krome

Krome Technologies

Head Office

Krome House

Pound Road

Chertsey

Surrey

KT16 8ER

Telephone: 01932 232345

Website: www.krome.co.uk

Registration Number: 7031219

VAT Number: 977 8629 40

Security Posture Assessment

Prepared for:

TEST Co Plc

Date: 01 February 2026

Document Contents

1 Document Details

1.1 Key Contact Details

Name	Project Role, Company	Email
TEST CONTACT	Head of IT, TEST Co Plc	test.contact@testcoplc.com

1.2 Document Revisions

Date	Revision ID	Details	Author(s)
01.02.2026	1.0	Document creation	Head of SOC, Krome

Note: for minor changes increment revision ID by 0.1, for major changes increase by 1.

2 Current Security Posture

The organisation's overall security posture reflects mixed maturity across key security domains.

SaaS Security: **62%**

SaaS Security sits at a developing level, indicating that controls protecting cloud-hosted applications need further strengthening to reduce risks such as data exposure or unauthorised access.

Endpoint Security: **72%**

Endpoint Security is moderately mature, showing that most devices have baseline protections in place but would benefit from improvements like tighter configuration management, stronger malware defences, or reduced local admin rights.

Cloud Security: **92%**

Cloud Security is the strongest area, suggesting that core cloud platforms and configurations follow recommended best practices, providing robust protection against common cloud-based threats.

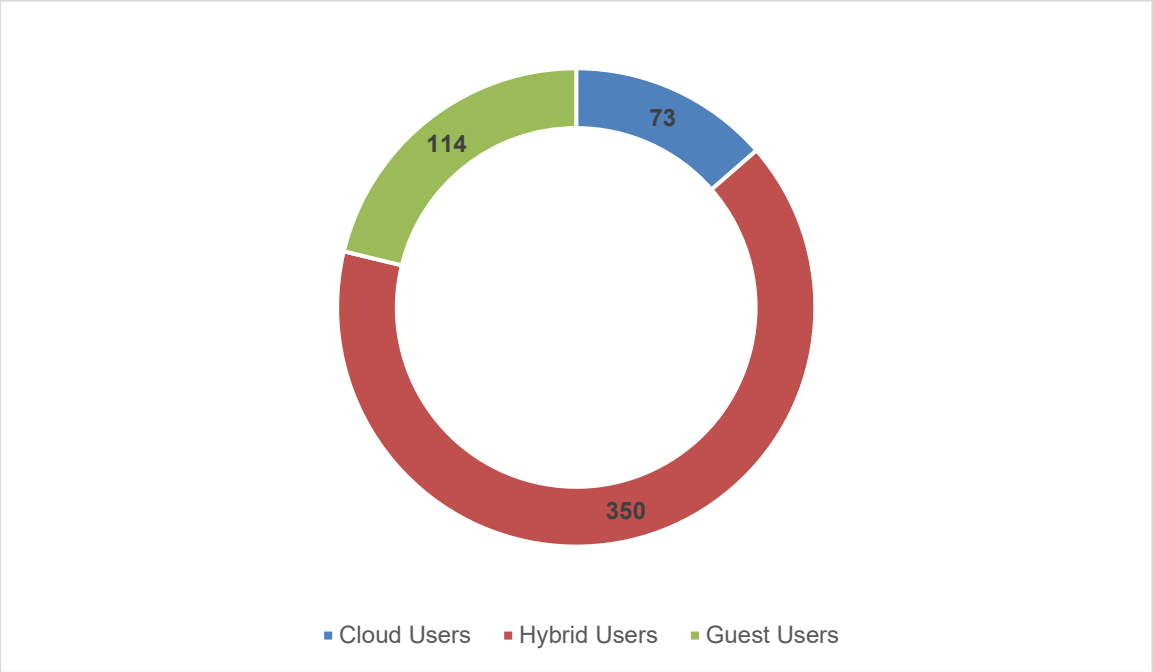
Identity Security: **67%**

Identity Security shows room for improvement, highlighting the importance of strengthening identity governance, enforcing consistent MFA usage, reducing legacy authentication paths, and tightening privileged access to prevent attackers from exploiting identity-related weaknesses.

Overall, the scores indicate that improving identity-based controls and SaaS governance would have the greatest impact on risk reduction, while maintaining strong cloud controls and further maturing endpoint protections will help ensure a more balanced and resilient security posture.

