Use of this framework
This document is part of the *Access Denied* collection by Jemma Davis. You are welcome to adapt or apply it for internal learning, accessibility planning, or research. If you intend to use it as part of paid consultancy, training, or commercial work, please request permission first at **info@accessdeniedbook.co**.

Vendor Security Product Accessibility Assessment Framework

When evaluating security vendor accessibility claims against real-world performance, systematic testing reveals concerning patterns. The following table illustrates common discrepancies between vendor statements and actual product functionality based on accessibility evaluations:

Assessment Area	**Critical Requirements**	**Verification Methods**	**Pass/Fail Criteria**
Screen Reader Compatibility	Must work with JAWS, NVDA, and VoiceOver	Independent testing with each screen reader on critical functions	All critical security functions must be operable with each screen reader
Keyboard Navigation	Complete keyboard navigability without mouse dependency	Testing all features with keyboard-only navigation	No functionality requiring mouse or touch interaction without keyboard equivalent
Visual Design	Minimum AA contrast ratios for all text and interactive elements	Automated contrast testing plus manual verification	No content below 4.5:1 contrast for normal text, 3:1 for large text
Navigation Structure	Consistent navigation patterns and predictable interactions	Structured user testing with diverse participants	No unexpected behaviour when navigating between sections
Error Handling	Clear error identification with specific recovery instructions	Testing of error states with assistive technologies	Errors must be programmatically identifiable with clear recovery instructions
Time Constraints	No time-limited functions without user-controlled extensions	Testing of all timed functions with various interaction speeds	All timed operations must allow extensions or adjustments
Independent Verification	Third-party accessibility audit (within last 12 months)	Review of complete audit reports, not just summaries	Audits must be conducted by certified accessibility specialists

User Testing Evidence	Recorded testing sessions with participants using assistive technologies	Review of unedited testing recordings	Must include users with various disabilities completing realistic security tasks
Remediation Planning	Specific, time-bound remediation plans for identified issues	Review of detailed roadmaps with accountabilities	Plans must include clear milestones and verification methods
Expertise Verification	Evidence of accessibility expertise within product team	Review of team qualifications and development processes	Must have dedicated accessibility resources with recognised qualifications
Compatibility Verification	Compatibility with your specific assistive technologies	On-site testing with your actual technology stack	Must work with your organisation's supported assistive technologies
Support Capabilities	Dedicated support for accessibility-related issues with SLAs	Review of support processes and historical performance	Clear escalation paths and resolution timeframes for accessibility issues