KAMIND®
Cloud Solutions Advisors

Guard+

Guard+

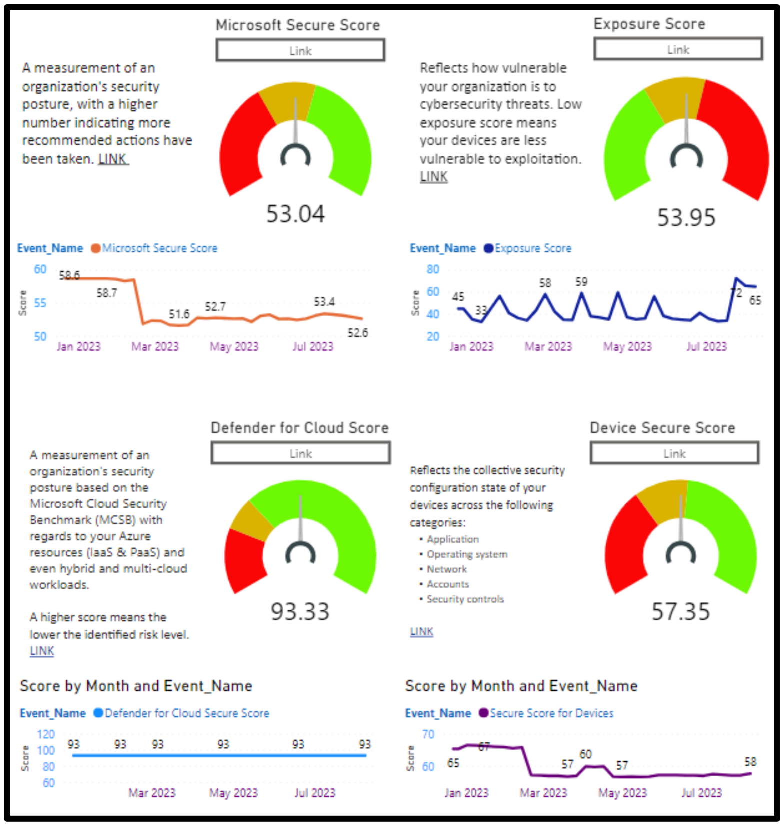
Improving your Security Posture

KAMIND® Cloud Solutions Advisors

Guard+

Improve Your Security Posture

KAMIND GUARD+ is an advanced cybersecurity solution that empowers IT Leaders to manage and improve their Security Posture. It gives them weekly IT Security Scores, a list of Security Events, recommendations and helps track actions.



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

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

Reflects the collective security configuration state of your devices across the following categories:
- Application
- Operating system
- Network
- Accounts
- Security controls

LINK

Benefits:
- Security Transparency
- Improved Planning and Tracking
- Reduction of Exposure
- Cost Effective
- Documentation & Audit Control
- Verification of Control Status

Exposure Score: The 4 exposure scores help IT Managers gain an understanding of what their security posture is and where to focus the changes they need to make.

Learn more about KAMIND Guard™ and KAMIND Guard+ at http://www.kamind.com

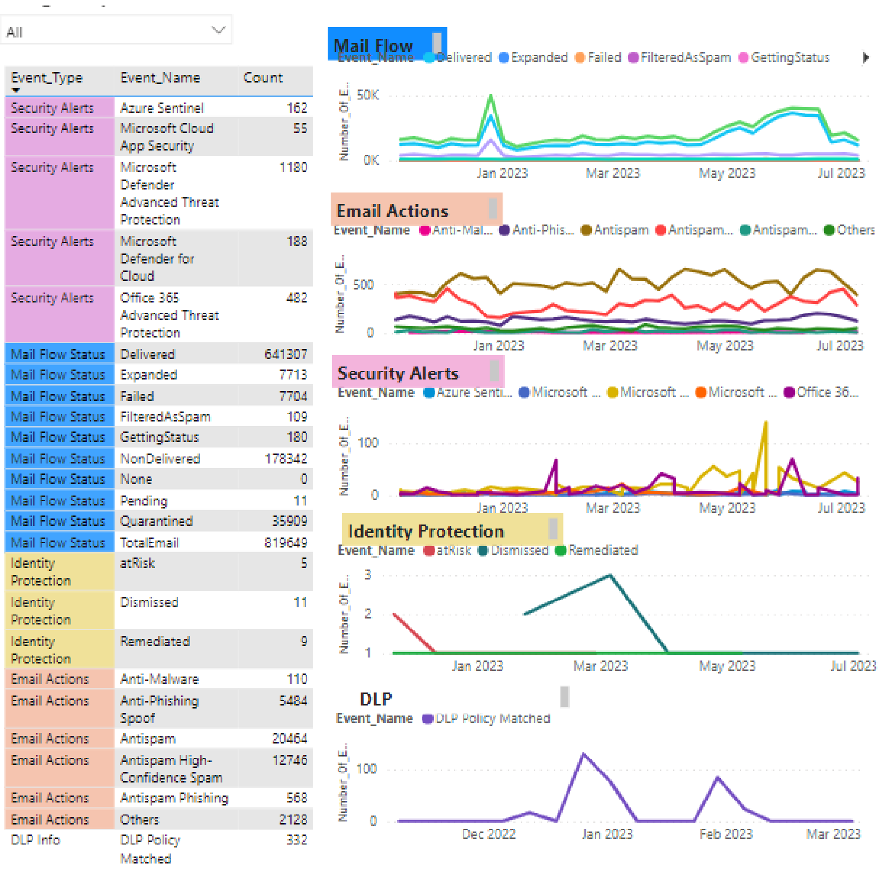
503-726-5933

KAMIND® Cloud Solutions Advisors

Improve Your Security Posture

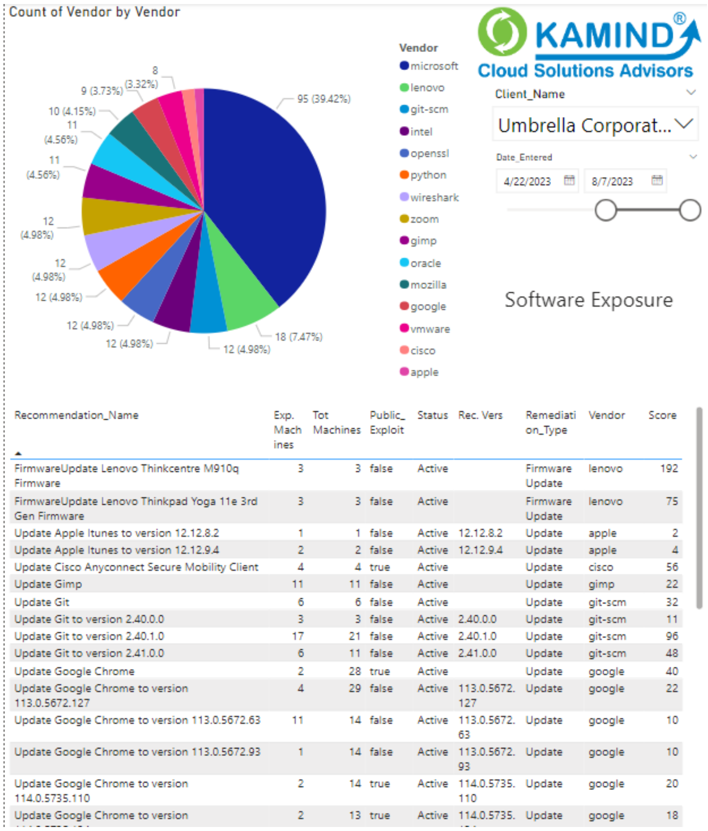
Security Events: Guard+ will pull Security events from your subscription and to enable a clear historical view of Security Events logged in your environment.

For Medium and High Security Events Guard+ breaks the items down into Type and description of the Event.



All

Event_Type	Event_Name	Count
Security Alerts	Azure Sentinel	162
Security Alerts	Microsoft Cloud App Security	55
Security Alerts	Microsoft Defender Advanced Threat Protection	1180
Security Alerts	Microsoft Defender for Cloud	188
Security Alerts	Office 365 Advanced Threat Protection	482
Mail Flow Status	Delivered	641307
Mail Flow Status	Expanded	7713
Mail Flow Status	Failed	7704
Mail Flow Status	FilteredAsSpam	109
Mail Flow Status	GettingStatus	180
Mail Flow Status	NonDelivered	178342
Mail Flow Status	None	0
Mail Flow Status	Pending	11
Mail Flow Status	Quarantined	35909
Mail Flow Status	TotalEmail	819649
Identity Protection	atRisk	5
Identity Protection	Dismissed	11
Identity Protection	Remediated	9
Email Actions	Anti-Malware	110
Email Actions	Anti-Phishing Spoof	5484
Email Actions	Antispam	20464
Email Actions	Antispam High-Confidence Spam	12746
Email Actions	Antispam Phishing	568
Email Actions	Others	2128
DLP Info	DLP Policy Matched	332



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

Software Exposure: Reports show what vulnerable software exists in an Environment.

