GUARD+

White Paper

Product Overview:

KAMIND GUARD+ is an advanced cybersecurity solution that empowers IT Managers to manage and improve their Security Posture. It gives them weekly IT Security Scores, List of Security Events, Recommendations and helps them track improvement actions.

- Endpoints
- Vulnerable Operating Systems and Software
- Azure Cloud Security
- Microsoft 365 Security
- Security Events and the details
- Compliance Baseline

Benefits:

Security Transparency: Guard+ gives you clear, industry recognized Security and Policy Scoring on a weekly basis.

Improved Planning and Tracking: IT managers can see what parts of their Security Posture need to be improved and how. The tool allows you to isolate a recommendation, group them based on type and efficiently deal with them rather than jumping from issue to issue. Guard+ retains the historical recommendations for you well beyond the classic 90 Days.

Reduction of Exposure: Guard+ clients that take corrective actions exposed through the tool, can see a Score Improvement from 10-35%

Cost Effective: Guard+ saves you 6-8 hours a month gathering scores, events and recommendations, further users save on Azure and Data Analytics and Data Warehousing Licensing by aggregating the most essential security recommendations.

Documentation and Audit Trail: Guard+ allows IT managers to have independent Evidence of their Security posture Insurance companies and compliance boards.

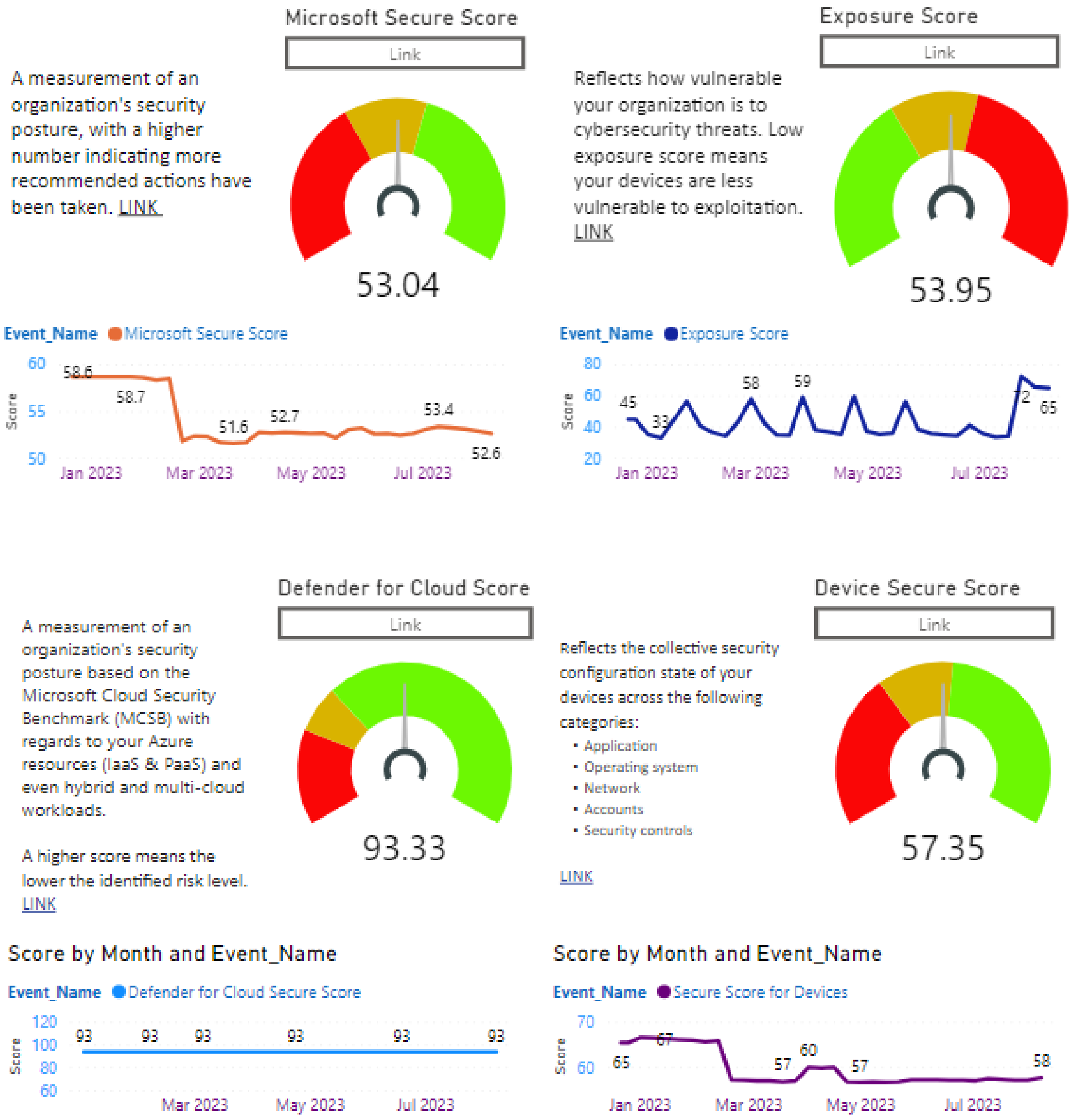
Simplifies a Complex Subject: Guard+ simplifies the job of Analyzing Gigabytes of data into a simple to understand graphical view for managers.

