FORTRESS™

Secure your future with Fortress

In an era where digital threats are evolving at an unprecedented pace, safeguarding your organization's data and infrastructure is not just a necessity, but a strategic imperative. **Fortress**, the pinnacle of security services in Azure, is meticulously designed to fortify your modern workplace with intelligence and strategy.

At the heart of Fortress lies a commitment to the foundational principles of security, ensuring that every aspect of your organization's digital presence is protected.

- **Sentinel / Log Analytics:** Microsoft Sentinel and Log Analytics offer a comprehensive, cloud-native solution that enhances your company's security posture, providing advanced threat detection, investigation, and response capabilities. Microsoft Sentinel and Log Analytics provide a modern approach to security, leveraging the power of the cloud and artificial intelligence to protect your organization from potential threats.
- **Defender for Cloud:**
  Microsoft Defender for Cloud offers a comprehensive, cloud-native solution that enhances your company's security posture, providing advanced threat protection, continuous monitoring, and compliance management. This proposal outlines how Defender for Cloud can transform your security operations, making them more efficient, scalable, and intelligent.
  - Comprehensive Threat Protection:
  - Continuous Security Monitoring:
  - Automated Compliance Management
  - Seamless Integration and Scalability
- **Defender for Endpoint:**
  - Advanced Threat Detection
  - Comprehensive Endpoint Protection
  - Automated Incident Response
- **Compliance Manager:**

Built upon the frameworks of CMMC Level 2/ NIST-800-171R2, Fortress is not just about meeting standards—it's about exceeding them, for clients navigating the complexities of CMMC Level 2 implementation,

Choose Fortress for a security landscape that's not just about defense, but about enabling your organization to thrive in a world of uncertainties.

Approach

KAMIND believes that the most effective way to provide value is to act as the extension to the CIO, CISO and IT support. KAMIND believes that they can bring their knowledge of Intelligent security for the modern workplace to deliver a holistic security solution across users, devices, apps and data.

