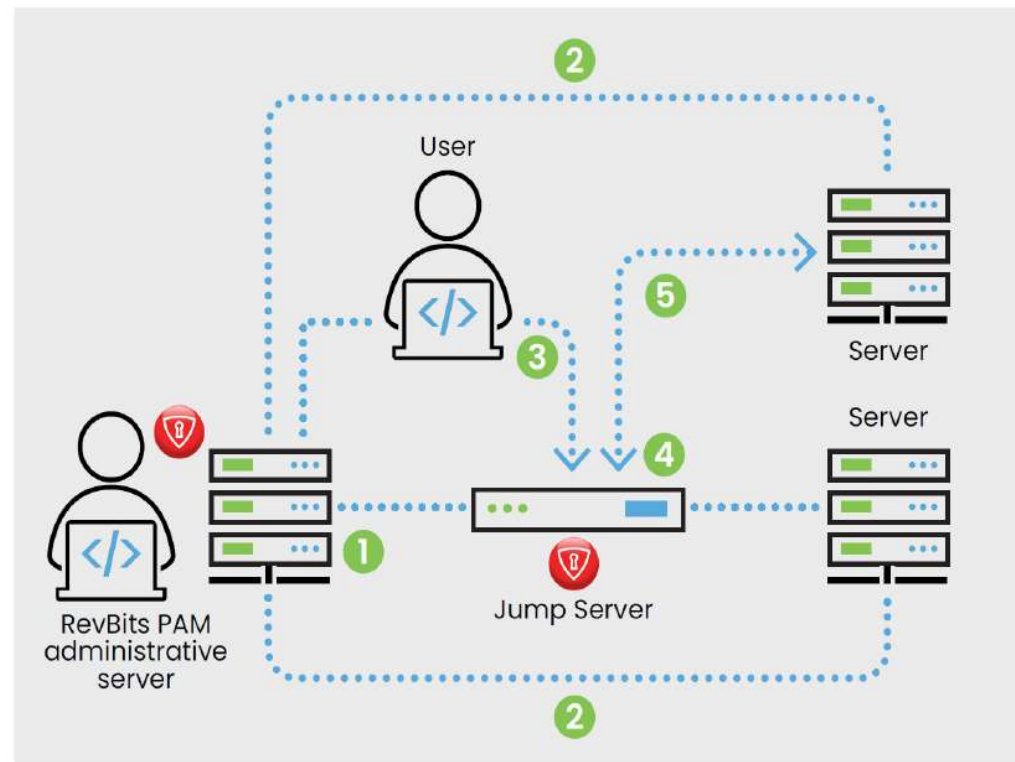
Privileged Access Management de RevBits

PAM real – Desplegable en tres ambientes (On-Premises)



RevBits Privileged Access Management – On-Premises

- 1 RevBits PAM administrative server is located, on-premises inside the network and controlled by the PAM administrator who onboards servers and users.
- 2 The RevBits PAM system administrator onboards determined network servers to the PAM solution. At this point, access to these servers is controlled through the PAM solution.
- 3 An onboarded RevBits PAM user initiates access to an onboard network server. The RevBits PAM user authenticates to the RevBits PAM Jump Server.
- 4 The RevBits PAM Jump Server authenticates the user and generates a one-time credential to the requested target server.
- 5 After the RevBits PAM Jump Server has authenticated to the target server, the user session is initiated and conducted at the RevBits Jump Server. The user does not have a direct connection to the target server and all sessions are monitored (key stroke and video recording) at the RevBits Jump Server.





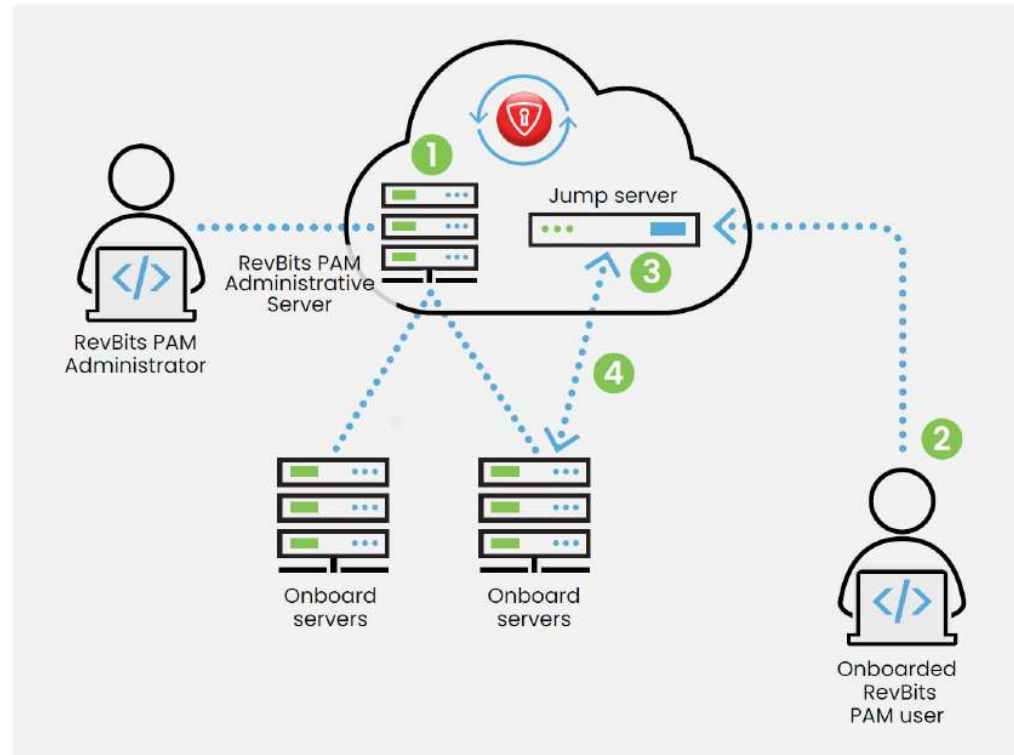
Privileged Access Management de RevBits

PAM real – Desplegable en tres ambientes (SaaS)