- Software
- Vendor
- Recommendation type
- Number of Exposed machines

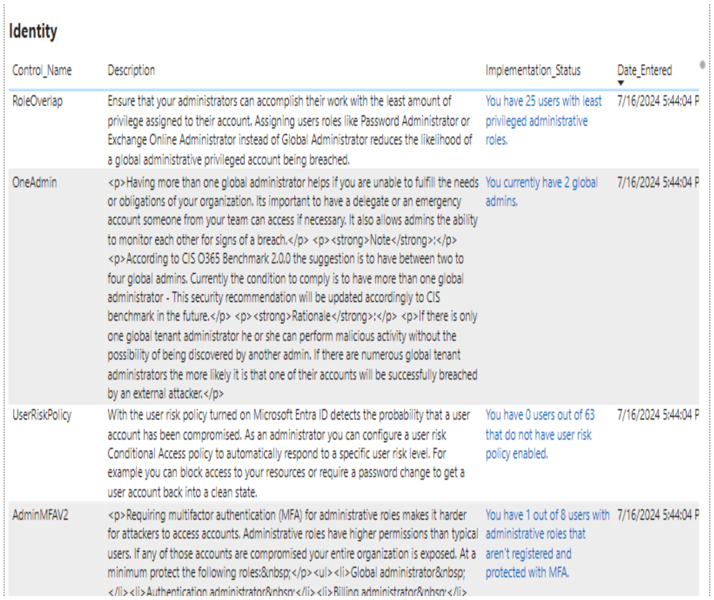
Learn more about KAMIND Guard™ and KAMIND Guard+ at http://www.kamind.com

KAMIND®
Cloud Solutions Advisors

Improve Your Security Posture

Security Recommendations: Guard+ takes the Microsoft recommended actions which are organized into:

•**Identity** Microsoft Entra accounts & roles
•**Data** through Microsoft Information Protection
•**Apps** email and cloud apps, including Office 365 and Microsoft Defender for Cloud Apps
•**ASR -** Attack Surface Reduction
•**Endpoint** Microsoft Defender for Endpoint

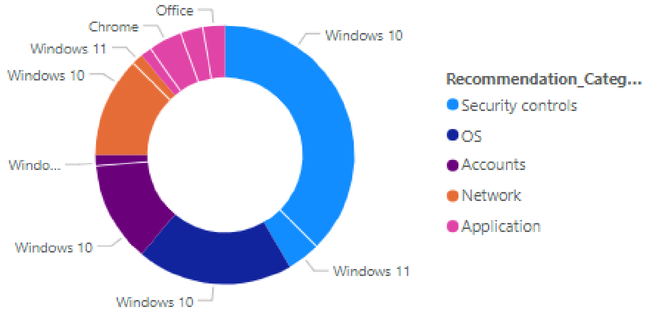


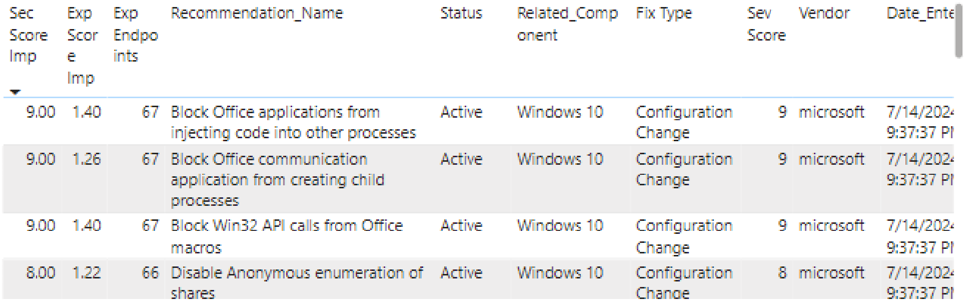
Identity

Control_Name	Description	Implementation_Status	Date_Entered
RoleOverlap	Ensure that your administrators can accomplish their work with the least amount of privilege assigned to their account. Assigning users roles like Password Administrator or Exchange Online Administrator instead of Global Administrator reduces the likelihood of a global administrative privileged account being breached.	You have 25 users with least privileged administrative roles.	7/16/2024 5:44:04 P
OneAdmin	<p>Having more than one global administrator helps if you are unable to fulfill the needs or obligations of your organization. Its important to have a delegate or an emergency account someone from your team can access if necessary. It also allows admins the ability to monitor each other for signs of a breach.</p> <p><strong>Note</strong>:</p> <p>According to CIS O365 Benchmark 2.0.0 the suggestion is to have between two to four global admins. Currently the condition to comply is to have more than one global administrator - This security recommendation will be updated accordingly to CIS benchmark in the future.</p> <p><strong>Rationale</strong>:</p> <p>If there is only one global tenant administrator he or she can perform malicious activity without the possibility of being discovered by another admin. If there are numerous global tenant administrators the more likely it is that one of their accounts will be successfully breached by an external attacker.</p>	You currently have 2 global admins.	7/16/2024 5:44:04 P
UserRiskPolicy	With the user risk policy turned on Microsoft Entra ID detects the probability that a user account has been compromised. As an administrator you can configure a user risk Conditional Access policy to automatically respond to a specific user risk level. For example you can block access to your resources or require a password change to get a user account back into a clean state.	You have 0 users out of 63 that do not have user risk policy enabled.	7/16/2024 5:44:04 P
AdminMFAV2	<p>Requiring multifactor authentication (MFA) for administrative roles makes it harder for attackers to access accounts. Administrative roles have higher permissions than typical users. If any of those accounts are compromised your entire organization is exposed. At a minimum protect the following roles:&nbsp;</p><ul><li>Global administrator&nbsp;</li><li>Authentication administrator&nbsp;</li><li>Billing administrator&nbsp;</li>	You have 1 out of 8 users with administrative roles that aren't registered and protected with MFA.	7/16/2024 5:44:04 P

Secure score for Devices: Show vulnerabilities that exist in the areas :

•Application
•Operating system
•Network
•Accounts
•Security controls

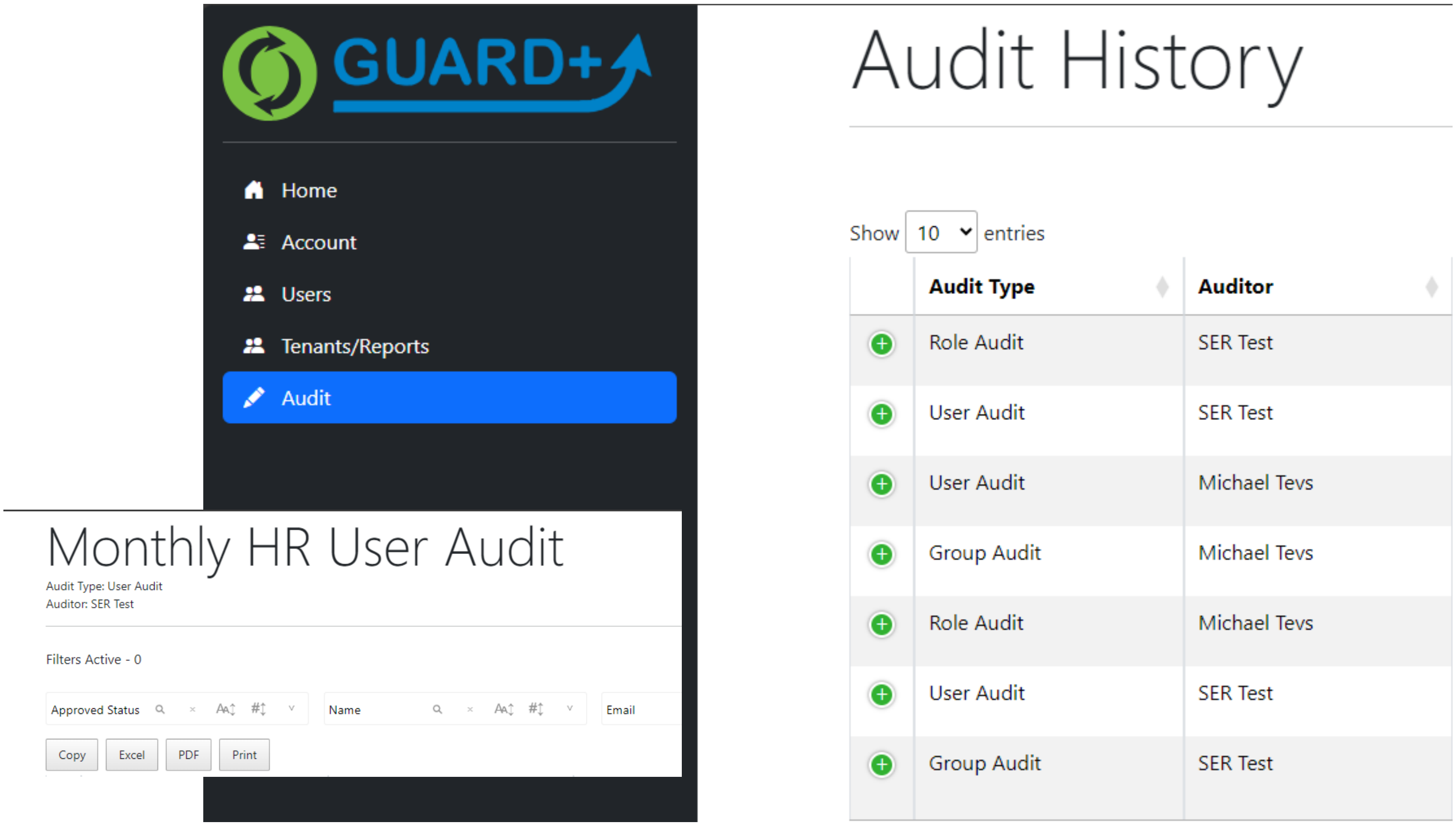




Sec Score Imp	Exp Score Imp	Exp Endpoints	Recommendation_Name	Status	Related_Component	Fix Type	Sev Score	Vendor	Date_Ente
9.00	1.40	67	Block Office applications from injecting code into other processes	Active	Windows 10	Configuration Change	9	microsoft	7/14/2024 9:37:37 PI
9.00	1.26	67	Block Office communication application from creating child processes	Active	Windows 10	Configuration Change	9	microsoft	7/14/2024 9:37:37 PI
9.00	1.40	67	Block Win32 API calls from Office macros	Active	Windows 10	Configuration Change	9	microsoft	7/14/2024 9:37:37 PI
8.00	1.22	66	Disable Anonymous enumeration of shares	Active	Windows 10	Configuration Change	8	microsoft	7/14/2024 9:37:37 PI

