Zero Trust Network Access for the Everywhere Workplace

Ivanti Neurons for Zero Trust Access (ZTA) has partnered with **Lookout** to provide zero trust secure access and visibility across highly distributed application ecosystems on-premises, private-or-public clouds, or on the open internet while protecting your users, their data and their devices from accidental and malicious data exfiltration and threats such as viruses, malware and ransomware.

How do you proactively protect your users and their data?

In the Everywhere Workplace, companies are relying more and more on cloud applications to connect and empower their users. These cloud applications bring convenient access from any device, allowing users to be productive from anywhere. With this unprecedented access comes new challenges that all businesses must face:

- How do you control access to company applications both on-premises and in the cloud?
- How are users interacting with your sensitive company data, where is it going and how can you identify it?
- Are user devices and personal apps putting the company at risk?

Visibility and control in the Everywhere Workplace

As your organization continues to rely more and more heavily on cloud applications, you need to ensure your users, their devices, and the applications they use are safe, secure, and productive while protecting sensitive data from falling into the wrong hands. You need to limit access to corporate applications to only those who need it while also providing a seamless experience for the end user. You also need to safeguard your sensitive digital assets and stay compliant with regulations, no matter where your data goes or who is using it. You need to have the control, visibility, and peace of mind that your users, their devices, and their data are secure.

Secure access and keep sensitive data safe

With ZTA get on-demand protected access to corporate applications on-premises, and on private and public clouds from any device, anywhere. Automatically authenticate and authorize users, devices, and application connections according to flexible, granular policies, ensuring users can access the applications they need, when they need them. Prevent lateral-movement threats with per-app micro-segmentation control and identify risky user behavior before it becomes a problem with User and Entity Behavioral Analytics (UEBA). Assess device risk prior to giving access to corporate applications and quarantine unpatched devices running risky applications through Ivanti Neurons for Risk Based Vulnerability Management Vulnerability Risk Ratings. Enforce client security and health posture with automatic remediation with the Ivanti Secure Access Client.

Through Ivanti's partnership with Lookout, ZTA adds data loss prevention (DLP), enterprise digital rights management (E-DRM), optical character recognition (OCR), exact data matching (EDM), malware detection, incident response and data classification for internet and SaaS-based applications, protecting your sensitive data and digital assets from accidental or malicious leakage.

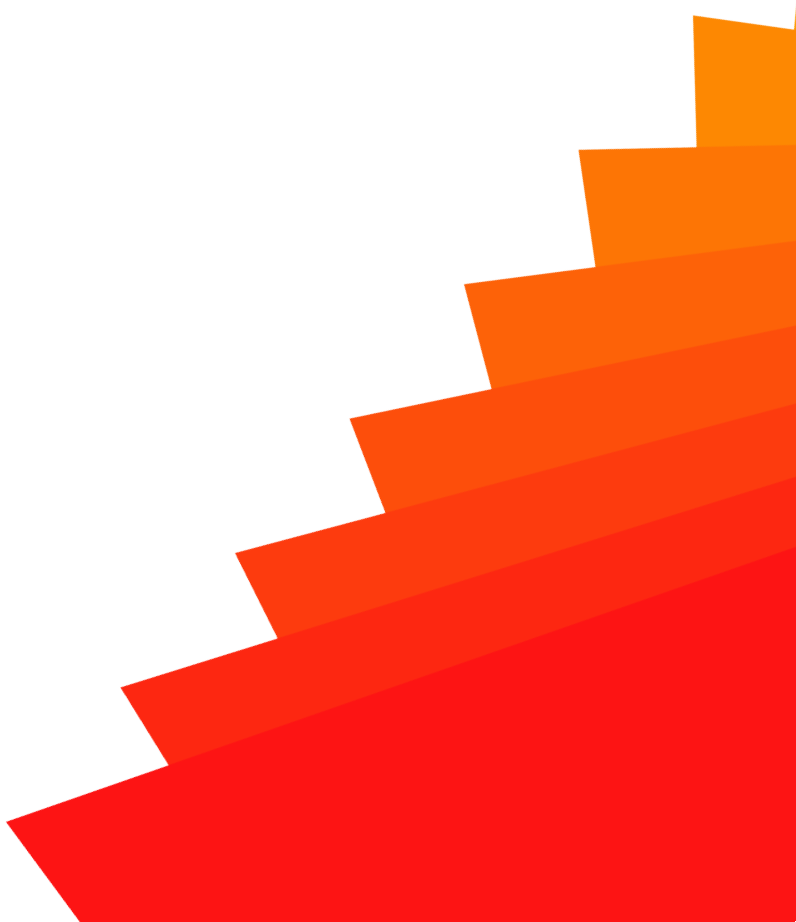
How it works

Neurons for Zero Trust Access (ZTA) is a SaaS-delivered zero trust network access solution designed to work with your VPN solution or with cloud-first organizations.