RevBits Privileged Access Management – SaaS Deployment

- 1** RevBits PAM Administrative Server is located in the RevBits SaaS Datacenter and is controlled by the PAM administrator who onboards servers and users.
- 2** An onboarded RevBits PAM user initiates access to an onboard network server. The RevBits PAM user authenticates to the RevBits PAM Jump Server.
- 3** The RevBits PAM Jump Server authenticates the user and generates a one-time credential to the requested target server.
- 4** After the RevBits PAM Jump Server has authenticated to the target server, the user session is initiated and conducted at the RevBits Jump Server. The user does not have a direct connection to the target server and all sessions are monitored (key stroke and video recorded) at the RevBits Jump Server





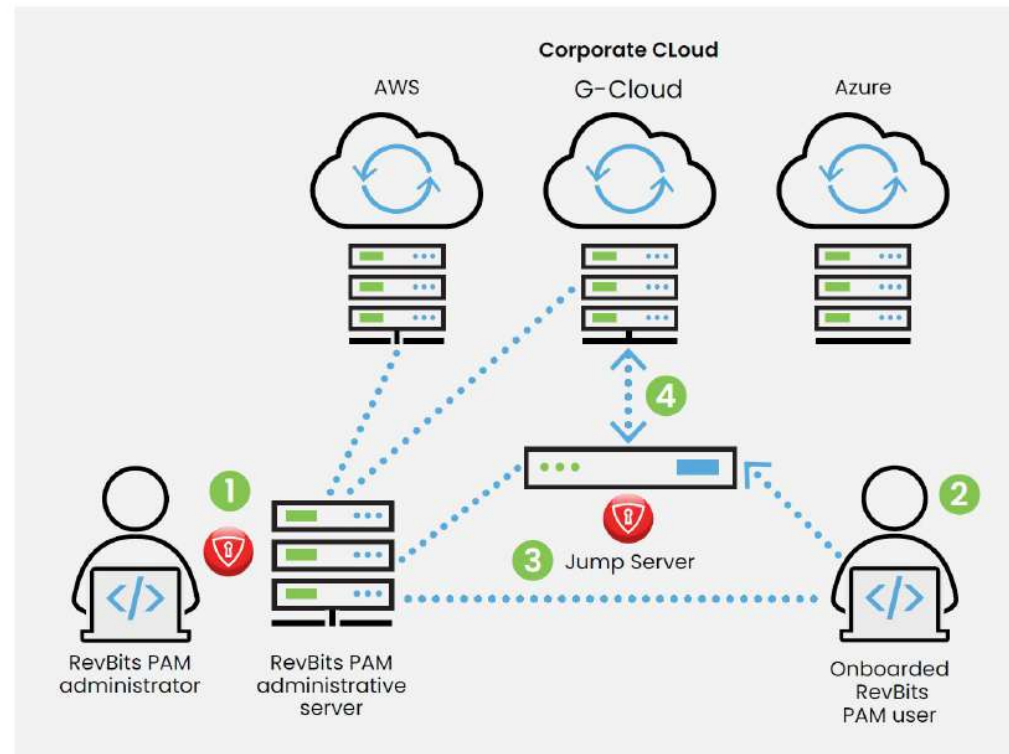
Privileged Access Management de RevBits

PAM real – Desplegable en tres ambientes (Nube híbrida)



RevBits Privileged Access Management – Hybrid Cloud Deployment

- 1 RevBits PAM Administrative Server is located on-premises inside the network or on the corporate cloud and controlled by the PAM administrator who onboards servers and users. Once onboarded, access to these servers is controlled through the RevBits PAM solution.
- 2 An onboarded RevBits PAM user initiates access to an onboard network server. The RevBits PAM user authenticates to the RevBits PAM Jump Server.
- 3 The RevBits PAM Jump Server authenticates the user and generates a one-time credential to the requested target server.
- 4 After the RevBits PAM Jump Server has authenticated to the target server, the user session is initiated and conducted at the RevBits Jump Server. The user does have a direct connection to the target server and all sessions are monitored (key stroke and video recorded) at the RevBits Jump Server.



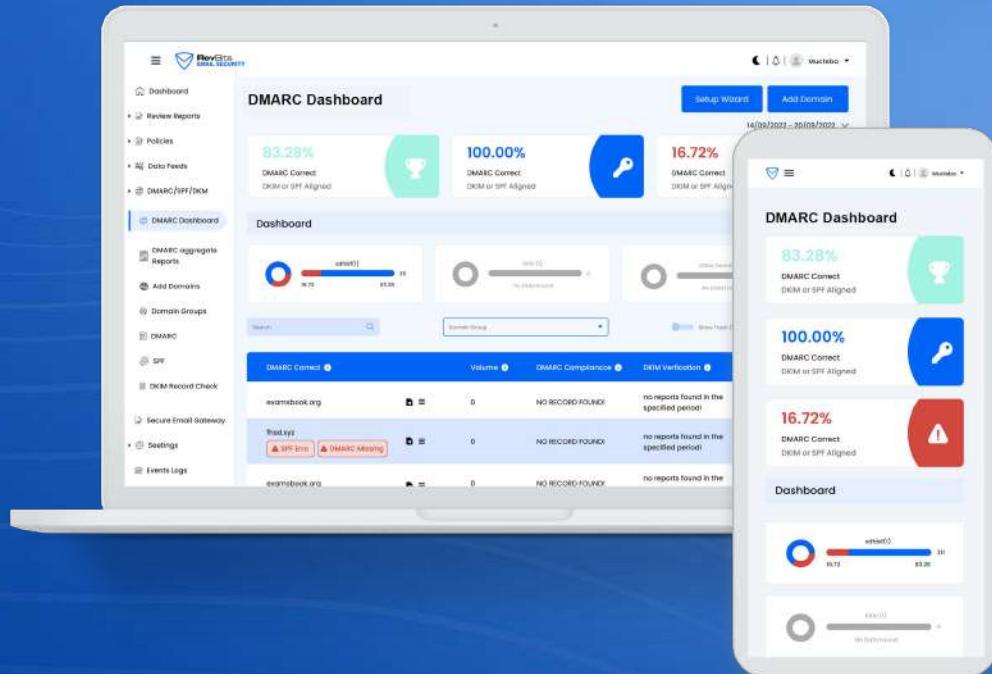


Seguridad de Email de RevBits



Seguridad de Email con el doble de protección

- Seguridad de interfaz (SEG) – Seguridad de destino (agente de inbox)
- Reportes en dashboard profundos y robustos para los administradores
- Control de políticas a nivel de usuario, grupos o toda la red
- Mejora la seguridad de Email de Microsoft Defender (E5)