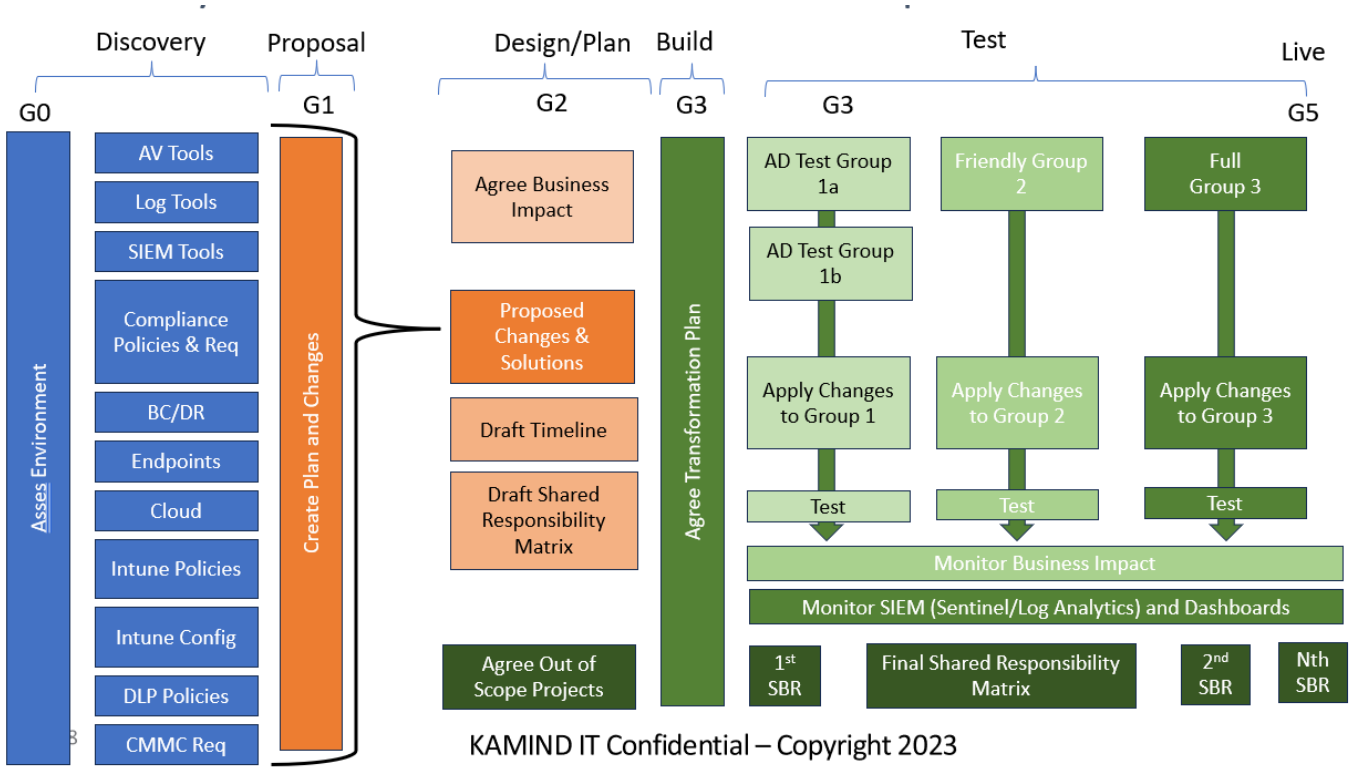


Figure 1 KAMIND Security transformation process

There are multiple steps required to deploy Fortress security services in a new environment. Fortress covers the onboarding of the client, through the deployment of security associated services and licenses. Microsoft 365 E5 is required due to the requirement of the Endpoint DLP component to meet CMMC L2 certification . As part of the Fortress configuration, KAMIND will deploy Azure security services, such as an Azure Sentinel SIEM, Azure defender for cloud and other Azure security services as needed.

The Fortress services deployed in Fortress includes.

- Microsoft Entra P2 - Azure Active Directory Premium Conditional Access
- Microsoft 365 Defender
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Defender Vulnerability Management
- Microsoft Defender for Cloud
- Microsoft Defender for Key Vault
- Microsoft Defender for DNS
- Microsoft Defender for Resource Manager

- Microsoft Defender Threat Intelligence
- Build out Microsoft Defender Threat Intelligence
- Deploy MFA and conditional access for All users.
- Build out additional device management policies
    - Configure Microsoft Endpoint Manager proactive tools
    - Define baseline for Company managed data on BYOD devices using, MAM Basic
    - Deploy Office mobile under MAM configuration.
    - Configure Windows Information Protection (WIP)
    - Configure Microsoft Sentinel for monitoring and alerts
    - Configure device registration for device control.

- Deploy Mobile/Desktop test groups and Cybersecurity Management
    - Deploy for test group for validation.
    - Deploy companywide for all users and the following devices.
        - Fortress Managed all licensed mailbox users.
        - Fortress Managed Users and workstations.
        - Fortress Managed web only users.
    - Deploy Window Update service and Defender endpoint for all managed workstations.
- Deploy DLP Services
    - Deploy DLP for financial and Company confidential documents (Basic Fortress-G Groups)
    - Deploy DLP for endpoint (requires MS 365 E5)
- Compliance Management Services
    - Supply monthly SER reports in PDF to CLIENT
    - Supply artifact for CMMC L2 (NIST 800-171R2) Configuration
    - Deploy document sensitivity for CUI based on Client supplied data flow diagram.
    - Deploy document sensitivity for PHI/PII based on CLIENT supplied data flow diagram
- Compliance Management Services
    - Insider Risk Management
    - Copilot management (AI Hub)
    - Communication Compliance
- Microsoft Document Sensitivity and/or additional Document protection services besides what is committed in Fortress-G deployment.
    -