Learn more about KAMIND Guard™ and KAMIND Guard+ at http://www.kamind.com

KAMIND® Cloud Solutions Advisors



Monthly HR User Audit

Audit Type: User Audit
Auditor: SER Test

Filters Active - 0

Audit History

Show 10 entries

	Audit Type	Auditor
⊕	Role Audit	SER Test
⊕	User Audit	SER Test
⊕	User Audit	Michael Tevs
⊕	Group Audit	Michael Tevs
⊕	Role Audit	Michael Tevs
⊕	User Audit	SER Test
⊕	Group Audit	SER Test

Audits: Help clients provide the evidence that they need for proof of monitoring user access. This covers:

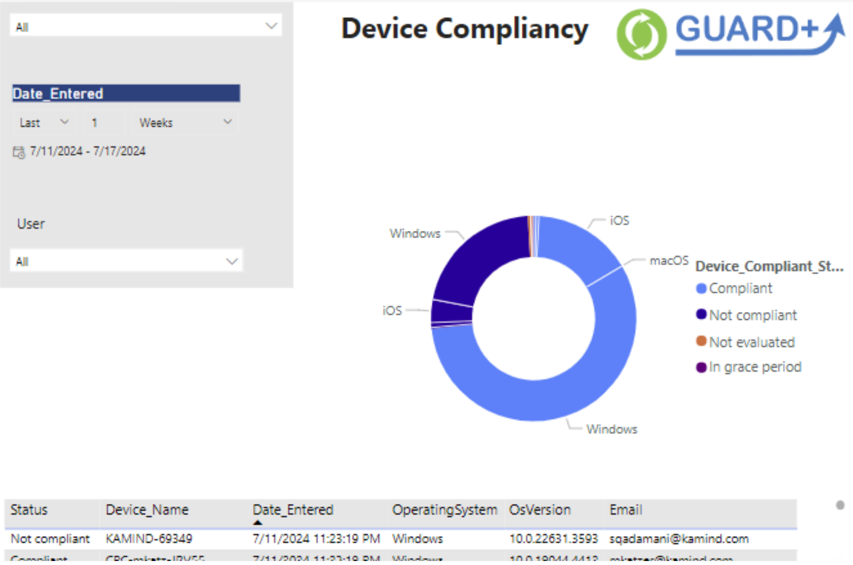
•Users
•Groups
•Roles

Guard+ provides an audit tool for the client Admins , giving them the ability to create a report that the company has reviewed the users, what roles they have and groups that they are a part of.

Guard+ clients can have a clear view of users that can authenticate and use their O365 Cloud Environment.

Learn more about KAMIND Guard™ and KAMIND Guard+ at http://www.kamind.com

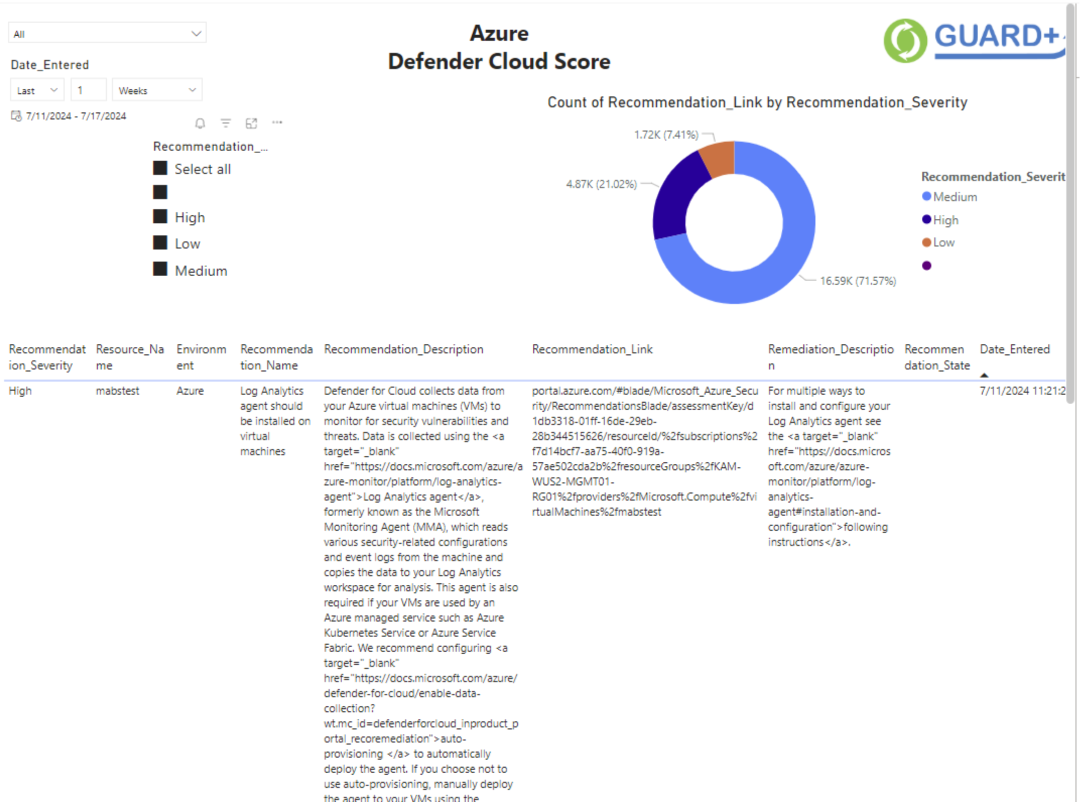
Improve Your Security Posture



Status	Device_Name	Date_Entered	OperatingSystem	OsVersion	Email
Not compliant	KAMIND-69349	7/11/2024 11:23:19 PM	Windows	10.0.22631.3593	sqadamani@kamind.com
Compliant	CPC-mkatz-IRV55	7/11/2024 11:23:19 PM	Windows	10.0.19044.4412	mkatzer@kamind.com

Device Compliance: Provides a weekly view of which devices are not compliant, who owns them and probable reasons as to why. It covers:

- •Windows devices
- •Android devices
- •IOS devices
- •MAC devices



Recommendation_Severity	Resource_Name	Environment	Recommendation_Name	Recommendation_Description	Recommendation_Link	Remediation_Description	Recommendation_State	Date_Entered
High	mabstest	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>, formerly known as the Microsoft Monitoring Agent (MMA), which reads various security-related configurations and event logs from the machine and copies the data to your Log Analytics workspace for analysis. This agent is also required if your VMs are used by an Azure managed service such as Azure Kubernetes Service or Azure Service Fabric. We recommend configuring <a target="_blank" href="https://docs.microsoft.com/azure/defender-for-cloud/enable-data-collection?wt.mc_id=defenderforcloud_inproduct_portal_recoremediation">auto-provisioning </a> to automatically deploy the agent. If you choose not to use auto-provisioning, manually deploy the agent to your VMs using the	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%2fvirtualMachines%2fmabstest	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>.		7/11/2024 11:21:2

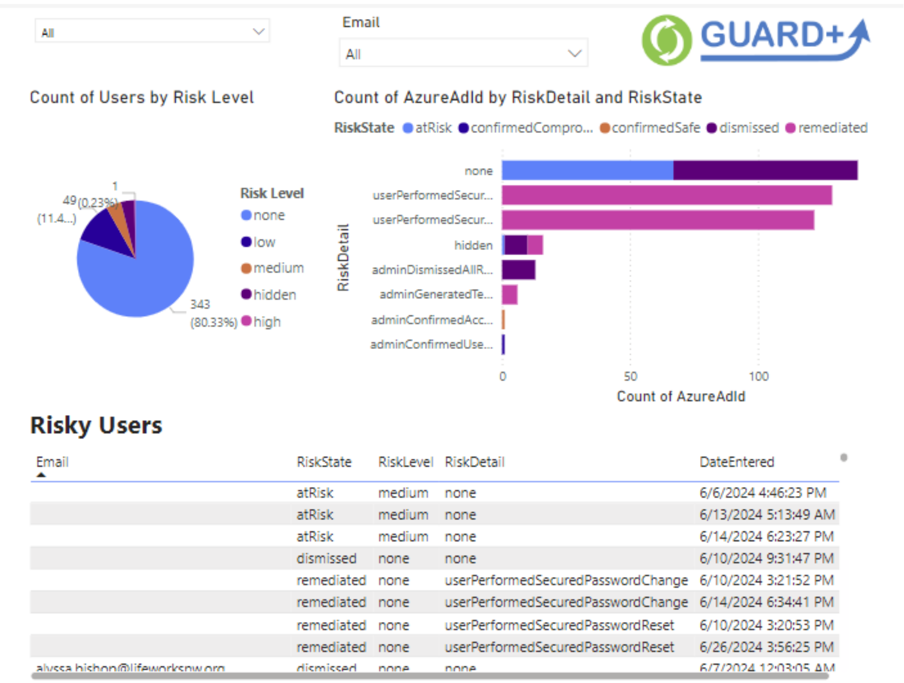
Azure Defender for Cloud: provides a secure score that aggregates security findings into a single score.

Guard+ View – Azure Recommendations

Guard+ pulls the recommendations and lists what needs to be changed and how to fix it.