Seguridad de Email con su diseño

- Seguridad de Email diseñada para detectar y bloquear ataques de suplantación de páginas
- Defiende todos los entornos importantes de acceso organizacional
- Protege contra el robo de credenciales de acceso de Office 365
- Personalizable a la red
- Automatización de DMARC, DKIM, SPF



Seguridad de Email de RevBits

Seguridad de Email con el doble de protección



Header Information

- Subject: [063] include docx with OLE
- To Email: Jason@revbits-demo.com
- IP Address: N/A
- Domain Address: N/A
- From Email: andrly_hudz_admin@outlook.com
- Total Emails: 3

Analysis section shows: 2 Malicious

Files:

- Reason: [Attachments] Found executable in attachments
- Message: [Attachments] calc.exe is an executable
- Score: 10 points

Análisis de la bandeja de entrada de Email llevado a cabo con el plugin de mail Security Outlook de RevBits O también con el motor de análisis de Email propio

Completa capacidad automatizada de DMARC/DKIM/SPF

DMARC Dashboard

0% DMARC Correct (20% of SPF signed)

0% Authenticated (100% of SPF signed)

0% Invalid Files (20% of SPF signed)

EMEA Outreach (1) No Data Found

Other Domains (20) No Data Found

From Domain	Volume	DMARC Compliance	DKIM Verification	SPF Verification
adchicks.com	0	NO RECORD FOUND	No reports found for the specified period.	No reports found in the specified period.
aps.com	0	NO RECORD FOUND	No reports found for the specified period.	No reports found in the specified period.
manj.com	0	NO RECORD FOUND	No reports found for the specified period.	No reports found in the specified period.
harkibabai.in	0	NO RECORD FOUND	No reports found for the specified period.	No reports found in the specified period.



Seguridad de Email de RevBits

Seguridad de Email con el doble de protección



The screenshot shows the RevBits Email Security dashboard. The left sidebar contains navigation options: Dashboard, Review Reports, Policies, Data Feeds, DMARC/SPF/DKIM, Secure Email Gateway, Domains and Servers (selected), Settings, and Event Logs. The main content area is titled 'Domains' and features a search bar for 'Company SMTP'. Below the search bar is a table with the following columns: Domain, MX Record Pointing, MX Record Status, and Actions.

Domain	MX Record Pointing	MX Record Status	Actions
achilles.com	eu-smtp-inbound-1.mimecast.com, eu-smtp-inbound-2.mimecast.com	Error : Invalid MX Configuration	
dev.in	smtp.secureserver.net, mailstore.secureserver.net	Error : Invalid MX Configuration	
revbits-demo.com	revbits-demo.us-east1.revbits-esg.com, mx1.emailsrvr.com, mx2.emailsrvr.com	Warning : Extra MX detected	
tester.io	-	-	
ishop2k.com	mx.mail-data.net	Error : Invalid MX Configuration	
xyz.com	aspmx1.google.com, alt1.aspmx1.google.com, alt2.aspmx1.google.com, aspmx2.googlemail.com, aspmx3.googlemail.com	Error : Invalid MX Configuration	
papcornfarm7.com	park-mx.above.com	Error : Invalid MX Configuration	
test.com	-	-	
hab.io	-	-	
1.com	-	-	

Page: 1 | 10

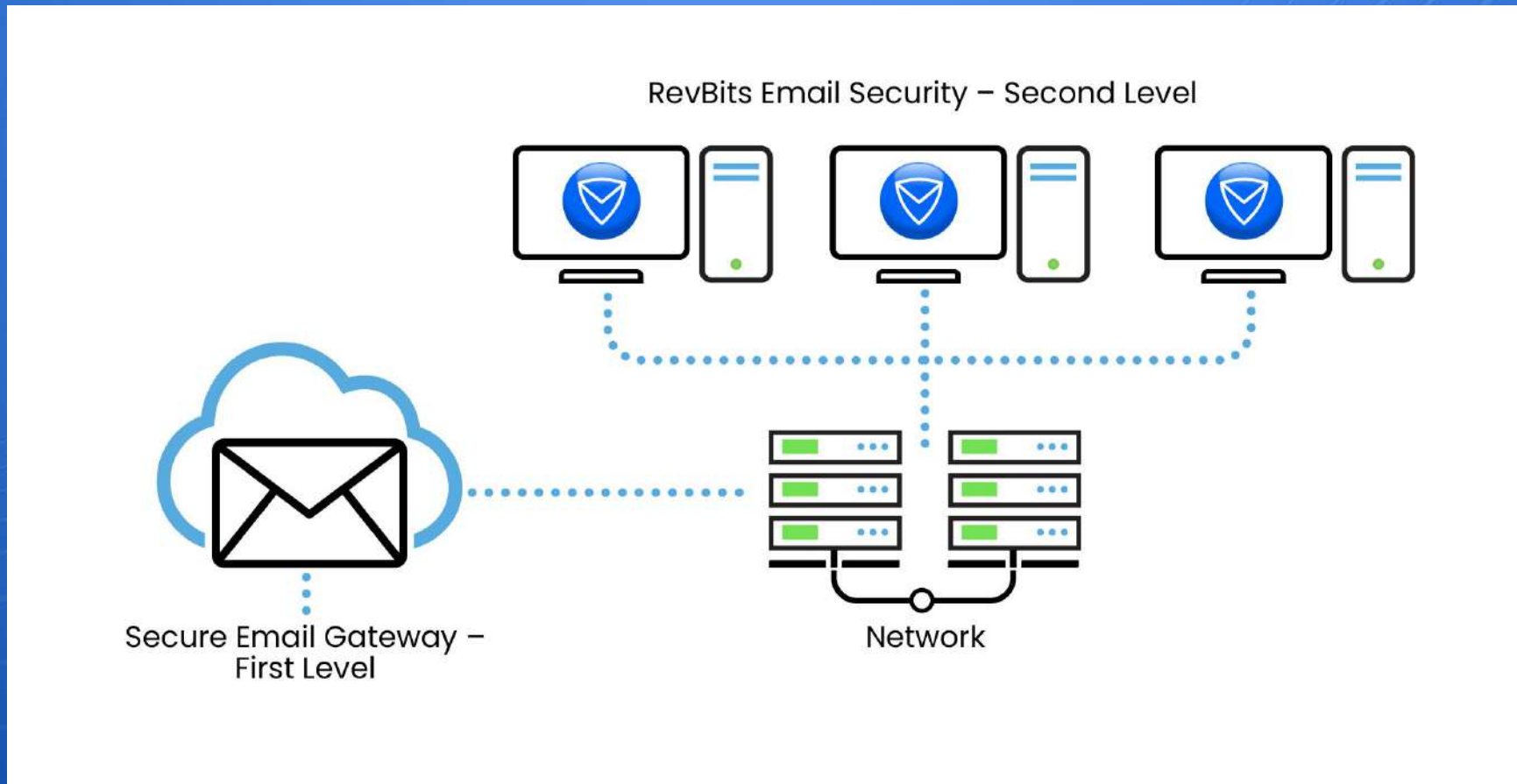
© 2020 RevBits Email Security by RevBits All Rights Reserved. v2.0.2