3 Identity and Account Protection

The distribution of identities shows that most users rely on a hybrid setup, with a smaller portion using cloud-only accounts and an additional group made up of guests. This mix suggests that the greatest security emphasis should be placed on strengthening controls around hybrid identities, because they depend on both on-premises infrastructure and cloud services, making them more susceptible to legacy configuration issues and lateral-movement risks. Cloud-only users still require strong modern protections such as multifactor authentication and conditional access, while guest accounts highlight the need for careful access governance to prevent unnecessary exposure. Overall, the balance of user types indicates that securing the hybrid environment and enforcing consistent identity policies across all groups will have the most meaningful impact on reducing risk.



The top identity-related Secure Score recommendations directly target the weaknesses attackers most often exploit, such as excessive privilege, unmanaged or dormant accounts, and insecure legacy configurations. Implementing these actions helps tighten control over who has elevated access, ensures service and privileged accounts are properly governed, and corrects misconfigurations that could allow impersonation or lateral movement. Collectively, they strengthen your overall identity posture by reducing opportunities for privilege escalation, limiting lateral movement, and ensuring only the right users and systems have the access they truly need and ultimately making it much harder for a threat actor to gain or maintain access within your network.

Recommended Actions	Score Impact
Identify Entra ID privileged accounts that are also privileged in Active Directory	0.59%
Identify service accounts in privileged groups	0.46%
Resolve unsecure domain configurations	0.33%
Remove dormant accounts from sensitive groups	0.33%
Modify unsecure Kerberos delegations to prevent impersonation	0.33%
Resolve unsecure account attributes	0.33%
Prevent users to request a certificate valid for arbitrary users based on the certificate template (ESC1)	0.33%
Change password for krbtgt account	0.33%
Change password of built-in domain Administrator account	0.33%
Ensure privileged accounts are not delegated	0.33%

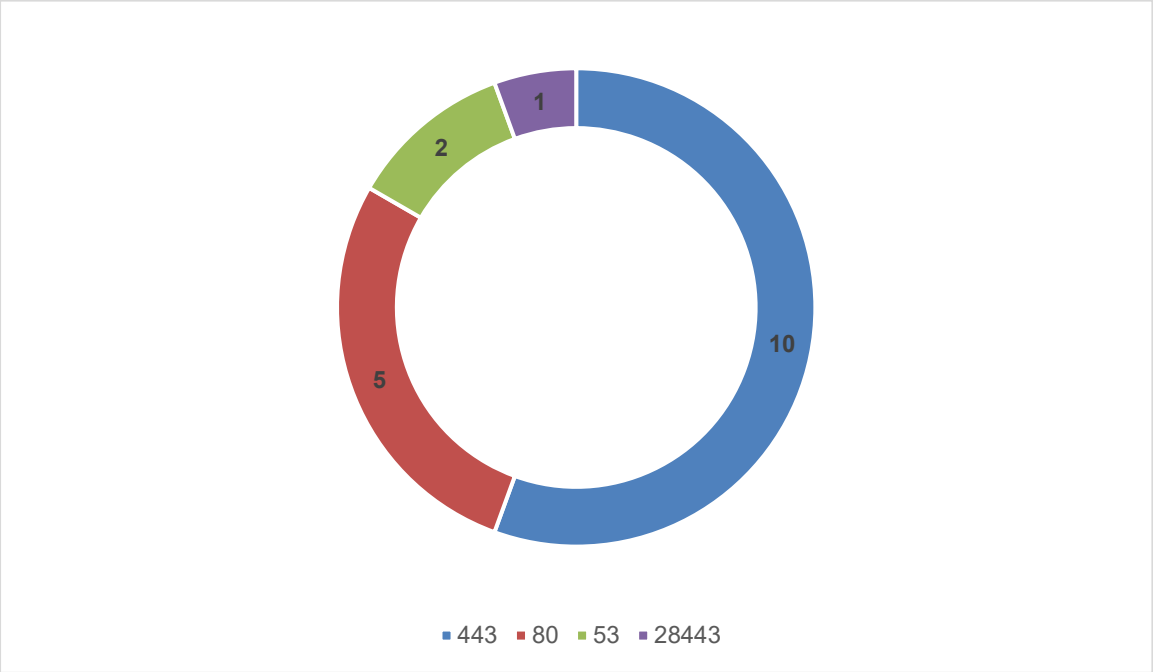
4 External Exposure and Attack Surface

Open ports are potential entry points for attackers and pose risks if the service behind the port is misconfigured, unpatched, or vulnerable. Firewalls are typically used to restrict access to these ports, ensuring only trusted traffic can pass through.

