

DATA SHEET

Absolute Self-Healing, Intelligent Security Solutions

Address your risk across
endpoints, applications, and
networks with a single vendor

absolute.com



It has become abundantly clear that widely distributed, hybrid work environments are here to stay and, as a result, organizations are seeking security approaches that fully integrate endpoint and access assessments to ensure that Zero Trust principles are fully applied. Absolute's unique ability to enable visibility and self-healing from the endpoint to the network edge means we can offer you truly differentiated solutions to maximize security as well as assure uncompromised productivity and network performance for your end users.

ABSOLUTE[®]

68%

of organizations suffered a successful endpoint attack within the last 12 months.
Ponemon Institute, 2020 State of Endpoint Security Risk

25%–30%

of devices had unhealthy security controls.
Absolute, 2023 Resilience Index

51%

of organizations have seen evidence of compromised endpoints being used to access company data.
HP Wolff Security, 2021 Blurred Lines and Blindspots Report

The underlying foundation of a reliable and productive work-from-anywhere environment is anchored around your employees' endpoints, as well as secure and reliable network connectivity that allows them to exchange information and access enterprise resources independent of their location.

Considering that endpoints serve as the main points of access to an enterprise network, many threat actors exploit the security gaps of endpoints. Often the efficacy of established security controls on endpoints has been impeded – this can occur due to decay, software collision, or simply because a threat actor turns them off to operate without disruption and risk of detection.

Remote access devices are the most vulnerable because their immediate physical environment is not usually secured and the employees using them are more casual in their vigilance and behavior when operating remotely. Thus, it's not surprising that many organizations have seen evidence of compromised endpoints being used to gain access to the corporate network.

In turn, it's imperative to secure both endpoints and remote access controls to be able to confidently establish resilient Zero Trust principles.

We've Got You Covered: From the Firmware Boot through the Network Access

That's where Absolute comes into play. Embedded in more than 600 million devices, Absolute® is the only intelligent security solutions provider capable of delivering visibility and control capabilities to endpoints, applications, and network connections. When our unique self-healing capability is combined with the power of Absolute Secure Endpoint and Absolute Secure Access, you can not only protect devices, data, and users alongside an optimal remote and mobile user experience, but also ensure that critical security controls operate at maximum effectiveness.