Un análisis de Email en bloque llevado a cabo con Email Security SEG de RevBits



Seguridad de Email de RevBits

Seguridad de Email con el doble de protección



Seguridad de Email de RevBits se despliega como una solución On-premises, nube híbrida, o SaaS

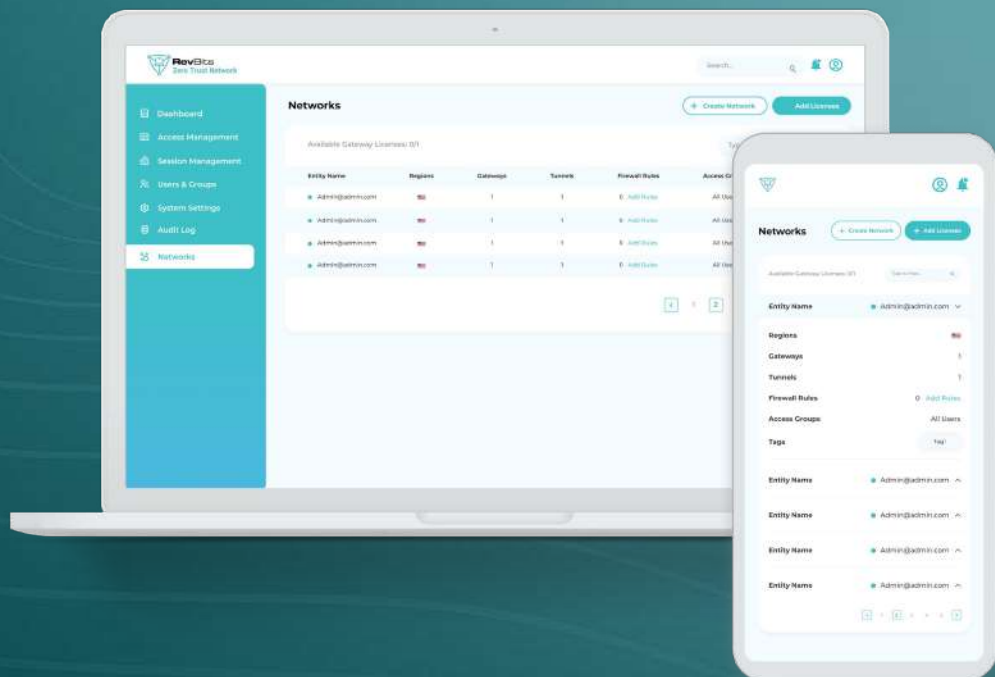


Zero Trust Network de RevBits



Zero Trust para seguridad más allá de una VPN

- Todo el tráfico de ZTN es seguro y completamente cifrado
- Arquitectura auto escalable para satisfacer todos los requerimientos de los usuarios
- Aplicación de cliente liviano
- Provee conectividad segura de Internet para los usuarios (SWG)



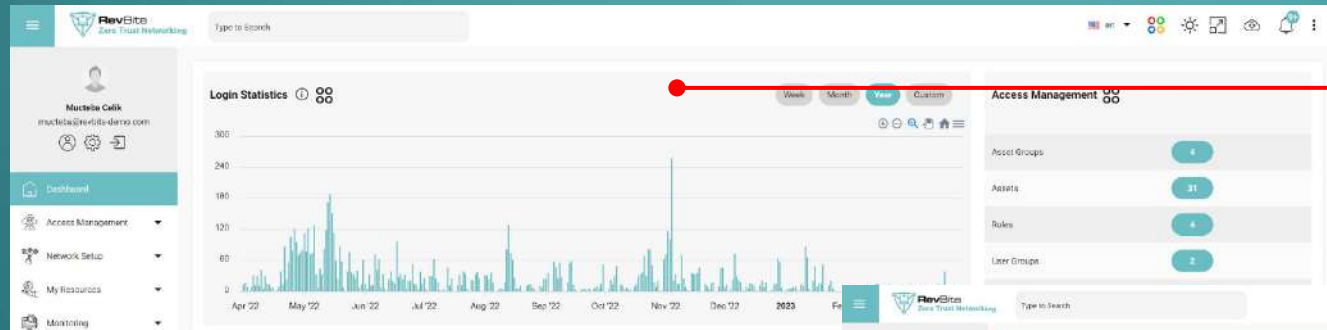
Zero Trust en cualquier lugar, para todo el mundo, y en cualquier momento

