

Synthesize a solution to a potential real-life scenario

ACCA4024 NETWORKS AND CYBER SECURITY
ESSENTIALS

TOM OWEN (2520277)

Contents

Contents

Contents	1
Abstract	2
Introduction	2
Modern Threats Facing VTAM	3
Zero Trust Security Policies	3
Technical Mitigation Measures	4
Monitoring, Incident Response and Training	4
Conclusion	5
References	5

Abstract

This report examines the cyber security risks facing Vigilant Trust & Asset Management (VTAM), a medium-sized financial services company that has experienced phishing and ransomware-related threats. It proposes a modern security framework based on Zero Trust principles to strengthen the organisation's security posture. The report identifies current and emerging threats, outlines suitable security policies, recommends practical technical mitigation measures, and explains the importance of continuous monitoring, incident response, and staff awareness training. Together, these measures are intended to improve VTAM's resilience and reduce the likelihood and impact of successful cyber-attacks.

Introduction

Vigilant Trust & Asset Management (VTAM) is a medium-sized financial services company operating in a threat landscape where cyber-attacks are becoming increasingly advanced and frequent. The company has recently become the target of a sophisticated phishing campaign and an attempted ransomware attack. These events highlight weaknesses that could place sensitive data, operations, and customer trust at risk. Financial organisations such as VTAM are high-value targets because they handle sensitive data and critical services.

Traditional perimeter-based security is no longer feasible by itself in today's modern work environment, which is shaped by hybrid working, cloud adoption, mobile access, and increasingly convincing social engineering attacks [1], [2]. For this, VTAM needs to build a stronger and more modern approach to security threats. It must assume that threats may come from both outside and inside the network, and that users, devices and systems should not automatically be trusted.

This report proposes a modern security framework for VTAM based on Zero Trust principles [1], [3]. It examines current and emerging threats, suitable security policies, practical technical mitigation measures, and explains how continuous monitoring, incident response, and staff awareness training can improve the organisation's resilience against cyber threats.

Modern Threats Facing VTAM

VTAM faces both external and internal cyber threats, which are especially serious in the financial services sector [6]. Companies like VTAM are appealing targets because they handle sensitive financial and customer data and provide services that attackers may want to disrupt. RaaS (Ransomware-as-a-Service) has become a more common method of attack because criminals can rent ransomware tools without needing advanced technical expertise [4], [5], [6].

Another major threat is phishing and AI-powered vishing, which can manipulate employees into revealing confidential information, clicking malicious links, or authorising fraudulent actions [6]. VTAM also needs to recognise the risk of supply chain compromise, where attackers target third party software or services to exploit vulnerabilities or gain access to the organisation. Hybrid working and cloud adoption have also expanded the attack surface by increasing remote access, the use of multiple devices, and the risk of device and cloud misconfiguration [6], [9]. Internal threats must also be considered, as employees may accidentally or deliberately expose sensitive information or undermine security controls. These threats show why VTAM needs a more modern and proactive security approach.

Zero Trust Security Policies

VTAM should begin implementing a Zero Trust security policy [1], [3]. The Zero Trust model is based on least privilege access, where users are only given the permissions needed to use the systems, programmes, and data required for their role [1], [3]. Strong user authentication should also be used through Multi-Factor Authentication (MFA). For example, Microsoft Authenticator can require users to approve or verify a login on a trusted device. Remote and cloud access should also be protected by MFA to ensure that only authorised personnel have access [1], [2], [3].

Further controls should also apply to company machines and workers' personal devices. A patching and update policy should ensure devices remain up to date so that newly discovered vulnerabilities are fixed before they can be exploited. Backup and recovery policies should also be implemented so that, in the event of data loss or hardware failure, the company can recover quickly. These policies support the NIST CSF functions of Identify, Protect, Detect, Respond, and Recover by reducing unnecessary trust, tightening access control, and improving VTAM's ability to prevent and respond to threats [1], [2].

Technical Mitigation Measures

To support these policies, VTAM should introduce practical technical mitigation measures [2], [4]. MFA would be a strong start in preventing unauthorised access to systems. This can work through a smartphone app, biometric verification such as Face ID or fingerprint recognition, or a USB device used as a hardware token. Email filtering and anti-phishing detection should also be strongly considered. DKIM checks can help mitigate phishing attempts by adding a digital signature to show that an email has not been tampered with in transit [8]. AI-based filtering can also help identify emails that use tactics such as urgency, fear, or impersonation to trick users. Endpoint protection and anti-malware tools should be installed on company devices to detect suspicious activity, ransomware behaviour, and unauthorised software [4].

