****

# Practices for Secure Software Report

**Table of Contents**

[**Document Revision History 3**](#_94s8siuhp6lv)

[**Client 3**](#_lo7sga6w89zr)

[**Instructions 3**](#_ux5u9c7zc0oe)

[**Developer 4**](#_u7f7viubaz4d)

[**1. Algorithm Cipher 4**](#_nlcpajw186f3)

[**2. Certificate Generation 4**](#_biuy97i9z8c)

[**3. Deploy Cipher 4**](#_68a4dktd3x7d)

[**4. Secure Communications 4**](#_mp0mh941pyfx)

[**5. Secondary Testing 4**](#_2e6wauiup40h)

[**6. Functional Testing 4**](#_t0hiyfgk7m3z)

[**7. Summary 4**](#_lgf7x2a3442v)

[**8. Industry Standard Best Practices 4**](#_z19dcwapvfbc)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **04/17/2025** | **Austin Antles** |  |

## Client



## Instructions

Submit this completed practices for secure software report. Replace the bracketed text with the relevant information. You must document your process for writing secure communications and refactoring code that complies with software security testing protocols.

* Respond to the steps outlined below and include your findings.
* Respond using your own words. You may also choose to include images or supporting materials. If you include them, make certain to insert them in all the relevant locations in the document.
* Refer to the Project Two Guidelines and Rubric for more detailed instructions about each section of the template.

## Developer

Austin Antles

## Algorithm Cipher

SHA-256 is a powerful security tool that creates a unique digital data fingerprint. It is a one-way process that turns any message into a fixed-length code. No matter how long or short your original data is, SHA-256 produces a 256-bit output (32 bytes long). This makes it perfect for checking if financial data has been changed during transfer. The National Security Agency created this method as part of the SHA-2 family, and it's now widely used in banking systems and cryptocurrency.

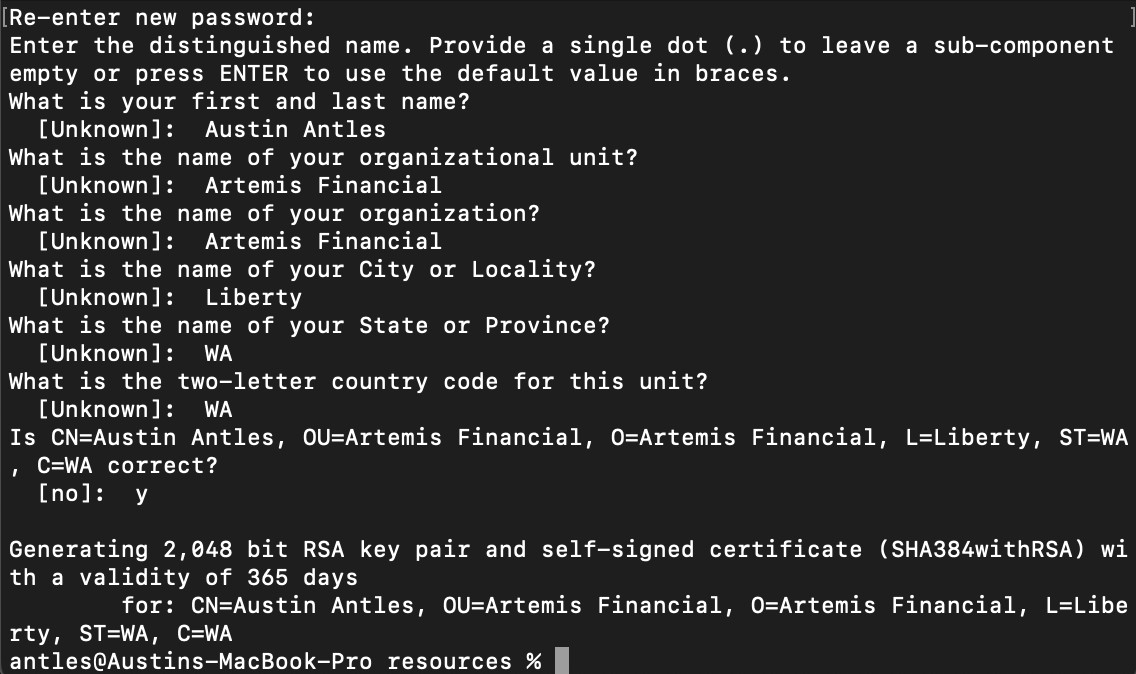
The strength of SHA-256 comes from how it handles data. It breaks information into chunks and runs them through multiple mixing steps. The process ensures that changing even a single character in the original message completely changes the output code. This 256-bit security level means it's practically impossible for attackers to create fake data that matches a real fingerprint. This protection is crucial for maintaining customer trust when working with Artemis Financial’s sensitive information.

