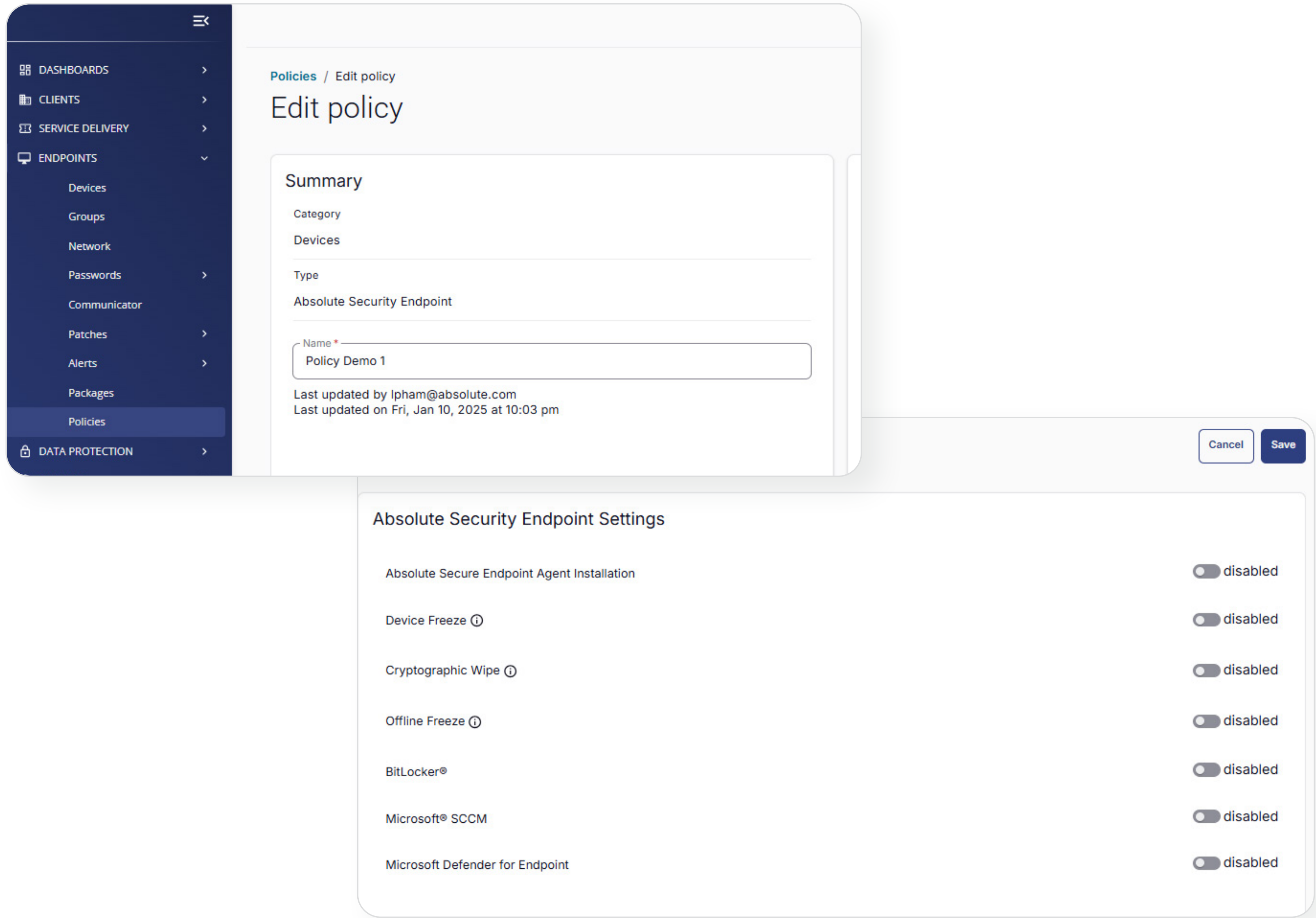
DATASHEET

Absolute Resilience for ConnectWise

Managing Disparate and Remote Client Endpoint Environments

With the complexity of remote work policies, a rise in sophisticated cyberthreats such as ransomware and a general shortage in cybersecurity skills, organizations are now commissioning Managed Services Providers (MSPs) to handle the management of their endpoint environments and security operations. This may involve overseeing device lifecycle management from cradle to grave, provisioning end-users with the right tools, applications and resources to remain productive while enforcing policies to maintain their clients' security posture. In the event of an IT or security incident, MSPs are expected to aid in restoration efforts to ensure downtime in business operations is minimized.