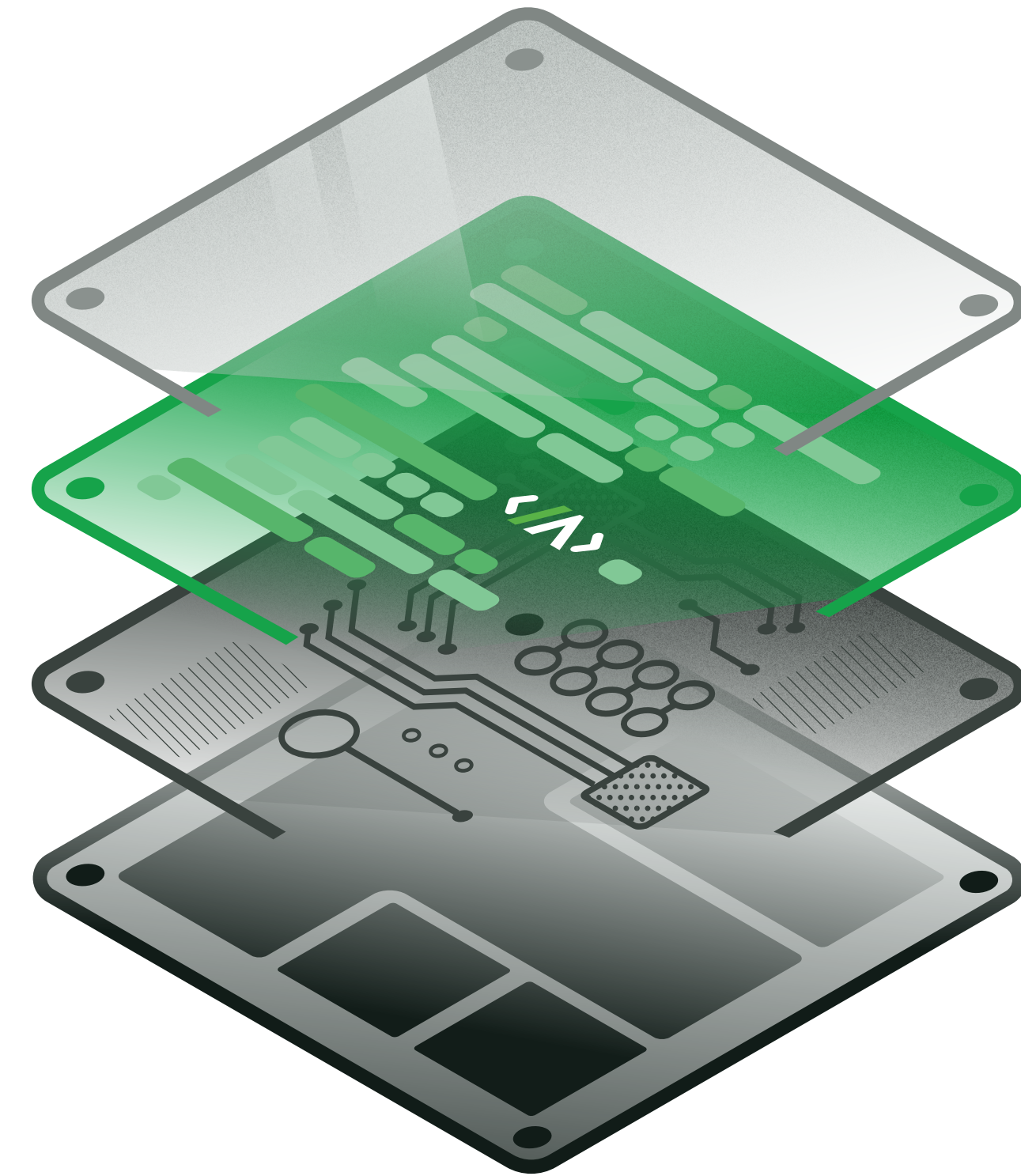


A Common Platform to Serve Your IT and Security Needs

All of our product lines and individual product offerings are powered by the **Absolute Platform**. One of the essential platform components is our patented **Persistence**[®] technology, which is embedded in the firmware of more than 600 million devices, providing a secure, always-on connection between the Absolute Platform and the endpoint. Once activated, this technology is fiercely resilient and is the only solution to survive attempts to disable it, even if the device is re-imaged, the hard drive is replaced, or the firmware is updated.

No other technology can do this.

We're able to extend these self-healing capabilities to mission-critical applications that are covered in our Application Resilience™ catalog. Once taken under policy, customers can monitor the health of their application and automatically repair and/or reinstall the application if its integrity is deemed impeded. This ensures that no matter what – be it common software decay, software collision, unintentional deletion, or malicious actions – the application will always function as intended. We also have patented Network Resilience™ technology that assures that a tunnel or network connection is resilient to external factors and even optimizes audio and video transmissions.



Persistence[®] technology is embedded in the firmware of more than 600 million devices.



Absolute Secure Endpoint

Our Secure Endpoint product line enables your IT and security personnel to monitor and address computers' problems and enables the laptops and their mission-critical applications to self-heal.

This helps with IT management, strengthening your company's security posture, and maintaining compliance. Within this product line, we offer a variety of products:

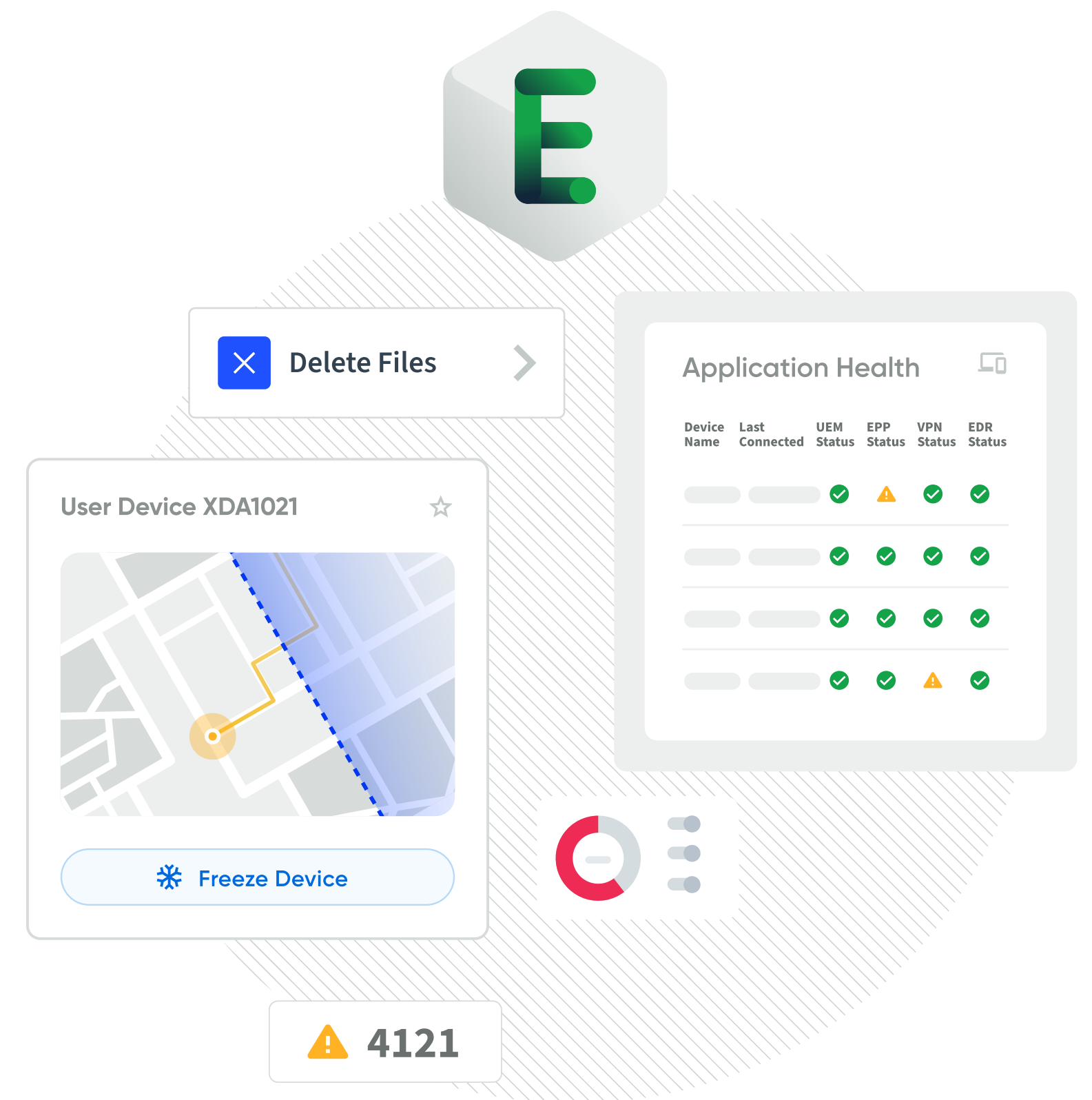
Absolute Visibility collects data about the endpoints' location, security posture, and hardware/software inventory. It provides analysis of software, Web applications, and hardware utilization and identifies potential failure points, sensitive data, and suspicious use patterns.