The following WAN IPs were scanned:

- [REDACTED] /26
- [REDACTED] /26

From these IPs, **18** open ports have been identified:



Open ports across the scanned IP ranges indicate a mixture of standard web traffic, DNS services, and one non-standard encrypted service. Port 80 is used for unencrypted HTTP traffic, which typically suggests publicly accessible websites or device interfaces. Port 443 supports encrypted HTTPS traffic and usually indicates secure web services, APIs, VPN portals, or administrative interfaces. Port 53 handles DNS queries and may reflect the presence of authoritative DNS servers or publicly exposed DNS resolvers. Port 28443 is a non-standard encrypted port commonly associated with vendor appliances, management consoles, or custom applications running over HTTPS on an alternative port.

Overall, the repeated presence of HTTP and HTTPS services indicates multiple externally reachable web interfaces, while the DNS exposures should be validated to ensure they are intentionally public. The single instance of the custom port 28443 should be investigated to confirm the service's purpose and to ensure appropriate access control is in place.

Some known vulnerabilities were observed on a few the open ports identified. However, it is important to note that this assessment was optimised for speed and may not be exhaustive, so further in-depth testing is recommended for comprehensive assurance. Any found vulnerabilities were based solely on version information contained in the replies and should be confirmed manually.

Public IP	Open Ports	Service Header/Version	Known CVEs (Vulnerabilities)
[REDACTED]	80/443	HTTP/1.1 404 Not Found HTTP/1.1 301 Moved Permanently	None
[REDACTED]	443	HTTP/1.1 200 OK Server: nginx/1.22.1	CVE-2025-23419 CVE-2023-44487
[REDACTED]	443	HTTP/1.1 404 Not Found	None
[REDACTED]	53	*No data returned*	N/A
[REDACTED]	80/443	HTTP/1.1 301 Moved Permanently Server: nginx/1.14.0 (Ubuntu) HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu)	CVE-2025-23419 CVE-2023-44487 CVE-2021-23017 CVE-2021-3618 CVE-2019-20372 CVE-2019-9516 CVE-2018-16845
[REDACTED]	80/443	HTTP/1.1 404 Not Found HTTP/1.1 302 Found	None
[REDACTED]	443	HTTP/1.1 302 Found	None
[REDACTED]	80/443	HTTP/1.1 404 Not Found HTTP/1.1 302 Found	None
[REDACTED]	443	HTTP/1.1 404 Not Found	None
[REDACTED]	53	HTTP/1.1 404 Not Found content-type:	None

		text/html; charset=us-ascii server: Microsoft-HTTPAPI/2.0	
[REDACTED]	443	HTTP/1.1 404 Not Found	None
[REDACTED]	443	HTTP/1.1 503 Service Unavailable	None
[REDACTED]	28443	HTTP/1.1 400 Bad Request No required SSL certificate was sent	None

5 Email Accounts in Data Breaches

A total of **540** individual entries were identified with **263** unique email addresses observed. Additionally, **3** email addresses were found in Pastebin (or similar) where attackers often dump stolen information as a method of exfiltration.

Data Breach	Count
Onliner Spambot	154
DemandScience by Pure Incubation	61
Data Enrichment Exposure From PDL Customer	61
Apollo	40
LinkedIn Scraped Data (2021)	34
Verifications.io	33
LinkedIn Scraped and Faked Data (2023)	29
Synthient Credential Stuffing Threat Data	19
Adobe	11
Collection #1	10
Cit0day	8
Covve	8
Exploit.In	7
Anti Public Combo List	6
Nitro	6
Dropbox	5
LinkedIn	4
MyFitnessPal	3
Trik Spam Botnet	3
Combolists Posted to Telegram	3
Twitter (200M)	3
123RF	2
Public Business Data	2
QuestionPro	2

