

Cyber Resilience Isn't a Press Release

When corporate giants shrug off trust, it's the cyber defenders left holding the bag.

Dave Hoon
Chief Technology Officer, Norseman Defense Technologies · February 2026

Another "oops" from a big-name vendor has been in the news lately. When corporate giants shrug off trust, it's the government networks and—more importantly—the cyber defenders left holding the bag.

At Norseman, we don't shrug trust.

The Structural Problem

Federal agencies depend on a complex ecosystem of commercial vendors. That dependency is unavoidable—agencies can't build everything themselves. But it creates a structural vulnerability: the security posture of a federal network is only as strong as the weakest vendor in its supply chain.

Supply chain attacks have caused some of the most significant federal security incidents of the past decade. The answer isn't to stop using commercial vendors. It's to build architectures that don't implicitly trust them.

Zero Trust Extends to Vendors

Zero Trust is most commonly discussed in the context of user access. But the same principle applies to vendor software and vendor-managed systems. A Zero Trust architecture for vendor risk means:

- **Least-privilege access for vendor systems.** Vendor tools should not have broader access than they need. Every permission granted is a potential attack surface.

- **Network segmentation.** Vendor-managed components should operate isolated from sensitive mission data. Lateral movement from a compromised vendor system should be architecturally impossible—not just policy-prohibited.
- **Immutable backups.** When a vendor system is compromised, recovery capability determines mission impact. Immutable backups that can't be encrypted or deleted by ransomware—even ransomware that has compromised vendor credentials—are non-negotiable.
- **Continuous monitoring.** Vendor behavior should be monitored with the same rigor as user behavior. Anomalous data access by a vendor system should trigger the same response as a compromised user account.

Norseman + Rubrik

We pair with Rubrik to lock down data with zero-trust security and ensure rapid recovery—because resilience isn't a press release, it's a requirement.

Rubrik's architecture ensures backup data is immutable and recoverable even when primary systems—including vendor-managed systems—are fully compromised. Combined with Norseman's network architecture and compliance expertise, agencies get a recovery capability that doesn't depend on trusting that a vendor had good security practices.

Explore our **Zero Trust Architecture** and **compliance** use cases. Procurable via **ITES-4H**, **SEWP V**, **SEWP VI**, and **CIO-CS**. SEWP VI ordering opens November 1, 2026, and SEWP V ordering is extended through January 31, 2027.

Published at norseman.com/insights/cyber-resilience-vendor-trust. To talk with Norseman Defense Technologies, call 410.579.8600 or email sales@norseman.com.