Ivanti Neurons für Zero Trust Access

Sicherer Zugang für den Everywhere Workplace

Ivanti Neurons for Zero Trust Access (nZTA) stellt eine sichere Verbindung zwischen dem Gerät und web-basierten Anwendungen vor Ort und in der Cloud her. Dies erhöht die Sicherheit, Produktivität sowie Compliance und verbessert gleichzeitig die Erfahrungen der Administratoren und Endanwender deutlich.

Umfassender Zero Trust Access

Erreichen Sie kontinuierliche Benutzer- und Geräte-Authentifizierung und einen stets geschützten Zugriff auf Unternehmensanwendungen vor Ort, im Rechenzentrum sowie in privaten und öffentlichen Clouds.

Automatisieren Sie Authentifizierung und Autorisierung von Benutzern, Geräten und Anwendungsverbindungen entsprechend flexibler, granularer Einschränkungen – dadurch wird eine adaptive Steuerung, Mikrosegmentierung und eine reduzierte Angriffsfläche gewährleistet.

Bessere Transparenz und Analytik

Greifen Sie auf Echtzeit-Stati und historische Trends zu und nutzen Sie die von nZTA gelernten Nutzungs- und Verhaltensinformationen – z. B. von wo aus sich ein Benutzer anmeldet, welche Geräte er normalerweise verwendet und auf welche Geräte er normalerweise zugreift – um Maßnahmen proaktiv zu ergreifen und Sicherheitsrisiken zu mindern.

Verbesserung der Produktivität und Agilität

Führen Sie neue Services sicher ein und nehmen Sie granulare Policy-Änderungen schneller vor. nZTA beseitigt Traffic-Hairpinning und verbessert die Nutzererfahrung durch direkten Zugriff auf Anwendungen. Und mit einem einzigen Client für den Zugriff vor Ort, remote und direkt in die Cloud beschleunigen Sie Ihre Zero-Trust-Bemühungen ohne Reibungsverluste.

Wahlmöglichkeiten und Flexibilität: granulare Richtlinien und Platzierung von Gateways

Platzieren Sie die Gateways, wo Sie wollen. Unterstützen Sie bis zu fünf Geräte pro benanntem Benutzer und fügen Sie eine flexible Anzahl von Gateways hinzu, um Ihre optimale Security-Umgebung zu gewährleisten.

Entlastung bei Netzwerkstau und Gebühren

Mit nZTA werden Ihre Daten nie über unsere Plattform geleitet, was die Belastung der Bandbreite verringert und Datengebühren für SWGs und CASBs eliminiert.

VPN-Integration

Steigern Sie die Produktivität und vermeiden Sie lange Implementierungszeiten für Infrastruktur oder Software, indem Sie nZTA in das bestehende VPN integrieren. Stellen Sie einfach und schnell einen sicheren Zugang zu neuen Anwendungen bereit, integrieren Sie neue Business Units oder erleichtern Sie Fusionen und Übernahmen.

