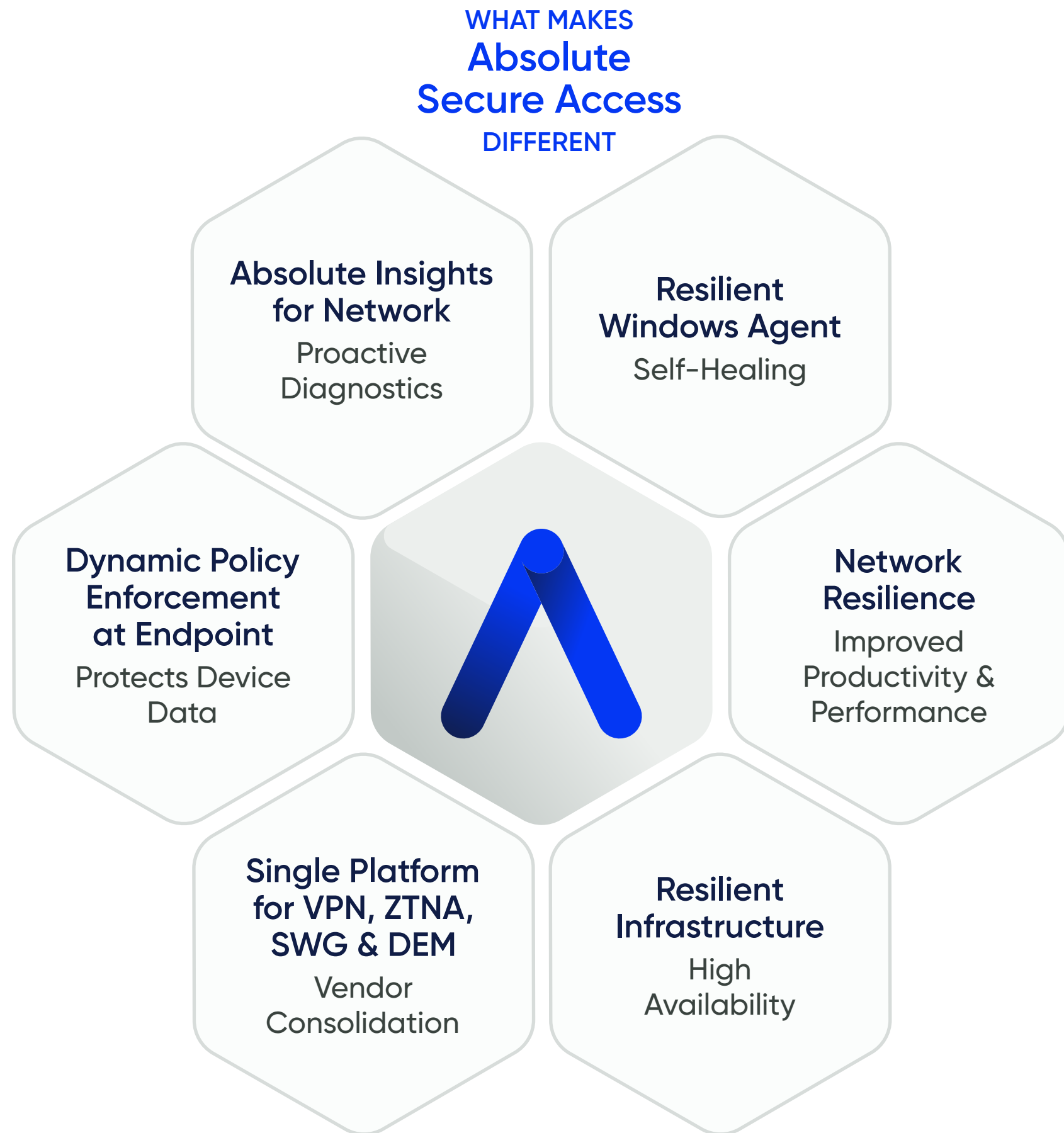DATA SHEET

# Absolute Secure Access

## Reliable, resilient access for the anywhere workforce

To enable a secure and productive work-from-anywhere environment, it is vital to extend the concept of cyber resilience beyond the endpoint and include network connectivity and critical applications as they're providing the necessary means for the anywhere workforce to get the job done. In this context, a mobile-first enterprise Virtual Private Network (VPN) and Zero Trust Network Access (ZTNA) are vital foundations to establishing a Security Service Edge (SSE) paradigm. This requires the network to form trust with an endpoint device that is constantly on the move and accessing a mix of corporate assets in the public cloud, on-premises, or in a data center using a host of Wi-Fi and cellular networks that aren't necessarily owned by the organization.

