ECSO 911
EMERGENCY COMMUNICATIONS
OF SOUTHERN OREGON

PUBLIC SAFETY

CASE STUDY

Emergency Communications of Southern Oregon Secures Endpoints and Field Officers

Emergency Communications of Southern Oregon Leverages Absolute Secure Endpoint to Meet Compliance and Security Demands

Emergency Communications of Southern Oregon (ECSO) is an emergency dispatch facility that provides public safety communication services for more than 200,000 residents and dispatch for 28 agencies. ECSO's small IT team supports the agency's entire network infrastructure, including servers and workstations, as well as always-operational mobile devices located in 220 fire and police vehicles.

> I was really impressed with Absolute's ability to see any device and remotely freeze or wipe it, as well as to monitor and prove encryption status. Field officers also need uninterrupted access to crucial data to make the right decision on the appropriate protocol in seconds, so keeping their computers up and running with Absolute Secure Endpoint could save their lives.
>
> COREY NELSON,
> MANAGER, IT, ECSO

THE STORY

Ensure Endpoints Remain in IT's View

When it comes to law enforcement and public safety organizations, protecting data and devices is a must. The stringent Criminal Justice Information Services (CJIS) Security Policy requires ECSO devices to be under IT control at all times. The challenge for ECSO came when the VPN connection between the network and the mobile devices in the field was broken. The lack of visibility and control over endpoints also had the potential to create critical situations for police officers and other emergency personnel.

Officers need to be able to use their devices securely in the field to aid in response and investigations. With this in mind, the IT team sought a solution that could help them ensure endpoints in the field remain visible to IT and connected to the network at all times. It was vital to ensure applications on all devices were working, and those that were not could be remediated using automation. The final piece was the ability to prove device encryption and the capability to wipe devices remotely as part of CJIS compliance.