VTAM should also implement network segmentation. This divides the network into isolated sections, helping prevent an attacker from moving laterally if one device is compromised. Patch management and secure backups are also important mitigation measures. Patch management should automate software and operating system updates, close vulnerabilities before they are exploited, and prioritise vulnerabilities listed in the CISA Known Exploited Vulnerabilities (KEV) catalogue [4], [10]. Encrypting backups and keeping data off-site can help systems recover quickly following ransomware or data loss. To strengthen visibility, VTAM could use a Security Information and Event Management (SIEM) system to collect and analyse logs, while Cloud Security Posture Management (CSPM) could help identify poor cloud configuration [7], [9]. Together, these measures would reduce the likelihood and impact of a successful cyber-attack.

Monitoring, Incident Response and Training

VTAM should implement continuous monitoring and maintain logs of system activity to spot suspicious behaviour as early as possible [7]. A SIEM system would support this by collecting and analysing data from across the network in one place, helping to identify complex attack patterns. Security Orchestration, Automation and Response (SOAR) tools could also automate parts of the response process, such as alert handling, investigation steps, and containment actions [7]. This would improve the speed and consistency of VTAM's response to threats.

Figure 1: VTAM Incident Response Process

Threat Detected → SIEM Alert → Investigation → Isolate Affected System → Recover from Backup → Post-Incident Review

VTAM also needs an incident response process that clearly explains how the security team should respond during a crisis [7]. If ransomware or another serious threat is detected, the affected device or system should be isolated quickly to prevent the spread of the attack [4], [7]. After every incident, the company should review what happened and take appropriate measures to prevent the issue from occurring again.

Alongside this, VTAM should provide continuous staff awareness training rather than relying on occasional one-off sessions. Training should include phishing and vishing simulations [8]. For example, staff could occasionally receive a fake phishing email as part of a training exercise. If they click the link, they would be informed that it was a test and shown how to identify warning signs. Training should also be role-specific, with finance and IT staff receiving guidance relevant to their duties. Staff should also be encouraged to report suspicious emails, phone calls, or system activity immediately [8]. This would help create a stronger security culture and reduce the chance of human error leading to a successful attack.

Conclusion

VTAM operates in a cyber threat environment where phishing, ransomware, supply chain compromise, and risks linked to cloud and hybrid working can cause serious damage to systems, data, and customer trust. For this reason, the organisation needs a stronger and more modern cyber security approach. A Zero Trust framework supported by clear security policies, practical technical controls, continuous monitoring, incident response planning, and ongoing staff awareness training would provide a more effective defence against both internal and external threats. By adopting these measures, VTAM would improve its resilience, reduce the likelihood and impact of cyber-attacks, and strengthen its ability to protect critical business operations and sensitive financial information [1], [2].

References

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207. Gaithersburg, MD, USA: National Institute of Standards and Technology, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

[2] National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Paper 29. Gaithersburg, MD, USA: National Institute

of Standards and Technology, Feb. 26, 2024. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>. [Accessed: Apr. 12, 2026].

[3] Cybersecurity and Infrastructure Security Agency, Zero Trust Maturity Model Version 2.0. Washington, DC, USA: CISA, Apr. 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf. [Accessed: Apr. 12, 2026].

[4] Cybersecurity and Infrastructure Security Agency, StopRansomware Guide. Washington, DC, USA: CISA, Mar. 2025. [Online]. Available: <https://www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20508.pdf>. [Accessed: Apr. 12, 2026].

[5] Cybersecurity and Infrastructure Security Agency, Stop Ransomware. Washington, DC, USA: CISA. [Online]. Available: <https://www.cisa.gov/stopransomware>. [Accessed: Apr. 12, 2026].

[6] European Union Agency for Cybersecurity, ENISA Threat Landscape: Finance Sector. Athens, Greece: ENISA, Feb. 21, 2025. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf. [Accessed: Apr. 12, 2026].

[7] National Institute of Standards and Technology, Computer Security Incident Response Recommendations and Considerations for Cyber Risk Management, NIST Special Publication 800-61 Revision 3. Gaithersburg, MD, USA: National Institute of Standards and Technology, Apr. 2025. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf>. [Accessed: Apr. 15, 2026].

[8] Cybersecurity and Infrastructure Security Agency, Recognize and Report Phishing. Washington, DC, USA: CISA. [Online]. Available: <https://www.cisa.gov/secure-our-world/recognize-and-report-phishing>. [Accessed: Apr. 15, 2026].

[9] Cybersecurity and Infrastructure Security Agency, Cloud Security Technical Reference Architecture. Washington, DC, USA: CISA, Jun. 2022. [Online]. Available: <https://www.cisa.gov/resources-tools/resources/cloud-security-technical-reference-architecture-tra>. [Accessed: Apr. 16, 2026].

[10] Cybersecurity and Infrastructure Security Agency, Known Exploited Vulnerabilities Catalog. Washington, DC, USA: CISA. [Online]. Available: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>. [Accessed: Apr. 16, 2026].