While SHA-256 doesn't encrypt data (it only creates fingerprints), we can pair it with other security methods for complete protection. To encrypt actual financial data, we would add AES-256, which uses the same key for locking and unlocking information. For secure communications between Artemis Financial and its clients, we would implement RSA-2048, which uses different keys for sending and receiving. These systems work with SHA-256 to create a robust security approach that protects data in storage and during transfer.

SHA-256 has stood the test of time since its release in 2001. Unlike older methods like MD5 and SHA-1, which security researchers have broken, SHA-256 remains secure against all known attacks. Its proven track record makes it trusted by financial institutions worldwide. For Artemis Financial, implementing SHA-256 offers strong security and reasonable computing requirements, ensuring clients' financial data stays protected without slowing down their systems.

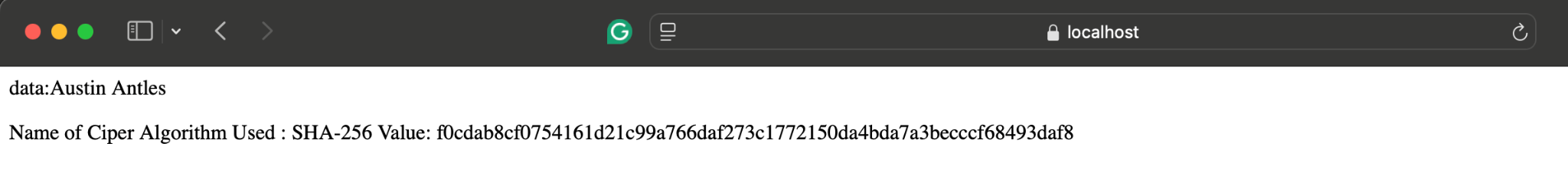
## Certificate Generation

Insert a screenshot below of the CER file.



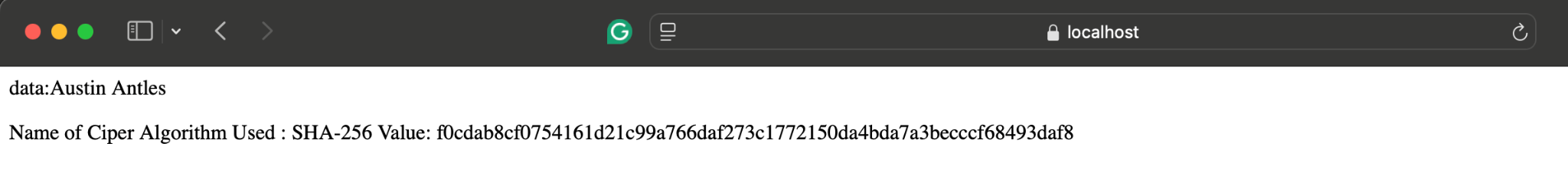
## Deploy Cipher

Insert a screenshot below of the checksum verification.



