Ivanti Neurons for Zero Trust Access

Zero Trust, Zero Hassle: Experience Effortless Everywhere Work

Ivanti Neurons for Zero Trust Access (ZTA) empowers organizations to embrace Everywhere Work in a borderless digital world. ZTA delivers secure, application-focused access with continuous authentication and adaptive controls.

By prioritizing identity and context, ZTA minimizes the attack surface, prevents lateral movement threats and enhances visibility across distributed application ecosystems, whether on-premises or in private or public clouds. Automated threat detection, granular policy enforcement and flexible gateway deployment options make ZTA the go-to solution for organizations seeking to confidently adopt zero trust principles and safeguard their users, applications and data.

Zero Trust Access Everywhere

In today's borderless digital environments, organizations face complex security challenges driven by the rise of remote work and the increasing adoption of cloud-based applications and services. The employee work-from-home "revolution" has expanded the traditional network perimeter, creating a distributed and dynamic workforce that demands access to corporate resources from virtually anywhere.

While this transformation has brought increased flexibility and efficiency, it has also introduced new vulnerabilities and points of exposure. Organizations must contend with a rapidly evolving threat landscape that includes advanced and sophisticated attacks, including those leveraging artificial intelligence. As a result, traditional security approaches are no longer adequate, and enterprises must reevaluate how they secure access to their applications and data.

Enter Ivanti Neurons for Zero Trust Access—a comprehensive solution designed to address modern security challenges and empower organizations to confidently embrace the principles of zero trust network access. With a focus on continuous verification, granular policy enforcement and real-time risk assessment, Ivanti Neurons for ZTA provides the foundation for a robust and resilient security and access management strategy.

Secure access for everywhere work

Empower your organization to uphold zero trust principles and support an Everywhere Work model. Continuously authenticate users, applications, devices and context, and protect access to corporate applications across diverse environments, including on-premises, across data centers, and public and private clouds.

Enhanced security with application-focused access

Strengthen your security posture and protect against lateral movement attacks with Zero Trust Network Access (ZTNA). ZTNA allows you to grant access based on least privilege principles, ensuring that only users needing access to applications or content are connected. Moreover, with ZTNA, you can continuously verify user identities and device security posture, all while providing application-focused access for enhanced security.

Adaptable application policy and control

Gain fine-grained control over application access based on user identity, device, location and more. Adapt access policies to align with your organization's business needs, whether managing contractor access or enforcing location-based authentication.

Proactive threat detection with user and entity behavior analytics (UEBA)

Leverage UEBA and advanced risk analytics to identify anomalies, assess risk and respond to potential threats in real time. Utilize Vulnerability Risk Rating (VRR) scores from Ivanti Neurons for VULN KB to evaluate endpoint applications, providing visibility into vulnerabilities and enabling efficient risk triage by admins.

Streamlined access management

Facilitate business operations while maintaining strong security by quickly granting users or groups access to the applications they need. Simplify access management during mergers and acquisitions and enable seamless integration of new business units.

Integration with cloud access security brokers (CASB) and secure web gateways (SWG)

Enhance your secure access strategy by integrating ZTA with CASB and SWG capabilities. Ensure secure access to SaaS and internet applications with features such as data loss prevention (DLP), enterprise digital rights management (EDRM), optical character recognition (OCR) and malware detection.

How It Works

Cloud-Hosted Authentication and Authorization

ZTA uses a cloud-hosted controller to authenticate and authorize user identity and device security posture for compliance before establishing an application session.

Centralized Policy Engine and UEBA

ZTA governs each access request and session through a centrally deployed policy engine, augmented with User and Entity Behavior Analytics (UEBA). Attributes for each session are monitored and assessed, and proprietary risk scores identify non-compliant, malicious, and anomalous activity for expedited threat mitigation.

Flexible Gateway Deployment

ZTA gateways are deployed where you choose, either on-premises or in your public or private cloud environments. Proximity to cloud applications optimizes user experience, reduces latency, and enables scalable hybrid IT deployment.