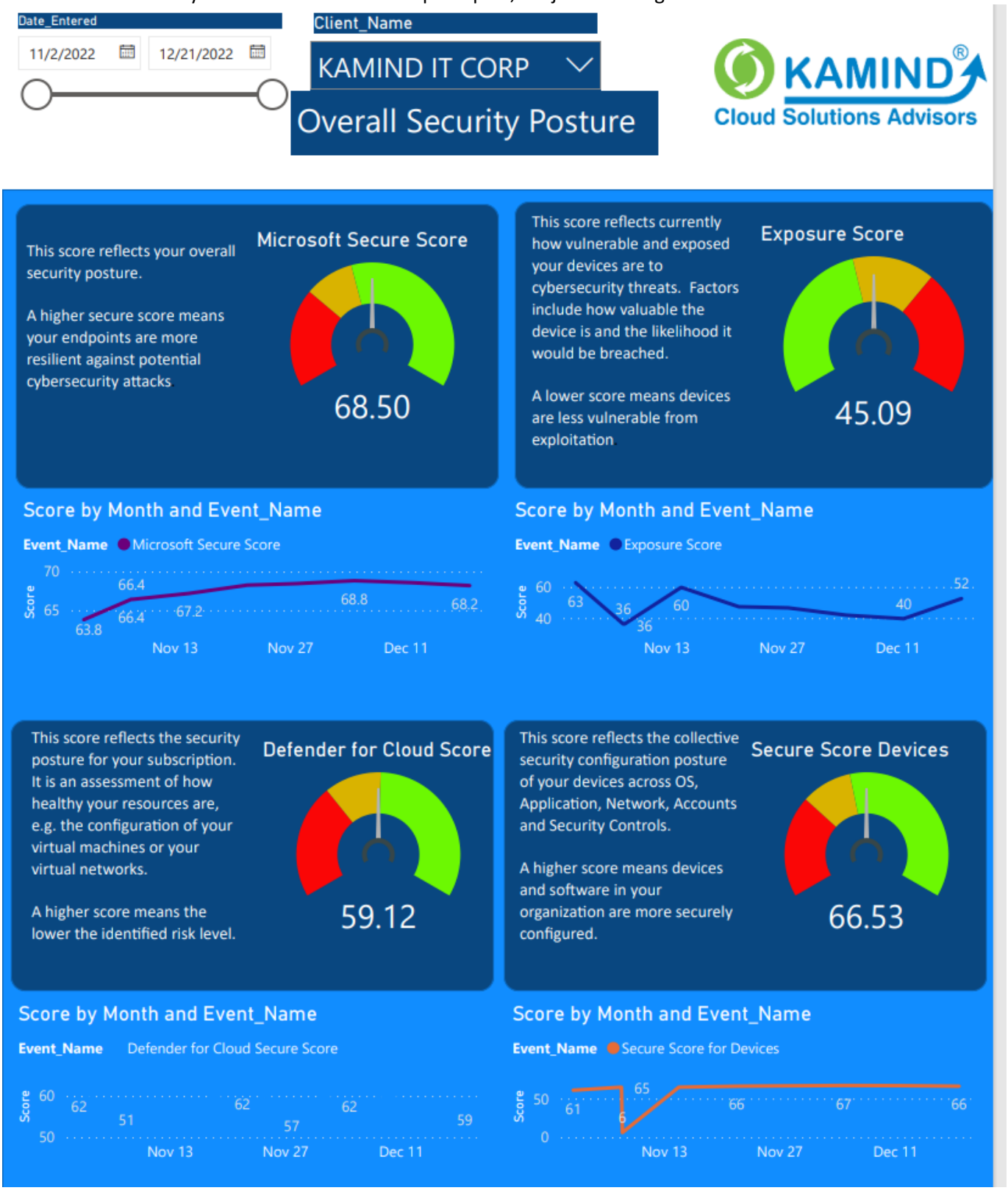
    - plan/process for security events (P1-P4) and Incidence (P0)

Services that are **NOT** included in the Fortress Security Onboarding:

- Any remediation of security issues discovered in the Security Deployment
- Any out-of-scope projects as determined by the future agreed shared responsibility matrix..
- Custom device management - MDM deployment is not included.

- **Sample of KAMIND Guard™ Security Summary Report**

This attachment is a sample of KAMIND IT Realtime security report. The report is reviewed monthly/quarterly with security clients. The security report gives you a 360 view of the KAMIND Security process and what data is recorded for our analysis to cover. This is a sample report, subject to change.