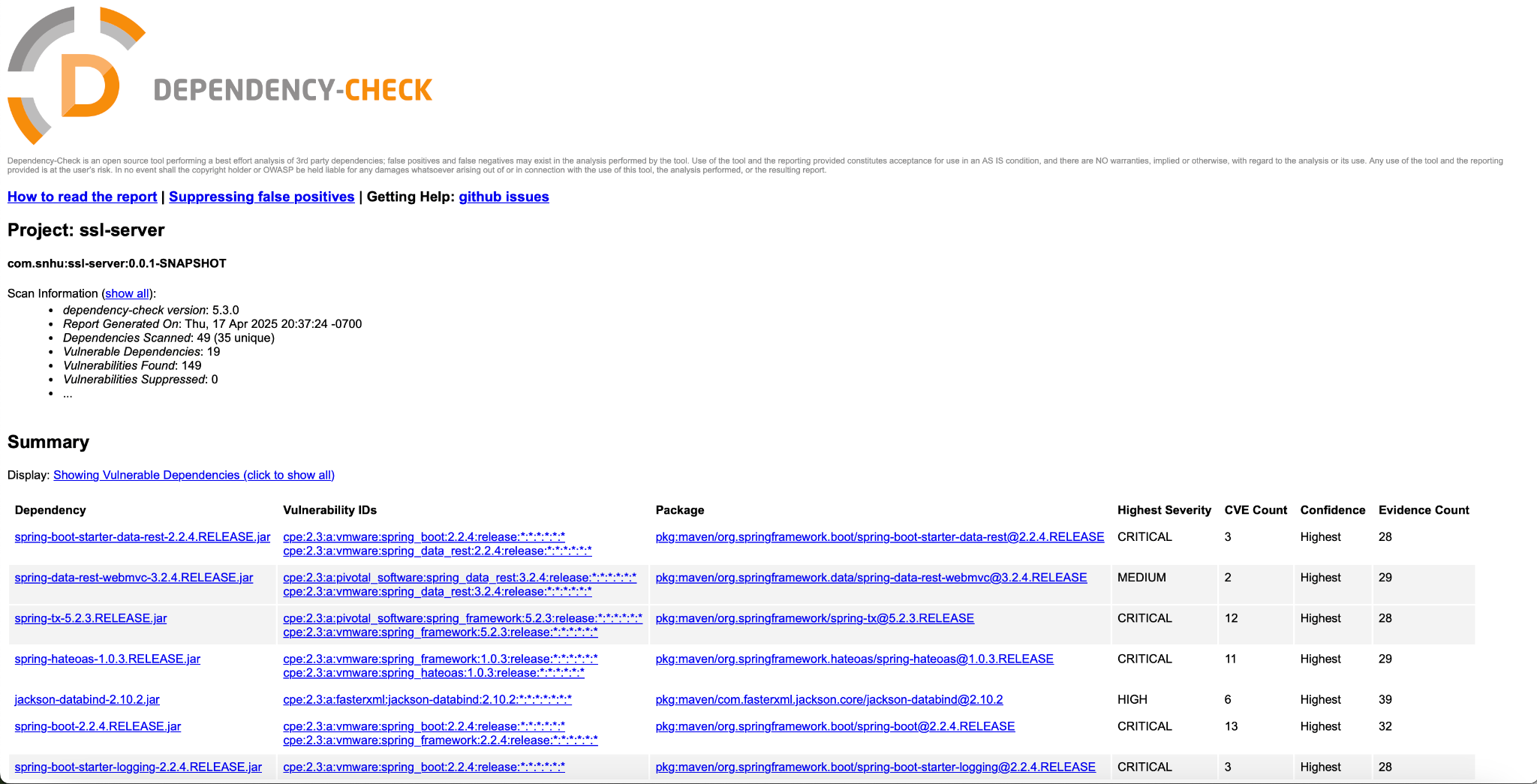
## Secure Communications

Insert a screenshot below of the web browser that shows a secure webpage.