Learn more about KAMIND Guard™ and KAMIND Guard+ at http://www.kamind.com

KAMIND®
Cloud Solutions Advisors



Risky Users

Email	RiskState	RiskLevel	RiskDetail	DateEntered
	atRisk	medium	none	6/6/2024 4:46:23 PM
	atRisk	medium	none	6/13/2024 5:13:49 AM
	atRisk	medium	none	6/14/2024 6:23:27 PM
	dismissed	none	none	6/10/2024 9:31:47 PM
	remediated	none	userPerformedSecuredPasswordChange	6/10/2024 3:21:52 PM
	remediated	none	userPerformedSecuredPasswordChange	6/14/2024 6:34:41 PM
	remediated	none	userPerformedSecuredPasswordReset	6/10/2024 3:20:53 PM
	remediated	none	userPerformedSecuredPasswordReset	6/26/2024 3:56:25 PM
alyssa.bishop@lifeworksnw.org	dismissed	none	none	6/7/2024 12:03:05 AM

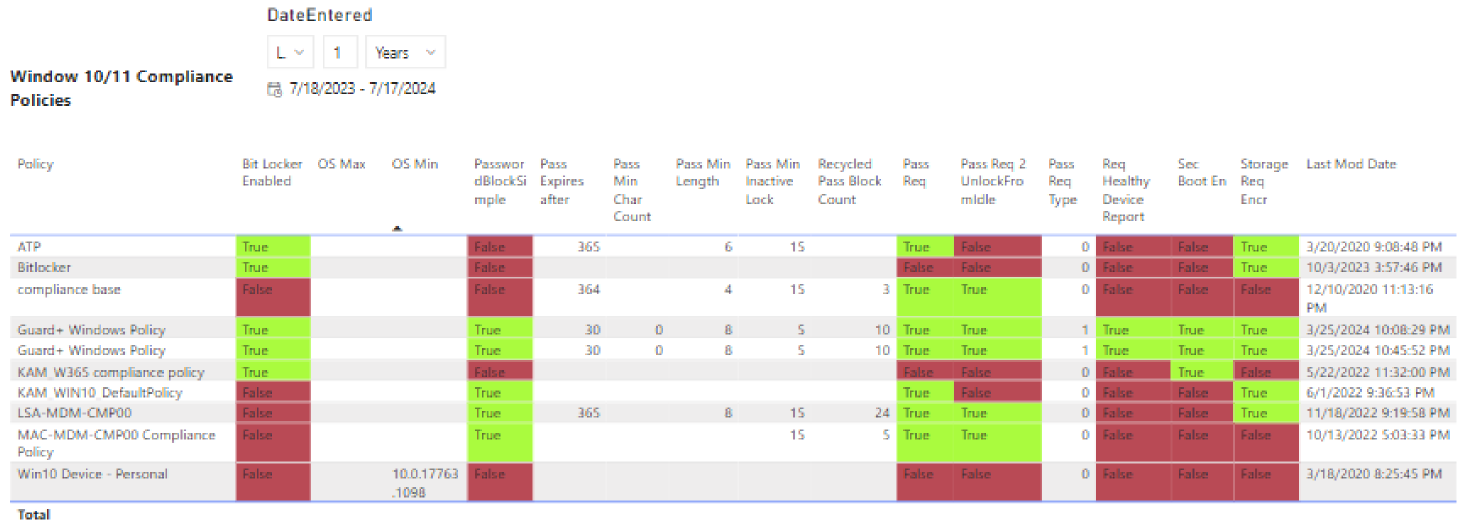
Risky Users:

- Have one or more risky sign-ins.
- One or more risks detected on the user's account, like Leaked Credentials.
- A behavior such as frequent failed sign ins, or multiple password changes in a short time frame.

The risky users report lists all users whose accounts are at risk of compromise.

Endpoint Compliance Settings:

Clients should set compliance settings for their devices (iOS, Android, Mac and Windows.) Guard+ enables clients to view their scored settings and plan changes.



Window 10/11 Compliance Policies

7/18/2023 - 7/17/2024

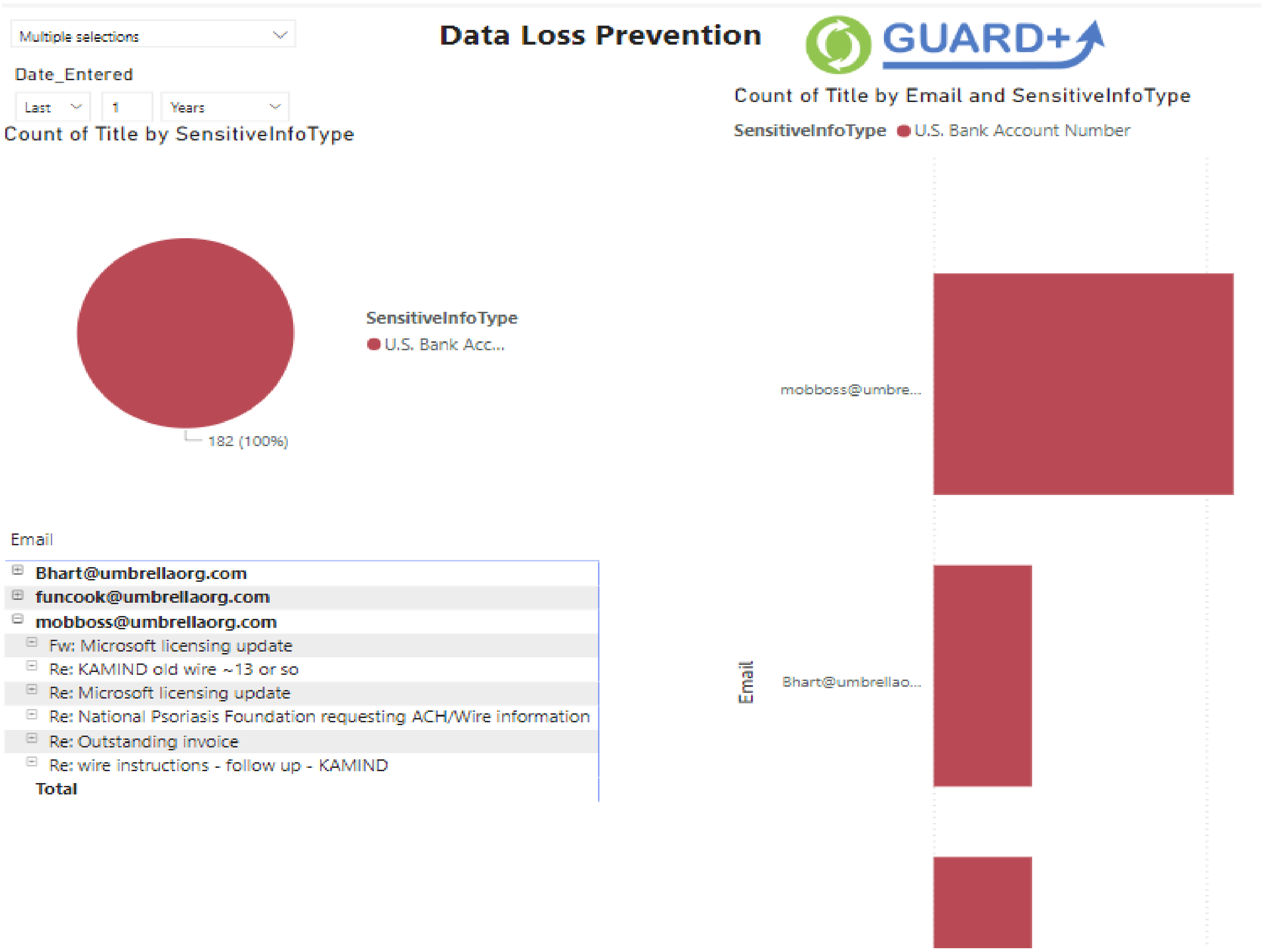
Policy	Bit Locker Enabled	OS Max	OS Min	PassworddBlockSimple	Pass Expires after	Pass Min Char Count	Pass Min Length	Pass Min Inactive Lock	Recycled Pass Block Count	Pass Req	Pass Req 2 UnlockFromIdle	Pass Req Type	Req Healthy Device Report	Sec Boot En	Storage Req Encr	Last Mod Date
ATP	True			False	365		6	15		True	False	0	False	False	True	3/20/2020 9:08:48 PM
Bitlocker	True			False						False	False	0	False	False	True	10/3/2023 3:57:46 PM
compliance base	False			False	364		4	15	3	True	True	0	False	False	False	12/10/2020 11:13:16 PM
Guard+ Windows Policy	True			True	30	0	8	5	10	True	True	1	True	True	True	3/25/2024 10:08:29 PM
Guard+ Windows Policy	True			True	30	0	8	5	10	True	True	1	True	True	True	3/25/2024 10:45:52 PM
KAM_W365 compliance policy	True			False						False	False	0	False	True	False	5/22/2022 11:32:00 PM
KAM_WIN10_DefaultPolicy	False			True						True	False	0	False	False	True	6/1/2022 9:36:53 PM
LSA-MDM-CMP00	False			True	365		8	15	24	True	True	0	False	False	True	11/18/2022 9:19:58 PM
MAC-MDM-CMP00 Compliance Policy	False			True				15	5	True	True	0	False	False	False	10/13/2022 5:03:33 PM
Win10 Device - Personal	False		10.0.17763.1098	False						False	False	0	False	False	False	3/18/2020 8:25:45 PM
Total																

Learn more about KAMIND Guard™ and KAMIND Guard+ at http://www.kamind.com

Data Loss Prevention: is a security solution that identifies and helps prevent unsafe or inappropriate sharing, transfer, or use of sensitive data. It can help your organization monitor and protect sensitive information across on-premises systems, cloud-based locations, and endpoint devices. It also helps you achieve compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR).