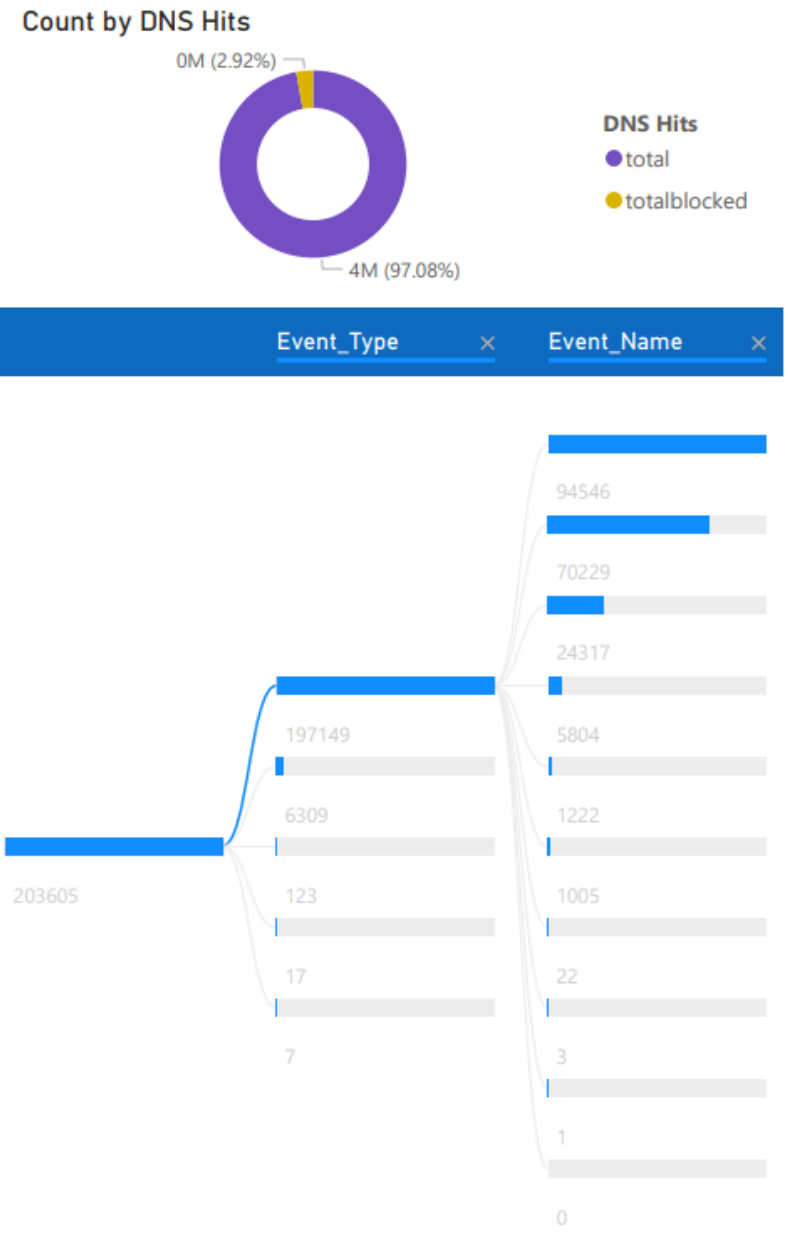


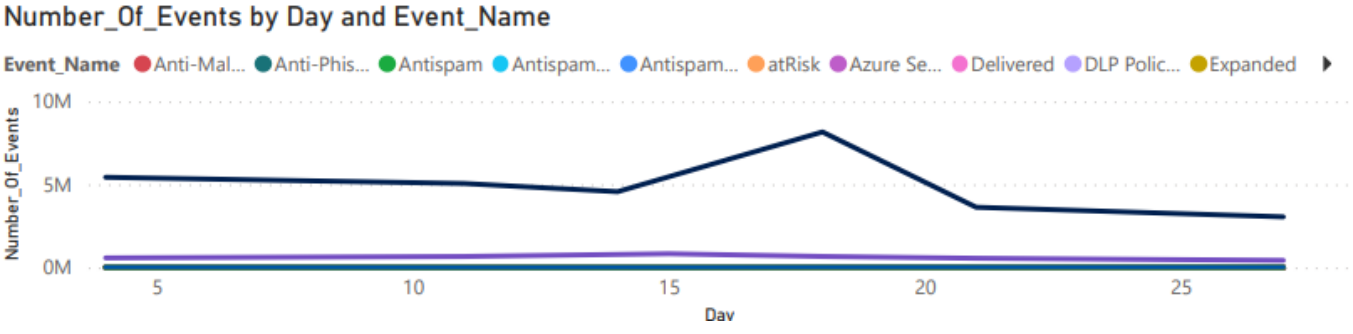
11/8/2022 12/21/2022

Client_Name

KAMIND IT CORP

Event_Type	Event_Name	Count
DLP Info	DLP Policy Matched	17
Email Actions	Anti-Malware	30
Email Actions	Anti-Phishing Spoof	839
Email Actions	Antispam	2883
Email Actions	Antispam High-Confidence Spam	2131
Email Actions	Antispam Phishing	111
Email Actions	Others	315
Identity Protection	atRisk	3
Identity Protection	Remediated	4
Mail Flow Status	Delivered	70229
Mail Flow Status	Expanded	1222
Mail Flow Status	Failed	1005
Mail Flow Status	FilteredAsSpam	22
Mail Flow Status	GettingStatus	3
Mail Flow Status	NonDelivered	24317
Mail Flow Status	None	0
Mail Flow Status	Pending	1
Mail Flow Status	Quarantined	5804
Mail Flow Status	TotalEmail	94546
Security Alerts	Azure Sentinel	21
Security Alerts	Microsoft Cloud App Security	7
Security Alerts	Microsoft Defender Advanced Threat Protection	40
Security Alerts	Microsoft Defender for Cloud	19
Security Alerts	Office 365 Advanced Threat Protection	36