Edit policy

Summary

Category
Devices

Type
Absolute Security Endpoint

Name *
Policy Demo 1

Last updated by lpham@absolute.com
Last updated on Fri, Jan 10, 2025 at 10:03 pm

Absolute Security Endpoint Settings

Absolute Secure Endpoint Agent Installation	disabled
Device Freeze ⓘ	disabled
Cryptographic Wipe ⓘ	disabled
Offline Freeze ⓘ	disabled
BitLocker®	disabled
Microsoft® SCCM	disabled
Microsoft Defender for Endpoint	disabled

Editing policies through the ConnectWise Asio platform utilizing Absolute's capabilities.

Challenges faced by MSPs in managing multiple client environments:

- Adoption of remote work policies leading to irregular endpoint visibility and rise in device loss.
- Utilizing multiple tools to track hardware, software and network health leading to inefficiency and overhead.
- Ensuring critical security applications and controls such as Anti-Malware, Encryption, Endpoint Security and Endpoint Management are functioning across client devices.
- Ensuring sensitive data such as personally identifiable information, financial details and corporate intellectual property is protected throughout customer environments, specifically when devices are decommissioned or reassigned to new employees.
- Responding effectively to mass-scale IT or security incidents or zero-day vulnerabilities to ensure downtime across client environments is minimized.

MSPs typically offer services that utilize a variety of products, such as Remote Monitoring and Management (RMM), to track and secure their client environments. The ConnectWise RMM Asio™ platform offers MSPs automation, scalability and centralized IT management to track customer endpoints, applications and network, automate patching and run workflows through AI-assisted scripting to respond to potential issues. Absolute Security has partnered with ConnectWise to supplement this feature set by seamlessly integrating Absolute Secure Endpoint's tailored capabilities to be accessible through the ConnectWise Asio™ console.

The Solution: Absolute Resilience for ConnectWise

The Absolute Resilience for ConnectWise product integration empowers MSPs to boost cyber resilience across their customers' environments by enhancing endpoint visibility, enforcing security posture through application self-healing and responding to device risks or compliance breaches through integrated device actions. Track granular information such as device location, protect stored sensitive information, maintain the health of critical security applications and respond remotely to device risks or compliance breaches.

The product surfaces up Absolute Secure Endpoint's device telemetry and device actions to be accessible through the ConnectWise Asio console. Resilience for ConnectWise leverages Absolute Persistence® technology embedded in the firmware of PCs manufactured by leading OEMs such as Dell, Lenovo, HP and others.