Guard+ View – Data Loss Prevention

Guard+ deploys templated DLP policies into a client's environment and then reports against them each week to understand what types of data are at risk.



Data Loss Prevention

Multiple selections

Date_Entered

Last 1 Years

Count of Title by SensitiveInfoType

Count of Title by Email and SensitiveInfoType

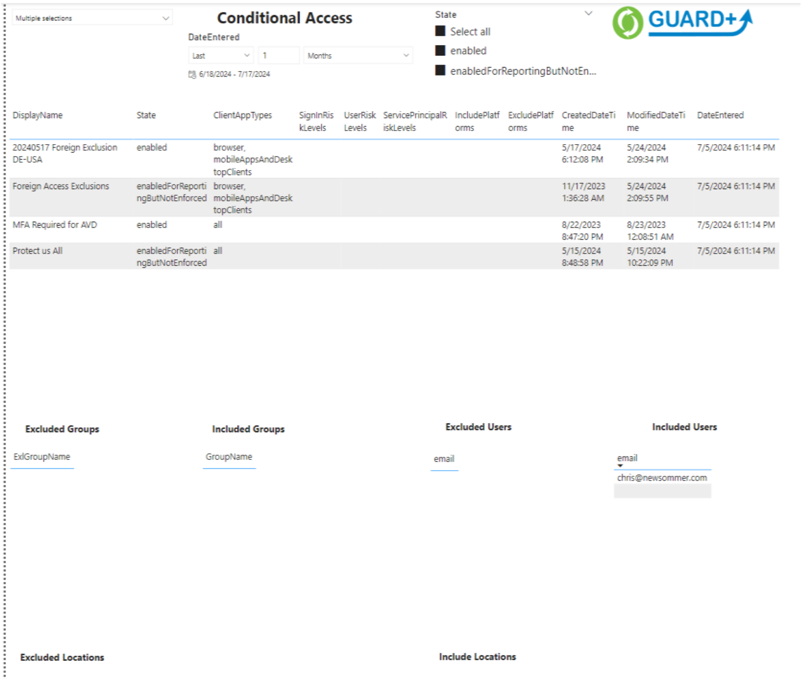
Email

- ⊞ Bhart@umbrellaorg.com
- ⊞ funcook@umbrellaorg.com
- ⊟ mobboss@umbrellaorg.com
  - ⊟ Fw: Microsoft licensing update
  - ⊟ Re: KAMIND old wire ~13 or so
  - ⊟ Re: Microsoft licensing update
  - ⊟ Re: National Psoriasis Foundation requesting ACH/Wire information
  - ⊟ Re: Outstanding invoice
  - ⊟ Re: wire instructions - follow up - KAMIND
- Total

Learn more about KAMIND Guard™ and KAMIND Guard+ at http://www.kamind.com

KAMIND® Cloud Solutions Advisors

Conditional Access (CA) is a **security policy enforcement solution** available with your Azure AD Premium P1 or Microsoft 365 Business Premium subscription. Once users initiate the log-in process with a password, the application employs If/Then logic to grant access or deny access based on certain conditions or "signals."



Multiple selections

Conditional Access

DateEntered

Last | 1 | Months

6/18/2024 - 7/17/2024

State

■ Select all

■ enabled

■ enabledForReportingButNotEn...

DisplayName	State	ClientAppTypes	SignInRiskLevels	UserRiskLevels	ServicePrincipalRiskLevels	IncludePlatforms	ExcludePlatforms	CreatedDateTime	ModifiedDateTime	DateEntered
20240517 Foreign Exclusion DE-USA	enabled	browser, mobileAppsAndDesktopClients						5/17/2024 6:12:08 PM	5/24/2024 2:09:34 PM	7/5/2024 6:11:14 PM
Foreign Access Exclusions	enabledForReportingButNotEnforced	browser, mobileAppsAndDesktopClients						11/17/2023 1:36:28 AM	5/24/2024 2:09:55 PM	7/5/2024 6:11:14 PM
MFA Required for AVD	enabled	all						8/22/2023 8:47:20 PM	8/23/2023 12:08:51 AM	7/5/2024 6:11:14 PM
Protect us All	enabledForReportingButNotEnforced	all						5/15/2024 8:48:58 PM	5/15/2024 10:22:09 PM	7/5/2024 6:11:14 PM

Excluded Groups

ExlGroupName

Included Groups

GroupName

Excluded Users

email

Included Users

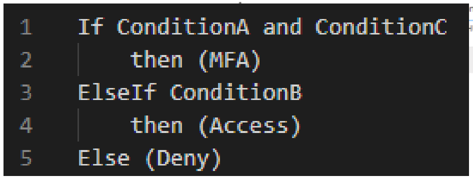
email
chris@newsommer.com

Excluded Locations

nCC
HU', 'DE', 'CZ', 'AT']

Include Locations

LocationName	IncludeLocations	LocationCC
	All	
Axis of Evil	18328f23-1860-4f0f-9208-5bed370f42fd	['SO', 'IR', 'KP']



```
If ConditionA and ConditionC
    then (MFA)
ElseIf ConditionB
    then (Access)
Else (Deny)
```

Guard+ View – Conditional Access

Conditional Access Policies:

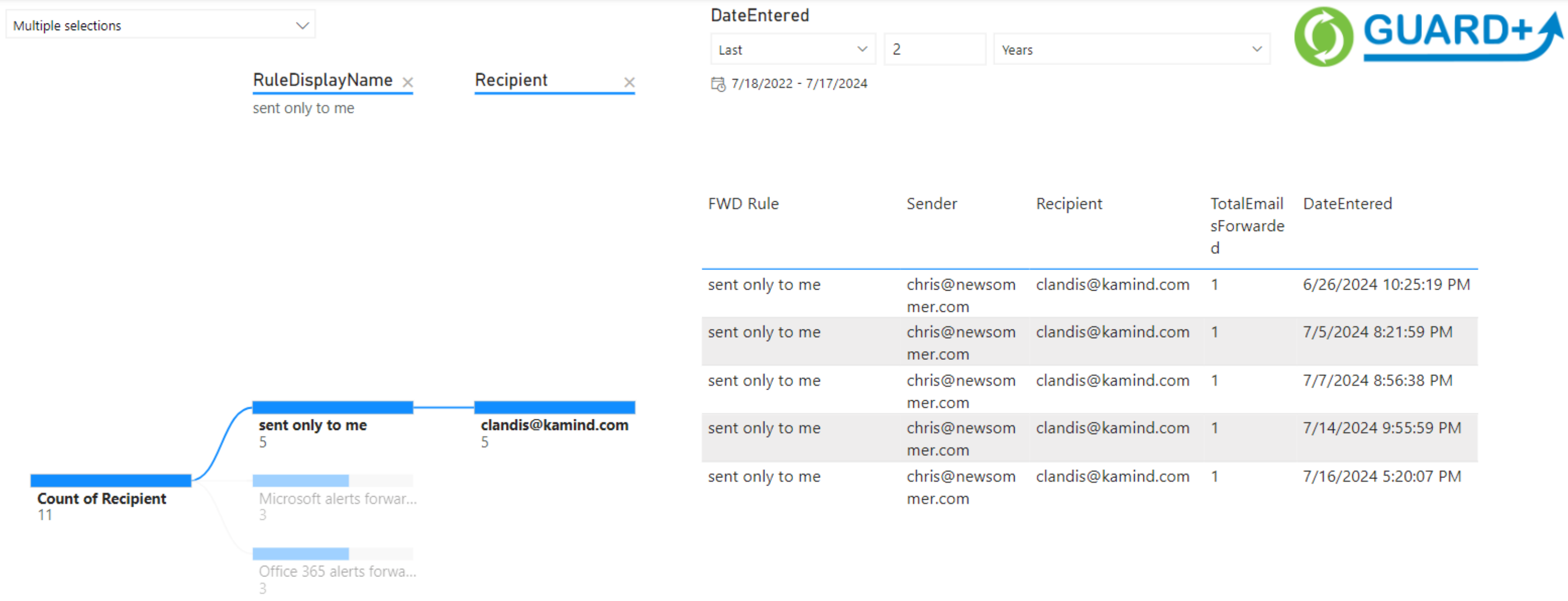
Guard+ presents all the Policies that are in place

- Policy status
- Associated client applications
- Assigned Risk Level
- Service Principal Risk Levels
- Included/excluded (Platforms/Users/Groups/Locations)

Guard+ presents both top down and bottom-up views, enabling clients to view the interactions of the policies in one page.

Learn more about KAMIND Guard™ and KAMIND Guard+ at http://www.kamind.com

Mail Forwarding: Forwarding emails to personal accounts is both a security and compliance issue. If an email contains personally identifiable information, organizations are at risk of breaching Compliance Policies, Data Loss and Standards like CMMC, GDPR and HIPAA Standards. Private accounts can be targeted by malicious attacks, and there is no telling who else could gain access to emails.



FWD Rule	Sender	Recipient	TotalEmailsForwarded	DateEntered
sent only to me	chris@newsommer.com	clandis@kamind.com	1	6/26/2024 10:25:19 PM
sent only to me	chris@newsommer.com	clandis@kamind.com	1	7/5/2024 8:21:59 PM
sent only to me	chris@newsommer.com	clandis@kamind.com	1	7/7/2024 8:56:38 PM
sent only to me	chris@newsommer.com	clandis@kamind.com	1	7/14/2024 9:55:59 PM
sent only to me	chris@newsommer.com	clandis@kamind.com	1	7/16/2024 5:20:07 PM

Guard+ View – Mail Forwarding

Guard+ evaluates and reports what Rules are in place, for each Sender, who the recipients and how often an email is forwarded. Allowing the IT manager to evaluate if something needs to be addressed or not.

