



CYBERSECURITY STANDARDS ENABLE SECURE, ENTERPRISE- CLASS SERVERS

August 2025

Derek E. Brink, CISSP

Vice President and Research Fellow, Cybersecurity and IT GRC

Executive Summary

Modern, enterprise-class servers that adhere to rigorous cybersecurity standards are well-positioned to **protect sensitive data, defend against emerging threats**, and **ensure rapid recovery** from unplanned downtime. This Aberdeen Knowledge Brief highlights the role of cybersecurity standards in achieving these important business outcomes, and underscores how selecting servers that leverage these standards to support a handful of critical capabilities makes it easier to build and sustain a secure, compliant, and resilient computing infrastructure.

Start with the end in mind: Be clear about the most important business outcomes.

From Aristotle (d. 322 BCE) to Stephen Covey (d. 2012), humans have been reminded to focus first on their desired *outcomes*, and then on the required *actions*. First the ends, then the means.

In the context of cybersecurity for enterprise-class servers, three of the most important business outcomes are:

1. Protect Sensitive Data from Unauthorized Access

In our digital age, safeguarding valuable and sensitive data is fundamental for maintaining trust, privacy, and compliance with regulatory requirements.

In Aberdeen's recent research, **nearly three out of five (58%)** respondents experienced one or more cybersecurity-related incidents in the previous 12 months that resulted in unauthorized access to enterprise data.

Cybersecurity standards to support this goal generally emphasize encryption, identities and authentication, and access controls designed to ensure *data confidentiality* and *data integrity*.

2. Defend Against Emerging Threats

Years of relentless headlines of successful cybersecurity incidents have broadly raised awareness about the threats of data breaches, ransomware, and intellectual property theft. Perhaps less widely known is the growing frequency and sophistication of attacks targeting firmware, BIOS, and cryptographic systems.

Cybersecurity standards to address this goal include those that mitigate cybersecurity risks at the hardware and firmware levels.

In addition, forward-looking standards bodies and solution providers are already working on ways to mitigate future threats, for example:

- ▶ **Post-Quantum Cryptography (PQC)**, which refers to emerging public-key encryption algorithms that are designed to be implemented today, while providing future protections against known threats to public-key encryption from quantum computers.
- ▶ **Perfect Forward Secrecy (PFS)**, which refers to the frequent and automatic replacement of encryption keys to minimize the amount of data exposure if those keys are accessed by unauthorized parties.

3. Ensure Resilience and Rapid Recovery

Modern organizations face relentless challenges — from IT outages to global crises — that require rapid and reliable detection, response, and recovery to keep their digital operations running and their people safe.

In Aberdeen's recent research, **about eight out of nine (88.5%)** respondents experienced one or more cybersecurity-related incidents in the previous 12 months that resulted in the unplanned downtime or slowdown of enterprise endpoints, networks, applications, or data.

Continuous data protection capabilities (e.g., storage, backup, recovery) are key to *operational resilience*, accelerating time-to-recovery and minimizing negative business impact. Note that the *personal resilience* of the organization's technical staff (e.g., based on complementary "soft skills" such as communication, collaboration, and conflict resolution) has come to be equally important to the traditional "hard skills" related to technologies.

Security standards and frameworks to address these goals include a mix of higher-level capabilities to manage cybersecurity risks — particularly *Detect, Respond, and Recover*.

Select the servers that are designed to help you achieve your key business outcomes.

By selecting enterprise-class servers that support relevant cybersecurity standards, you're making it easier to build and sustain a secure, compliant, and resilient computing infrastructure. Table 1 summarizes several buying considerations that map directly to our three important business outcomes.

Table 1: Buying Considerations for Secure Enterprise-Class Servers, in Support of Key Business Outcomes

