RevBits®

CYBER BRIEF

Zero Trust Networking is Digital Transformation’s Response to Enterprise Security.

Ensuring the security of vital corporate resources and assets requires granular access control that is highly managed with authentication and authorization policies. The challenge lies in finding solutions that reliably protect against the overwhelming number of untrusted users and devices that threaten to exploit software vulnerabilities, device misconfigurations, and users lured into social engineering tactics.

Protecting today’s dynamically expanding perimeter of on-premises, multi-cloud, and diverse remote and mobile users requires zero trust networking with identity-based privileged access management. Zero trust network access (ZTNA) provides secure remote access that enables organizations to clearly define access control policies for their business-critical IT resources, applications, data, and services.

Zero trust provides granular control, with flexible authentication models, and can control which user population has access to certain applications. Zero trust is a journey that allows organizations to begin with small steps, identifying a business function or small user population, enable access, monitor their use, and grow the deployment from there.

A zero-trust cybersecurity model eliminates implicit trust and replaces it with explicit, real-time adaptive trust levels for just-in-time, just enough access to digital resources. The “explicit trust zone” is between the policy decision and enforcement point, and the applications, servers, systems, services, and data.

The challenge lies in finding solutions that reliably protect against the overwhelming number of untrusted users and devices.

Multiple forces are causing the adoption of zero trust

When the Covid-19 pandemic hit, companies were forced to quickly shift from a primarily business workplace to a mostly work from anywhere environment. VPN became the go-to technology to secure connectivity for remote workers and third-parties to corporate networks. However, many companies found that while VPN protected user connections outside the network, it also gave them complete access to all the resources and assets inside the corporate network. This approach violates the fundamental principles of a zero-trust model. It exposes resources and vulnerabilities to potential hackers, giving them free rein to move throughout the corporate network. In addition to the security challenges, VPNs can be difficult to manage and notoriously slow.

As a result of this workplace shift and VPN inadequacies, ZTNA adoption has accelerated. Protecting against malware exploits, complying with growing regulatory privacy requirements, and avoiding financial and other business losses due to cyber breaches, are just a few of the many reasons to adopt a zero-trust model.

RevBits adds ZTNA to its broad product portfolio

RevBits ZTN enables an explicit and risk appropriate zero trust security posture. Users are granted access based upon their identity and device. This includes attributes and context, like roles and responsibilities, time and date, location and more. Identity-related device data includes operating systems, browser versions, disk encryption and security software update status. RevBits combines policies for applications, users, devices, IP addresses, locations, workloads and risk, and utilizes identity data to define and enforce access control policies, allowing the appropriate level of access and trust.

RevBits ZTN ensures the identity, integrity and authorization of all users and devices. Access is provided only after verification is completed, regardless of location or network connection. No access is allowed before establishing a ZTN-brokered session between a user, including non-managed IoT devices, and an enterprise resource. When access is granted, users have least privileges to complete a task.

The most common use case for ZTNA is a partial or complete replacement of VPNs. A major flaw with VPNs is the enterprise-wide access to internal resources after users are authorized. Conversely, RevBits ZTN confines access to internal resources, limiting access to one resource at a time (e.g., server, application, service, etc.). This eliminates the opportunity for bad actors using stolen credentials to laterally move within the network.