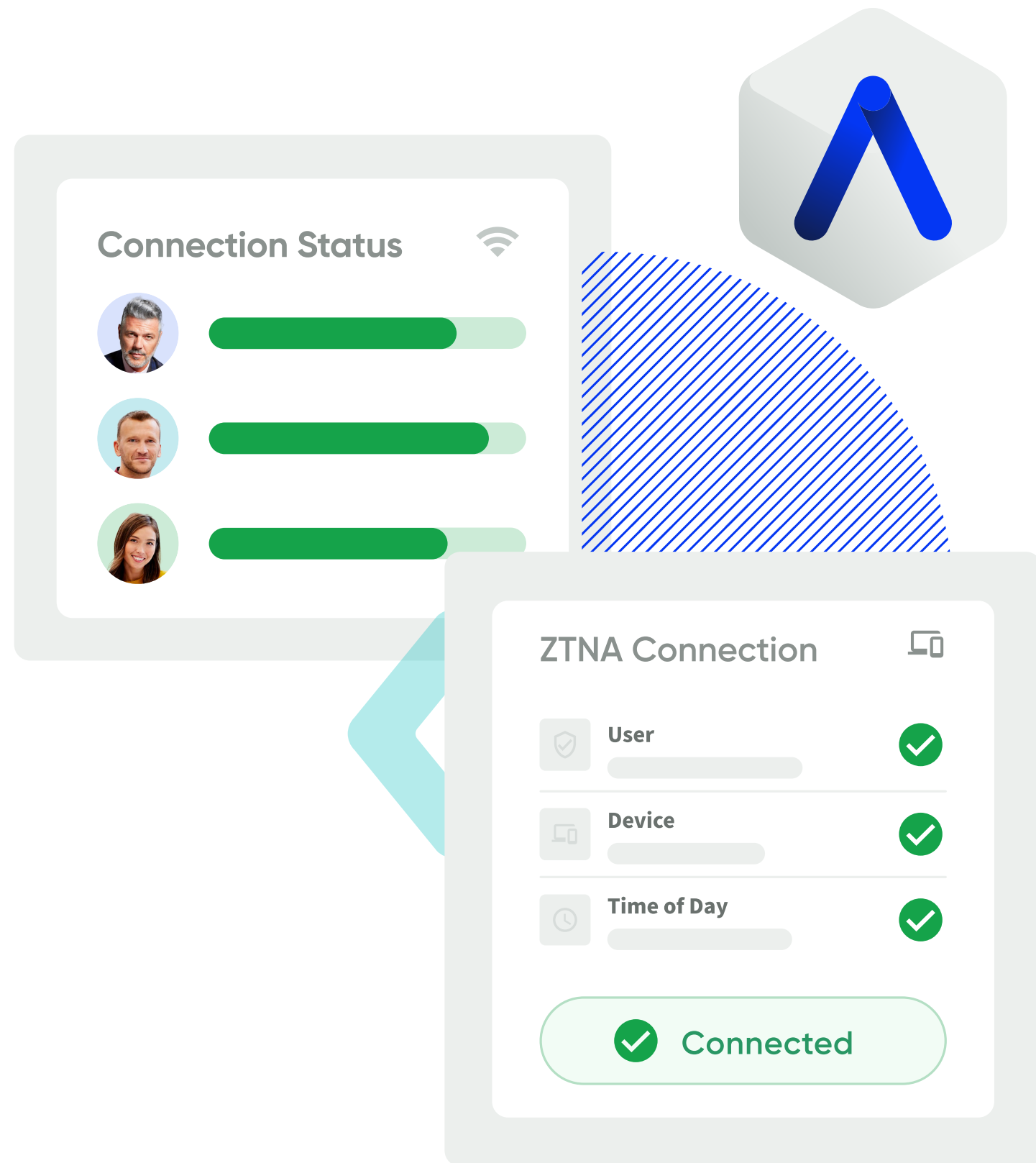
Absolute Control adds to these capabilities to control endpoints over the Internet, allowing for remote file deletion and data wipe, freezing devices on demand when at-risk, as well as establishing geofences and alerts.

Absolute Resilience adds further capabilities to secure endpoints from threats and vulnerabilities, and to respond to security breaches and incidents. It ensures that your devices are resilient to changes, e.g., by self-healing mission-critical applications.

Secure Endpoint packages are easily upgradeable, allowing you to move between Visibility, Control, and Resilience service tiers via a simple license feature key to expand your capabilities and the use cases you can cover. To accommodate your specific business needs, you can mix and match the different service tiers across your device fleet.

For those customers that are primarily concerned about their capability to recover their device fleet from ransomware attacks, we offer **Absolute Ransomware Response**. This offering provides capabilities and services to assess your organization's ransomware preparedness and cyber hygiene across endpoints; ensures mission-critical security applications such as anti-malware and device management tools remain healthy and capable of self-healing; and expedites the quarantine and recovery of your endpoints if a ransomware attack occurs.





Absolute Secure Access

The second product line was added to our portfolio through the acquisition of a company called NetMotion in July 2021. The Secure Access product portfolio provides reliable network connectivity for users to gain secure access to critical resources in the public cloud, private data centers, or on-premises. These products allow users to transition from traditional secure remote access technologies to a Zero Trust approach, without affecting productivity or admin controls. It also helps to allow for reliable network connectivity as well as improved network performance and optimization. As the industry's first mobile Security Service Edge (SSE) solution, Absolute extends the same level of protection normally only associated with office or hybrid workers to mobile, deskless, and field workers.