Key Business Outcomes	Secure Enterprise-Class Server Capabilities that Support These Business Outcomes	Cybersecurity Standards and Frameworks that Underpin Enterprise-Class Server Capabilities (illustrative)
<p>Protect Sensitive Data from Unauthorized Access</p>	<p>Hardware-Based Security Features</p> <ul style="list-style-type: none"> Look for servers with a <i>silicon root of trust</i> to ensure firmware integrity from manufacturing to end-of-life. Seek tamper-evident designs and secure boot processes to prevent unauthorized modifications. For more information, see 8 Ways a Silicon Root of Trust Can Lay the Foundation of Security and Integrity for Your Business-Critical Servers. 	<p>NIST SP 800-171: Protecting Controlled Unclassified Information</p> <ul style="list-style-type: none"> Secure firmware updates to prevent unauthorized modifications. Encryption support for data protection. Role-based access control for critical functions. <p>NIST SP 800-53: Security and Privacy Controls for Information Systems</p> <ul style="list-style-type: none"> Role-based access controls (RBAC) for restricted access. Integrated logging and monitoring for auditing and accountability. <p>NIST SP 800-88: Guidelines for Media Sanitization</p> <ul style="list-style-type: none"> Secure erase functions for storage devices to comply with media sanitization guidelines.
<p>Defend Against Emerging Threats</p>	<p>Advanced Cryptographic Capabilities</p> <ul style="list-style-type: none"> Prioritize servers with standards-validated cryptographic modules for high-assurance encryption. Ensure support for quantum-resistant algorithms to future-proof against quantum threats. <p>Management and Automation Tools</p> <ul style="list-style-type: none"> Choose servers with integrated management systems for remote monitoring, updates, and threat detection, aligning with an emphasis on proactive risk management. Look for automation features to streamline ongoing patch management and compliance checks. 	<p>FIPS 140-3: Cryptographic Module Security</p> <ul style="list-style-type: none"> Validated cryptographic algorithms and modules. Secure storage of sensitive data. Secure management communications. Tamper-detection mechanisms. <p>Forward-looking initiatives</p> <ul style="list-style-type: none"> Post-Quantum Cryptography (PQC) Perfect Forward Secrecy (PFS) Commercial National Security Algorithm (CNSA) Suite <p>NIST SP 800-53: Security and Privacy Controls for Information Systems</p> <ul style="list-style-type: none"> Secure boot and firmware validation for system integrity. <p>NIST SP 800-193: Platform Firmware Resiliency</p> <ul style="list-style-type: none"> Secure boot for firmware integrity. Runtime verification for detecting unauthorized changes. Automatic recovery mechanisms for restoring firmware. <p>NIST SP 800-147B: BIOS Protection</p> <ul style="list-style-type: none"> Secure boot and secure firmware updates for BIOS integrity.

		<ul style="list-style-type: none"> • Cryptographic signing of BIOS updates. • Recovery mechanisms for BIOS.
<p>Ensure Resilience and Rapid Recovery</p>	<p>Resiliency and Recovery Mechanisms</p> <ul style="list-style-type: none"> • Select servers with continuous data protection and rapid recovery capabilities to minimize downtime and support resiliency goals. • Ensure integration with zero-trust frameworks to isolate threats and maintain operational continuity. 	<p>NIST Cybersecurity Framework (CSF) 2.0</p> <ul style="list-style-type: none"> • Provides a voluntary framework to manage cybersecurity risks, with six core functions — <i>Identify, Protect, Detect, Respond, Recover, and Govern</i>. <p>These six core functions are further divided into 22 categories and 106 subcategories.</p> <ul style="list-style-type: none"> • For more information, see Cheers to the Governor: A Practical Guide for IT Pros on a Key Update to NIST Cybersecurity Framework (CSF) 2.0

Source: Aberdeen, August 2025

Summary and Key Takeaways

- ▶ In the context of cybersecurity for enterprise-class servers, three of the most important *business outcomes* are **protecting data from unauthorized access, defending against emerging threats, and ensuring resilience and rapid recovery**.
- ▶ Buying considerations for secure enterprise-class servers that support these business outcomes include a handful of *critical capabilities*, such as **hardware-based security features, advanced cryptographic capabilities, and resiliency and recovery mechanisms**.
- ▶ **Specific cybersecurity standards and frameworks** that underpin these critical server capabilities are numerous (see Table 1), underscoring the importance of selecting servers that align with these standards.
- ▶ **Selecting enterprise-class servers that align with these cybersecurity standards and support these critical capabilities** makes it easier for you to build and sustain a **secure, compliant, and resilient computing infrastructure**.

About Aberdeen Strategy & Research

Aberdeen Strategy & Research (a division of Spiceworks Ziff Davis), with over three decades of experience in independent, credible market research, helps **illuminate** market realities and inform business strategies. Our fact-based, unbiased, and outcome-centric research approach provides insights into technology, customer management, and business operations to **inspire** critical thinking and **ignite** data-driven business actions.

This document is the result of primary research performed by Aberdeen and represents the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent from Aberdeen.