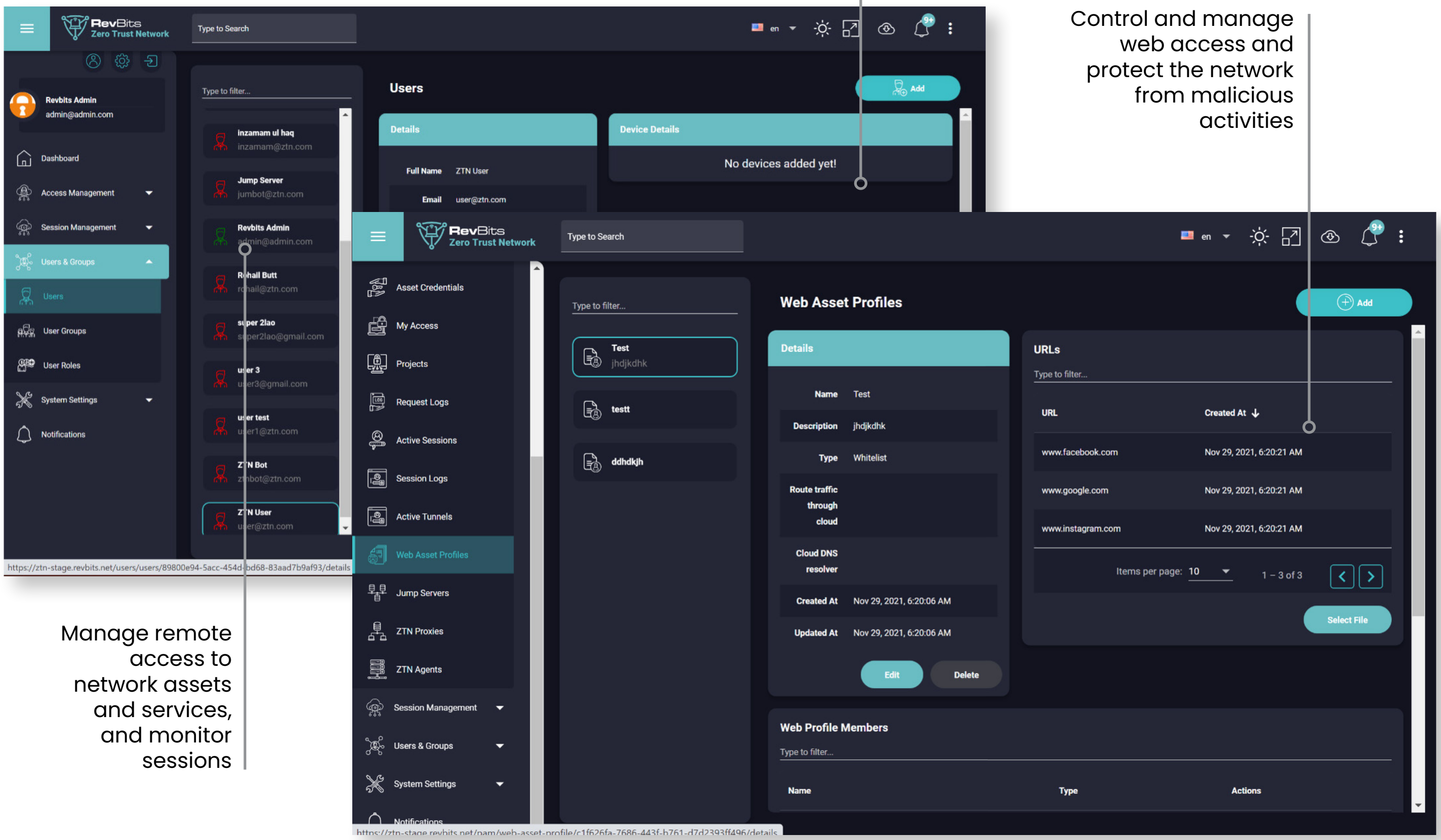
Authenticating access on the ever-expanding computing perimeter

RevBits ZTN's user-to-resource access approach is a completely different model than a network-centric methodology. RevBits encrypts, authenticates, and securely connects remote employees and third-parties over SSL/TSL, to internal resources and applications to which they have specific access, without access to other resources.

To ease management, admins can easily group resources (servers, databases, applications, services, etc.), users (internal and external) and projects (pen testing, development, etc.). Automating the onboarding of large numbers of users and endpoints can be easily accomplished on-premises with Active Directory and in the cloud with Azure AD.

Build user profiles to include known devices

Control and manage web access and protect the network from malicious activities



Revbits Admin
admin@admin.com

inzamam ul haq
inzamam@ztn.com
Jump Server
jumbot@ztn.com
Revbits Admin
admin@admin.com
Rohail Butt
rohail@ztn.com
super 2lao
super2lao@gmail.com
user 3
user3@gmail.com
user test
user1@ztn.com
ZTN Bot
ztnbot@ztn.com
ZTN User
user@ztn.com

Users

Details

Full Name ZTN User
Email user@ztn.com

Device Details

No devices added yet!

https://ztn-stage.revbits.net/users/users/89800e94-5acc-454d-bd68-83aad7b9af93/details

Web Asset Profiles

Test
jhdjkdhk
testt
ddhdkjh

Details

Name Test
Description jhdjkdhk
Type Whitelist
Route traffic through cloud
Cloud DNS resolver
Created At Nov 29, 2021, 6:20:06 AM
Updated At Nov 29, 2021, 6:20:06 AM

URLs

URL	Created At ↓
www.facebook.com	Nov 29, 2021, 6:20:21 AM
www.google.com	Nov 29, 2021, 6:20:21 AM
www.instagram.com	Nov 29, 2021, 6:20:21 AM

Items per page: 10 1 – 3 of 3

Web Profile Members

Name	Type	Actions

https://ztn-stage.revbits.net/pam/web-asset-profile/c1f626fa-7686-443f-b761-d7d2393ff496/details

Manage remote access to network assets and services, and monitor sessions

RevBits Zero Trust Network admin dashboard for creating user profiles to manage remote access.