Absolute VPN provides security and confidentiality for data in motion by means of encryption and access controls. It also offers benefits to the end user, such as making tunnel and network sessions resilient and optimizing streaming video and audio.

Absolute ZTNA provides a software-defined perimeter via Zero Trust Network Access, creating a context-based, logical access boundary around an application or set of applications – wherever they're hosted. It shields applications from the Internet, making them invisible to unauthorized users. Access policies are enforced at the endpoint, protecting device data and eliminating choke points.

Absolute Insights for Network offers diagnostic and experience monitoring capabilities across endpoints and network, allowing organizations to proactively monitor, investigate, and remediate end user performance issues quickly and at scale, even on networks that are not company-owned or managed.

Secure Access packages are offered in two flavors, Absolute Core (includes Absolute VPN only) and Absolute Edge (includes all three products mentioned above). Absolute Edge customers can add the Absolute Secure Web Gateway Service (powered by Ericom), which tightly integrates with the extensive policy capabilities in Absolute Secure Access. In turn, they can strengthen their organization's security posture while improving their end user experience. Absolute Secure Web Gateway Service delivers a secure browsing experience for all - desk, mobile, or hybrid users.

One Vendor, Endless Benefits

You can leverage the Secure Endpoint and Secure Access product portfolio for a multitude of use cases and across different stakeholders within your organization – all from a single vendor, helping you to conserve budget and allowing for easier vendor management.

Improve operational efficiency and productivity

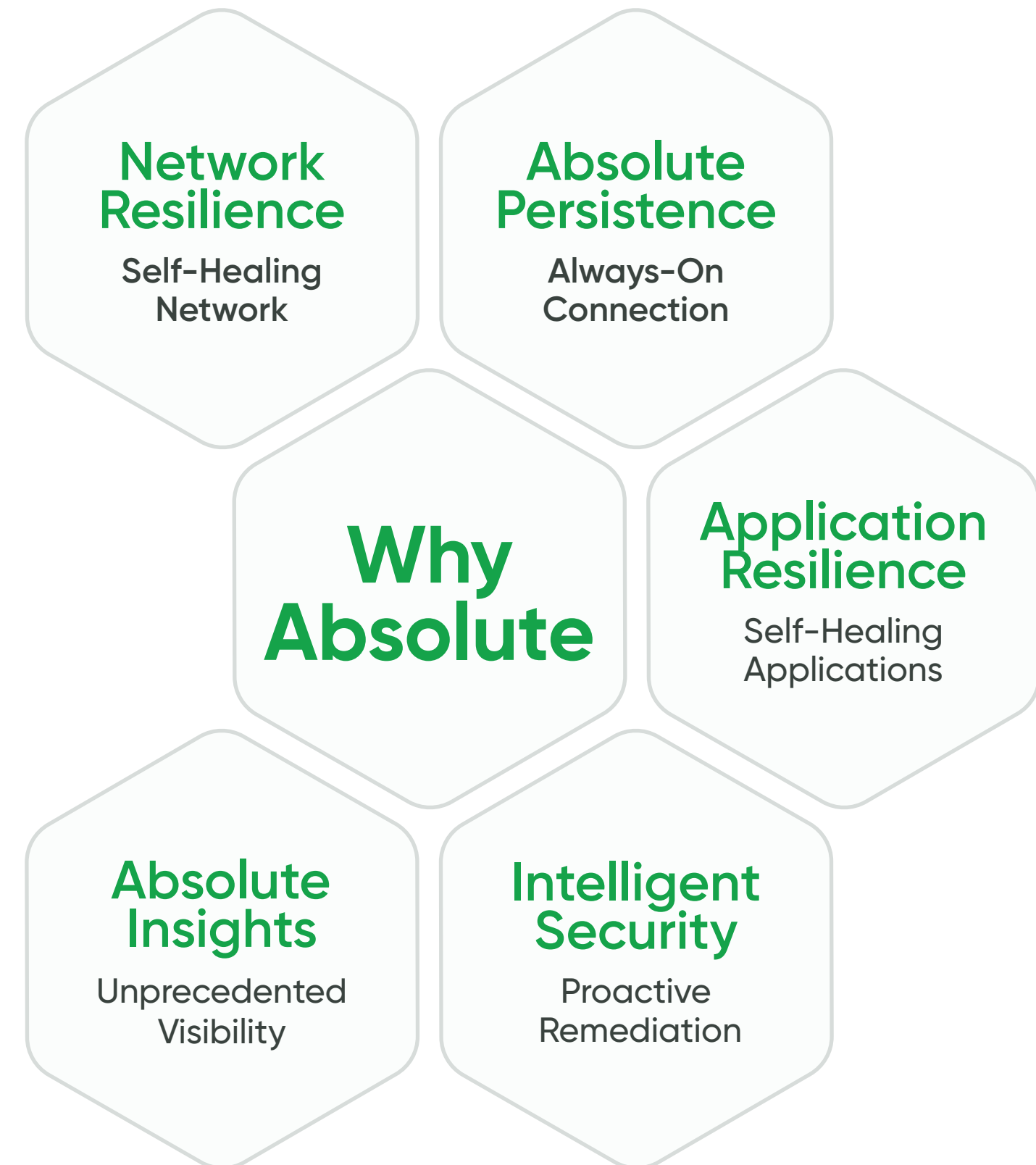
- ✓ Optimize hardware and software inventory utilization
- ✓ Understand device, application, and network usage
- ✓ Assure continued network connectivity
- ✓ Optimize network and application performance
- ✓ Reduce lost and stolen devices by tracking and locating devices
- ✓ Enable remote device lifecycle management (e.g., device reclamation or re-provisioning of devices)
- ✓ Autonomously monitor and self-heal applications to assure availability
- ✓ Improve helpdesk effectiveness for endpoints and network access