Key Capabilities

Discover/Guard

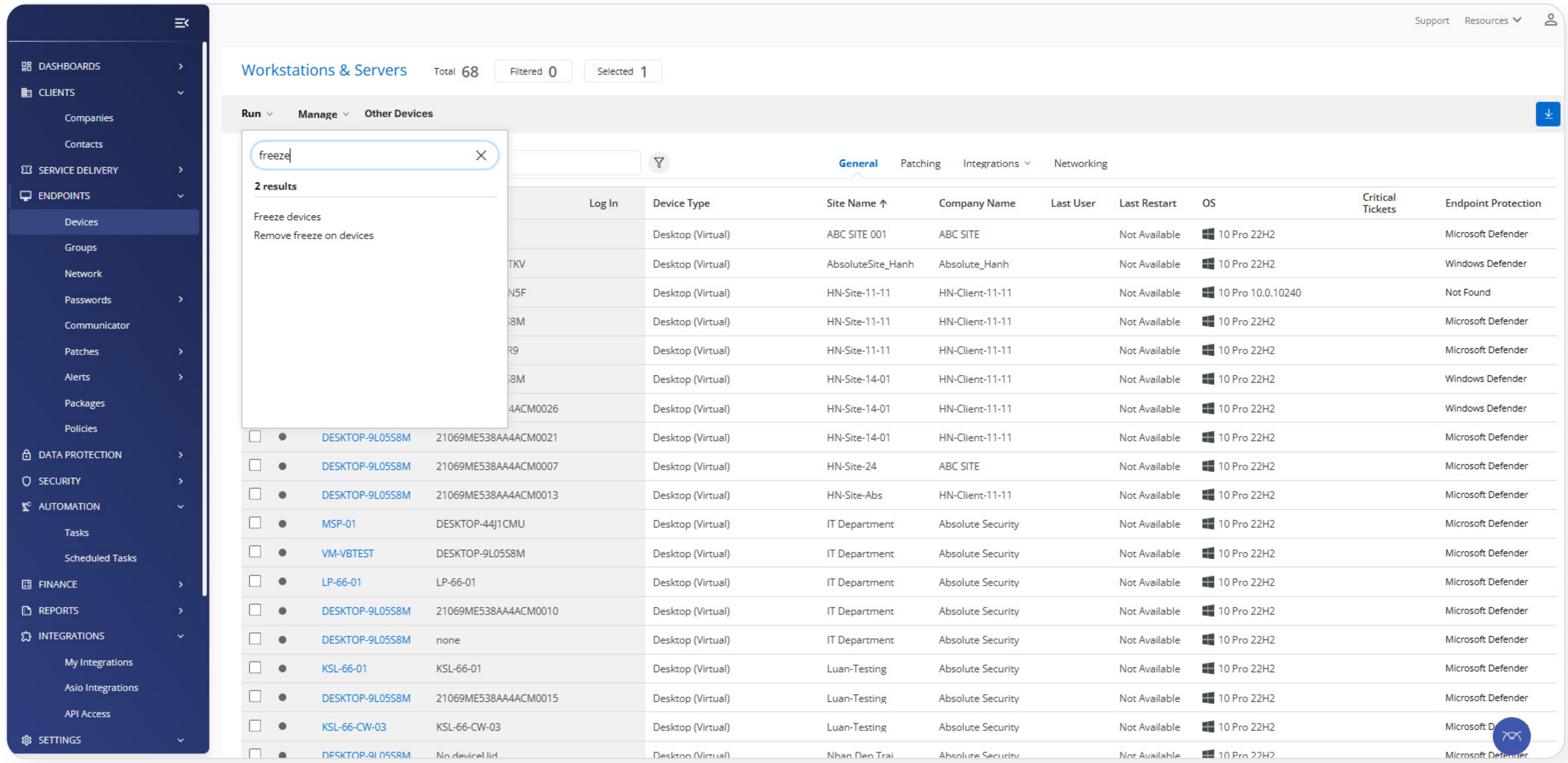
- Tracking encryption status across devices.
- Geolocation to monitor the device's current location.
- Device Freeze to quarantine at-risk or compromised devices.
- Offline Freeze to quarantine devices that have been offline for over a specified period.
- Device Wipe to protect sensitive information on compromised, decommissioned or reassigned devices from falling in the wrong hands. Obtain a certificate of sanitization as proof for device audits. Comply with NIST SP 800-88 media sanitization standards.

Heal

- Application Resilience to report on and repair the health of critical Microsoft applications. Supported applications include:
  - Microsoft BitLocker
  - Microsoft SCCM
  - Microsoft Defender ATP

Rehydrate

- Restore compromised endpoints within client environments back to a fully trusted and compliant state in response to an IT or security incident.



