Survey: Federal Government Data Remains Unsecure at the Edge

Recent survey of 200 federal decision-makers, from both defense and civilian agencies, shows disconnect between leadership and security practitioners around data protection.

Scottsdale, AZ - JUNE 26, 2019 - Acronis SCS, a data security and cyber protection company, in partnership with research firm Market Connections, released the findings of a survey of 200 federal decision-makers, from both defense and civilian agencies, on perceptions and practices regarding edge data security. The survey report describes edge data as data at rest or in transit outside of a data center, and that with the proliferation of IoT devices and an increasingly mobile workforce, security must extend to the very edges of agency networks.

The survey data shows a clear discrepancy between leadership and those directly on the front lines of security. It suggests leadership might be overstating levels of edge security knowledge, and be unaware of how vulnerable their agencies are.

- Senior executives (42%) and mid-management (66%) overall feel confident about their security posture, yet only one third of those in hands-on IT or technical roles feel positively about cyber security at the edge.
- 79 percent of senior executives considered themselves to know quite a bit or be an expert on edge security, while only 29 percent of IT staff can say the same.
- 48 percent of senior executives believe cloud backup solutions are how edge data is protected and secured in their agencies, supported by only 25 percent of technical practitioners.

“For any agency, lack of confidence from IT or security staff should raise red flags,” said Acronis SCS CEO John Zanni. “From the top down, agencies need to take a closer look at how they are protecting their datasets, and what tools and processes might need updating.”

The data from the survey also highlights a severe lack of knowledge of the edge environment and tools and best practices to secure edge data. Almost half of the respondents expressed concerns with the lack of IT staff knowledge and only nearly a third could say they have the appropriate tools and procedures in place. The majority of federal leaders are focused on traditional security methods, including encryption (70 percent), two-step authentication (64 percent), and antivirus (63 percent). But in the case of ransomware attacks where attackers simply reencrypt data, these traditional methods can only go so far; agencies need layers of protection to prepare for the inevitability of data loss.

“As an US Army officer who recently entered the civilian workforce, I have seen firsthand that agencies need edge data security solutions that are easy to implement, cost effective, and future-proof,” said Adam Morton, twenty-year military veteran and newly-named Director of Business Development for Acronis SCS. “Tools that can integrate with other technology solutions while offering utmost protection now and well into the future will help safeguard the nations data and our people.”

Download the full report, or learn more about Acronis SCS at acronisscs.com

About Acronis SCS

Acronis SCS is an American cyber protection and edge data security company dedicated to delivering products designed to meet the unique requirements of the U.S. Public Sector. The company’s innovative backup, anti-ransomware, disaster recovery and enterprise file sync and share products ensure data security across federal, state and local government, education, and non-profit computing environments. Acronis SCS products are built, validated by sophisticated third-party agencies, and supported in the United States by U.S. citizens.

Press Contact:
Emily Goodwin - goodwin@merrittgrp.com
703.380.7740