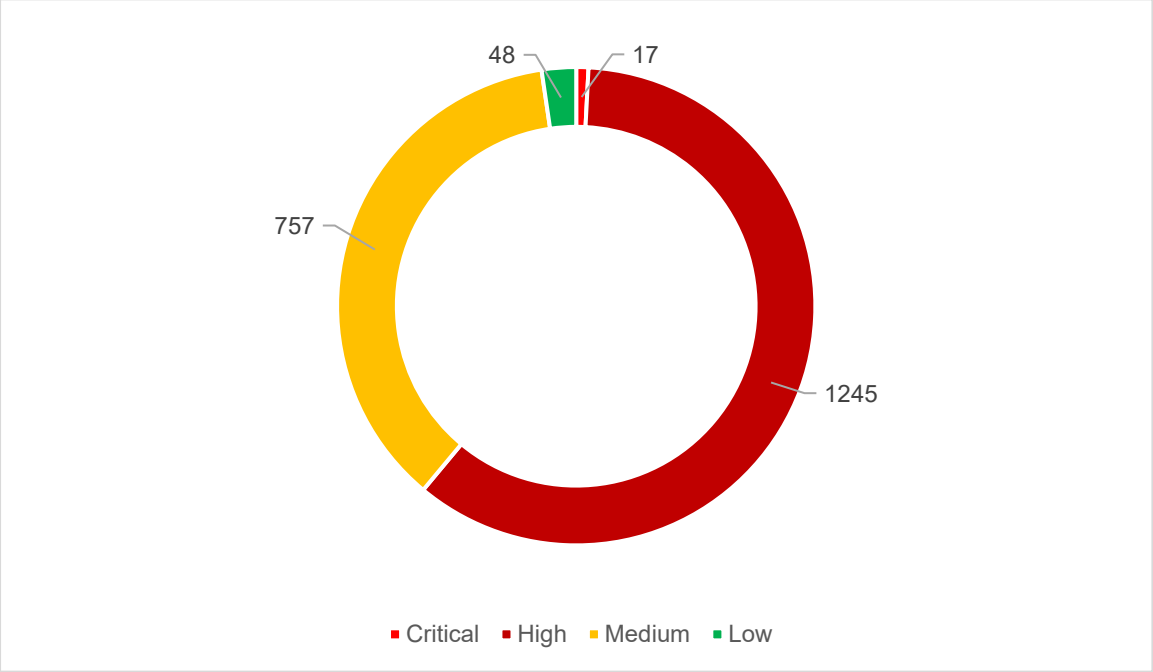
You've Been Scraped	2
Not SOCRadar	2
ALIEN TXTBASE Stealer Logs	1
Kayo.moe Credential Stuffing List	1
Epik	1
Naz.API	1
Canva	1
Elasticsearch Instance of Sales Leads on AWS	1
QuinStreet	1
Jobandtalent	1
Ticketfly	1
Instagram	1
Lookiero	1
ShareThis	1
Glofox	1
Bitly	1
Deezer	1
Army Force Online	1
2,844 Separate Data Breaches	1
Planet Ice	1
Gravatar	1
Exactis	1
River City Media Spam List	1
Synthient Stealer Log Threat Data	1

6 Vulnerability Exposure Overview

The vulnerability data shows a clear imbalance, with a very small number of critical issues compared to a much larger volume of high- and medium-severity vulnerabilities.

This indicates that while there may be only a few immediately severe threats, there is a substantial backlog of weaknesses that attackers could exploit if left unaddressed.

High-severity items often include outdated software, misconfigurations, or missing patches which significantly increase risk when present at scale.



Addressing these vulnerabilities is important because attackers commonly target the easiest and most numerous weaknesses.

Large volumes of high and medium-risk exposures create many possible entry points, increasing the likelihood of compromise. Reducing this overall vulnerability load strengthens your security posture, limits opportunities for exploitation, and ensures that even if an attacker attempts to gain a foothold, the available attack paths are significantly reduced.

7 Best Practice Benchmark

The best practice benchmark reflects how well the environment aligns with established security standards across several key frameworks.

CIS M365 Foundations Benchmark: **73%**

The CIS Microsoft 365 Foundations Benchmark score shows a strong but improvable level of adherence to baseline security configuration guidance, which is important because CIS controls help minimise common misconfigurations that attackers frequently exploit.

Zero Trust (Foundational): **51%**

The Zero Trust foundational score highlights that more work is needed to shift toward an identity-centric, least-privilege model, which is crucial for reducing lateral movement and strengthening protection against account-based compromise.

Ransomware Protection: **84%**

The ransomware protection score indicates a high level of readiness against common ransomware techniques, showing that strong backup, containment, and endpoint controls are already in place.