SECURITY CHALLENGES

CJIS COMPLIANCE

INCREASED EFFICIENCY

SAVES LIVES

THE SOLUTIONS

How They Did It

Improved Control and Visibility of Endpoints in the Field

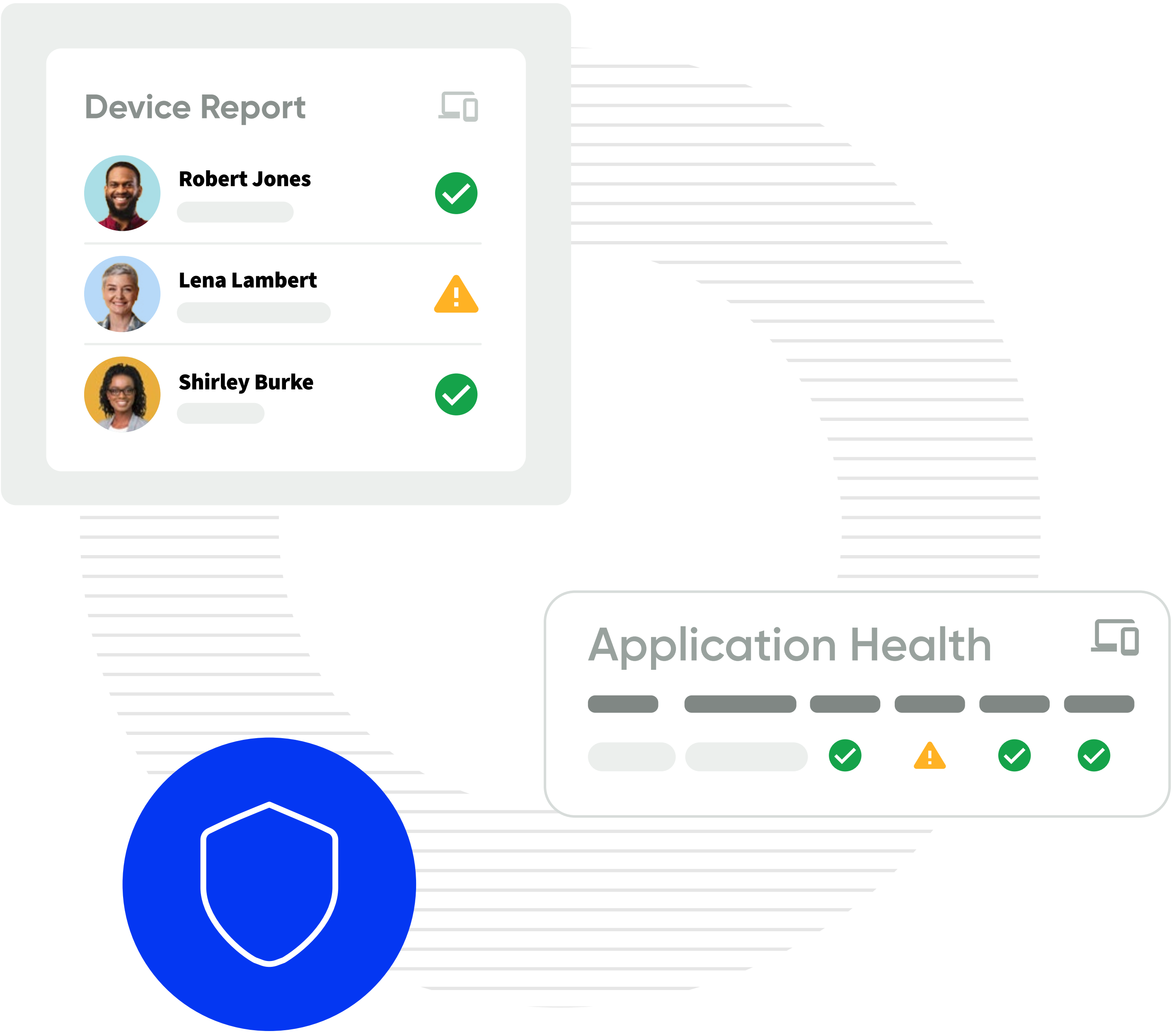
By leveraging Absolute Secure Endpoint, ECSO gained improved visibility and control over their devices in the field. “I’ve now got a single pane of glass to see each device and its status,” said Corey Nelson, Manager of IT at ECSO. “It’s been wonderful seeing where our devices are and all the information about them. I don’t have to worry or dig into the data. I just turn on the reports I want and let Absolute tell me, ‘hey, you need to look at this; there’s a problem here.’”

Keeping Mission-Critical Applications Accessible and Connected

Uninterrupted access to critical applications and data allows field officers to follow situation-appropriate protocols. Absolute Secure Endpoint enables IT to make those mission-critical applications that are covered in the Absolute Application Resilience™ catalog resilient to external factors, keeping them available for field officers who rely on the information when deciding which protocol to use. “Field officers need crucial data to make the right decision in seconds,” Nelson continued. “So keeping their computers up and running with Absolute could save their lives.”

Maintaining Compliance Through Asset Management

Deploying Absolute Secure Endpoint means the ECSO IT team can see, manage, and secure their endpoints. It is now much easier for ECSO to comply with CJIS Security Policy through device tracking, encryption status monitoring, and remote-wipe capabilities.



> If we see some unusual activity, we notify the local security officers and the agency. Depending on the risk, we can either freeze or wipe the computer. I was really impressed with Absolute's ability to still see that device, check its status, and remotely freeze or wipe it, as long as it has any kind of Internet connection, even if all the security has been removed, which is a great feature I never expected.
>
> COREY NELSON,
> MANAGER, IT, ECSO

THE RESULTS

Secured Endpoints + Uninterrupted Access = Saved Lives

Instant deployment and automated processes free up IT for other mission-critical tasks. With a lean team, any time saved can be put toward ensuring the personnel in the field are optimally set up to help protect their community. For the ECSO team. Absolute Secure Endpoint:

- ✓ Helps ECSO comply with CJIS Security Policy mandates
- ✓ Provides a quick deployment, improving IT efficiency
- ✓ Enhances the IT team's visibility and control of devices in the field

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