Target Audience:

GUARD+ is designed for IT and Security Managers who need help exposing their security vulnerabilities, structuring their response and provides actions and evidence of the improvements to internal management, clients, regulatory bodies and insurance providers.

Key Features:

Exposure Score: The 4 secure scores help IT Managers determine where their security posture stands and where to focus on the changes they need to make.



Microsoft Secure Score

Link

A measurement of an organization's security posture, with a higher number indicating more recommended actions have been taken. LINK

53.04

Exposure Score

Link

Reflects how vulnerable your organization is to cybersecurity threats. Low exposure score means your devices are less vulnerable to exploitation. LINK

53.95

Defender for Cloud Score

Link

A measurement of an organization's security posture based on the Microsoft Cloud Security Benchmark (MCSB) with regards to your Azure resources (IaaS & PaaS) and even hybrid and multi-cloud workloads.

A higher score means the lower the identified risk level. LINK

93.33

Device Secure Score

Link

Reflects the collective security configuration state of your devices across the following categories:

- Application
- Operating system
- Network
- Accounts
- Security controls

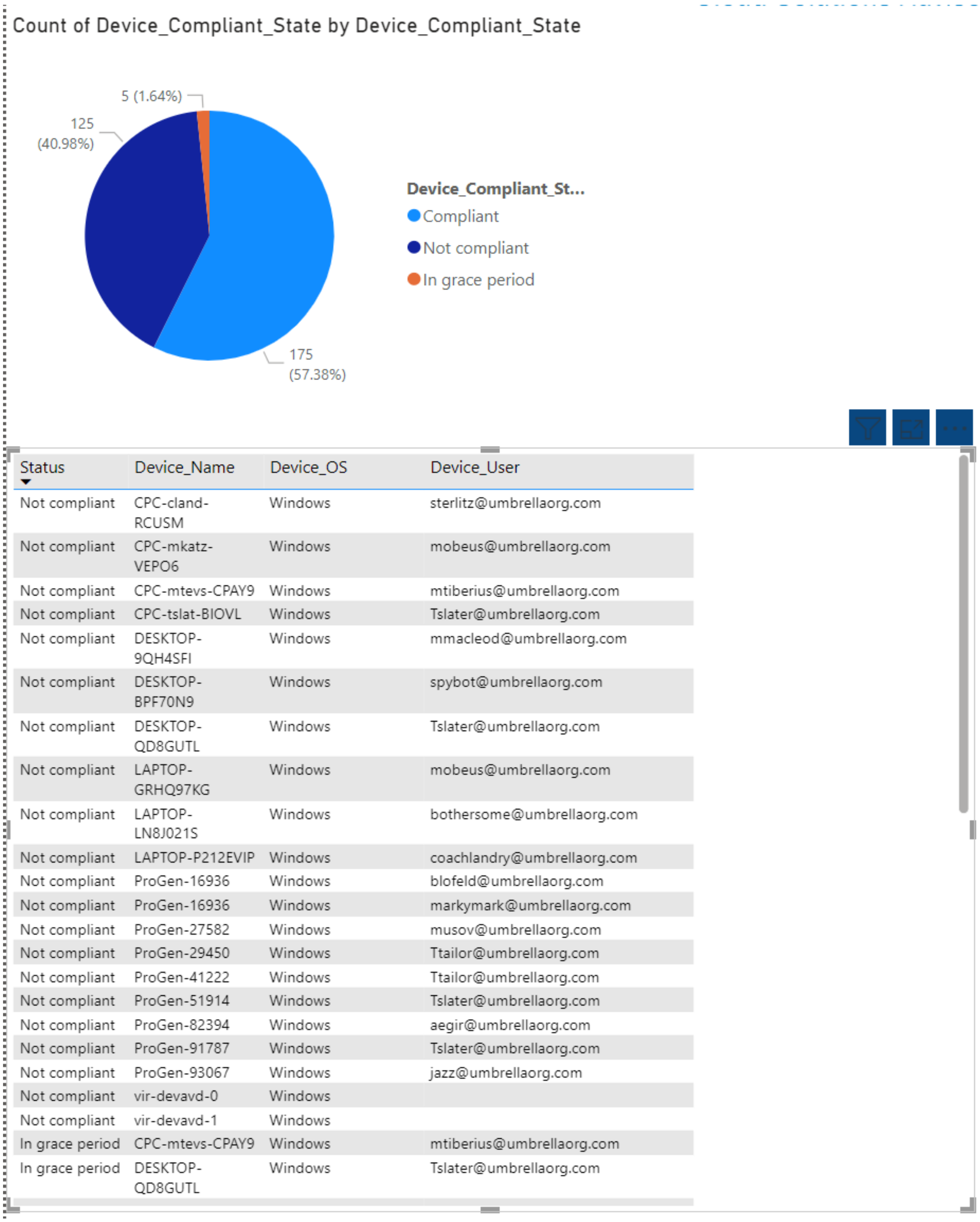
LINK

57.35

Score by Month and Event_Name

Score by Month and Event_Name

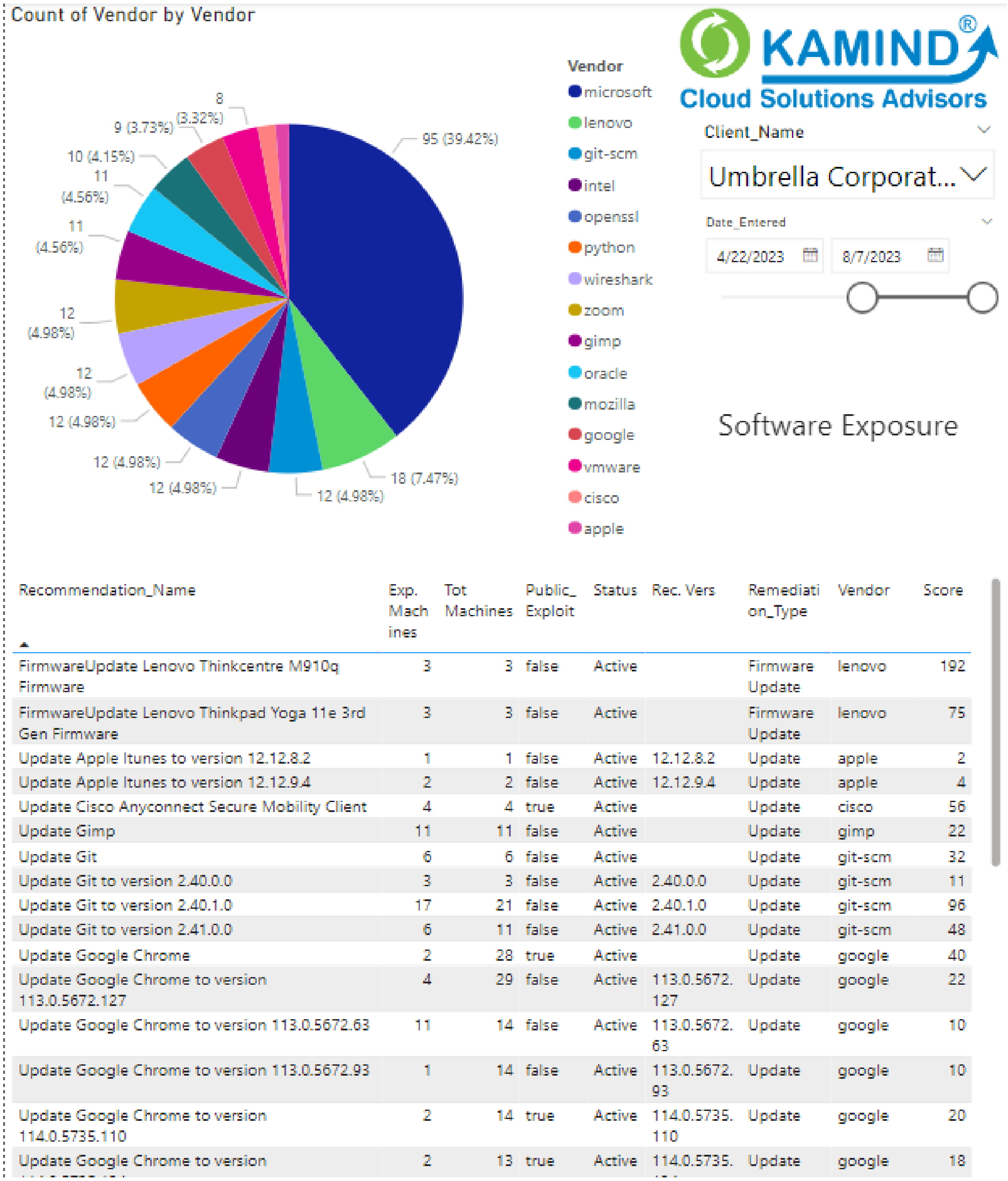
Device Compliancy: shows which of your devices are at risk and who the users of those devices are. Enabling you to see patterns over time and make educated decisions.


