Axcess Payment Services deploys GuardWare to close data protection gap in remote-first environment

Thursday 23 July, 2026

Leeds-based payments firm selects persistent, file-level encryption platform to underpin PCI DSS Level 1 compliance and defend against insider threat and supply-chain risk

Axcess Payment Services, the Leeds-based regulated payments business, has partnered with GuardWare to address a material gap in its data security architecture, the point at which sensitive data leaves controlled environments entirely.

The deployment, documented in a white paper authored by Axcess Payments Group CEO Nick Fox, marks a strategic shift in the company's security posture: from infrastructure-centric defence to persistent, data-centric protection that follows files wherever they are, regardless of location, device, or network state.

Axcess Payment Services operates as a PCI DSS Level 1 compliant organisation, the highest tier of the payment card industry's data security standard, and runs a security stack that includes CrowdStrike Enterprise, Microsoft Defender, Microsoft 365, and AWS-native controls. Despite sustained investment in these platforms, a structured internal review identified a critical limitation shared by all of them: none provide persistent file-level protection once data leaves controlled environments.

In a remote-first organisation, where data routinely crosses device, network, and organisational boundaries, that limitation is significant. Encrypted at rest and in transit, files become readable the moment they are opened, including by an unauthorised party who has obtained them through exfiltration, insider action, or supply-chain compromise.

"We adopted the assumption that data compromise is possible," Fox states in the white paper, "and that controls must ensure any exfiltrated data remains unusable to an attacker."

“Following a structured market evaluation, we selected GuardWare for its ability to extend protection to the data itself rather than the perimeter containing it. The platform's three core modules, Insight, Discover and Protect, introduce a data-centric security layer that operates independently of network boundaries and persists across all data states, including during active use,” explained Fox.

Protect applies hybrid AES-256 and RSA-2048 encryption at the file level, with unique per-file keys, automated rotation, and decentralised key management that eliminates single-point compromise. Critically, encryption is maintained not just at rest and in transit, but while files are being actively used, a capability that directly addresses the window of exposure that conventional controls leave open. Discover performs deep content inspection across endpoints, Microsoft 365, and SharePoint environments, including data embedded within images, a vector that routinely evades conventional data loss prevention tools. And Insight provides real-time visibility into data movement, anomalous access patterns, and potential exfiltration activity across online, offline, and air-gapped environments.

The white paper sets out a detailed mapping of GuardWare capabilities to ten specific PCI DSS Level 1 requirements, covering stored cardholder data protection, cryptographic key management, least-privilege access enforcement, forensic audit trail generation, and incident response.

Key points of alignment include the ability to render cardholder data unreadable even after exfiltration, identity-bound access controls that apply beyond the corporate perimeter, and the capacity to instantly revoke access or destroy encryption keys during an active incident, enabling rapid containment without relying on network-level controls.

“The deployment responds to a threat environment that we characterise as increasingly difficult for perimeter-based defences to address. The white paper identifies AI-driven phishing and social engineering, deepfake impersonation targeting financial workflows, ransomware-as-a-service operations, and advanced persistent threats as among the primary vectors now bypassing traditional network controls, all of which target users and data rather than infrastructure,” concluded Fox.

Supply chain and third-party access risk is identified as a particular concern, with GuardWare's file-level governance extending access controls to external participants regardless of the device or network.

Media:

Related Sectors:

Business & Finance :: Computing & Telecoms :: Crypto Currency :: Public Sector & Legal ::

Related Keywords:

Cybersecurity ::

Scan Me:

"Nick's comments reflect exactly what we're seeing across the payments sector: the assumption that a breach is a question of when, not if, and there is a need to protect the data itself rather than just the environment around it," said Ian McKinley, CEO of GuardWare. "Payment files carry some of the most sensitive information any organisation handles, and once they leave a controlled network, traditional perimeter tools simply can't follow them. Our platform keeps encryption and governance attached to the file itself, whether it's sitting in storage, moving through a supply chain, or open on a remote device, so the data stays worthless to anyone who shouldn't have it. Working with a PCI DSS Level 1 provider like Axcess shows how data-centric security can sit alongside existing tools like CrowdStrike and Microsoft Defender to close that gap. It's a model we believe the wider payments industry will need to adopt as attackers keep shifting their focus from networks to the data itself. However, preparing for the inevitability of a data security breach is not unique to the payments industry; it is incumbent on all industries, whatever their sector or operation.

Axcess Payment Services reports that the GuardWare deployment strengthened evidence of PCI DSS Level 1 compliance, reduced exposure to insider and supply chain risks, improved forensic visibility and audit readiness, and maintained productivity across remote and offline workflows, with no operational disruption to existing Microsoft, AWS, and CrowdStrike environments.

–ends–

Company Contact:

GuardWare

T. 01433445001
E. paul@vividink.info
W. https://guardware.com/

Additional Contact(s):
Paul Richardson

View Online

Additional Assets:

Newsroom: Visit our Newsroom for all the latest stories:
https://www.guardware.pressat.co.uk