



Employees trust voices. Attackers know it.

Voice communication is still implicitly trusted even when the speaker’s identity is unverifiable. isVerified closes this risk gap for employee-to-employee voice calls in the Public Sector.

Your security stack has a gap.

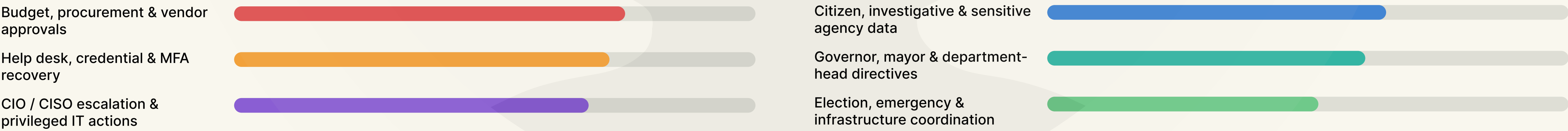
MFA verifies the account. EDR protects the device. Email security inspects the message.

But what happens when a trusted voice says “reset my MFA,” “approve this vendor,” or “take this system offline”?

Right now you have no technical control proving who is actually on the other end of the call.

- ✓ Network traffic & endpoints
- ✓ Email (phishing, spoofing)
- ✓ Identity & access (MFA, SSO)
- ✓ Physical access & devices
- ✗ **Voice communications — unverified**

WHERE A CLONED VOICE CAN BECOMES AN OPERATIONAL EVENT



ISVERIFIED CLOSES THE GAP

Verified identity. Verified voice. Every protected call.

Help desk, identity, finance, executive protection and managed security all converge around these workflows. The opportunity is to add technical identity assurance at the moment existing controls are weakest.

For More Information:
publicsector@isverified.ai