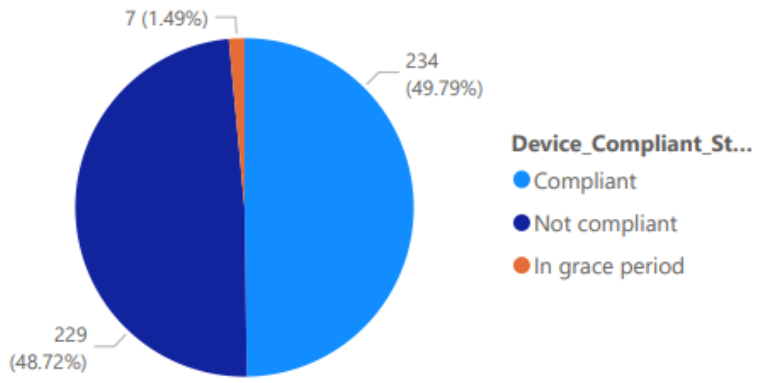
10/27/2022 12/21/2022

Client_Name

KAMIND IT CORP

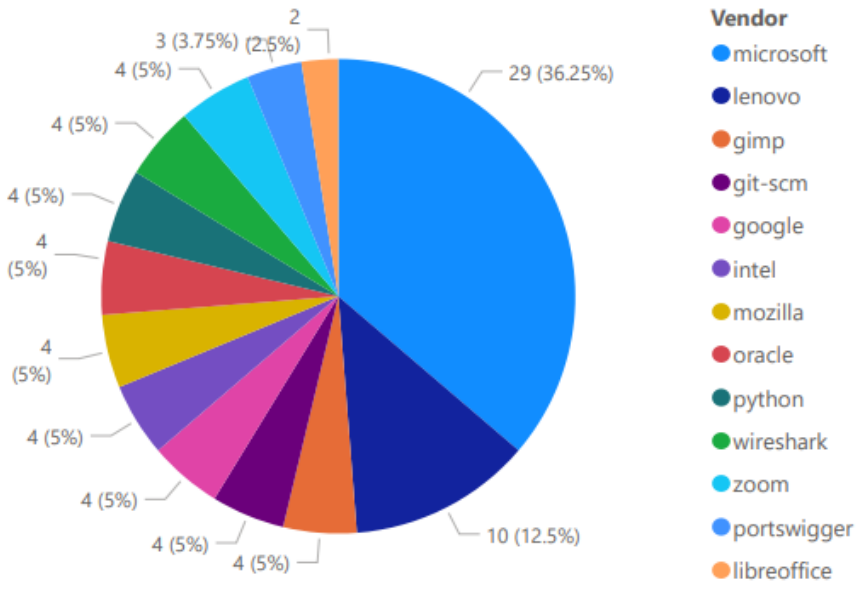
KAMIND®
Cloud Solutions Advisors

Count of Device_Compliant_State by Device_Compliant_State



Status	Device_Name	Device_OS	Device_User
Not compliant	avd-0	Windows	
Not compliant	avd-1	Windows	
Compliant	AVDVM-0	Windows	
Not compliant	AVDVM-0	Windows	
Not compliant	BARBARADESKTOP	Windows	bdawson@kamind.com
Compliant	CPC-mkatz-W6TZU	Windows	mkatzer@kamind.com
Compliant	CPC-mlica-I1NDU	Windows	mlicano@kamind.com
Compliant	CPC-Win365Ap-12	Windows	Win365Apps@kamind.com
Not compliant	DESKTOP-9KFBAC0	Windows	dlagood@kamind.com
Compliant	DESKTOP-9QH4SFI	Windows	bdawson@kamind.com
Not compliant	DESKTOP-9QH4SFI	Windows	bdawson@kamind.com
In grace period	DESKTOP-BPF70N9	Windows	huddleusers@kamind.com
Not compliant	DESKTOP-BPF70N9	Windows	huddleusers@kamind.com
Compliant	DESKTOP-C7P6I4Q	Windows	msmith@kamind.com
Not compliant	iPhone 12 Pro	iOS	bdawson@kamind.com
Not compliant	iPhone 12 Pro (2)	iOS	bdawson@kamind.com
Not compliant	kam-avd01-0	Windows	
Not compliant	kam-avd01-1	Windows	
Compliant	KAMIND-01457	Windows	tslater@kamind.com
Not compliant	KAMIND-01957	Windows	mclass@kamind.com
Compliant	KAMIND-02057	Windows	cwilfong@kamind.com
Compliant	KAMIND-104957	Windows	clandis@kamind.com

Count of Vendor by Vendor



Client_Name

KAMIND IT CORP

Recommendation_Name	Exp. Machines	Public_Exploit	Status	Rec. Vers	Remediation_Type	Tot Machines	Vendor	Score
