BW OFFSHORE

CASE STUDY

Absolute Secure Endpoint Provides BW Offshore with Full Endpoint Visibility and Control

Using Absolute Secure Endpoint, BW Offshore Improves IT Efficiencies and Asset Management

BW Offshore is a global provider of floating production services, engineered to progress the future of energy. Founded in 1982, the company is headquartered in Singapore and Oslo, Norway, but operates globally, with a presence in the Americas, Europe, Africa, and Asia.

/ABSOLUTE®

THE STORY

Guarantee Uninterrupted Visibility Across Device Fleet

BW Offshore has a global presence, often with multiple worksites and employees travelling around. One of BW Offshore's biggest challenges was not having visibility into its global device fleet. "I do believe you can't secure what you can't see," explained Peter Tham, Technical Lead, Servers and Hardware at BW Offshore. To mitigate risk and prevent incidents of stolen devices or data from occurring, BW Offshore needed to find a solution that could provide its team with constant endpoint visibility and more security capabilities, including the ability to freeze the device or wipe data remotely.
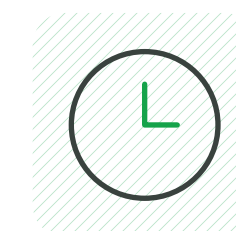
SECURITY NEEDS
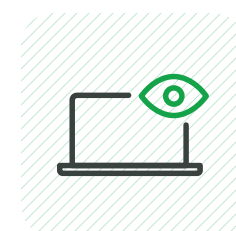
COMPLETE ENDPOINT
VISIBILITY

REPAIR MISSION-
CRITICAL APPLICATIONS

SAVES TIME
AND MONEY

THE SOLUTIONS

How They Did It

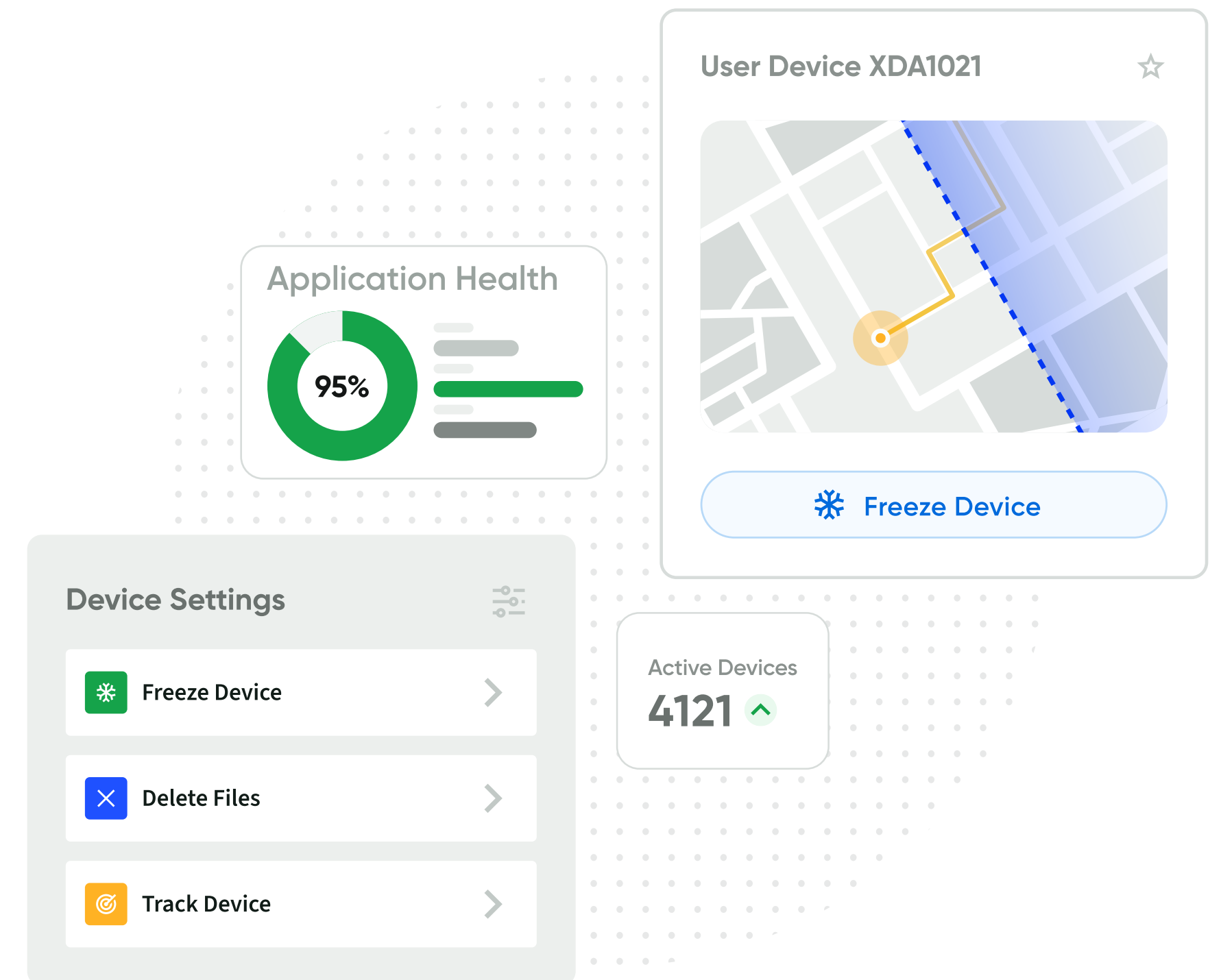### Improve Missing and Offline Device Return Rates