- Servidores proxy de ZTN pre configurados alrededor del mundo con capacidad de acceso inmediato
- Conexión de acceso remoto a los activos/aplicaciones internas de la compañía creadas por el agente proxy de ZTN de RevBits
- Todas las sesiones se graban en video con el proxy de ZTN de RevBits
- Todos los activos/aplicaciones se acceden transparentemente por los usuarios en forma remota y desde cualquier dispositivo. No se requiere instalación de cliente
- Control de acceso de terceros
- Soporta todos los dispositivos móviles con aplicaciones nativas

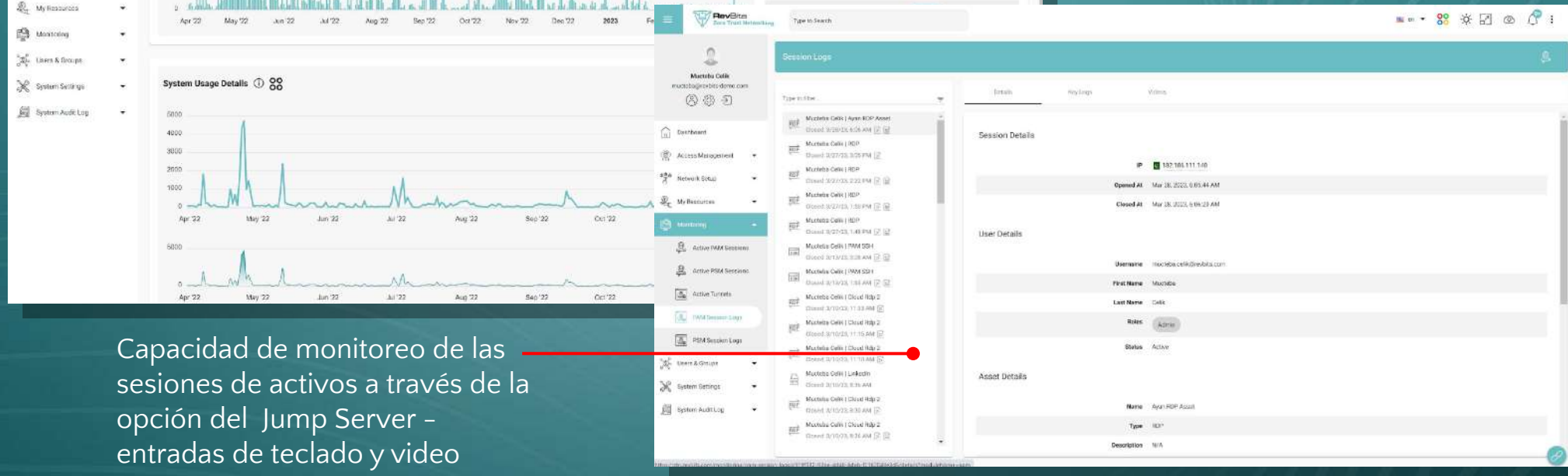


Zero Trust Network de RevBits

Zero Trust para seguridad más allá de una VPN



Acceso con control remoto a la red más allá de cifrado de datos con una VPN – autenticación para servicios, activos y aplicaciones privilegiadas y autorizadas

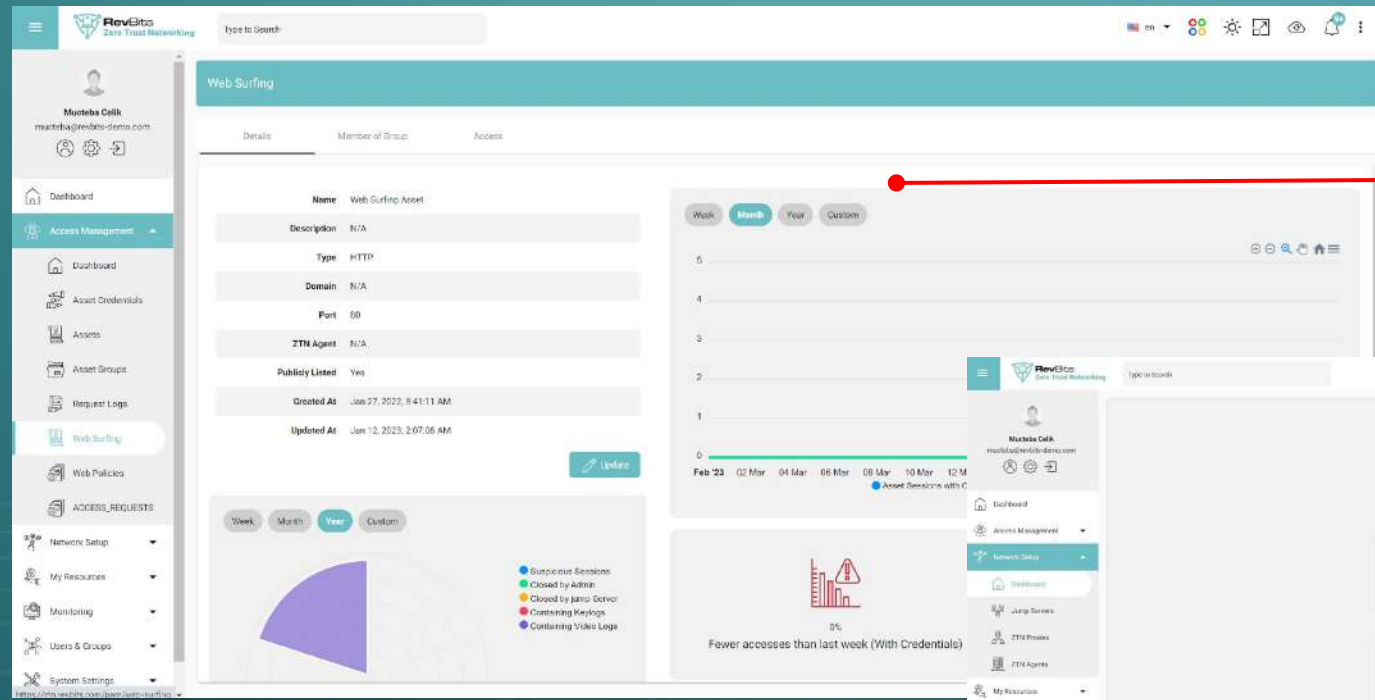


Capacidad de monitoreo de las sesiones de activos a través de la opción del Jump Server – entradas de teclado y video



