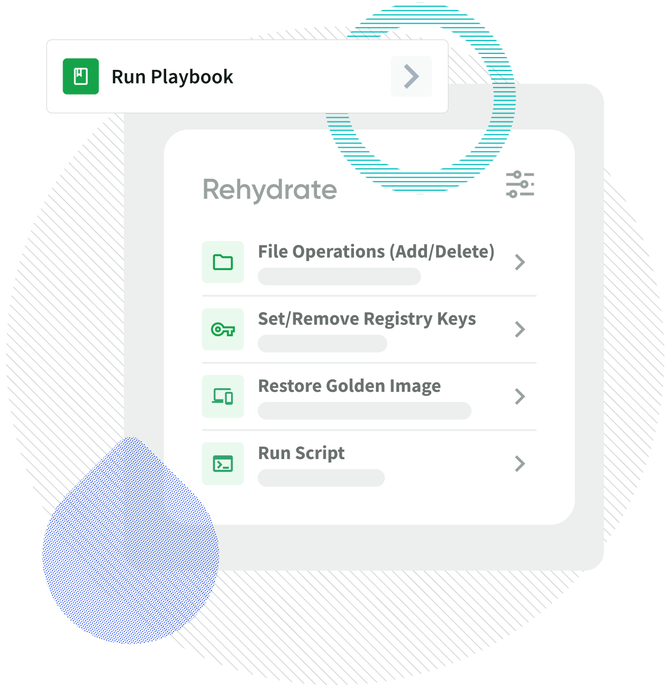
DATASHEET

Absolute Rehydrate

Remote Endpoint Recovery for the Anywhere Work Environment

With the ever-present scourge of today's complex malware and ransomware attacks targeting vulnerable users and endpoints alike, IT and security practitioners at Enterprise organizations as well as Managed Service Providers (MSPs or MSSPs) require the means to swiftly and securely restore devices that have been compromised at the operating system layer from bare metal back to a state of efficacy and compliance.

Most endpoint restoration tools in the market typically rely on IT either having physical possession of the impacted device or providing impacted end users a USB stick with a pre-loaded restoration image to perform the recovery. Even under best case conditions, where IT and impacted users happen to be co-located and can freely exchange devices or USB sticks, this is still an expensive, time-consuming and productivity-impacting process. Under today's remote work hybrid environment where IT and Security operations have often been outsourced to even more remotely located MSP/MSSPs, the expense, time and productivity impacts all increase substantially.



Challenges Recovering Endpoints After Unexpected Disruptions (e.g. an IT or security incident)

- Endpoint recovery solutions typically require physical possession of compromised devices, which is unmanageable, time consuming and costly for large enterprises with geographically dispersed employees.
- An alternative is to ship USB drives with the pre-loaded restoration image to employees for them to carry out the recovery process. Again, this is time consuming, costly and productivity impacting.
- Most endpoint recovery solutions in the market just cater to the case of recovering devices by deploying the golden OS image either through the cloud or a USB stick. In some IT or security scenarios, having more options or flexibility in the types of remediation actions that can be executed is beneficial.

The Solution: Absolute Rehydrate

Built on Absolute's Persistence technology embedded in the firmware of 600 million devices, Absolute Rehydrate empowers organizations and MSP/MSSPs to respond more efficiently and effectively to bring devices back to a controlled, trusted and compliant state when IT or security incidents occur or when devices become non-compliant. This unique solution offers IT teams and MSPs the ability to perform device restoration remotely through the Absolute Console which then percolates down to the device's firmware, hence circumventing the operating system in cases where it has been corrupted or when its controls are no longer functioning due to the IT or security incident at hand.

The restoration playbooks offer practitioners the flexibility of either running a full restore of the operating system's golden image when needed or applying more surgical actions such as adding or deleting files, modifying registry details or running a script if they suffice in restoring the device.