Absolute Secure Endpoint was recommended to BW Offshore by Dell, which was already embedded in its fleet of Windows devices. Initially, Absolute Secure Endpoint was deployed to BW Offshore's IT teams' devices to test out the capabilities. Satisfied with its performance, Absolute Secure Endpoint was deployed to the majority of BW Offshore's device fleet. Once deployed, BW Offshore's IT team was surprised to see their device fleet grow, due to some offline devices not being effectively managed or accounted for; many of these devices have been offline for months, some over a year. This kicked off a project to locate and return these offline devices from various locations across the globe.

Safeguard Devices and Data to Keep Devices Compliant

Now armed with greater visibility and control across its device fleet, BW Offshore is able to see any devices that are non-compliant, with some of these devices having been reformatted outside the company's standard system. With Absolute Secure Endpoint's remote freeze and file delete capabilities, BW Offshore can freeze and wipe these non-compliant devices, ensuring their data remains secure.

Ensure Mission-Critical Applications Remain Installed and Healthy

In addition to Absolute Secure Endpoint's ability to monitor, locate, and manage devices on or off the corporate network, BW Offshore also leverages other capabilities provided by this solution. BW Offshore also enables Absolute Application Resilience to ensure its critical applications remain installed and in a healthy state, while also repairing any applications that are not working well, helping reduce IT support time. BW Offshore also leverages Absolute's End User Messaging capability to send a message to users with malware detected on their device; this allows the BW Offshore IT team to remotely freeze the device while waiting for the user to respond, further preventing the malware from spreading or escalating.

User Device XDA1021 ☆

❄ Freeze Device

Application Health

95%

Device Settings ⚙

❄ Freeze Device →

✕ Delete Files →

◎ Track Device →

Active Devices
4121 ⌃

> ❝
>
> Absolute Secure Endpoint decreases a lot of the IT support time and creates a better user experience.

**PETER THAM,
TECHNICAL LEAD,
SERVERS AND HARDWARE,
BW OFFSHORE**

THE RESULTS

Complete Control of Endpoints Saves Time and Money

Now that BW Offshore has improved insights from Absolute Secure Endpoint into the devices that have been collected and not fully utilized, they have plans to launch an asset management system to better understand the devices they have in place and how they can be used or repurposed, saving IT time and money in purchasing new devices.

For the BW Offshore team, Absolute Secure Endpoint:

- ✓ Provides complete visibility across entire device fleet, whether on or off the corporate network
- ✓ Streamlines missing or offline device reclamation process, saving the IT team time and money
- ✓ Informs users of important messages regarding their device
- ✓ Enables IT to remotely freeze at-risk devices and remotely delete data, keeping devices secure
- ✓ Repairs mission-critical applications when they have been disabled or not running in a healthy state

/ABSOLUTE®

Absolute Software makes security **work**. We empower mission-critical performance with advanced cyber resilience. Embedded in more than 600 million devices, our cyber resilience platform delivers endpoint-to-network access security coverage, ensures automated security compliance, and enables operational continuity. Nearly 21,000 global customers trust Absolute to protect enterprise assets, fortify security and business applications, and provide a frictionless, always-on user experience.

Request a Demo