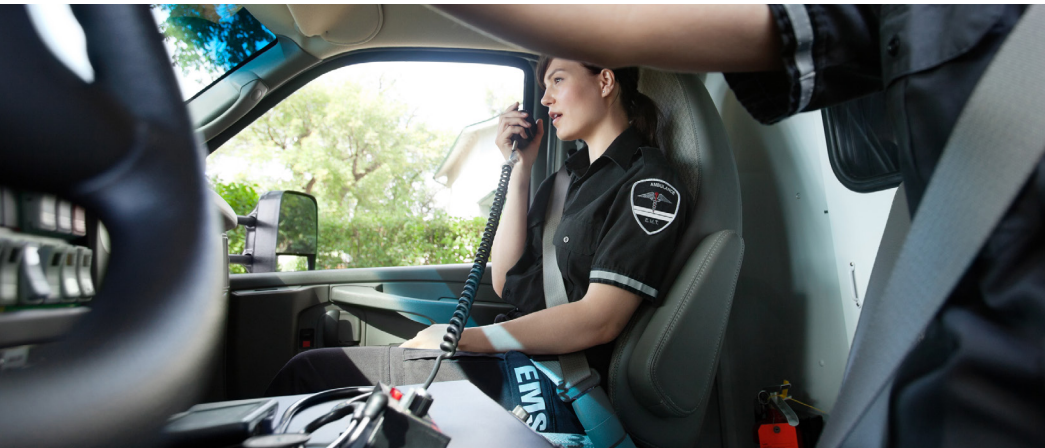# Emergency Communications of Southern Oregon Secures Endpoints and Field Officers

BACKGROUND

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.

CHALLENGE

The stringent Criminal Justice Information Service (CJIS) Security Policy requires ECSO devices to be under IT control at all times. The challenge for ESCO came when the VPN connection between the network and the mobile devices in the field were broken. The lack of visibility and control over endpoints also had the potential to create critical situations for police officers and other emergency personnel. The IT team needed a solution that would help them:

- Prove device encryption and remote-wipe capability to meet CJIS regulations

- Ensure endpoints in the field remain in IT's view and connected to the network at all times

- Ensure applications on all devices were working and remediation could be automated if broken

RESULTS

Save Lives

CJIS Compliance

Increased Efficiency

INDUSTRY   GOVERNMENT

PLATFORM

Government entity achieves CJIS compliance through Absolute's self-healing technology.

SOLUTION

By activating Absolute across their endpoints, 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. It's been wonderful seeing where our devices are, and all the information about

/ABSOLUTE®

absolute.com

"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 could save their lives."

COREY NELSON,
MANAGER, IT, ECSO

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,'" said Corey Nelson, Manager of IT.

Uninterrupted access to critical applications and data allows field officers to follow situation-appropriate protocols.

With Absolute providing persistence of applications, IT can also keep critical applications and data 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."

RESULTS

Deployment of Absolute means the ECSO IT team can see, manage, and secure their endpoints. It is now much easier for ECSO to comply with CJIS too, 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," said Nelson.

Instant deployment and automated processes frees 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 more information about Absolute's solutions, please visit: **absolute.com**

ABOUT ABSOLUTE

Absolute empowers more than 12,000 customers worldwide to protect devices, data, applications, and users against theft or attack — both on and off the corporate network. With the industry's only tamper-proof endpoint visibility and control solution, Absolute allows IT organizations to enforce asset intelligence, automated agent remediation, and data compliance for today's remote digital workforces. Absolute's patented Persistence® technology is embedded in the firmware of Dell, HP, Lenovo, and other leading manufacturers' devices for vendor-agnostic coverage, tamper-proof resilience, and ease of deployment. See how it works at **absolute.com** and follow us at **@absolutecorp**.

EMAIL:
sales@absolute.com

PHONE:
North America: 1-877-660-2289
EMEA: +44-118-902-2000

SALES:
absolute.com/request-info

WEBSITE:
absolute.com

/ABSOLUTE®

absolute.com