Count of Device_Compliant_State by Device_Compliant_State

Status	Device_Name	Device_OS	Device_User
Not compliant	CPC-cland-RCUSM	Windows	sterlitz@umbrellaorg.com
Not compliant	CPC-mkatz-VEPO6	Windows	mobeus@umbrellaorg.com
Not compliant	CPC-mtevs-CPAY9	Windows	mtiberius@umbrellaorg.com
Not compliant	CPC-tslat-BIOVL	Windows	Tslater@umbrellaorg.com
Not compliant	DESKTOP-9QH4SFI	Windows	mmacleod@umbrellaorg.com
Not compliant	DESKTOP-BPF70N9	Windows	spybot@umbrellaorg.com
Not compliant	DESKTOP-QD8GUTL	Windows	Tslater@umbrellaorg.com
Not compliant	LAPTOP-GRHQ97KG	Windows	mobeus@umbrellaorg.com
Not compliant	LAPTOP-LN8J021S	Windows	bothersome@umbrellaorg.com
Not compliant	LAPTOP-P212EVIP	Windows	coachlandry@umbrellaorg.com
Not compliant	ProGen-16936	Windows	blofeld@umbrellaorg.com
Not compliant	ProGen-16936	Windows	markymark@umbrellaorg.com
Not compliant	ProGen-27582	Windows	musov@umbrellaorg.com
Not compliant	ProGen-29450	Windows	Ttailor@umbrellaorg.com
Not compliant	ProGen-41222	Windows	Ttailor@umbrellaorg.com
Not compliant	ProGen-51914	Windows	Tslater@umbrellaorg.com
Not compliant	ProGen-82394	Windows	aegir@umbrellaorg.com
Not compliant	ProGen-91787	Windows	Tslater@umbrellaorg.com
Not compliant	ProGen-93067	Windows	jazz@umbrellaorg.com
Not compliant	vir-devavd-0	Windows	
Not compliant	vir-devavd-1	Windows	
In grace period	CPC-mtevs-CPAY9	Windows	mtiberius@umbrellaorg.com
In grace period	DESKTOP-QD8GUTL	Windows	Tslater@umbrellaorg.com

Software Exposure: shows what vulnerable software exists in an Environment.

- Vendor
- Software
- Recommended Version
- Recommendation type
- No of Exposed machines
- Public Vulnerabilities that exist



Client_Name: Umbrella Corporat...