ZTA authenticates and authorizes user identity and device security posture for compliance with the cloud-hosted ZTA Controller before establishing an application session. ZTA governs each access request and session via a centrally deployed and managed policy engine and augments these policies with built-in User and Entity Behavior Analytics (UEBA), where attributes for every session are monitored and assessed. Proprietary risk scores identify non-compliant, malicious, and anomalous activity—enabling expedited threat mitigation actions.

ZTA gateways are flexibly deployed where you want, either on-premises or in your public or private cloud environments. This proximity optimizes user experience, reduces latency, and enables hybrid IT deployment at scale. The ZTA controller verifies application access policies, then instructs the Ivanti Unified client to create a direct secure per-application mTLS tunnel between the device and the ZTA gateway, eliminating any data interaction with the ZTA controller. The Ivanti Unified Client automatically steers the traffic to the most optimal gateway for connecting the application tunnel, no costly backhauling or hair-pinning of traffic required.

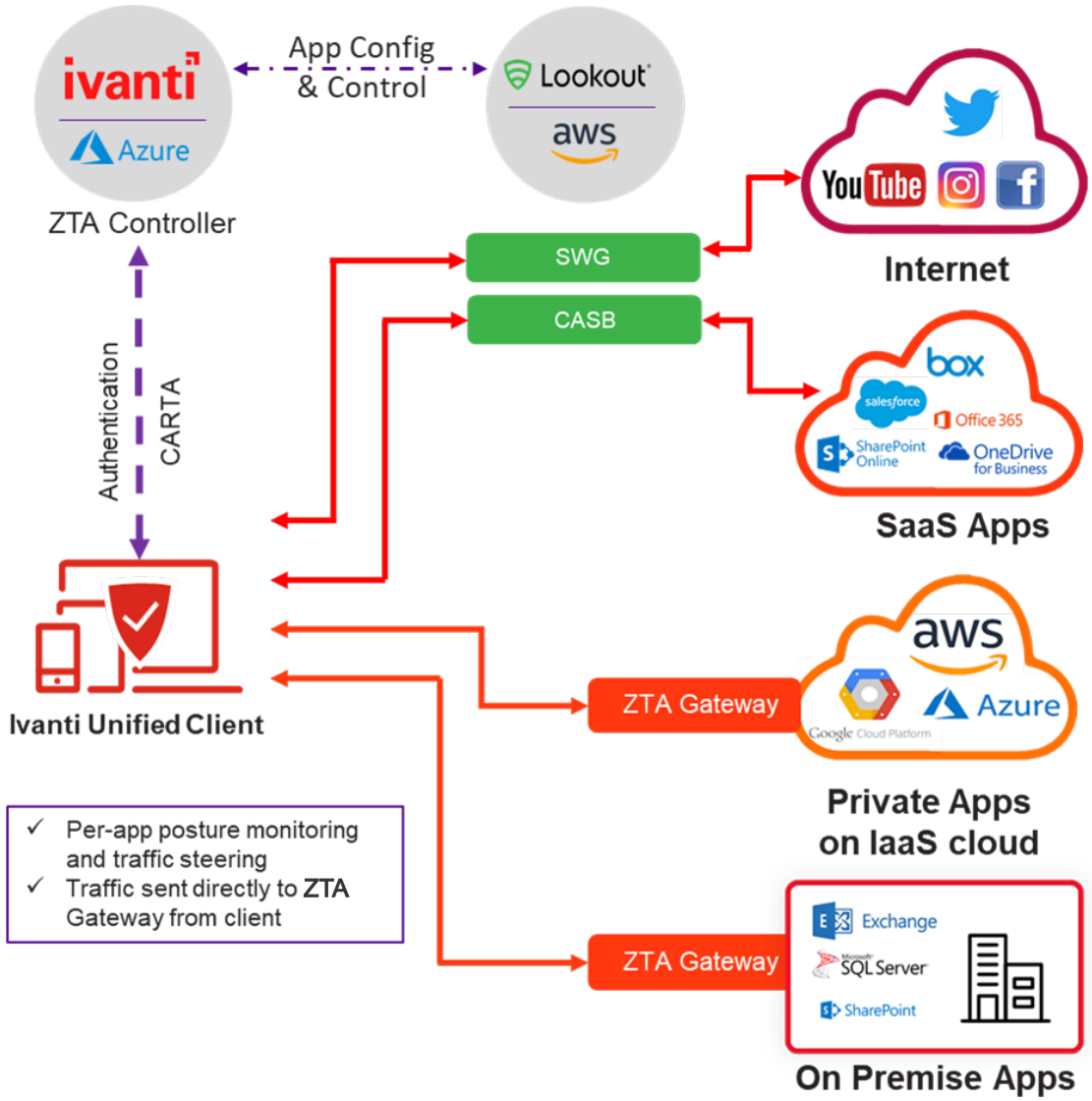
Through our partnership with Lookout, ZTA lets you identify, classify, and protect your sensitive data and documents across internet and SaaS-based cloud services, users, and devices, in real-time. Through centralized data loss prevention (DLP) policies, you can detect, classify, and protect sensitive data across any cloud deployment, email, and applications consistently, while preserving the integrity of your regulatory data such as Personally Identifiable Information (PII), Protected health Information (PHI), and information classified as Payment Card Industry (PCI-DSS) data.