**/ABSOLUTE®**

WHAT MAKES
## Absolute
## Secure Access
DIFFERENT



**Absolute Insights for Network**
Proactive Diagnostics

**Resilient Windows Agent**
Self-Healing

**Dynamic Policy Enforcement at Endpoint**
Protects Device Data

**Network Resilience**
Improved Productivity & Performance

**Single Platform for VPN, ZTNA, SWG & DEM**
Vendor Consolidation

**Resilient Infrastructure**
High Availability

In addition to security and reliability, today's workers expect access to business applications to be seamless, which can be challenging with people regularly roaming between networks, traveling to rural or remote locations, and working in traffic-dense areas. Connections can stall or break completely, resulting in performance issues, poor user experience, and downtime. And the lack of visibility into the root causes of issues can create inefficiencies for the IT team.

Whether it is an employee working from a home office, a first responder constantly on the move, or a utility worker completing projects in the field, providing seamless, resilient connectivity significantly reduces mobile-related IT problems. It also empowers the anywhere workforce to focus on doing their jobs rather than troubleshooting technical issues.

## Harvest the Power of Resilience

For the modern digital business, enabling safe, reliable access is mission-critical. That's where Absolute® comes into play. The Absolute Secure Access™ product portfolio provides reliable, resilient network connectivity for users to gain secure access to critical resources in the public cloud, private data centers, or on-premises. These products allow you to transition from traditional secure remote access technologies like the built-in, mobile-first enterprise VPN to a Zero Trust approach without affecting productivity or admin controls.

Combining VPN, ZTNA, Secure Web Gateway (SWG), and Digital Experience Monitoring (DEM) capabilities in a single solution delivers the industry's first mobile SSE offering. This allows us to extend the same level of protection normally only associated with office or hybrid workers to mobile, deskless, and field workers.

But that's not all. Absolute Secure Access is the only undeletable secure access technology capable of automatically repairing or reinstalling itself if tampered with, accidentally removed, or has otherwise stopped working. This ensures that it remains healthy and delivers its full intended value. Absolute Network Resilience™ technology monitors and automatically restores, as well as optimizes unhealthy network connections. In turn, networked applications continue to operate without end user-impacting interruptions that would otherwise require manual application restarts, network re-connects, and/or re-authentications. The result is superior connectivity and reliability, allowing end users to focus on their tasks and not network behavior.

## Empower IT, Security, and Business

Based on its versatility, you can leverage the Absolute Secure Access product portfolio for a multitude of use cases across different stakeholders within your organization—all from a single vendor, helping you to conserve budget and allowing for simplified vendor management.

# Absolute Secure Access Key Use Case Examples



**Data Risk Report**

176

341

365

✓ Connected

GOAL

## Improve Operational Efficiency & Productivity

✓ **Optimize Network Performance** Actively improve the employee experience, deliver always-on connectivity, using tunnel and session resilience, conduct diagnostics on device and network, as well as run network performance analytics outside the corporate perimeter

✓ **Empower the Anywhere Workforce** Enable seamless remote access, optimize audio and video for end users, assure reliable network apps access for end users, deliver resilient connections and apps, even in the most turbulent network conditions

✓ **Understand Network Usage** Identify the network connectivity status, gain access to application metrics and geolocation, assess configuration statuses and impact of overall network connectivity health, as well as analyze usage patterns and prove ROI

✓ **Control Cost** Track data usage, reduce data backhaul, shift from VPN to ZTNA without costly infrastructure overhaul, and analyze network performance to drive more informed purchase decisions

✓ **Improve Helpdesk Effectiveness** Conduct root cause analysis of connection problems, minimize downtime by quickly identifying problems, automatically trigger bandwidth and connection diagnostics, as well as visualize ZTNA policy enforcement effectiveness

GOAL

## Mitigate Risk & Strengthen Compliance Posture

✓ **Protect Resources** Shield SaaS, on-prem, or private cloud resources from intruders and attacks, treat resources equally, regardless of where they are hosted, block lateral movement between applications, and conduct continuous risk assessment

✓ **Protect Users** Limit user exposure to online threats and inappropriate content, allow for complete control, inside and outside the firewall, block automatically phishing and smishing attacks, as well as provide frictionless security via granular policy enforcement at the endpoint

✓ **Deliver a secure browsing experience** for all—desk, mobile, or hybrid users. Defend organizations from viruses, malware, malicious code, zero-day threats, as well as data loss and leakage.