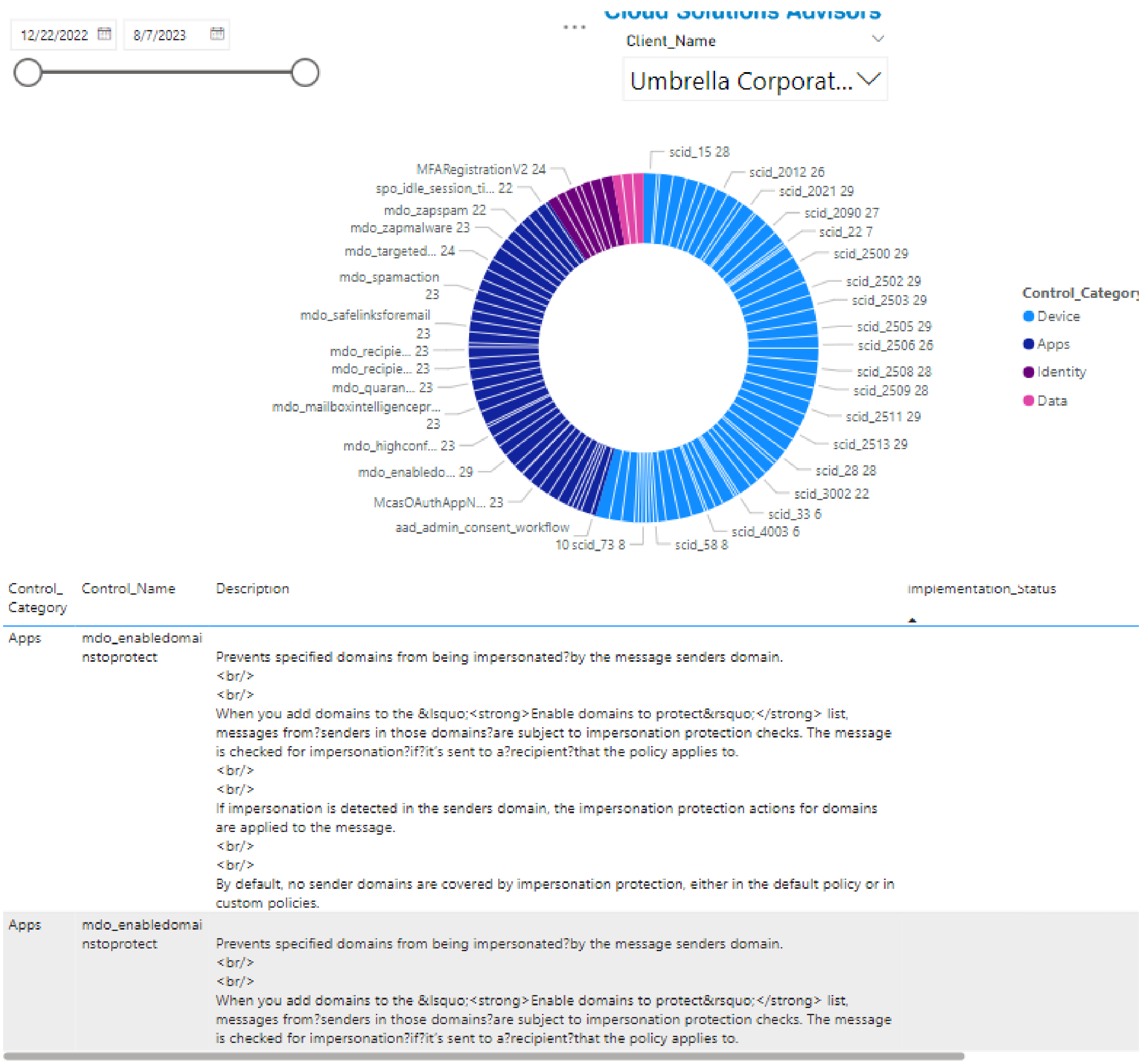
Date_Entered: 4/22/2023 – 8/7/2023

Software Exposure

Recommendation_Name	Exp. Machines	Tot Machines	Public_Exploit	Status	Rec. Vers	Remediation_Type	Vendor	Score
FirmwareUpdate Lenovo Thinkcentre M910q Firmware	3	3	false	Active		Firmware Update	lenovo	192
FirmwareUpdate Lenovo Thinkpad Yoga 11e 3rd Gen Firmware	3	3	false	Active		Firmware Update	lenovo	75
Update Apple Itunes to version 12.12.8.2	1	1	false	Active	12.12.8.2	Update	apple	2
Update Apple Itunes to version 12.12.9.4	2	2	false	Active	12.12.9.4	Update	apple	4
Update Cisco Anyconnect Secure Mobility Client	4	4	true	Active		Update	cisco	56
Update Gimp	11	11	false	Active		Update	gimp	22
Update Git	6	6	false	Active		Update	git-scm	32
Update Git to version 2.40.0.0	3	3	false	Active	2.40.0.0	Update	git-scm	11
Update Git to version 2.40.1.0	17	21	false	Active	2.40.1.0	Update	git-scm	96
Update Git to version 2.41.0.0	6	11	false	Active	2.41.0.0	Update	git-scm	48
Update Google Chrome	2	28	true	Active		Update	google	40
Update Google Chrome to version 113.0.5672.127	4	29	false	Active	113.0.5672.127	Update	google	22
Update Google Chrome to version 113.0.5672.63	11	14	false	Active	113.0.5672.63	Update	google	10
Update Google Chrome to version 113.0.5672.93	1	14	false	Active	113.0.5672.93	Update	google	10
Update Google Chrome to version 114.0.5735.110	2	14	true	Active	114.0.5735.110	Update	google	20
Update Google Chrome to version	2	13	true	Active	114.0.5735.	Update	google	18

Microsoft Secure Score: Lists out specific actions to take in your total environment to protect you against vulnerabilities.

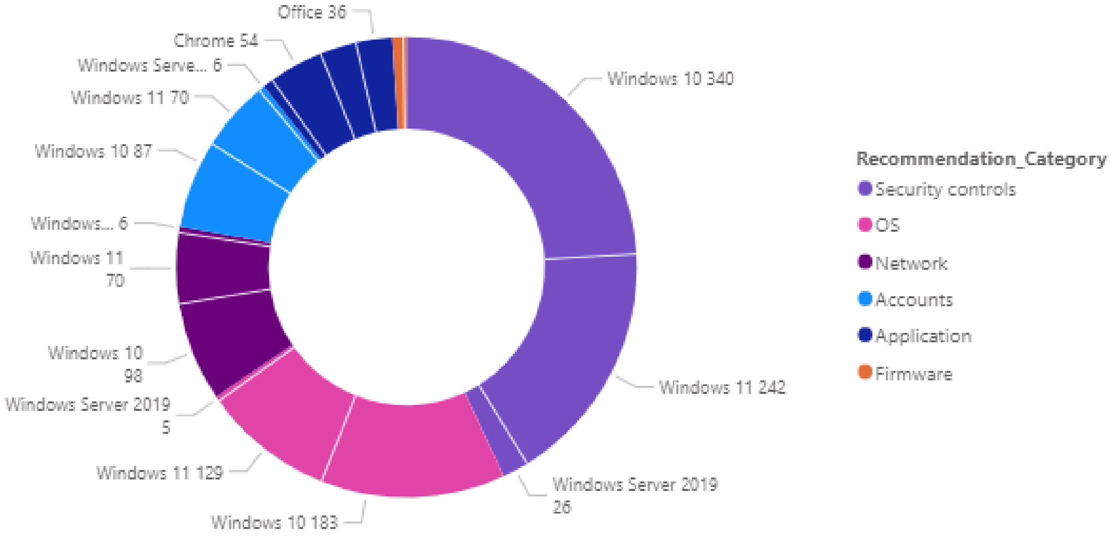
Microsoft Secure Score is a measurement tool provided by Microsoft that assesses the security posture of your organization's Microsoft 365 environment.

