

the hidden risks of multi-vendor technology stacks

More vendors don't always mean less risk.

Many financial institutions adopt a "best-of-breed" technology strategy to diversify vendors. While this approach can appear safer on the surface, it often introduces new challenges that increase operational complexity, cybersecurity exposure, and accountability issues.

Understanding these trade-offs can help you make more informed technology decisions and strengthen your overall risk management strategy.



Increased Complexity

more providers



more integration



more complexity



more more risk



Every additional provider introduces another connection, workflow, and relationship to manage – creating the need to integrate each of these disparate solutions and resulting in higher costs, risk, complexity, and maintenance requirements. As advanced AI accelerates vulnerability discovery and attack execution, that complexity can become more difficult to secure and manage.

Bigger Attack Surface

As your vendor count rises, so does your cybersecurity risk.

Cybercriminals don't need to attack your primary systems. They only need to find the weakest link in your vendor ecosystem to springboard onto your network. Advanced AI accelerates vulnerability discovery and attack execution which leaves larger vendor ecosystems to face increased exposure to cyber risk.

Less Security Visibility

More vendors = less visibility into your overall security posture.

Advanced AI can accelerate the identification and exploitation of security gaps, making end-to-end visibility more critical across complex environments.

While security tools can help monitor your environment, they can't provide complete visibility into each vendor's security stack, creating:

- Limited insight into third-party security controls
- Visibility gaps in your security posture
- Reduced effectiveness of security monitoring
- Slower identification of threats

Less Accountability

When an issue occurs, multiple vendors often mean multiple parties investigating, troubleshooting, and assigning responsibility.

- Who owns the problem?
- Who owns the outcome?
- Who will pay if you can't serve your accountholders and lose business?
- Who should have caught the security gap?



The result: longer resolution times, more finger-pointing, and greater impact on your accountholders.

Reduced Effectiveness

Performance issues frequently require involvement from multiple vendors, each with limited visibility into only part of your environment.

A more integrated approach can provide:

- Greater end-to-end visibility
- Faster troubleshooting
- Improved security oversight
- More efficient operations

The more disconnected systems you manage, the harder it becomes to identify and resolve issues.



The Bottom Line

Vendor diversification may reduce dependence on a single provider, but it can also increase complexity, cybersecurity exposure, visibility gaps, and operational inefficiencies. Operational simplicity isn't just an efficiency benefit anymore. In an AI-driven threat landscape, it can become a security advantage. Evaluating the trade-offs can help you build a technology strategy that balances resiliency, security, and performance.



operational simplicity can become a security advantage in an ai-driven threat landscape.

your cloud. our expertise.

Bring security, resilience, compliance, and proactive management together with a cloud model built around your financial institution's needs with [Jack Henry® Managed Secure Cloud](#), delivered through the Gladiator® Suite of Services.

For more information about Jack Henry®, visit [jackhenry.com](#).