GOAL

## Enable the Business

✓ **Assure Continued Service Delivery** Assure field workers have reliable connectivity, assure proper service fees are applied based on geolocation, identify and resolve failures and outages quickly, as well as enforce service SLAs

getac.com
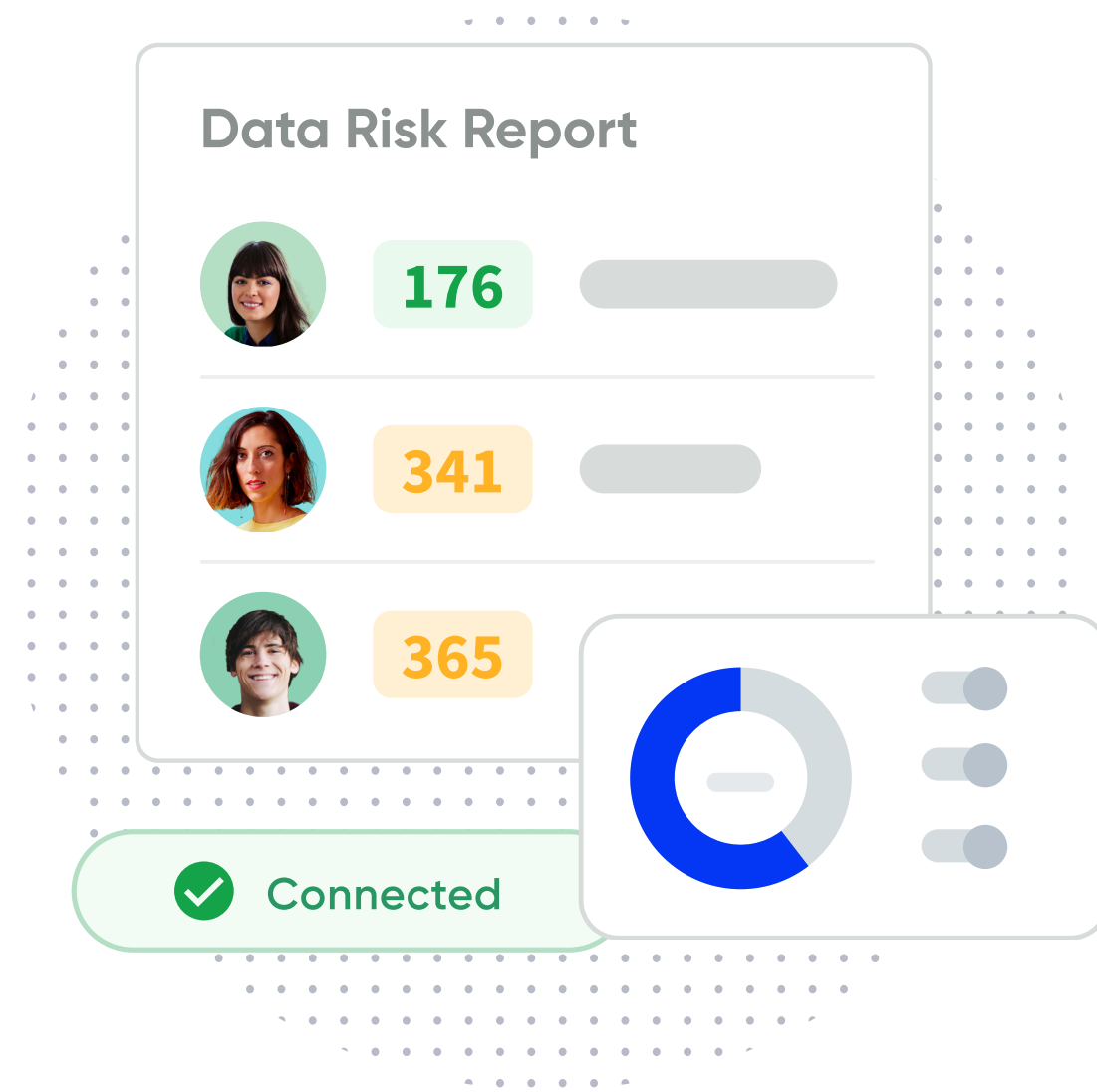
# Choose According to Your Business Needs

Absolute Secure Access packages are offered in two flavors,
Absolute Core™ and Absolute Edge™.

**MOST POWERFUL**

## Absolute Core

### Absolute VPN
Built from ground up for mobility and the modern edge

### What's Included
- ✓ Actively improve the employee experience
- ✓ Always-on connectivity, using tunnel and session resilience
- ✓ Video and audio optimizations
- ✓ Secure application access via mobile-first enterprise VPN

## Absolute Edge

**All Core capabilities, plus**

### Absolute ZTNA
Best user experience for the software-defined perimeter

- ✓ Full visibility outside the corporate perimeter
- ✓ Continuous risk assessments, using multiple data points to power access policies
- ✓ Restrict access to enterprise resources, no matter where they're hosted

### Absolute Insights for Network
Best diagnostics and remediation for digital experience monitoring

- ✓ Patented, proactive diagnostics on device and network
- ✓ Network performance analytics outside the corporate perimeter; from cellular to public Wi-Fi
- ✓ Real-time geolocation dashboards
- ✓ Threat categorization of domains visited by remote workers

**ABSOLUTE EDGE ADD-ON**
- ✓ **Absolute Secure Web Gateway Service**
  Delivers a secure browsing experience for all—desk, mobile, or hybrid users.