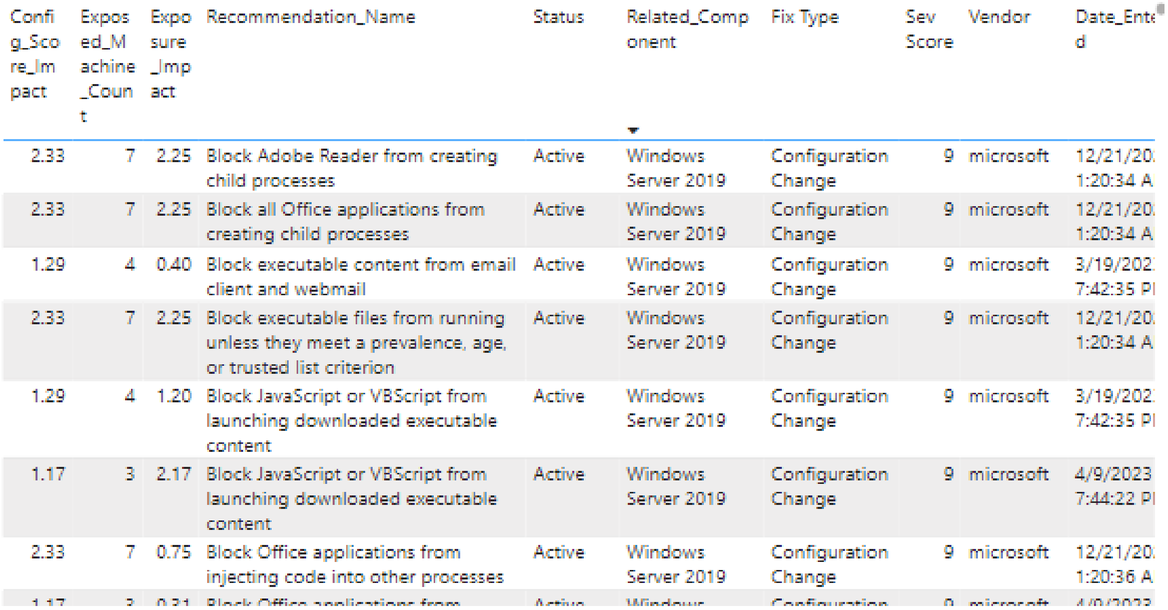


Control_Category	Control_Name	Description	Implementation_Status
Apps	mdo_enabledomainstoprotect	Prevents specified domains from being impersonated?by the message senders domain. <br/> <br/> When you add domains to the &lsquo;<strong>Enable domains to protect&rsquo;</strong> list, messages from?senders in those domains?are subject to impersonation protection checks. The message is checked for impersonation?if?it's sent to a?recipient?that the policy applies to. <br/> <br/> If impersonation is detected in the senders domain, the impersonation protection actions for domains are applied to the message. <br/> <br/> By default, no sender domains are covered by impersonation protection, either in the default policy or in custom policies.	
Apps	mdo_enabledomainstoprotect	Prevents specified domains from being impersonated?by the message senders domain. <br/> <br/> When you add domains to the &lsquo;<strong>Enable domains to protect&rsquo;</strong> list, messages from?senders in those domains?are subject to impersonation protection checks. The message is checked for impersonation?if?it's sent to a?recipient?that the policy applies to.	

Device Score: is an aggregated score that takes helps IT managers discover the configuration changes they need to apply to endpoints.

- Compares collected configurations to the collected benchmarks to discover misconfigured assets
- Maps configurations to vulnerabilities that can be remediated or partially remediated (risk reduction)
- Collects and maintain best practice configuration benchmarks (vendors, security feeds, internal research teams)
- Collects and monitor changes of security control configuration state from all assets