Learn more about KAMIND Guard™ and KAMIND Guard+ at http://www.kamind.com

Provide Proof of Execution

KAMIND recognizes that you or your clients are potentially starting the journey to CMMC compliance, which requires you to capture evidence of your environment's maturity.

Guard+ is beginning to capture evidence from Microsoft environments to provide a consistent weekly view of your environment's settings.

AC
IA
CM
SI

Back to Security Reports

Guard+ is Available for Commercial Office 365, Azure Government and Office 365 GCC High.

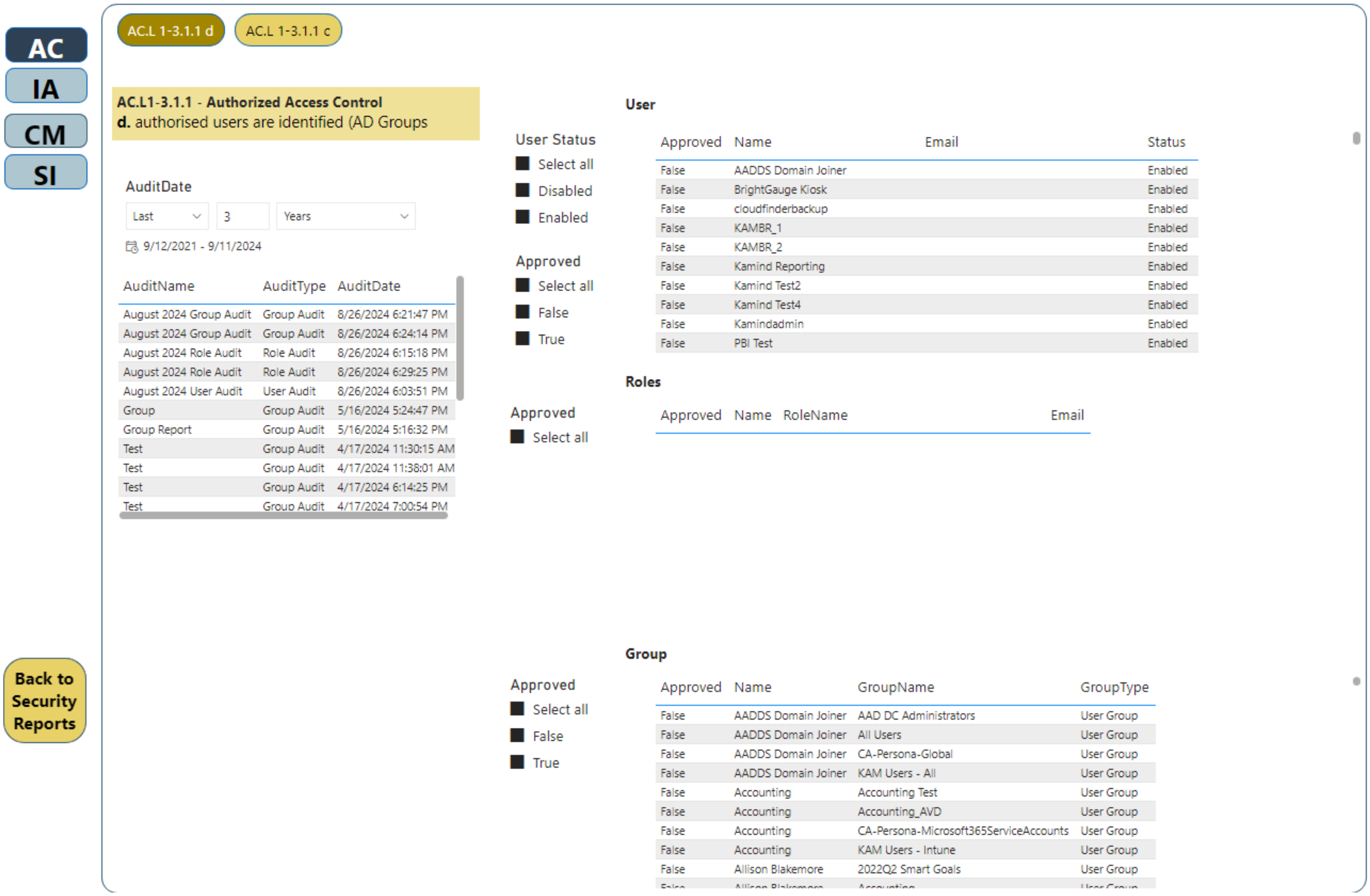
Learn more about KAMIND Guard™ and KAMIND Guard+ at http://www.kamind.com

KAMIND® Cloud Solutions Advisors

Provide Proof of Execution

Guard+ provides a supplementary service that enables an authorized user to audit your Users / Groups / Roles.

The report provides evidence that you have reviewed access to your environment.



AC.L1-3.1.1 - Authorized Access Control
d. authorised users are identified (AD Groups

AuditDate

Last | 3 | Years

9/12/2021 - 9/11/2024

AuditName	AuditType	AuditDate
August 2024 Group Audit	Group Audit	8/26/2024 6:21:47 PM
August 2024 Group Audit	Group Audit	8/26/2024 6:24:14 PM
August 2024 Role Audit	Role Audit	8/26/2024 6:15:18 PM
August 2024 Role Audit	Role Audit	8/26/2024 6:29:25 PM
August 2024 User Audit	User Audit	8/26/2024 6:03:51 PM
Group	Group Audit	5/16/2024 5:24:47 PM
Group Report	Group Audit	5/16/2024 5:16:32 PM
Test	Group Audit	4/17/2024 11:30:15 AM
Test	Group Audit	4/17/2024 11:38:01 AM
Test	Group Audit	4/17/2024 6:14:25 PM
Test	Group Audit	4/17/2024 7:00:54 PM

User Status
■ Select all
■ Disabled
■ Enabled

Approved
■ Select all
■ False
■ True

User

Approved	Name	Email	Status
False	AADDS Domain Joiner		Enabled
False	BrightGauge Kiosk		Enabled
False	cloudfinderbackup		Enabled
False	KAMBR_1		Enabled
False	KAMBR_2		Enabled
False	Kamind Reporting		Enabled
False	Kamind Test2		Enabled
False	Kamind Test4		Enabled
False	Kamindadmin		Enabled
False	PBI Test		Enabled

Approved
■ Select all

Roles

Approved	Name	RoleName	Email

Approved
■ Select all
■ False
■ True

Group

Approved	Name	GroupName	GroupType
False	AADDS Domain Joiner	AAD DC Administrators	User Group
False	AADDS Domain Joiner	All Users	User Group
False	AADDS Domain Joiner	CA-Persona-Global	User Group
False	AADDS Domain Joiner	KAM Users - All	User Group
False	Accounting	Accounting Test	User Group
False	Accounting	Accounting_AVD	User Group
False	Accounting	CA-Persona-Microsoft365ServiceAccounts	User Group
False	Accounting	KAM Users - Intune	User Group
False	Allison Blakemore	2022Q2 Smart Goals	User Group
False	Allison Blakemore	Accounting	User Group

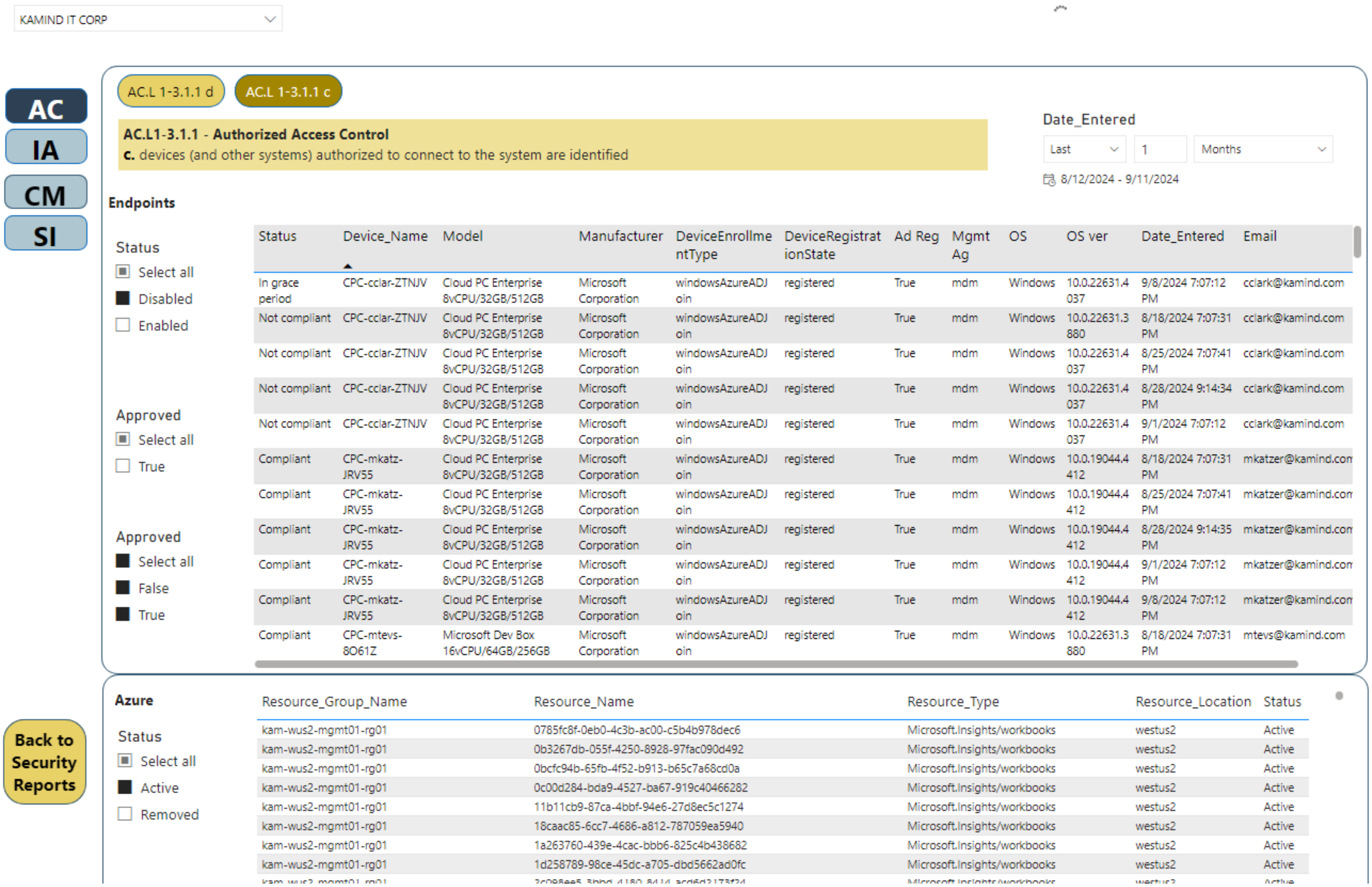
You can filter the audits by date, type, user, group, role as well as approved, enabled or disabled.