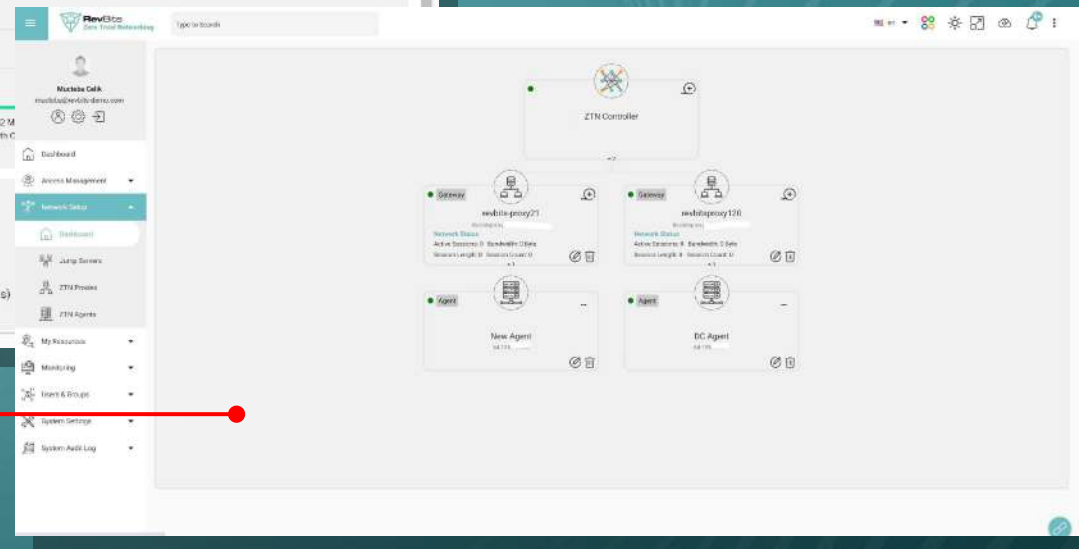
Zero Trust Network de RevBits

Zero Trust para seguridad más allá de una VPN



Controle el acceso a Internet de los empleados y los sitios visitados a través de la capacidad de Secure Web Gateway (SWG)

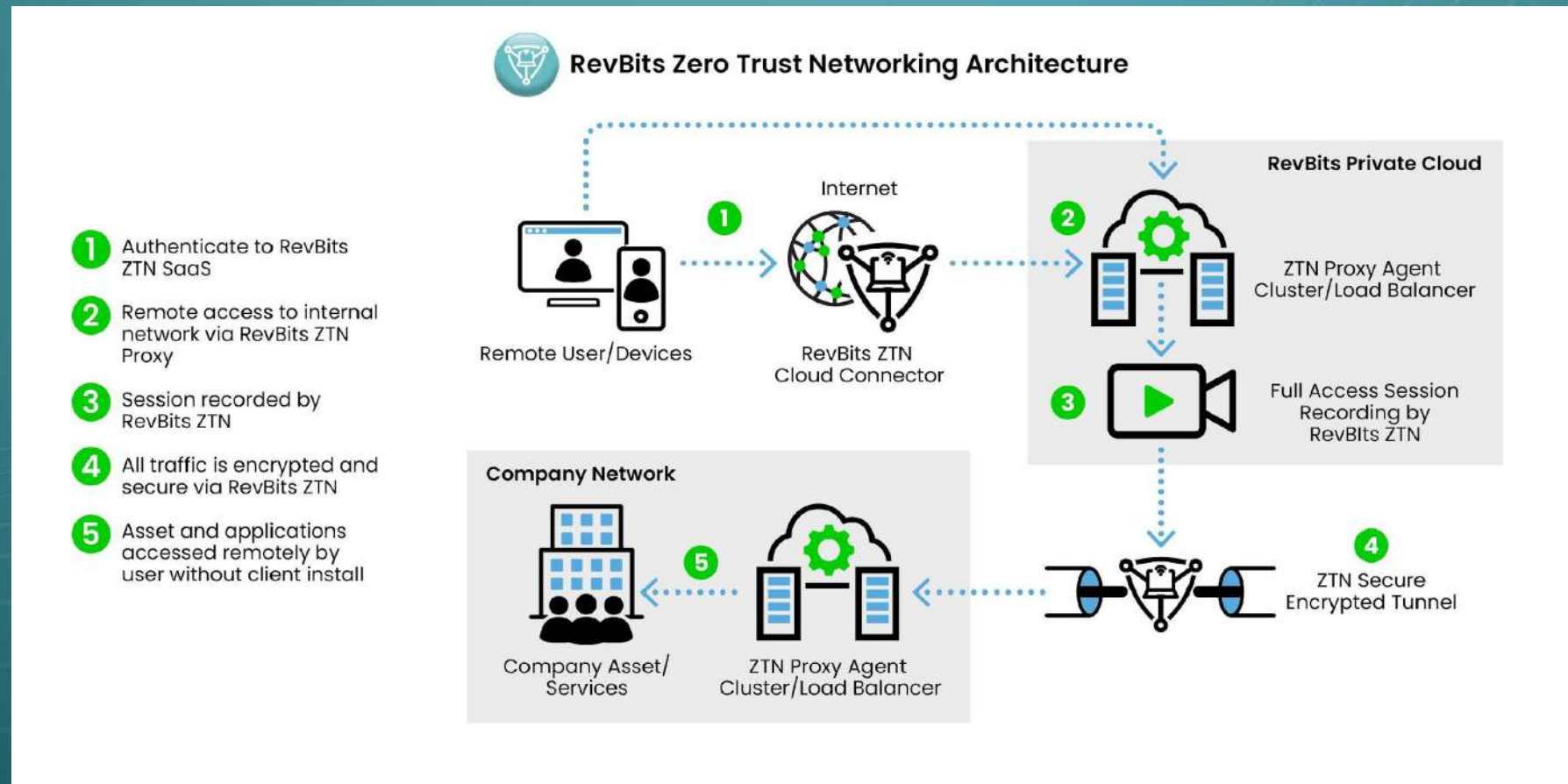
Acceso remoto y control 24 horas al día desde cualquier ubicación alrededor del mundo