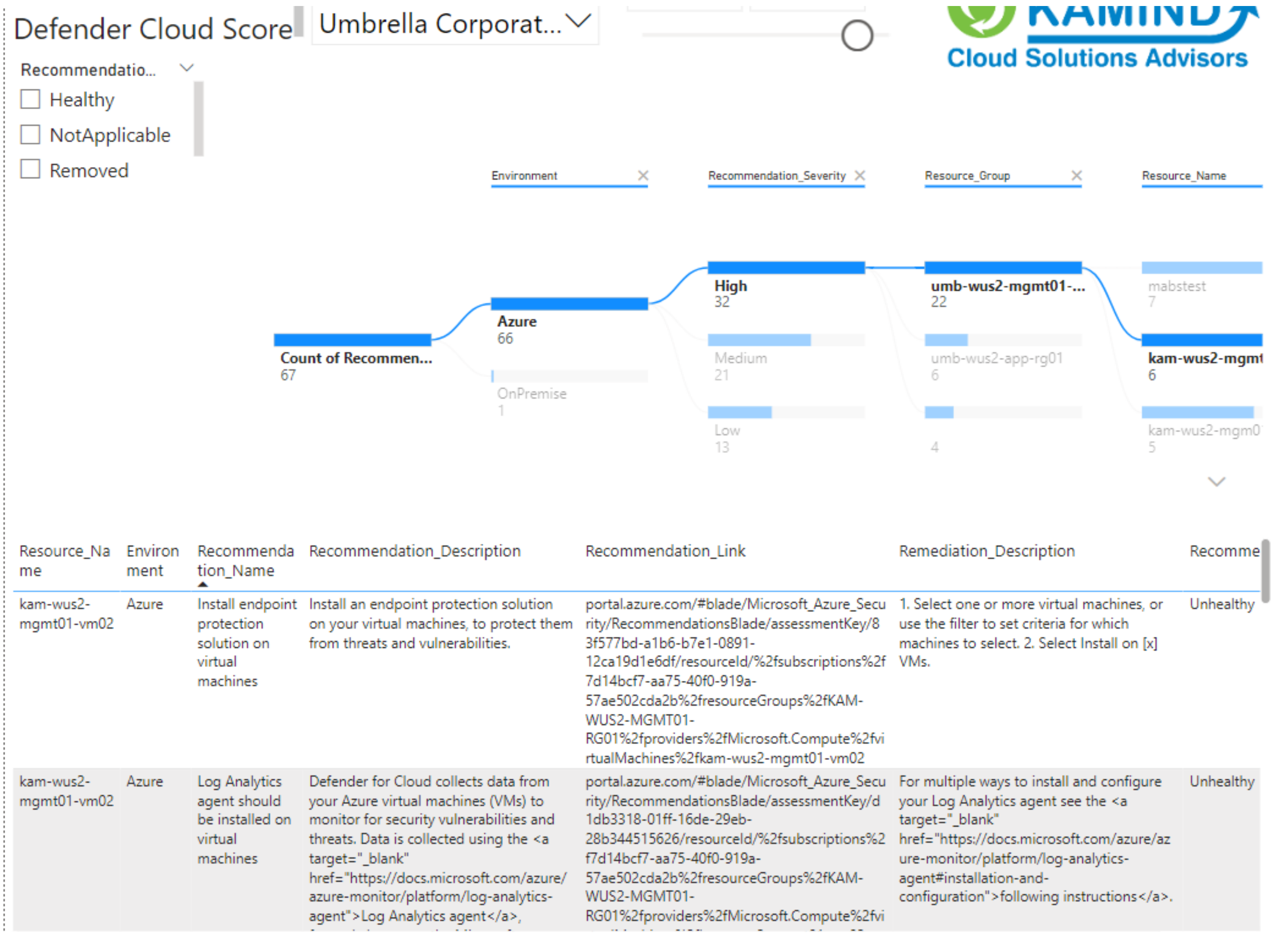


Config_Score_Impact	Exposed_Machine_Count	Exposure_Impact	Recommendation_Name	Status	Related_Component	Fix Type	Sev Score	Vendor	Date_Ente d
2.33	7	2.25	Block Adobe Reader from creating child processes	Active	Windows Server 2019	Configuration Change	9	microsoft	12/21/20 1:20:34 A
2.33	7	2.25	Block all Office applications from creating child processes	Active	Windows Server 2019	Configuration Change	9	microsoft	12/21/20 1:20:34 A
1.29	4	0.40	Block executable content from email client and webmail	Active	Windows Server 2019	Configuration Change	9	microsoft	3/19/202 7:42:35 PI
2.33	7	2.25	Block executable files from running unless they meet a prevalence, age, or trusted list criterion	Active	Windows Server 2019	Configuration Change	9	microsoft	12/21/20 1:20:34 A
1.29	4	1.20	Block JavaScript or VBScript from launching downloaded executable content	Active	Windows Server 2019	Configuration Change	9	microsoft	3/19/202 7:42:35 PI
1.17	3	2.17	Block JavaScript or VBScript from launching downloaded executable content	Active	Windows Server 2019	Configuration Change	9	microsoft	4/9/2023 7:44:22 PI
2.33	7	0.75	Block Office applications from injecting code into other processes	Active	Windows Server 2019	Configuration Change	9	microsoft	12/21/20 1:20:36 A
1.17	3	0.31	Block Office applications from	Active	Windows	Configuration	9	microsoft	4/9/2023

Defender for Cloud shows your Azure cloud security posture. It helps you

- understand your current security situation.
- efficiently and effectively improve your security posture.

Defender for Cloud continually assesses your cross-cloud resources for security issues.