Update Wireshark to version 4.0.1.0	8	false	Active	4.0.1.0	Update	8	wireshark	9
Update Git to version 2.38.1.0	9	false	Active	2.38.1.0	Update	15	git-scm	16
Update Google Chrome to version 108.0.5359.99	1	true	Active	108.0.5359.99	Update	14	google	24
Update Google Chrome to version 108.0.5359.71	7	true	Active	108.0.5359.71	Update	11	google	40
Update Google Chrome to version 108.0.5359.125	2	false	Active	108.0.5359.125	Update	14	google	5
Update Mozilla Firefox to version 108.0.0.0	4	false	Active	108.0.0.0	Update	9	mozilla	56
Update Google Chrome to version 107.0.5304.121	9	true	Active	107.0.5304.121	Update	11	google	18
Update Mozilla Firefox to version 107.0.1.0	1	false	Active	107.0.1.0	Update	8	mozilla	24
Update Mozilla Firefox to version 107.0.0.0	1	false	Active	107.0.0.0	Update	8	mozilla	24
Update Microsoft Windows Defender to version 1.1.19900.2	2	false	Active	1.1.19900.2	Update	47	microsoft	2
FirmwareUpdate Lenovo Thinkcentre M910q Firmware	3	false	Active		Firmware Update	3	lenovo	138
FirmwareUpdate Lenovo Thinkpad Yoga 11e 3rd Gen Firmware	3	false	Active		Firmware Update	3	lenovo	75
Update Gimp	4	false	Active		Update	4	gimp	8
Update Intel Proset Wireless	4	false	Active		Update	4	intel	4
Update Lenovo System Interface Foundation	8	false	Active		Update	8	lenovo	32
Update Libreoffice	2	false	Active		Update	2	libreoffice	8
Update Microsoft .net	1	false	Active		Update	1	microsoft	1
Update Microsoft .net Core	1	false	Active		Update	1	microsoft	1
Total	**241**					**554**		**2108**