Zero Trust Network de RevBits

Zero Trust para seguridad más allá de una VPN



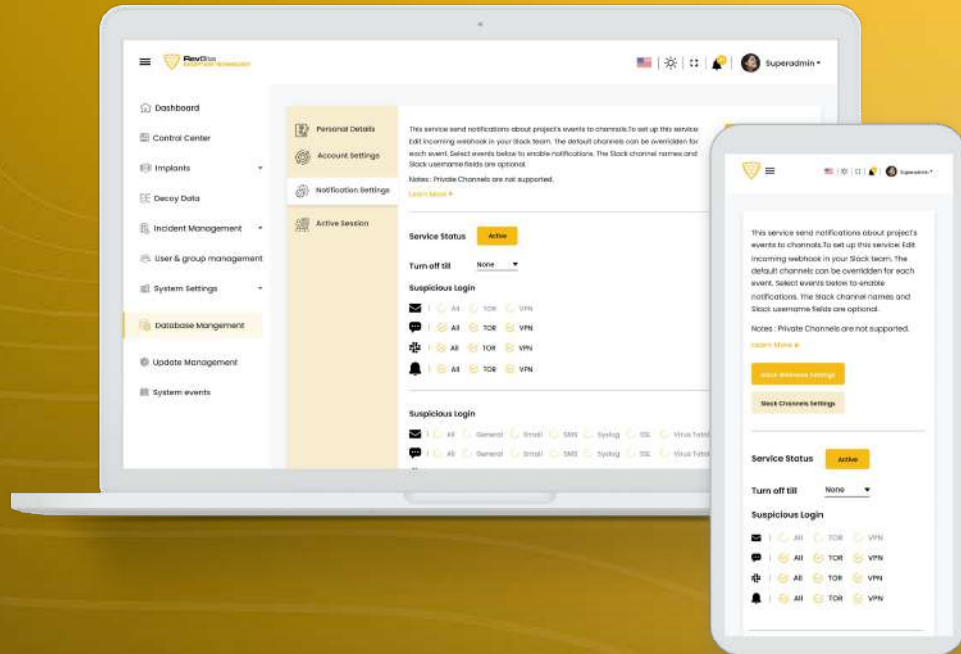
Zero Trust Network de RevBits se despliega como una solución SaaS únicamente



Tecnología de Engaño de RevBits

Engaño para detección de trasgresión temprana

- Honeyots basados en servidores reales
- Credenciales de señuelo desplegables
- Bajo consumo de recursos
- Completa integración con SIEM



Engaño para detener la amenaza del atacante interno

- Capture los intentos del atacante interno para acceder los datos valiosos
- Cargue datos falsos para crear un ambiente real
- Los Honeypots no se emulan o simulan, son servidores reales
- El contacto con un Honeypot indica una posible ruptura
- Los Honeydrops indican la ubicación de la posible ruptura
- Aleje las amenazas de los activos y servidores valiosos



Tecnología de Engaño de RevBits

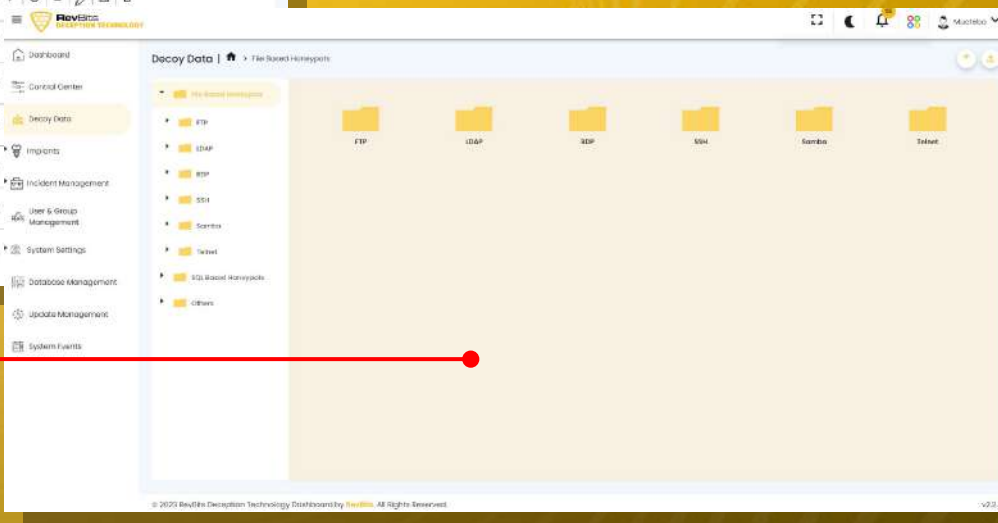
Honeypots basados en servidores reales para engaño efectivo