Direct Secure Per-Application Tunnels

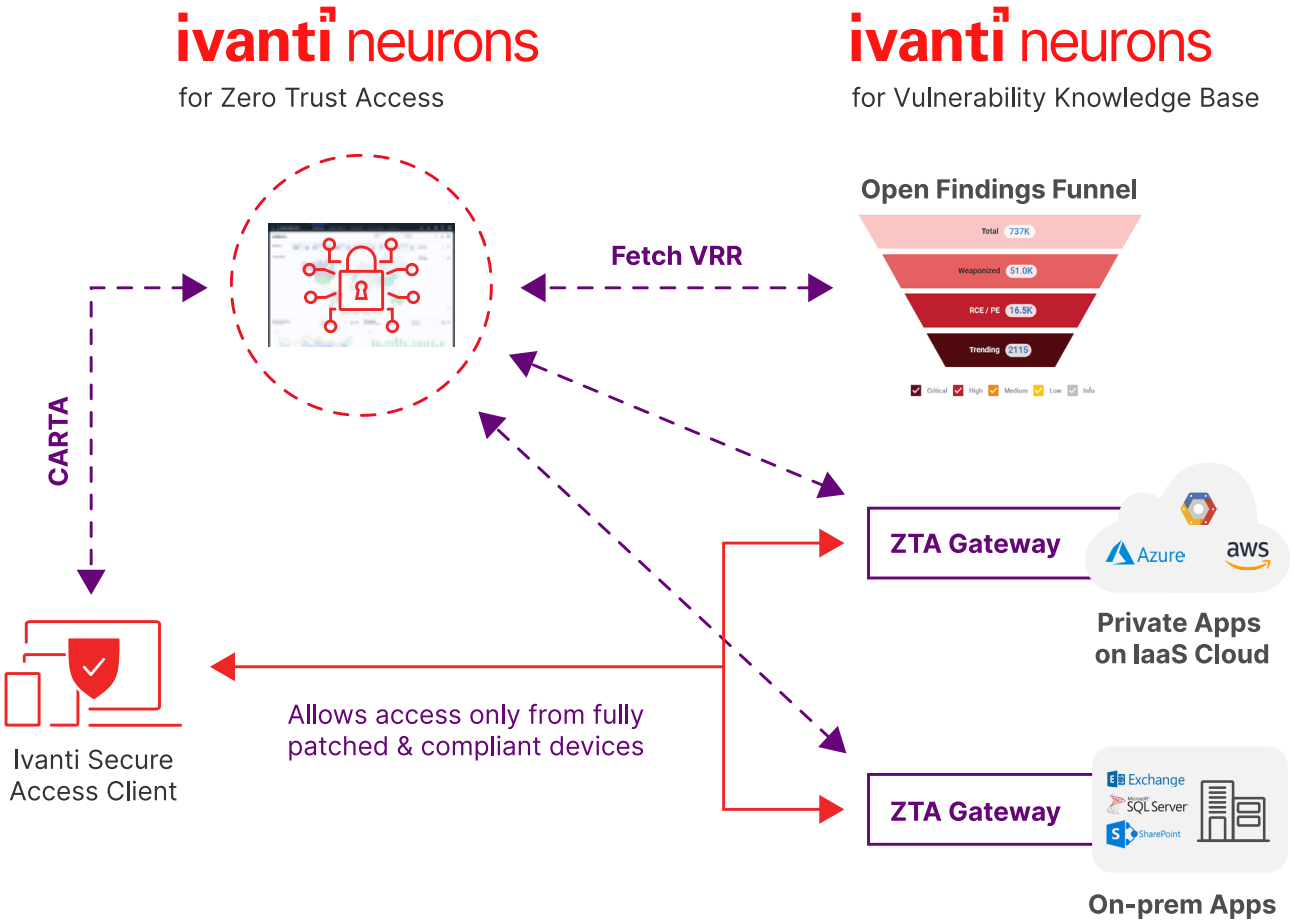
The ZTA controller verifies application access policies and instructs the Ivanti Unified Client to create a direct secure per-application mTLS tunnel between the device and the ZTA gateway. Data interaction with the ZTA controller is eliminated.