Recommendatio...
□ Healthy
□ NotApplicable
□ Removed

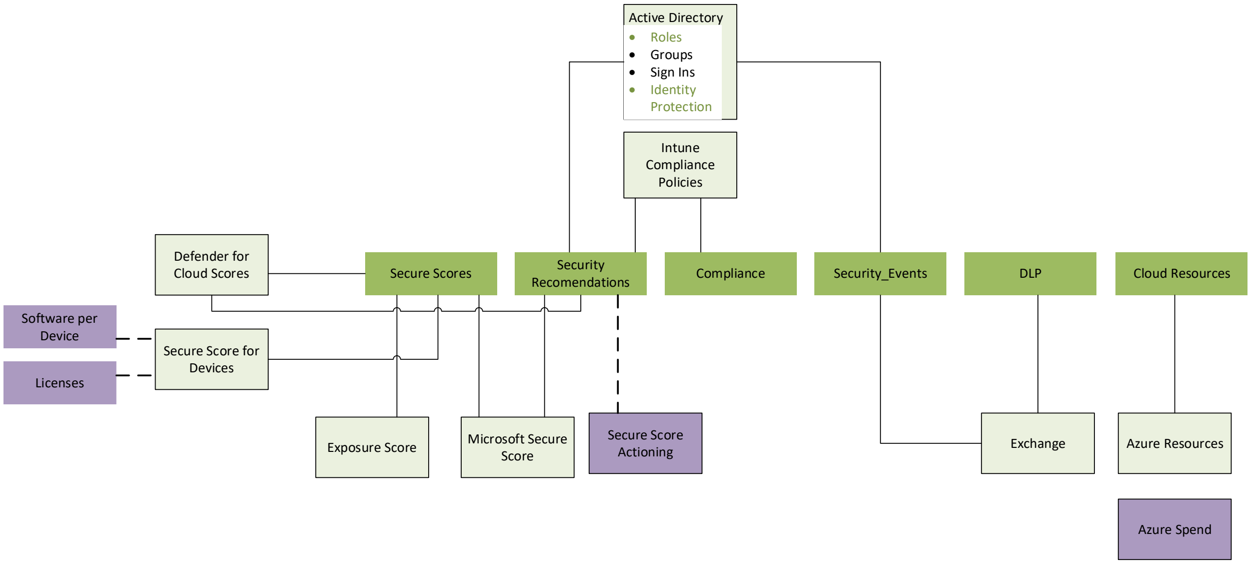
Resource_Name	Environment	Recommendation_Name	Recommendation_Description	Recommendation_Link	Remediation_Description	Recomme
kam-wus2-mgmt01-vm02	Azure	Install endpoint protection solution on virtual machines	Install an endpoint protection solution on your virtual machines, to protect them from threats and vulnerabilities.	portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/83f577bd-a1b6-b7e1-0891-12ca19d1e6df/resourceId/%2fsubscriptions%2f7d14bcf7-aa75-40f0-919a-57ae502cda2b%2fresourceGroups%2fKAM-WUS2-MGMT01-RG01%2fproviders%2fMicrosoft.Compute%2fvirtualMachines%2fkam-wus2-mgmt01-vm02	1. Select one or more virtual machines, or use the filter to set criteria for which machines to select. 2. Select Install on [x] VMs.	Unhealthy
kam-wus2-mgmt01-vm02	Azure	Log Analytics agent should be installed on virtual machines	Defender for Cloud collects data from your Azure virtual machines (VMs) to monitor for security vulnerabilities and threats. Data is collected using the <a target="_blank" href="https://docs.microsoft.com/azure/azure-monitor/platform/log-analytics-agent">Log Analytics agent</a>,	portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/d1db3318-01ff-16de-29eb-28b344515626/resourceId/%2fsubscriptions%2f7d14bcf7-aa75-40f0-919a-57ae502cda2b%2fresourceGroups%2fKAM-WUS2-MGMT01-RG01%2fproviders%2fMicrosoft.Compute%2fvi	For multiple ways to install and configure your Log Analytics agent see the <a target="_blank" href="https://docs.microsoft.com/azure/azure-monitor/platform/log-analytics-agent#installation-and-configuration">following instructions</a>.	Unhealthy

Data

Guard+ pulls data from multiple sources from within the Microsoft/Azure environment. During the Deployment stage, it sets up several Key Enablers utilizing a Service Principal to securely set up and pull data from.

1. Log Analytics
2. Sentinel
3. Microsoft Defender Products
4. Intune Compliance Policies (Windows/Android/Mac/iOS)
5. Microsoft 365 Events

Guard+ is constantly adding further details and feeds into the roadmap to provide additional value to its clients. It is built to handle Security Data in a secure and safe manner. Storing any confidential data in key vaults and secure and encrypted databases utilizing Row Level Security to guarantee data is safely stored and transported to the correct audiences.



Pricing and Availability:

Pricing is a *Flat Subscription Fee* + *Charge based on number of AD Users* + *Charge based on the Scale of Azure* Consumption For pricing details and availability, please contact our sales team directly sales@kamind.com.

Support and Onboarding:

We offer comprehensive technical support and assistance to our customers during their onboarding period, ensuring the optimal functionality and performance is provided. Optionally if you need support deploying the recommendations Guard+ exposes, KAMIND has a dedicated security and consulting team that can be engaged in a separate support agreement to help you actualize the recommendations.

Competitor Analysis:

While there may be other tools available for security posture assessment and compliance management, GUARD+ differentiates itself by providing comprehensive weekly recommendations and evidence of actions taken. This feature enhances an organization’s ability to satisfy compliance requirements and insurance mandates, giving GUARD+ a competitive advantage.

Testimonials or Case Studies:

Here are a few testimonials from our satisfied customers:

- [Customer Name]: "GUARD+ has been instrumental in providing us with solid evidence of our security measures, ensuring compliance with industry regulations and satisfying our insurance provider."

- [Customer Name]: "The documentation and reporting capabilities of GUARD+ have significantly streamlined our compliance processes and strengthened our relationships with regulatory bodies and insurance providers."

Conclusion:

KAMIND GUARD+ is a powerful cybersecurity solution that offers a comprehensive view of security posture and recommendations to manage your improvements. It logs evidence of actions taken to comply with industry regulations and satisfy insurance requirements.

GUARD+ empowers organizations to demonstrate their proactive approach to security and risk mitigation while ensuring transparency and accountability.

Frequently Asked Questions:

How long is the Trial Period:

We offer a trial period of 4-6 weeks within which you are able to evaluate the value of the data and security recommendations.

What is the commitment after the Trial Period:

Guard+ is a 1 year commitment.

System/Environment requirements:

- **Azure AD P2 License** this is for the AD logs into Sentinel,PIM and other information we pull.
- **Azure Subscription**This is for us to install the base loganalytics and Sentinal tools that we use to pull data.
- **Administrative/Owner Access** to your subscription
- **Microsoft 365**
- **Purview**
- **Defender for Endpoint** ??