Learn more about KAMIND Guard™ and KAMIND Guard+ at http://www.kamind.com

Provide Proof of Execution

AC.L1-3.1.1(c) is a Cybersecurity Maturity Model (CMMC) practice that controls system access based on a user's, process's, or device's identity.

Guard+ captures all devices that are managed by Microsoft and registered in the Active Directory.



KAMIND IT CORP

AC.L1-3.1.1 - Authorized Access Control
c. devices (and other systems) authorized to connect to the system are identified

Date_Entered
Last | 1 | Months
8/12/2024 - 9/11/2024

Endpoints

Status
▣ Select all
■ Disabled
□ Enabled

Approved
▣ Select all
□ True

Approved
■ Select all
■ False
■ True

Status	Device_Name	Model	Manufacturer	DeviceEnrollmentType	DeviceRegistrationState	Ad Reg	Mgmt Ag	OS	OS ver	Date_Entered	Email
In grace period	CPC-cclar-ZTNJV	Cloud PC Enterprise 8vCPU/32GB/512GB	Microsoft Corporation	windowsAzureADJoin	registered	True	mdm	Windows	10.0.22631.4037	9/8/2024 7:07:12 PM	cclark@kamind.com
Not compliant	CPC-cclar-ZTNJV	Cloud PC Enterprise 8vCPU/32GB/512GB	Microsoft Corporation	windowsAzureADJoin	registered	True	mdm	Windows	10.0.22631.3880	8/18/2024 7:07:31 PM	cclark@kamind.com
Not compliant	CPC-cclar-ZTNJV	Cloud PC Enterprise 8vCPU/32GB/512GB	Microsoft Corporation	windowsAzureADJoin	registered	True	mdm	Windows	10.0.22631.4037	8/25/2024 7:07:41 PM	cclark@kamind.com
Not compliant	CPC-cclar-ZTNJV	Cloud PC Enterprise 8vCPU/32GB/512GB	Microsoft Corporation	windowsAzureADJoin	registered	True	mdm	Windows	10.0.22631.4037	8/28/2024 9:14:34 PM	cclark@kamind.com
Not compliant	CPC-cclar-ZTNJV	Cloud PC Enterprise 8vCPU/32GB/512GB	Microsoft Corporation	windowsAzureADJoin	registered	True	mdm	Windows	10.0.22631.4037	9/1/2024 7:07:12 PM	cclark@kamind.com
Compliant	CPC-mkatz-JRV55	Cloud PC Enterprise 8vCPU/32GB/512GB	Microsoft Corporation	windowsAzureADJoin	registered	True	mdm	Windows	10.0.19044.4412	8/18/2024 7:07:31 PM	mkatzer@kamind.com
Compliant	CPC-mkatz-JRV55	Cloud PC Enterprise 8vCPU/32GB/512GB	Microsoft Corporation	windowsAzureADJoin	registered	True	mdm	Windows	10.0.19044.4412	8/25/2024 7:07:41 PM	mkatzer@kamind.com
Compliant	CPC-mkatz-JRV55	Cloud PC Enterprise 8vCPU/32GB/512GB	Microsoft Corporation	windowsAzureADJoin	registered	True	mdm	Windows	10.0.19044.4412	8/28/2024 9:14:35 PM	mkatzer@kamind.com
Compliant	CPC-mkatz-JRV55	Cloud PC Enterprise 8vCPU/32GB/512GB	Microsoft Corporation	windowsAzureADJoin	registered	True	mdm	Windows	10.0.19044.4412	9/1/2024 7:07:12 PM	mkatzer@kamind.com
Compliant	CPC-mkatz-JRV55	Cloud PC Enterprise 8vCPU/32GB/512GB	Microsoft Corporation	windowsAzureADJoin	registered	True	mdm	Windows	10.0.19044.4412	9/8/2024 7:07:12 PM	mkatzer@kamind.com
Compliant	CPC-mtevs-8O61Z	Microsoft Dev Box 16vCPU/64GB/256GB	Microsoft Corporation	windowsAzureADJoin	registered	True	mdm	Windows	10.0.22631.3880	8/18/2024 7:07:31 PM	mtevs@kamind.com

Azure

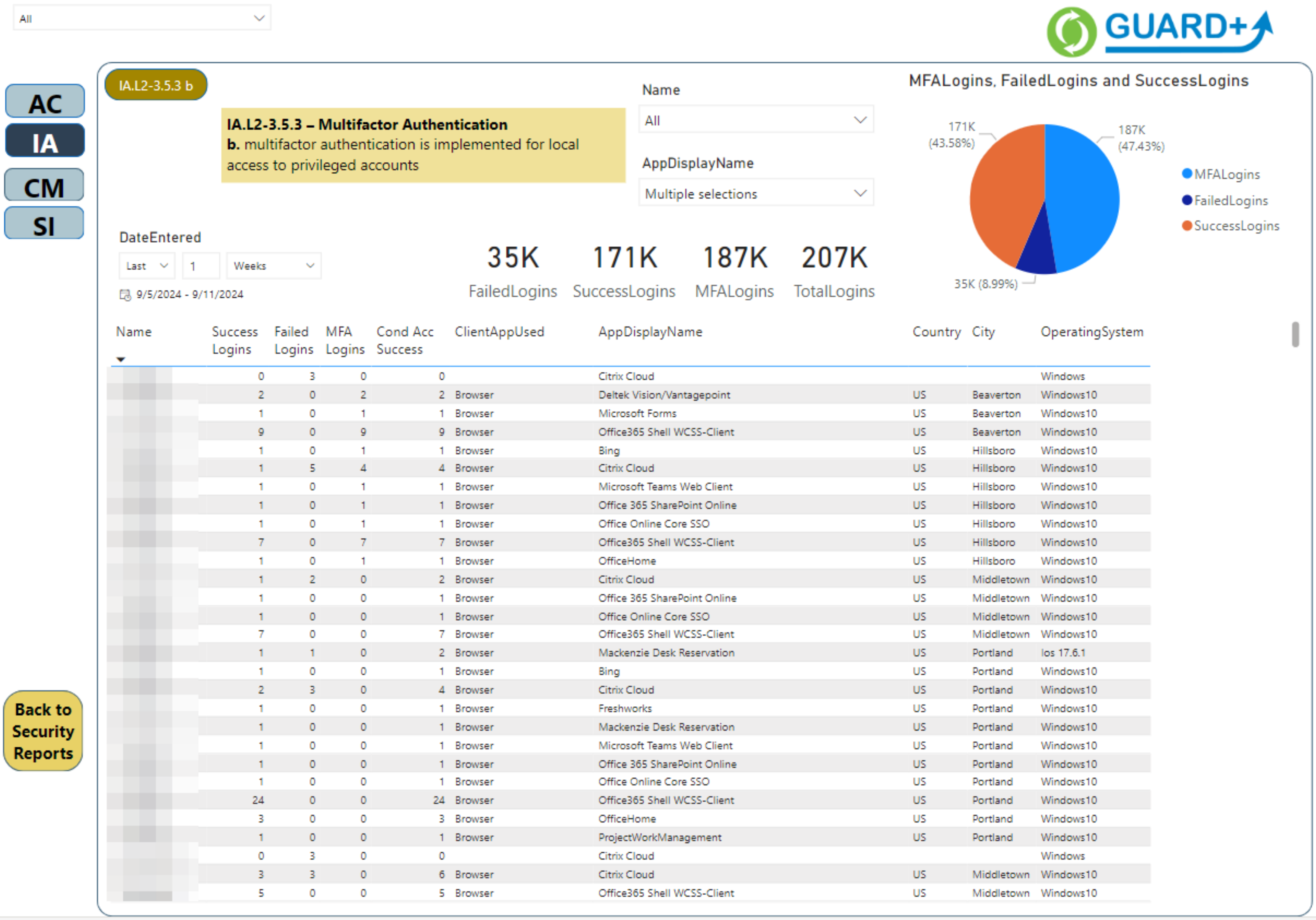
Status
▣ Select all
■ Active
□ Removed

Resource_Group_Name	Resource_Name	Resource_Type	Resource_Location	Status
kam-wus2-mgmt01-rg01	0785fc8f-0eb0-4c3b-ac00-c5b4b978dec6	Microsoft.Insights/workbooks	westus2	Active
kam-wus2-mgmt01-rg01	0b3267db-055f-4250-8928-97fac090d492	Microsoft.Insights/workbooks	westus2	Active
kam-wus2-mgmt01-rg01	0bcfc94b-65fb-4f52-b913-b65c7a68cd0a	Microsoft.Insights/workbooks	westus2	Active
kam-wus2-mgmt01-rg01	0c00d284-bda9-4527-ba67-919c40466282	Microsoft.Insights/workbooks	westus2	Active
kam-wus2-mgmt01-rg01	11b11cb9-87ca-4bbf-94e6-27d8ec5c1274	Microsoft.Insights/workbooks	westus2	Active
kam-wus2-mgmt01-rg01	18caac85-6cc7-4686-a812-787059ea5940	Microsoft.Insights/workbooks	westus2	Active
kam-wus2-mgmt01-rg01	1a263760-439e-4cac-bbb6-825c4b438682	Microsoft.Insights/workbooks	westus2	Active
kam-wus2-mgmt01-rg01	1d258789-98ce-45dc-a705-dbd5662ad0fc	Microsoft.Insights/workbooks	westus2	Active
kam-wus2-mgmt01-rg01	[illegible]	Microsoft.Insights/workbooks	westus2	Active