# Technical Specifications

**Encryption and Certifications**

- ✓ FIPS 140-2 validated encryption
- ✓ NSA Suite B cryptography
- ✓ Common Criteria EAL 4+ and SOC2 certified

**IPv6 Support**

- ✓ Full support for IPv6 applications, servers, and infrastructure; single-stack and dual-stack

**Active Directory Group Support**

- ✓ Update configuration settings and policies based on changes in Active Directory groups and group membership

**Absolute Console Access**

- ✓ Role-based access controls
- ✓ Role-based templates available (e.g., client admin, help desk user)
- ✓ Auditable logging of all changes made by Console users

**Authentication and Login**

- ✓ Authentication methods are configurable per user, device, or group
- ✓ Administrators can use the most appropriate method for their security requirements, workflows, or form factors; transparently presenting the designated authentication method to the user

- ✓ Authentication methods supported:
  - › NTLM
  - › RADIUS (PEAP, EAP-GTC, EAP-NTLM)
  - › Active Directory
  - › PKI x.509 v3 certificates
  - › RSA
  - › Other industry-standard two-factor solutions
  - › Federated authentication via SAML to enable integration with existing identity provider solutions (e.g., Microsoft Azure AD, Active Directory Federation Services, Okta, Cisco Duo)

**Control Data Collection and Privacy**

- ✓ Based on security events, business needs, or privacy standards

**Third-Party Integrations**

- ✓ API access for key real-time Absolute Console metrics

**Policy Enforcement at Endpoint**

- ✓ Mobile-friendly approach
- ✓ Assures high scalability, preventing the need to hairpin all traffic

**Supported Applications**

- ✓ Any application written for an IP network is supported (e.g., 3GPP QoS standards like FirstNet, AT&T ADTM, and Verizon Business Services)

getac.com

# Technical Specifications

## Absolute Secure Access Agents

- ✓ Android devices (running on Android 5.0 or later)
- ✓ Android for Work
- ✓ Windows Pro Tablets, laptops, and other devices running Windows 8, 10, and 11
- ✓ Support for Windows and macOS devices with ARM Processors
- ✓ Self-healing, resilient agent for Windows
- ✓ Clients available in English, Japanese, French, Italian, German and Spanish

## Capacity and Scalability

- ✓ Secure Access can support up to 60,000 concurrent users
- ✓ Hyper-resilient deployment architecture, allowing for high availability, horizontal scale-out, and zero downtime upgrades

## Server (applicable for on-premises deployment only)

- ✓ Windows Server 2016, 2019, and 2022 in Standard and Data Center versions only; the "Windows Server Essentials" editions are not supported
- ✓ Server specification vary based on deployment size
- ✓ Servers available in English and Japanese

## Deployment Options

- ✓ Secure Access Cloud
  - › No hardware or infrastructure costs with Secure Access Cloud
  - › No provisioning, patching, or maintenance overhead
  - › Reduced latency and elastic scalability as you grow
  - › Optimized for the mobile-first, cloud-first world
  - › Resilient deployment architecture, delivering high availability, horizontal scale-out, and zero downtime upgrades
  - › Controls and redundancy delivered by Microsoft® Azure with 99.999% uptime SLA – guaranteed

- ✓ On-Premises (available upon customer request)
  - › Total control over end-to-end security systems and infrastructure
  - › Deploy software within your on-premises data center or your own virtual private cloud instance
  - › Meet legal and regulatory obligations that require all data and systems to reside on-premises
  - › Resilient deployment architecture available, delivering high availability, horizontal scale-out, and zero downtime upgrades

*Absolute Secure Access platform also supports iOS, Mac OS and Samsung KNOX, for mixed fleet deployment

# /ABSOLUTE®

Trusted by nearly 21,000 customers customers, Absolute Software is the only provider of self-healing, intelligent security solutions. Embedded in more than 600 million devices, Absolute is the only platform offering a permanent digital connection that intelligently and dynamically applies visibility, control and self-healing capabilities to endpoints, applications, and network connections — helping customers to strengthen cyber resilience against the escalating threat of ransomware and malicious attacks.

**LEARN MORE**

Nasdaq | ABST    TSX | ABST

**getac.com**