RevBits ZTN protects corporate resources with identity-based authentication, multi-factor authentication (MFA), single sign-on (SSO), end-to-end encryption, session recording and more. Built upon the zero-trust principle of least privilege, when users have been authenticated and authorized, their access to an application or other resource is granted on a one-to-one basis. Granular, per-session access is granted based on verified user and risk profiles, with two-factor authentication enforcement.

Mapping users to digital resources, RevBits ZTN allows IT, security and risk teams to understand application nuances and data usage across the enterprise. This helps to govern and enforce a robust policy-based security posture, while eliminating user friction to ensure a positive experience logging in and accessing resources.

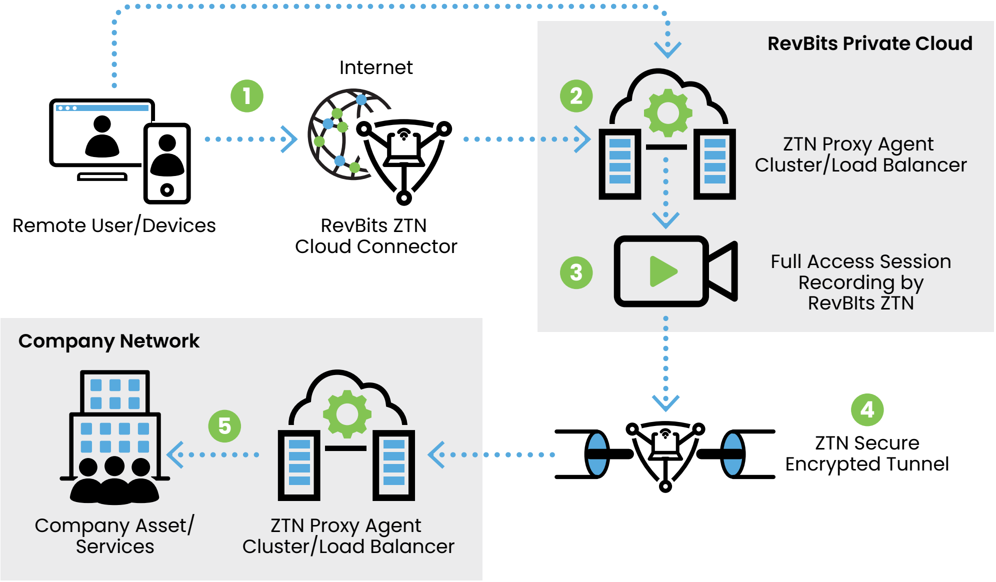
ZTNA uses strict business-based access policies built around privileged access limitations. RevBits ZTN includes integrated privileged access management (PAM), with native session recording. Remote access authentication and authorization protect resources inside the network, and encrypted tunnels secure connections for outside network traffic. Companies that already have another vendor's PAM solution will benefit from RevBits ZTN granular access protection for remote employees and third-parties with capabilities far beyond what a VPN delivers.

RevBits ZTN expands access management interests to the remote workforce and third-party providers. Integrated identity-based privileged access management provides granular control to limit resource access, restricting what users can do with a resource and locking-down access beyond that resource. Integrated identity and privileged access capabilities provide context around authentication. By leveraging identity data with context, RevBits ZTN automatically assesses risk and trust, and applies continuous adjustments that are explicit.

Users have secure connectivity and access to corporate applications and other IT resources without exposing the resource's IP addresses. All resources within the organization that are implemented within RevBits ZTN are protected from direct Internet access. Access is only granted to authenticated users, and network risks are reduced by restricting access and eliminating lateral movement to devices that may have been infected by a virus.

Providing a strong unified cybersecurity posture

RevBits has a broad range of integrated cybersecurity products that are best-in-class individually, and more importantly, provide superior protection by seamlessly working together within the RevBits Cyber Intelligence Platform (CIP).



1. Authenticate to RevBits ZTN SaaS
2. Remote access to internal network via RevBits ZTN Proxy
3. Session recorded by RevBits ZTN
4. All traffic is encrypted and secure via RevBits ZTN
5. Asset and applications accessed remotely by user without client install

Network access is now secure for remote users and third-party access.

RevBits CIP is an XDR (extended detection and response) platform that collects and automatically correlates data across its natively implemented multiple security layers. This enables faster threat detection and improves investigation and response times. With one glance at the RevBits integrated dashboard, a CISO can immediately see the status of all major components within their cyber defense.