Workstations & Servers Total 68 Filtered 0 Selected 1

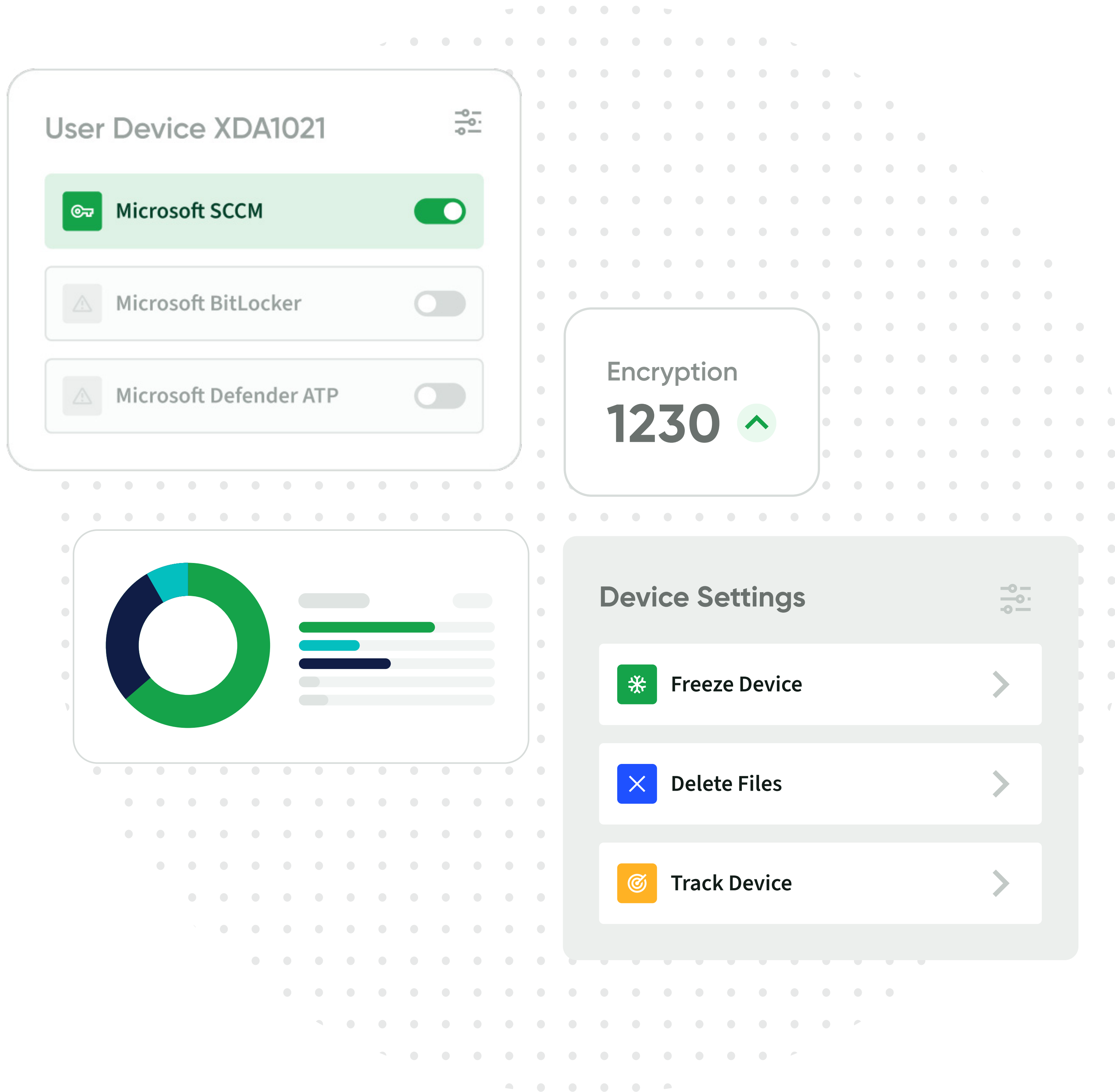
freeze

2 results

Freeze devices
Remove freeze on devices

				Log In	Device Type	Site Name ↑	Company Name	Last User	Last Restart	OS	Critical Tickets	Endpoint Protection
					Desktop (Virtual)	ABC SITE 001	ABC SITE		Not Available	10 Pro 22H2		Microsoft Defender
			TKV		Desktop (Virtual)	AbsoluteSite_Hanh	Absolute_Hanh		Not Available	10 Pro 22H2		Windows Defender
			N5F		Desktop (Virtual)	HN-Site-11-11	HN-Client-11-11		Not Available	10 Pro 10.0.10240		Not Found
			8M		Desktop (Virtual)	HN-Site-11-11	HN-Client-11-11		Not Available	10 Pro 22H2		Microsoft Defender
			R9		Desktop (Virtual)	HN-Site-11-11	HN-Client-11-11		Not Available	10 Pro 22H2		Microsoft Defender
			8M		Desktop (Virtual)	HN-Site-14-01	HN-Client-11-11		Not Available	10 Pro 22H2		Windows Defender
			4ACM0026		Desktop (Virtual)	HN-Site-14-01	HN-Client-11-11		Not Available	10 Pro 22H2		Windows Defender
☐	●	DESKTOP-9L05S8M	21069ME538AA4ACM0021		Desktop (Virtual)	HN-Site-14-01	HN-Client-11-11		Not Available	10 Pro 22H2		Microsoft Defender
☐	●	DESKTOP-9L05S8M	21069ME538AA4ACM0007		Desktop (Virtual)	HN-Site-24	ABC SITE		Not Available	10 Pro 22H2		Microsoft Defender
☐	●	DESKTOP-9L05S8M	21069ME538AA4ACM0013		Desktop (Virtual)	HN-Site-Abs	HN-Client-11-11		Not Available	10 Pro 22H2		Microsoft Defender
☐	●	MSP-01	DESKTOP-44J1CMU		Desktop (Virtual)	IT Department	Absolute Security		Not Available	10 Pro 22H2		Microsoft Defender
☐	●	VM-VBTEST	DESKTOP-9L05S8M		Desktop (Virtual)	IT Department	Absolute Security		Not Available	10 Pro 22H2		Microsoft Defender
☐	●	LP-66-01	LP-66-01		Desktop (Virtual)	IT Department	Absolute Security		Not Available	10 Pro 22H2		Microsoft Defender
☐	●	DESKTOP-9L05S8M	21069ME538AA4ACM0010		Desktop (Virtual)	IT Department	Absolute Security		Not Available	10 Pro 22H2		Microsoft Defender
☐	●	DESKTOP-9L05S8M	none		Desktop (Virtual)	IT Department	Absolute Security		Not Available	10 Pro 22H2		Microsoft Defender