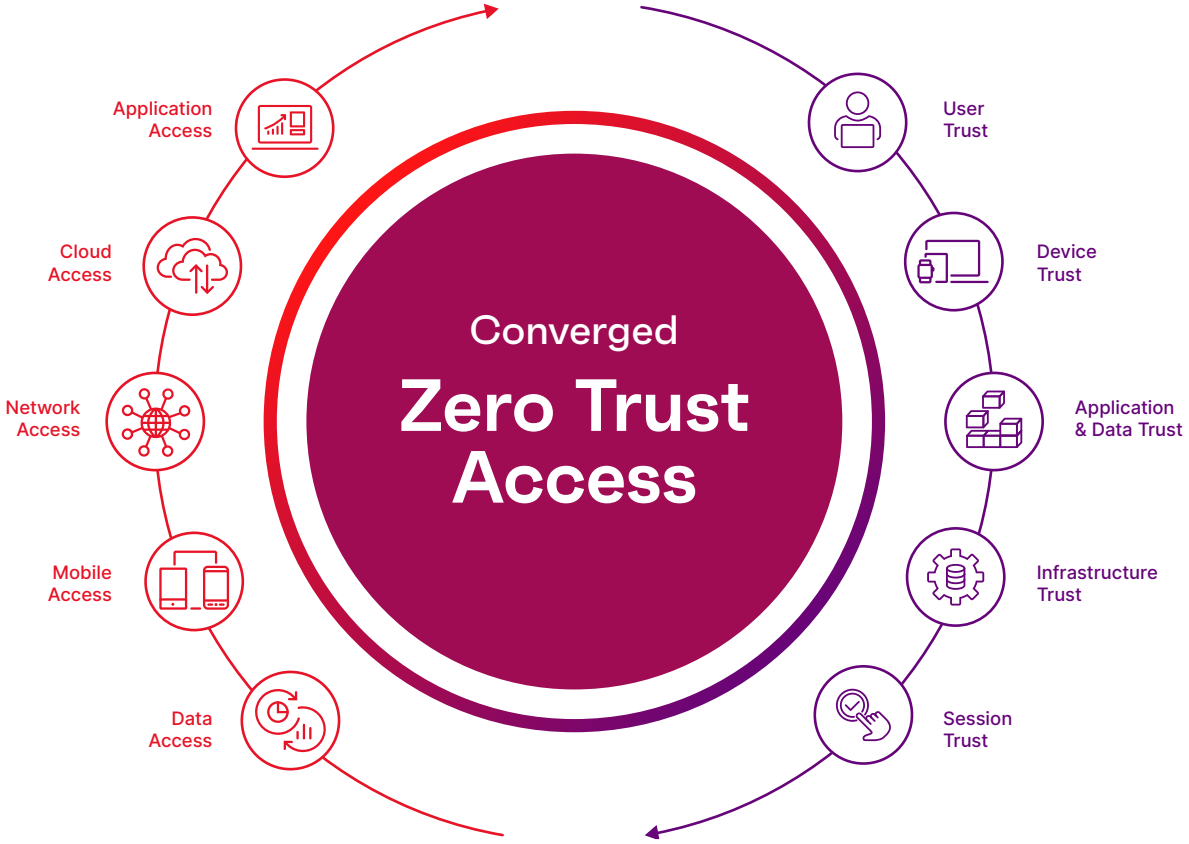
So funktioniert es

nZTA ist eine SaaS-Lösung für den Zero Trust-Netzwerkzugang, die mit Ihrer VPN-Lösung oder mit Cloud-first-Organisationen zusammenarbeiten kann.

nZTA authentifiziert und autorisiert die Benutzeridentität und den Sicherheitsstatus des Geräts, bevor eine Sitzung aufgebaut wird. nZTA steuert jede Zugriffsanfrage und -sitzung über eine zentral bereitgestellte und verwaltete Richtlinie. Diese Richtlinien werden ergänzt durch integrierte Verhaltensanalysen von Benutzern und Entitäten (User and Entity Behavior Analytics – UEBA), bei denen Attribute für jede Sitzung überwacht und bewertet werden. Proprietäre Risikobewertungen identifizieren nicht-konforme, bösartige und anormale Aktivitäten und ermöglichen schnelle Maßnahmen zur Bedrohungsabwehr.

nZTA-Gateways können flexibel dort eingesetzt werden, wo Sie es wünschen, entweder vor Ort oder in der Nähe Ihrer Cloud-Anwendungen. Diese Nähe optimiert das Benutzererlebnis, reduziert die Latenz und ermöglicht eine hybride IT-Bereitstellung in großem Umfang. Der Controller überprüft die Access Policies auf dem Gerät und dem Gateway und erstellt einen sicheren MTLS-Tunnel, der jegliche Dateninteraktion mit dem nZTA-Controller ausschließt.

nZTA bietet Flexibilität bei der Bereitstellung und ein kohärentes Policy-Management für die Anwendungsbereitstellung an jedem Ort. Die Lösung bietet gleichzeitig umfassende sichere Zugriffsfunktionen für Organisationen mit reinen Multi-Cloud-Umgebungen.



Feature	Vorteil
End-to-End Access Policy	Definieren Sie End-to-End Access Policies für jede Ressource, wobei die Unterscheidung zwischen Remote- und On-Premise-Anwendern entfällt.
Dark Cloud	Unsichtbare Anwendungen, die nur zugänglich sind, nachdem Benutzer und Gerät authentifiziert und autorisiert wurden.
Ganzheitliche Transparenz	Ganzheitliche Transparenz und Compliance Reports über Benutzer, Geräte, Anwendungen und Infrastruktur im gesamten Unternehmen.
Trennung von Steuerungs- und Datenebene	Der Benutzer- und Anwendungsverkehr wird direkt zwischen dem Benutzer und dem vorgesehenen Gateway übertragen, wodurch das Risiko von Datenverlusten verringert und die Benutzerfreundlichkeit verbessert wird.
Adaptives SSO	Integration über SAML 2.0 zur Bereitstellung von SSO für unterstützte SaaS- und 3rd Party Anwendungen.
Endpoint Compliance	Benutzer und Geräte werden anhand granularer Richtlinien authentifiziert, bevor der Zugriff gewährt wird, wodurch die Gefahr von Malware und anderen Bedrohungen verringert wird.
Verhaltensbasierte Analytik	Nutzen Sie analytische Daten, um Sicherheitsrisiken zu verringern, Anomalien zu erkennen, die Benutzerfreundlichkeit zu optimieren und sich an mobile Mitarbeiter anzupassen.
Datenschutz und -Souveränität	Alle Benutzer- und Anwendungsdaten werden zwischen Client und Gateway vollständig verschlüsselt – nZTA interagiert niemals mit Kundendaten.
On-Premise und Hybrid-Cloud	Die Gateways können in der öffentlichen Cloud, der privaten Cloud oder in den Rechenzentren der Kunden eingesetzt werden.

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