ZTNA represents a single component of what is needed for a robust security posture and complete remote access capabilities. For full cyber protection, RevBits CIP has a broad set of detection and response, zero trust, privileged access management, and deception capabilities for on-premises, cloud, and hybrid environments. RevBits addresses operational and business challenges associated with cybersecurity incidents within traditional and modern networks, wherever users are located.

RevBits CIP enables administrators to gain an unparalleled view into all sessions. Conducting a forensics investigation and assembling a timeline has never been so easy, intuitive, and seamless. RevBits ZTN can be deployed as a stand-alone security product, or as part of CIP that includes other security products:

- Email Security
- Privileged Access Management (PAM)
- Zero Trust Networking (ZTN)
- XDR/Endpoint Security
- Deception Technology

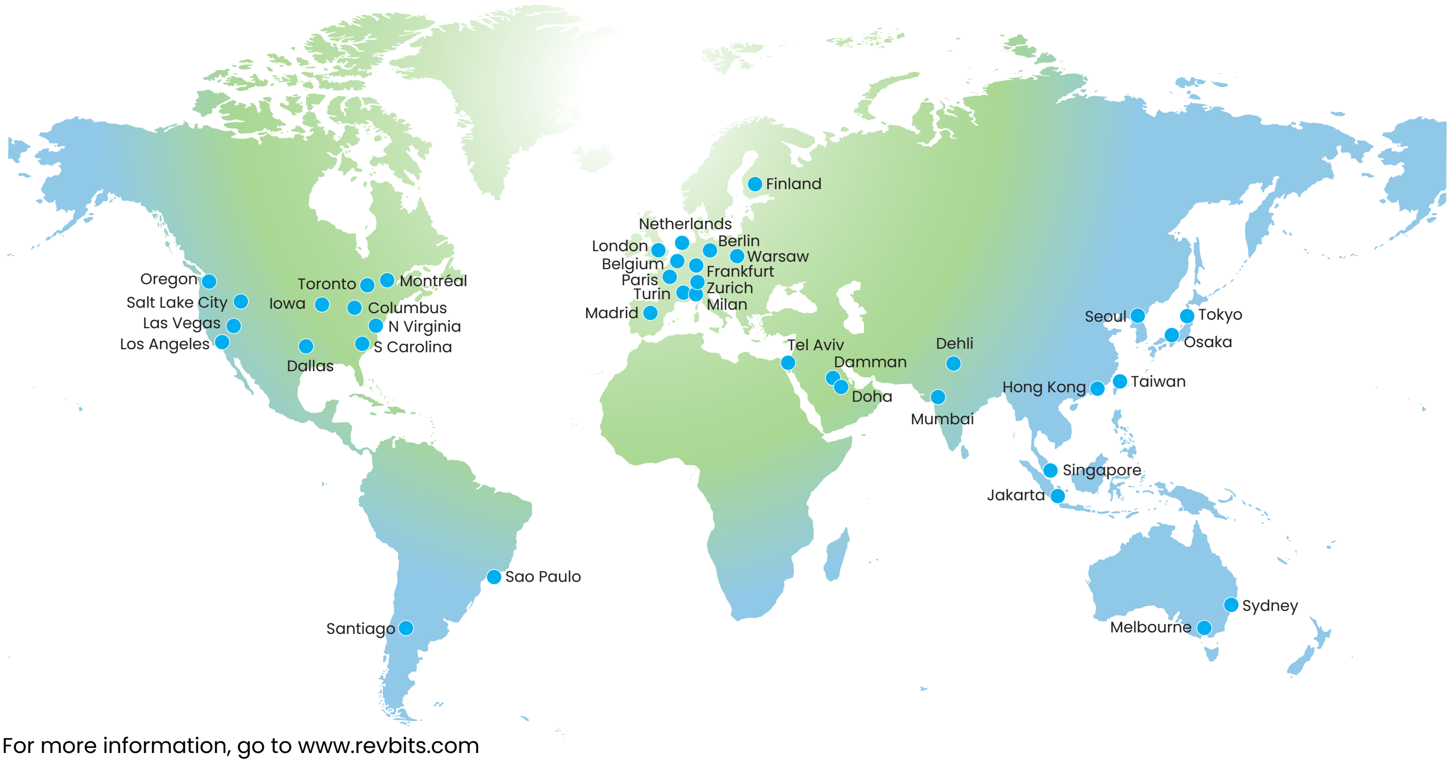
ZTNA use case scenarios

Securing the remote workforce

With today's expanded work from anywhere environment, the world of IT has been turned upside down. For many decades, IT has been responsible for securing a corporate perimeter consisting of one to a handful of corporate offices where, for larger businesses, thousands of employees came to work.