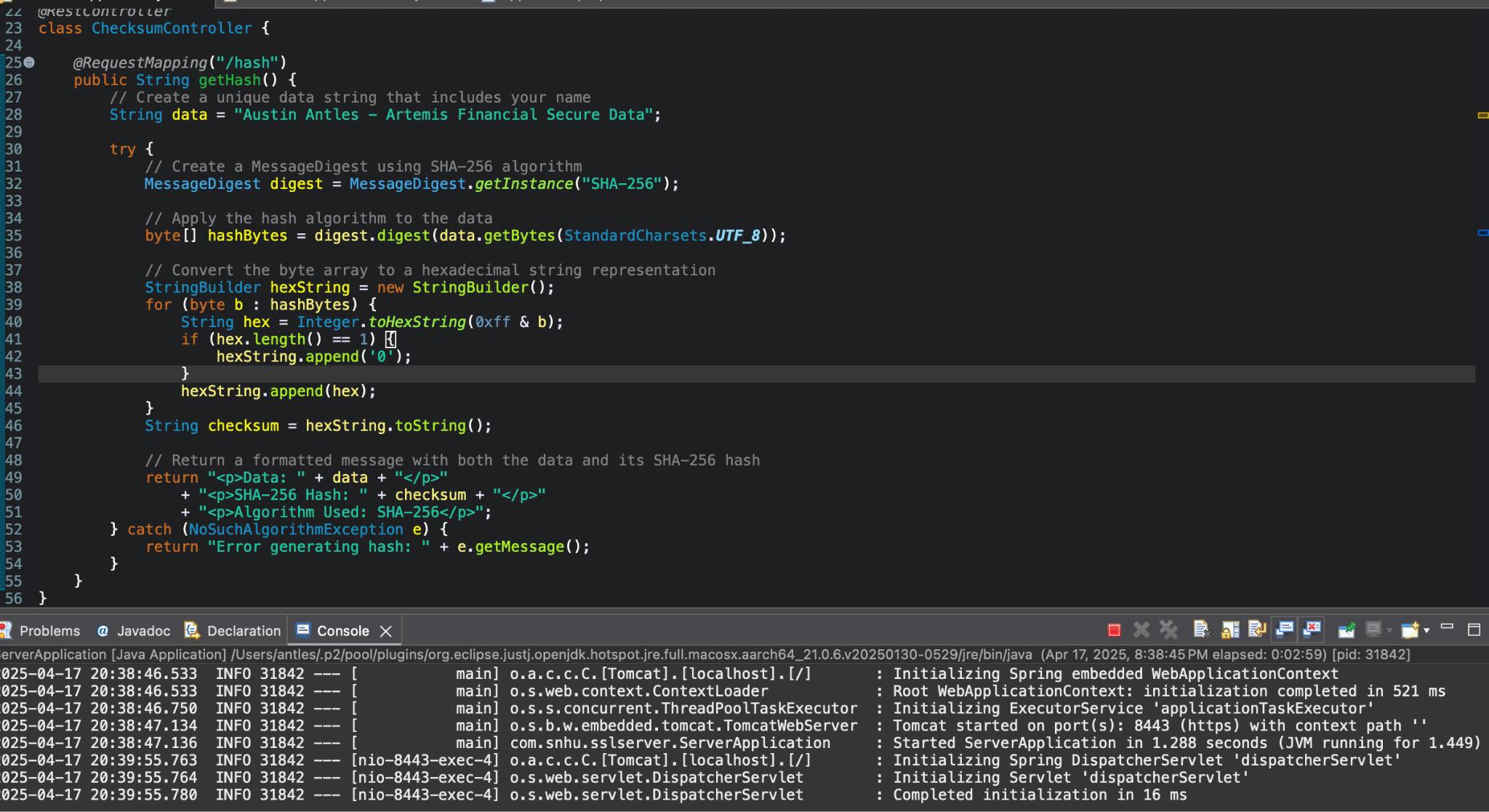
## Secondary Testing

Insert screenshots below of the refactored code executed without errors and the dependency-check report.



## Functional Testing

Insert a screenshot below of the refactored code executed without errors.



## Summary

My security enhancement approach for Artemis Financial's application addressed four critical vulnerability areas identified during the assessment. First, I implemented SHA-256 hashing to protect data integrity, creating digital fingerprints that make tampering immediately detectable. Next, I upgraded all communications from basic HTTP to encrypted HTTPS, preventing attackers from seeing sensitive financial information as it travels between systems. The certificate-based authentication I added ensures that clients connect only to legitimate Artemis Financial servers, not impostor sites. Finally, I conducted thorough dependency checks to eliminate vulnerable third-party components that could create hidden backdoors into the system.

This multi-layered security approach didn't happen by chance. I followed a methodical process, starting with understanding Artemis Financial's specific security needs. After selecting proven technologies rather than creating custom solutions, I carefully integrated these protections through targeted code changes. The testing phase was equally important. I verified functionality and security at each step, making adjustments when needed. This comprehensive approach means Artemis Financial now has several layers of defense working together. If one security measure fails, others remain active, significantly reducing the risk of successful attacks against client financial data.

## Industry Standard Best Practices

Throughout this project, I applied industry-recognized security practices that protect against common attack patterns. Instead of reinventing security solutions, I leveraged the OWASP Top 10 awareness framework to address critical risks like broken authentication and data exposure. I chose the battle-tested SHA-256 algorithm backed by extensive security research rather than creating custom cryptography that might contain unknown weaknesses. I created a defense-in-depth strategy that makes attacks significantly harder by implementing multiple security layers, hashing for data integrity, privacy encryption, and authentication certificates.

The practical value of these security improvements to Artemis Financial extends far beyond technical compliance. In the financial sector, security directly impacts business success. These enhancements help meet regulatory requirements like PCI DSS and GLBA, avoiding potential fines and legal complications. More importantly, they build client trust by seriously committing to protecting sensitive information. The financial impact is equally significant. Preventing a single data breach saves the company from remediation costs that often reach millions of dollars. Security-related system outages can halt business operations, making preventative security measures crucial for maintaining revenue streams. In today's competitive financial services market, robust security becomes a genuine market differentiator, helping Artemis Financial stand out when clients evaluate potential financial partners.