☐	●	KSL-66-01	KSL-66-01		Desktop (Virtual)	Luan-Testing	Absolute Security		Not Available	10 Pro 22H2		Microsoft Defender
☐	●	DESKTOP-9L05S8M	21069ME538AA4ACM0015		Desktop (Virtual)	Luan-Testing	Absolute Security		Not Available	10 Pro 22H2		Microsoft Defender
☐	●	KSL-66-CW-03	KSL-66-CW-03		Desktop (Virtual)	Luan-Testing	Absolute Security		Not Available	10 Pro 22H2		Microsoft D
☐	●	DESKTOP-9L05S8M	No deviceUid		Desktop (Virtual)	Nhan Den Trai	Absolute Security		Not Available	10 Pro 22H2		Microsoft Defender

Executing a freeze across devices through the ConnectWise Asio platform.



Use Cases and Benefits

- ✓ **Endpoint Compliance** – Monitor key device attributes such as location and encryption status to track compliance.
- ✓ **Maintain Security Posture** – Report on and repair the health of critical applications such as Microsoft BitLocker, SCCM, and Defender ATP to maintain the client's security posture.
- ✓ **Device Lifecycle Management** – Wipe devices as part of decommissioning end-of-life devices or reassigning devices at the end of an employee's tenure. Ensure sensitive data (e.g. personally identifiable information, financial details, corporate IP) is secured and can't be accessed maliciously.
- ✓ **Protect Devices** – Freeze or wipe devices that are lost, stolen or compromised to ensure threat actors can't access them and the corporate network illegally to initiate cyberattacks.
- ✓ **Device Audits** – Obtain a certificate of sanitization for every completed device wipe as proof during audits.
- ✓ **Minimize Unplanned Downtime** – espond to mass-scale IT or security incidents such as ransomware by restoring compromised endpoints within client environments back to a fully trusted and compliant state. Minimize downtime to clients' operations and impact on business.

For more information about Resilience for ConnectWise, check out the **product's landing page** and **ConnectWise Marketplace listing**.

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.

Learn More