Due to the pandemic, practically overnight the corporate perimeter exploded into thousands of home offices and mobile employees accessing applications, servers, databases, and other critical infrastructure within corporate data centers and an ever-expanding number of cloud services. Complicating matters, employees have been using company-owned computers, and employee-owned computers, smartphones, and tablets. This digital menagerie has created unprecedented complexity, diversity, and risk.

The ability to scale with an agile and highly secure model for granting access requires a zero-trust security model. As mentioned earlier, when the pandemic hit, organizations immediately deployed VPNs to secure remote employee access to their digital resources. But they've since realized VPN is a proverbial Band-aid to a gaping security gap that requires a more reliable, scalable, adaptable, and explicit trust-based solution.



For more information, go to www.revbits.com

In the same manner that cloud, mobility, and the need for more agile connectivity have caused organizations to move from legacy MPLS networks to the Internet via SD-WAN, ZTNA has already had a dramatic impact on organizations transitioning away from VPN.

RevBits ZTN secures work from anywhere employees with any type of app or device, including mobile, SaaS, client/server, laptop, terminal, and custom legacy. All app hosting environments, including on-premises, cloud, and hybrid are supported. Global points of presence with elastic auto-scaling support multi-site organizations with 24 locations around the world. With natively integrated PAM, admins can control every aspect of a remote access session, including monitoring, reviewing, recording, and killing any session with one click.

RevBits ZTN is agentless, and therefore, provides remote employees and devices with tightly secured access to corporate resources within minutes. RevBits real-time adaptive controls are managed via a web dashboard or portal that allows admins to quickly identify a specified resource and apply the appropriate policy that determines the user authentication and authorization. Users are given the least privileged access to the resource they need. That's all there is to it.

Securing third-party partner, supplier, and vendor access

Companies often have on-site visitors and/or remote contracted service providers that require access to their applications, servers, databases, and data. For example, onsite service contractors conducting maintenance on HVAC or lighting systems may need network connectivity and access to IT resources to perform their work.

Organizations must provide third-parties with connectivity and access to their resources, but without sacrificing security, visibility or control. Third-party access creates undue risk, and therefore, by default, they should not be trusted. RevBits ZTN agentless solution accomplishes this through zero-touch proxy servers that support any client type.

Organizations may also have gathering areas and conference rooms where visitors interact with employees. RevBits ZTN facilitates this by allowing visiting users to access specified resources while limiting what they can do on the resource and concealing the resource IP address. Visitors will not even be able to discover enterprise assets via network scans if they attempt to identify active devices.

Most of the problems associated with third-party access are giving users over-privileged access. In doing so, they are expanding their threat exposure. RevBits ZTN reduces third-party risk by never permitting broad access to network resources, providing only authenticated and authorized access to permitted resources or applications – one at a time. RevBits protects corporate IT resources by ensuring partners, suppliers, and vendors accessing the network have the appropriate verification, account privileges, and uninfected devices.

ZTNA recommendations for IT, security, and risk management leaders

- Beginning deployment, apply specific policies to user groups to control access to resources.
- Document application resource usage prior to starting a ZTNA implementation, then map users to resources within RevBits ZTN.
- Clean up access privileges by blocking employee and third-party access for those no longer associated with the organization.
- Managing resource access policies is an ongoing and iterative process, thus as business requirements change, resource access policies should too.
- Inventory all VPN instances that allow network access and replace them over time.
- Include unmanaged device access with the ZTNA architecture.
- Define policies to combine user attributes to enforce who has access to what.
- Develop a strategy to address heterogeneous workloads spanning on-premises, hybrid, virtual, and container environments.

Begin with a pilot project - Initiating a pilot project with RevBits ZTN will help with planning rollouts of WFH employee and third-party access. Testing resources with RevBits ZTN will help you learn access patterns by users and their roles and grow and apply policies as needed.

Best practices to enable a smooth and efficient ZTNA implementation - Before deploying RevBits ZTN, identify potential use cases. For example, grouping users and resources, or granting access to third-parties. Apply specific policies to appropriate user groups.

Document resource usage before implementing ZTNA - Documenting resource usage before implementing ZTNA will provide a better understanding of the relationships between users and resources. This can be accomplished with application discovery tools. Interviewing business leaders within different departments will help determine which resources their teams use, and which require third-party access. This also sets a standard for each team and helps accelerate ZTNA deployment.

Identify, isolate, and monitor remote network connections and access to corporate resources in real-time. Learn more about RevBits ZTN. Watch an informative RevBits ZTN video.

Keep Your Enterprise Protected. Get a Demo or Free Evaluation.
To learn more, visit www.revbits.com