ABSOLUTE®

Absolute Resilience™ Platform — Cyber Catalyst 2020 Designation

The Absolute Resilience™ Platform provides organizations with a secure connection to every device, even off the corporate network, using patented technology embedded in device firmware. This unbreakable digital tether powers Absolute's Endpoint Resilience™ solutions – enabling devices and security controls to recover from any incident to a secure operational state, automatically.

The Absolute Resilience Platform gives CIOs and CISOs the visibility, control, and intelligence needed to secure data, devices, and applications. It enables IT and security teams to easily manage device lifecycles and safeguard assets with a continuous stream of endpoint intelligence, including hardware, software, security status, usage, and geolocation data. And it is able to identify sensitive data and remediate vulnerabilities remotely – including the ability to freeze or wipe off-network devices.

70% of cyberattacks originate at the endpoint, and complexity across endpoints is growing, driven by three critical factors:

- An increasing number of security controls on devices — 10.2 on average, up from 9.8 in 2019.

- Device OS migration, resulting in fragmentation and stagnant patching practices.

- Fragile security controls, and their varying rates of decay and collision.

Dark Endpoints pose a considerable operational challenge and security threat to organizations because these devices may be missing or have outdated security or other applications, contain sensitive data, or be in the hands of unauthorized users. Dark

Endpoints are of particular current concern given the number of employees working remotely, which places devices outside the view and control provided by traditional network-based management and security tools.

The Absolute Resilience Platform addresses these specific risks, enabling organizations to:

- See all devices, on and off the network, and collect hundreds of hardware, software, security status, usage, and geolocation data points automatically, with 365 days of historical logs.

- Detect when endpoints enter an unauthorized area, and take remote action to remediate endpoints risks immediately by rendering devices useless or deleting the data they contain.

- Establish resilient security by ensuring critical apps remain active at all times. It addresses broken or missing endpoint security controls through Absolute's Application Persistence™ service, factory-installed technology embedded in the firmware of 500M+ PCs by leading system manufacturers, that when activated enables endpoints to automatically repair and restore mission-critical applications.

- Remotely identify sensitive data, track web usage, gather precise insights or remediate endpoint vulnerabilities, and investigate stolen devices.

Product information provided by Absolute Software

For more information about Absolute Software™, visit www.absolute.com.

Why The Absolute Resilience™ Platform is a 2020 Cyber Catalyst Designated Solution

ADDRESSES A TOP 5 CYBER RISK:

The 2020 program encouraged the submission of solutions that targeted the top five cyber risks identified by participating insurers: ransomware, supply chain/vendor management, cloud migration/management, social engineering, and privacy regulation/data management.

The Absolute Resilience Platform specifically targets privacy regulation/data management, but also has wider utility and applicability in addressing other types of cyber risk.

INSURER RATINGS AND COMMENTARY:

Cyber Catalyst participating insurers rated the Absolute Resilience Platform highest on the criteria of key performance metrics, efficiency, and flexibility.

In their evaluation, the insurers commented:

- "The capacity to provide visibility to all endpoints and look for sensitive information across those endpoints – on or off the network – really gives an enhanced level of control. In high risk sectors such as banking and financial services, pharmaceuticals, and manufacturing, this level of control is highly desirable."

- "A very comprehensive and interesting endpoint solution: it tackles the issue of dark endpoints, quite topical now with so many people working remotely. Intuitive dashboards with valuable reporting metrics out of the box. I like the feature that protects and reinstalls business critical applications."

- "The admin GUI seems easy to use; I like that it cannot be removed from the device because it's embedded in the firmware itself. Other strong features are the ability to freeze an asset and display a message; easy tracking of where assets are; software able to delete software, data, and remotely wipe a machine not in your possession."

Insurance Policies and Implementation Principle

Organizations that adopt Cyber Catalyst designated solutions may be considered for enhanced terms and conditions on individually negotiated cyber insurance policies with participating insurers.

Those insurers, when considering potential policy enhancements, will expect organizations to deploy Cyber Catalyst designated products and services in accordance with certain "implementation principles" that have been developed by the insurers and product vendors.

The implementation principle for the Absolute Resilience Platform is:

- The product has been deployed on 100% of critical assets and the firmware and Absolute agents are updated regularly. There is a designated individual within the organization to monitor activity and identify alerts.

Evaluation Process

Applications for evaluation of cybersecurity products and services were accepted from March 10 to May 15, 2020. More than 90 offerings, spanning a broad range of categories, were submitted.

The insurers evaluated eligible solutions along six criteria:

1. Reduction of cyber risk.

2. Key performance metrics.

3. Viability.

4. Efficiency.

5. Flexibility.

6. Differentiation.

Cyber Catalyst designation was awarded to solutions receiving positive votes from at least six of the eight insurers, which voted independently. Marsh did not participate in the Cyber Catalyst designation decisions.

More Information on Cyber Catalyst

The next Cyber Catalyst program will occur in 2021.

For more information on the 2020 Cyber Catalyst designated solutions, or the 2019 class of Cyber Catalyst solutions, visit the Cyber Catalyst pages on the Marsh website: www.marsh.com/cybercatalyst.

For more information about Marsh's cyber risk management solutions, email cyber.risk@marsh.com, visit www.marsh.com, or contact your Marsh representative.