Hostname	IP	Port	Status	Actions
beeidert-controller	10.120.0.5	-	Disconnected	✓ 🔄 🗑️ 🛠️ 📄 📊
ip-192-31-46-236	18.190.81.181	-	Disconnected	✓ 🔄 🗑️ 🛠️ 📄 📊
devmher	172.16.200.47	-	Disconnected	✓ 🔄 🗑️ 🛠️ 📄 📊
mustafa-01	31.223.43.213	-	Disconnected	✓ 🔄 🗑️ 🛠️ 📄 📊
RevBitsDemo	172.16.200.47	-	Disconnected	✓ 🔄 🗑️ 🛠️ 📄 📊
Samba Server	192.168.0.193	445	Stopped	+ ▶ 🔄 🗑️ 🛠️ 📄 📊
Elasticsearch	192.168.0.200	9200	Stopped	+ ▶ 🔄 🗑️ 🛠️ 📄 📊
Apache Tomcat	192.168.0.168	8080, 8443	Stopped	+ ▶ 🔄 🗑️ 🛠️ 📄 📊
FTP Server	192.168.0.177	21	Stopped	+ ▶ 🔄 🗑️ 🛠️ 📄 📊
Cassandra	192.168.0.109	9042	Stopped	+ ▶ 🔄 🗑️ 🛠️ 📄 📊
Redis Server	192.168.0.125	6379	Stopped	+ ▶ 🔄 🗑️ 🛠️ 📄 📊
PostgreSQL Database Server	192.168.0.108	5432	Stopped	+ ▶ 🔄 🗑️ 🛠️ 📄 📊
MongoDB Database Server	192.168.0.111	27017	Stopped	+ ▶ 🔄 🗑️ 🛠️ 📄 📊
Generic HTTP Auth	192.168.0.147	80, 443	Stopped	+ ▶ 🔄 🗑️ 🛠️ 📄 📊

Despliegue Honeypots en servidores reales, no servidores emulados o simulados. Los servidores reales son menos detectables como Honeypots

Cargue datos reales en los servidores de Honeypots para mayor autenticidad





Tecnología de Engaño de RevBits

Detección de trasgresión temprana



© 2023 RevBits Deception Technology Dashboard by RevBits. All Rights Reserved.

Username	Access Key	Secret Key	Created On	Actions
test_1896227027	AKIA1E2QPCRVBC7MEFV	UNj8FcaE2LrZdfeNfPR20wkaSE1hUk7pdyu	4 months ago	
test_1844936497	AKIA1E2QPCRVFF7624J	89jKx0x02mVJbVYdcn7ML4Xrp0wZn6ca95Mw	Last year	

Proteja los activos en la nube desplegando Honeydrones en la infraestructura de nube

© 2023 RevBits Deception Technology Dashboard by RevBits. All Rights Reserved.

Incident Details

192.168.0.105

user password

Mekhak NDOruDi

CHAMPION x12

192.168.0.108

Honeydrones

Service	Port	Controller	Used Credentials	Days Running	Launch Date	Previous Incidents
Apache Tomcat	8080	revbitsdemo	user / password	421	02/02/22 01:54:31 PM	1

Events

Reported On	Description	Attacker IP	Honeydrones IP Address	Service	Username	Password	Implant	Assigned To
Last year	Command run: [...]	192.168.0.105	192.168.0.108	Apache Tomcat	Mekhak	NDOruDi	-	Unassigned
Last year	Command run: [...]	192.168.0.105	192.168.0.108	Apache Tomcat	[BVPY]	[BVPY]	-	Unassigned

v2.2.0

El reporte de incidentes está enriquecido con funcionalidades y apunta a los lugares de ruptura o la máquina del trasgresor interno a través de las credenciales de Honeydrones usadas



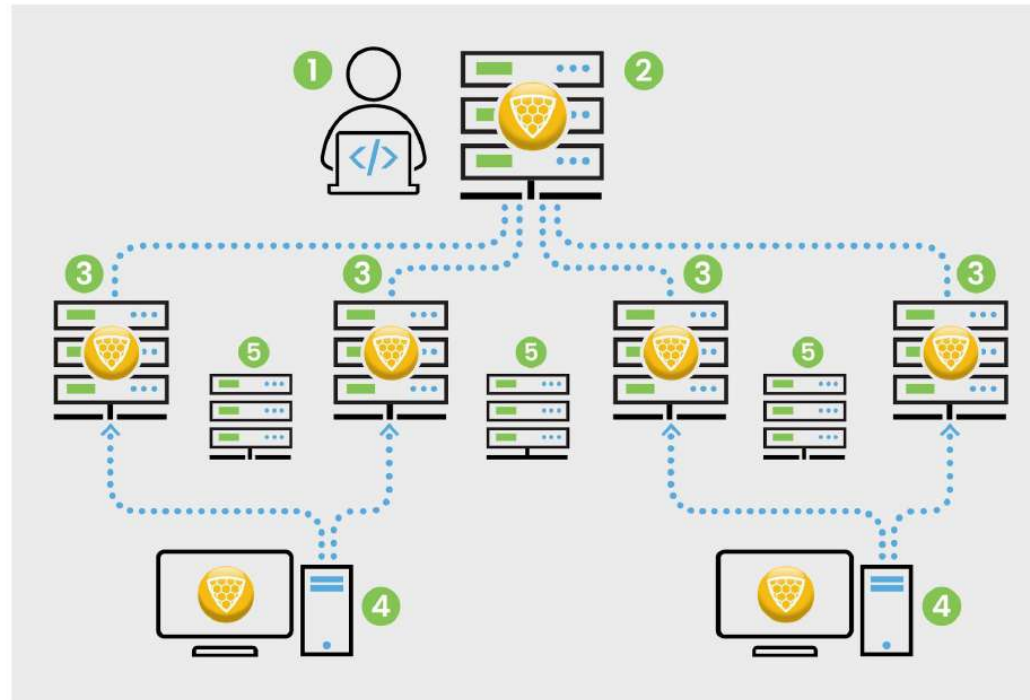
Tecnología de Engaño de RevBits

Engaño para detección de trasgresión temprana



RevBits Deception Technology Architecture

- 1 System administrator
- 2 Deploys RevBits Deception Technology honeypots through the RevBits Controller into the network.
- 3 Deployed Honeypots are secured from attacker escape through dual-layered virtualization. All honeypots are real server types - not emulations or simulations.
- 4 Through MSI, RevBits Honeydrop credentials are distributed onto network endpoints and servers so if harvested by an attacker, will point to the network deployed honeypots.
- 5 Critical servers are protected through an early breach detection capability.



La Tecnología de Engaño de RevBits se despliega como una solución On-premises, Nube Híbrida, o SaaS



¡Gracias!