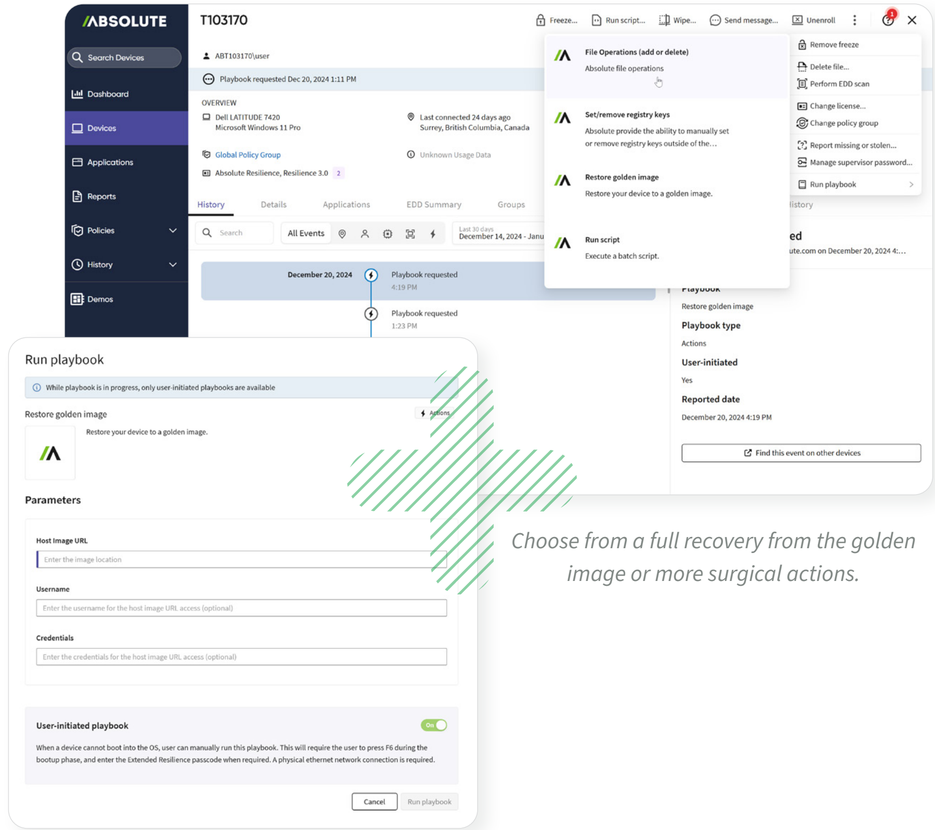
Key Capabilities

- Remote recovery and repair of affected endpoints after an IT issue causing a BSOD event or cyberattack (e.g. ransomware or malware) back to a fully trusted and compliant state.
- Full image recovery or more surgical endpoint recovery playbooks that execute via the firmware of devices and bypass the operating system in case it has been tampered with.
- Absolute defined recovery playbooks available through the Absolute Console include:
  - Rehydrate from trusted OS golden image
  - Add remedial file(s) or delete malicious file(s)
  - Add, modify or delete registry keys
  - Execute scripts (batch)
- Passcode-protected “break-glass” mechanism that runs at the device’s bootup to download and executes the chosen recovery playbook.
- Management and status tracking of the recovery playbooks through the Absolute Console.
- Role based access controls to ensure only certified users can execute recovery playbooks through the console.

Use Cases and Benefits

- Remotely and efficiently respond to cyberthreats or IT issues causing Blue Screen of Death (BSOD) instances to limit downtime to business operations.
- Recover quickly from cyberattacks and IT events that cause unexpected disruptions to limit the impact on business operations, financial penalties and the organization’s reputation.
- Firmware based endpoint recovery and remediation that bypasses the operating system in cases when it has been tampered with. Remotely repair and restore affected devices, even when the OS has been compromised by malware, ransomware or an IT issue.
- Alleviates incident response effort on capacity-strained IT teams post an IT or security event.
- Cost effective and remote endpoint recovery solution not requiring physical access to devices or a USB recovery drive.
- Being embedded at the firmware level provides unparalleled control and continuity across a company’s entire endpoint environment.

Absolute Rehydrate is available with the Absolute Resilience, Absolute Resilience for Security and Absolute Resilience for Automation product editions.



Choose from a full recovery from the golden image or more surgical actions.

Run the “Restore Golden Image” restoration playbook.

ABSOLUTE®

Absolute Security is partnered with more than 28 of the world's leading endpoint device manufacturers, embedded in the firmware of 600 million devices, trusted by thousands of global enterprise customers, and licensed across 16 million PC users. With the Absolute Security Cyber Resilience Platform integrated into their digital enterprise, customers ensure their mobile and hybrid workforces connect securely and seamlessly from anywhere in the world and that business operations recover quickly following cyber disruptions and attacks. Our award-winning capabilities have earned recognition and leadership status across multiple technology categories, including Zero Trust Network Access (ZTNA), Endpoint Security, Security Services Edge (SSE), Firmware-Embedded Persistence, Automated Security Control Assessment (ASCA), and Zero Trust Platforms.

Request a Demo