Business Email Compromise - Financial Fraud: **89%**

The Business Email Compromise and financial fraud score demonstrates that defensive measures for safeguarding email-based threats and protecting high-risk financial workflows are operating effectively.

Together, these scores help identify which security areas are well-developed and which require further maturity to reduce risk and improve resilience.

8 Security Monitoring Readiness

The environment shows a strong foundation for onboarding into a SOC service powered by Microsoft Sentinel, as most core Microsoft security products are already deployed.

With Intune, Defender for Endpoint Plan 2, Defender for Office 365 Plan 2, Defender for Identity, Defender for Cloud Apps, and Microsoft Sentinel all active, the organisation already generates the telemetry a SOC relies on for threat detection, correlation, and automated response. This means endpoint events, identity signals, email threats, cloud app activity, and SIEM analytics are available for centralised monitoring and alerting.

Product	Status
Intune	Deployed
Microsoft Sentinel	Deployed
Defender for Identity	Deployed
Defender for Endpoint Plan 2	Deployed
Defender for Office 365 Plan 2	Deployed
Defender for Cloud Apps	Deployed
Defender for Cloud	Unused
Defender for Servers	Unused

The only notable gaps are Defender for Cloud and Defender for Servers, which are listed as unused. If the SOC is expected to monitor workloads hosted in Azure or on-premises server infrastructure, enabling these products would significantly strengthen visibility into configuration drift, server-level threats, and cloud workload attacks.

Overall, the organisation is in a strong position to be onboarded into a Sentinel-powered SOC, with most key data sources already in place and only server and cloud-workload coverage needing attention to achieve full maturity.

9 Overall Summary

This security posture assessment demonstrates that the organisation has a strong and credible security foundation, with particularly high maturity in cloud security, ransomware protection, email threat defence, and security monitoring readiness.

Core Microsoft security platforms are already deployed and generating meaningful telemetry, placing the organisation in a favourable position to detect, respond to, and recover from modern cyber threats.

At the same time, the assessment identifies several areas where targeted improvements would significantly reduce overall risk and improve balance across the security landscape. Identity security, SaaS governance, and vulnerability management represent the most impactful opportunities for improvement, as weaknesses in these areas are frequently exploited by attackers and can undermine otherwise strong technical controls.

Overall, the organisation is well positioned from a security maturity perspective, with many strong controls already in place. By focusing on identity hardening, SaaS governance, vulnerability reduction, and expanded monitoring coverage, the organisation can achieve a more balanced, resilient, and future-ready security posture that is better equipped to withstand evolving cyber threats while supporting ongoing business growth.

10 Top 5 Recommendations

Recommendation	Priority Level
1. Lock Down Privileged and High-Risk Identity Access Actions required: ▪ Identify all privileged, service, and hybrid Entra ID / AD accounts ▪ Remove excessive and overlapping admin rights ▪ Enforce MFA on all privileged and high-risk accounts ▪ Remove dormant accounts from sensitive groups ▪ Disable legacy authentication methods	**Critical**
2. Reduce High and Medium Vulnerabilities at Scale Actions required: ▪ Prioritise remediation of high and medium severity vulnerabilities ▪ Patch or upgrade outdated software and exposed services ▪ Establish a regular vulnerability remediation cycle using Defender Vulnerability Management ▪ Track and reduce total vulnerability count over time	**High**
3. Strengthen SaaS Application Security and Governance Actions required: ▪ Review and control third-party and unmanaged SaaS applications ▪ Enforce conditional access and session controls for SaaS usage ▪ Limit data access and sharing permissions across cloud apps ▪ Monitor risky SaaS behaviour using Defender for Cloud Apps	**High**
4. Harden Internet-Facing Services and Network Exposure Actions required: ▪ Validate that all externally exposed ports and services are required ▪ Patch or upgrade externally facing services with known CVEs ▪ Restrict access to management or non-standard ports (e.g. alternative HTTPS ports) ▪ Ensure firewall rules and access controls follow least-exposure principles	**Medium**
5. Extend Security Monitoring to Cloud and Server Workloads Actions required: ▪ Enable Defender for Cloud to monitor Azure and cloud workload security ▪ Enable Defender for Servers for server-level threat and vulnerability visibility ▪ Integrate these data sources into Microsoft Sentinel for SOC monitoring	**Medium**