Mitigate risk and strengthen compliance posture

- ✓ Assess device security posture and detect security incidents
- ✓ Establish geo-fences to identify at-risk devices
- ✓ Enforce security standards by autonomously monitoring and self-healing mission-critical applications
- ✓ Detect sensitive data across your device fleet
- ✓ Provide evidence and reports for audit purposes
- ✓ Minimize exposure to vulnerabilities
- ✓ Respond to endpoint risks and confidently recover from incidents
- ✓ Protect users/enterprise resources by removing password reliance
- ✓ Adopt new, modern security frameworks

Enable Your Business

- ✓ Empower work-from-anywhere workforce
- ✓ Optimize user experience
- ✓ Assure continued service delivery (e.g., for first responders or field workers)



See What Our Users Have to Say



AVERAGE SCORE ACROSS BOTH SECURE ENDPOINT AND SECURE ACCESS PRODUCTS IS

4.7 out 5.0



"Peace of mind for any security team"

I can tell any manager what was on a lost computer, when it was lost, where it was lost. I can verify it was encrypted; I can say who used it last. The amount of information and control they give is critical to complying with HIPAA.

IT SECURITY ENGINEER /
ENTERPRISE > 1000 EMP.



"Just what we needed"

It has been one of the best device management solutions we have used by far. Absolute does exactly what it is intended for and has helped our organization manage all our devices! Within our organization we are required to have all devices up to date; Absolute has given us the ability to manage devices outside our network.

ENTERPRISE CUSTOMER / > 1000 EMP.



"More than just anti-theft"

Provides great asset recovery abilities at its core. However, the power lies within the ability to manage devices and applications on the endpoints as well. Absolute was a blessing for our company during COVID.

CHIEF TECHNOLOGY OFFICER /
ENTERPRISE > 1000 EMP.



AVERAGE SCORE ACROSS BOTH SECURE ENDPOINT AND SECURE ACCESS PRODUCTS IS

4.7 out 5.0



"Absolute Software helps maintain business software and develop extra security controls."

INFORMATION SECURITY THREAT ANALYST
BANKING / <50M



"Absolute is great for tracking your corporate assets within and outside the network"

SECURITY OPERATIONS LEAD
FINANCE / 250M - 500M USD



"Absolute provides exceptional products to stay in compliance and provide accuracy"

NETWORK ADMINISTRATOR
HEALTHCARE INDUSTRY / 500M - 1B USD





ABSOLUTE[®]

Trusted by nearly 21,000 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.

[Request a Demo](#)