ivanti

With enterprise digital rights management (E-DRM) you can secure sensitive files by automatically encrypting them as they are downloaded, stored, and shared, ensuring only those users with proper access rights can access sensitive files, securely. Protect your users and stop viruses, malware and ransomware attacks with inbound and outbound malware detection and automated quarantine and identify anomalous behavior and remediate potential threats through behavioral analytics.

Neurons for Zero Trust Access provides deployment flexibility and cohesive policy management for application deployments anywhere while also offering comprehensive secure access capabilities to those organizations with pure multi-cloud environments. Lookout provides unprecedented visibility into users' cloud and internet applications, protecting their sensitive data from leakage while protecting users and their devices from malicious threats.



Feature	Description
End-to-End Access Policy	Define end-to-end access policies for every resource, eliminating the distinction between remote and on-premises users.
Separation of Control and Data Plane	User and application traffic are sent directly between the user and designated gateway, reducing the risk of data loss, and improving user experience.
On-premises and Hybrid-Cloud	Gateways can be deployed in public cloud, private cloud, or customer data centers.
Adaptive Single Sign-On (SSO)	Integrate through SAML 2.0 to provide SSO to supported SaaS and 3rd party applications.
Endpoint Compliance	User and devices authenticated against granular policies before access is granted, reducing possibility of malware and other threats.
User Entity Behavioral Analytics (UEBA)	Leverage analytical data to reduce security risks, detect anomalies, optimize user experience, and adapt to mobile workforces.
Optimal Gateway Selection	Create gateway groups for access based on user location and gateway priority to deliver an optimal application access experience for end users.
Persistent Tunnel for Server to Client Communications	Option to create persistent tunnels between endpoint and ZTA gateway for server to client use-cases such as VoIP and application push updates.
Lockdown Mode	Disallows internet and network connectivity when users are not connected to ZTA and supports exceptions based on ports, protocols, processes and more.
Integrated Lookout CASB and SWG	Identify, analyze, and secure Software-as-a-Service (SaaS) applications with Lookout Cloud Security Access Broker and extend protection to internet applications with Lookout Secure Web Gateway.
Advanced Data Leakage Protection (DLP)	Detect and stop sensitive data leaks in real-time, enforcing data protection policies and ensuring compliance with privacy regulations.
Enterprise Digital Rights Management (E-DRM)	Classify sensitive company documents and enforce in-motion and at-rest encryption to ensure only authorized users can access sensitive files.
Optical Character Recognition (OCR) and Exact Data Matching (EDM)	Identify and protect sensitive documents and confidential key phrases in real-time, preventing accidental or malicious data exfiltration.
Malware Detection, Behavioral Analytics, and Incident Response	Scan and quarantine inbound and outbound SaaS and Internet application traffic for viruses, malware, and ransomware, identify risky behavioral patterns and automate incident response to stop attacks and protect your users and resources.

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