Intelligent Traffic Steering

The Ivanti Unified Client automatically steers traffic to the most optimal gateway for connecting the application tunnel, removing the need for costly backhauling or hair-pinning of traffic.

Real-Time Risk Assessment

ZTA continuously assesses risk levels based on user behavior, device security posture, and Vulnerability Risk Rating (VRR) scores, enabling proactive threat mitigation. Seamless Integration with Existing VPN: ZTA integrates with existing VPN solutions, enabling secure access to new apps and supporting business activities while maintaining robust security.



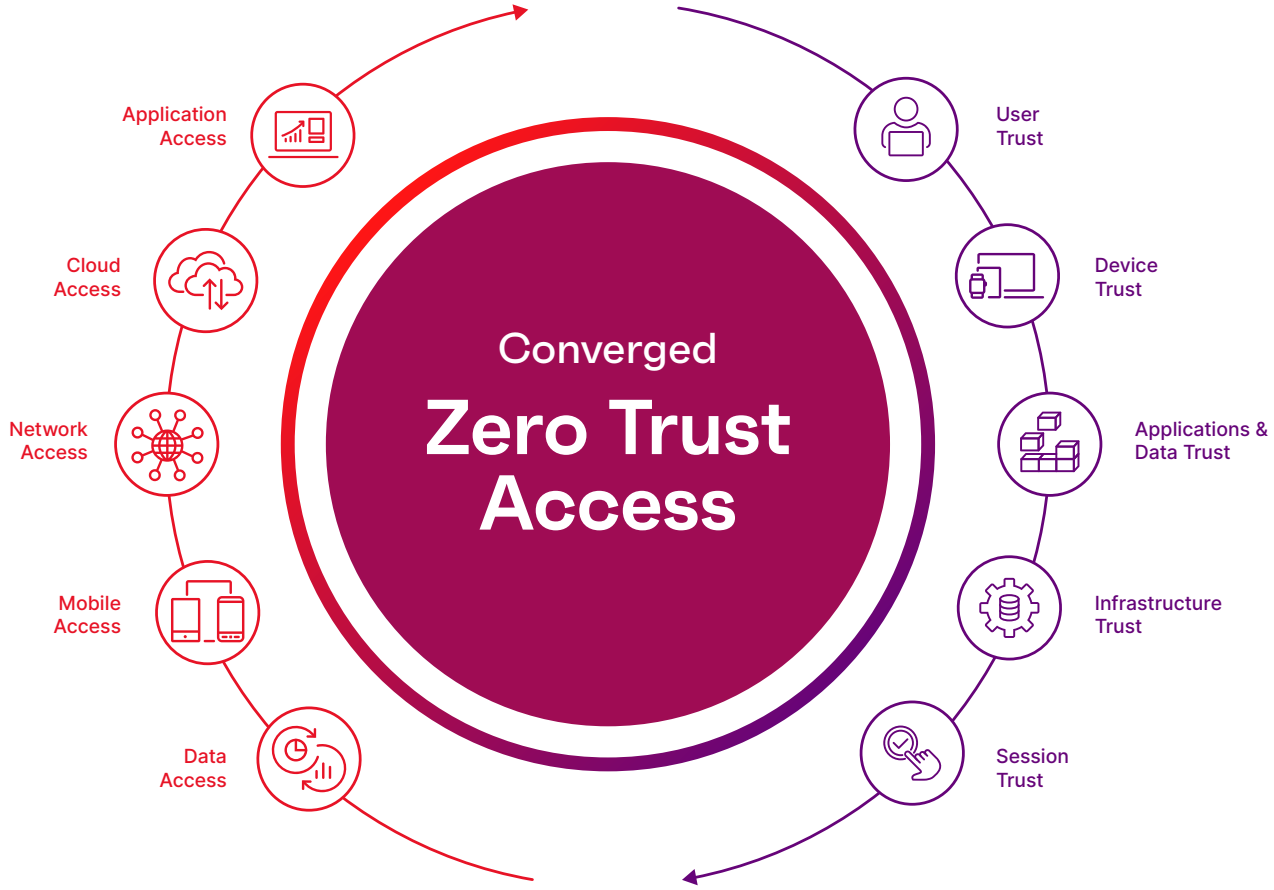
Let's explore the key use cases that Ivanti Neurons for Zero Trust Access addresses:

Implementing a Zero Trust Access Model

As organizations navigate an increasingly borderless network landscape and the shift towards Everywhere Work, implementing a zero-trust access model is essential for enhancing security. Ivanti Neurons for Zero Trust Access offers a robust solution that adopts an application-centric approach, focusing on securing access to applications rather than the broader network. With the principle of least privilege in place, users are granted access only to specific, authorized applications. Continuous verification of user identities and assessment of device security posture reinforce security measures. The solution also offers a unified client that seamlessly supports both Ivanti Connect Secure VPN and Ivanti Neurons for Zero Trust Access, allowing your organization to proactively protect against lateral movement attacks with granular access controls.

Controlling and Managing Application Access

Control and management of application access play a vital role in safeguarding your organization's data and resources. Ivanti Neurons for Zero Trust Access empowers you to implement fine-grained policies that control access based on user identity, device, and location. The solution is adaptable to your unique business needs, making it easy to manage contractor access, enforce location-based authentication, and streamline access management. Efficiently grant access to users or groups as needed and facilitate business operations, all while maintaining robust security standards.



Leveraging Analytics for Proactive Security

Proactive security is key to staying ahead of emerging threats in today's dynamic cybersecurity landscape. Ivanti Neurons for Zero Trust Access enables your organization to leverage advanced analytics for proactive security measures. Real-time anomaly detection and User and Entity Behavior Analytics (UEBA) help identify unusual behavior and potential risks. The solution utilizes Vulnerability Risk Rating (VRR) insights to assess endpoint vulnerabilities, giving you the visibility you need for effective risk triage. Automated actions respond to policy violations and risk scoring, including remediation measures, ensuring that your organization is equipped to respond swiftly to potential threats.

With Ivanti Neurons for Zero Trust Access, you gain a powerful solution that addresses critical security challenges and enables your organization to confidently implement a Zero Trust Access model, manage and control application access, and leverage powerful analytics for proactive security. Whether you're dealing with remote access, securing a hybrid workforce, or enhancing security visibility, our solution is here to support you every step of the way.

Feature	Advantage
End-to-end access policy	Define end-to-end access policies for every resource, eliminating the distinction between remote and on-premises users.
“Invisible” gateways	Go dark with ZTA, rendering application gateways undetectable to attackers while seamlessly granting access to authenticated and authorized users.
Single-pane-of-glass visibility	Gain holistic visibility and compliance reporting of users, devices, applications, context and infrastructure across the enterprise.
Adaptive SSO	Integrate through SAML 2.0 to provide SSO to supported SaaS and third-party applications.
Intelligent Traffic Steering	Provide the best possible user experience using automated optimal gateway selection to ensure your users’ app traffic is always routed to the fastest gateway.
Endpoint compliance	Authenticate users and devices against granular policies before granting access, minimizing the risk of malware and other threats.
Application Discovery	Get a comprehensive view of application usage and seamlessly create ZTA policies to manage those applications without disrupting the end user.
User behavior analytics	Leverage analytical data to reduce security risks, detect anomalies, optimize user experience and adapt to mobile workforces.
Data privacy and sovereignty	Achieve data sovereignty as user app traffic flows directly through customer-deployed gateways, segregated from the ZTA control plane, ensuring exclusive control over data flow.
DLP and AV monitoring	Prevent data loss and exfiltration by monitoring data communications with external and unmanaged resources, safeguarding end-user devices from compromise.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com