Learn more about KAMIND Guard™ and KAMIND Guard+ at http://www.kamind.com

IA.L2-3.5.3

Multifactor Authentication: Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.



IA.L2-3.5.3 – Multifactor Authentication
b. multifactor authentication is implemented for local access to privileged accounts

Name: All

AppDisplayName: Multiple selections

DateEntered: Last 1 Weeks

9/5/2024 - 9/11/2024

35K FailedLogins | 171K SuccessLogins | 187K MFALogins | 207K TotalLogins

MFALogins, FailedLogins and SuccessLogins

Name	Success Logins	Failed Logins	MFA Logins	Cond Acc Success	ClientAppUsed	AppDisplayName	Country	City	OperatingSystem
[redacted]	0	3	0	0		Citrix Cloud			Windows
[redacted]	2	0	2	2	Browser	Deltek Vision/Vantagepoint	US	Beaverton	Windows10
[redacted]	1	0	1	1	Browser	Microsoft Forms	US	Beaverton	Windows10
[redacted]	9	0	9	9	Browser	Office365 Shell WCSS-Client	US	Beaverton	Windows10
[redacted]	1	0	1	1	Browser	Bing	US	Hillsboro	Windows10
[redacted]	1	5	4	4	Browser	Citrix Cloud	US	Hillsboro	Windows10
[redacted]	1	0	1	1	Browser	Microsoft Teams Web Client	US	Hillsboro	Windows10
[redacted]	1	0	1	1	Browser	Office 365 SharePoint Online	US	Hillsboro	Windows10
[redacted]	1	0	1	1	Browser	Office Online Core SSO	US	Hillsboro	Windows10
[redacted]	7	0	7	7	Browser	Office365 Shell WCSS-Client	US	Hillsboro	Windows10
[redacted]	1	0	1	1	Browser	OfficeHome	US	Hillsboro	Windows10
[redacted]	1	2	0	2	Browser	Citrix Cloud	US	Middletown	Windows10
[redacted]	1	0	0	1	Browser	Office 365 SharePoint Online	US	Middletown	Windows10
[redacted]	1	0	0	1	Browser	Office Online Core SSO	US	Middletown	Windows10
[redacted]	7	0	0	7	Browser	Office365 Shell WCSS-Client	US	Middletown	Windows10
[redacted]	1	1	0	2	Browser	Mackenzie Desk Reservation	US	Portland	Ios 17.6.1
[redacted]	1	0	0	1	Browser	Bing	US	Portland	Windows10
[redacted]	2	3	0	4	Browser	Citrix Cloud	US	Portland	Windows10
[redacted]	1	0	0	1	Browser	Freshworks	US	Portland	Windows10
[redacted]	1	0	0	1	Browser	Mackenzie Desk Reservation	US	Portland	Windows10
[redacted]	1	0	0	1	Browser	Microsoft Teams Web Client	US	Portland	Windows10
[redacted]	1	0	0	1	Browser	Office 365 SharePoint Online	US	Portland	Windows10
[redacted]	1	0	0	1	Browser	Office Online Core SSO	US	Portland	Windows10
[redacted]	24	0	0	24	Browser	Office365 Shell WCSS-Client	US	Portland	Windows10
[redacted]	3	0	0	3	Browser	OfficeHome	US	Portland	Windows10
[redacted]	1	0	0	1	Browser	ProjectWorkManagement	US	Portland	Windows10
[redacted]	0	3	0	0		Citrix Cloud			Windows
[redacted]	3	3	0	6	Browser	Citrix Cloud	US	Middletown	Windows10
[redacted]	5	0	0	5	Browser	Office365 Shell WCSS-Client	US	Middletown	Windows10

Guard+ evaluates and reports what Rules are in place, for each Sender, who the recipients are and how often an email is forwarded. This allows the IT manager to evaluate if something needs to be addressed or not.

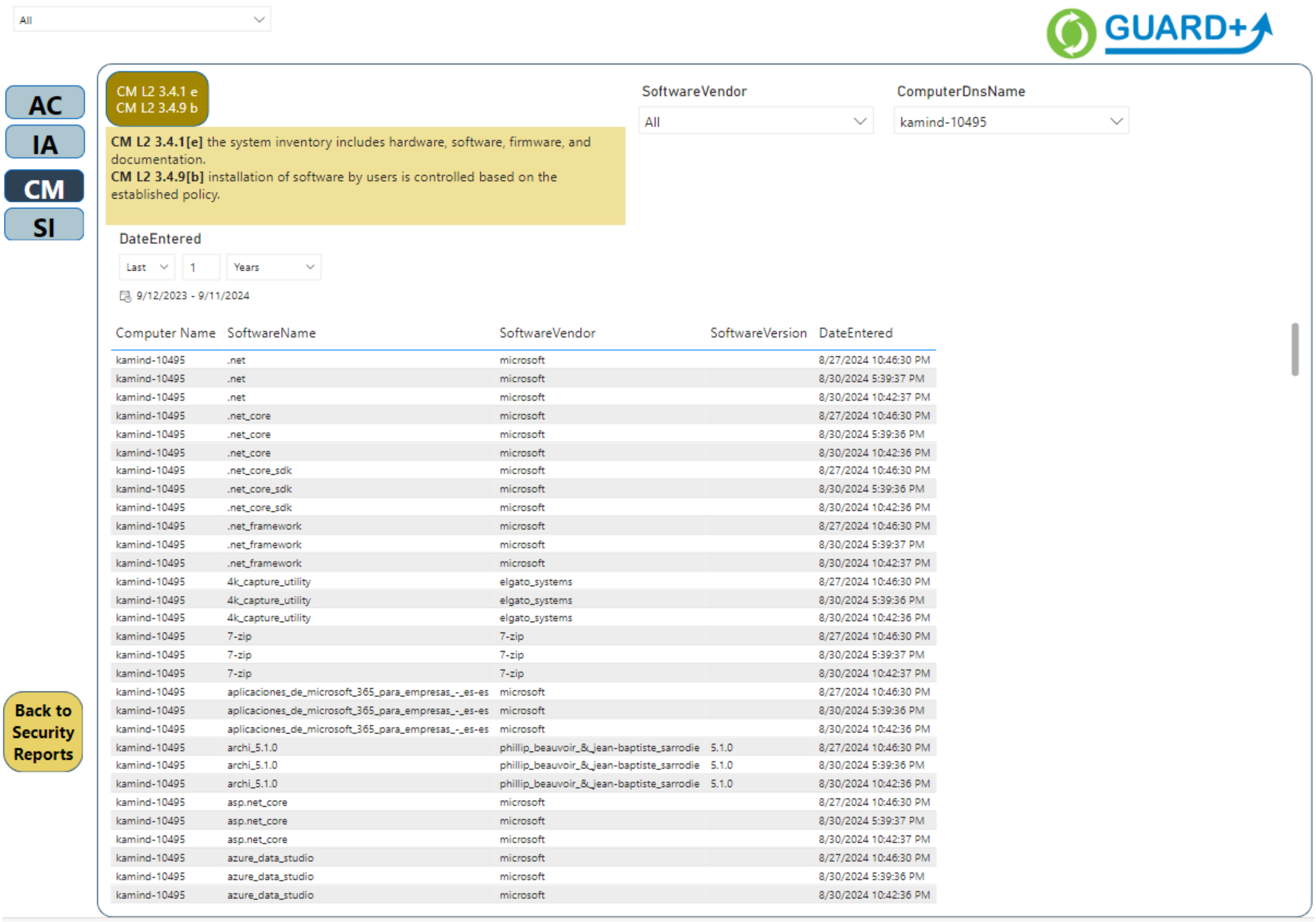
Learn more about KAMIND Guard™ and KAMIND Guard+ at http://www.kamind.com

KAMIND® Cloud Solutions Advisors

CM.L2-3.4.1 – SYSTEM BASELINING

Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective systems development life cycles.

Software per Device: Guard+ pulls the list of software that is running on each endpoint that is registered in Active Directory.



CM L2 3.4.1[e] the system inventory includes hardware, software, firmware, and documentation.
CM L2 3.4.9[b] installation of software by users is controlled based on the established policy.

SoftwareVendor: All

ComputerDnsName: kamind-10495

DateEntered: Last 1 Years

9/12/2023 - 9/11/2024

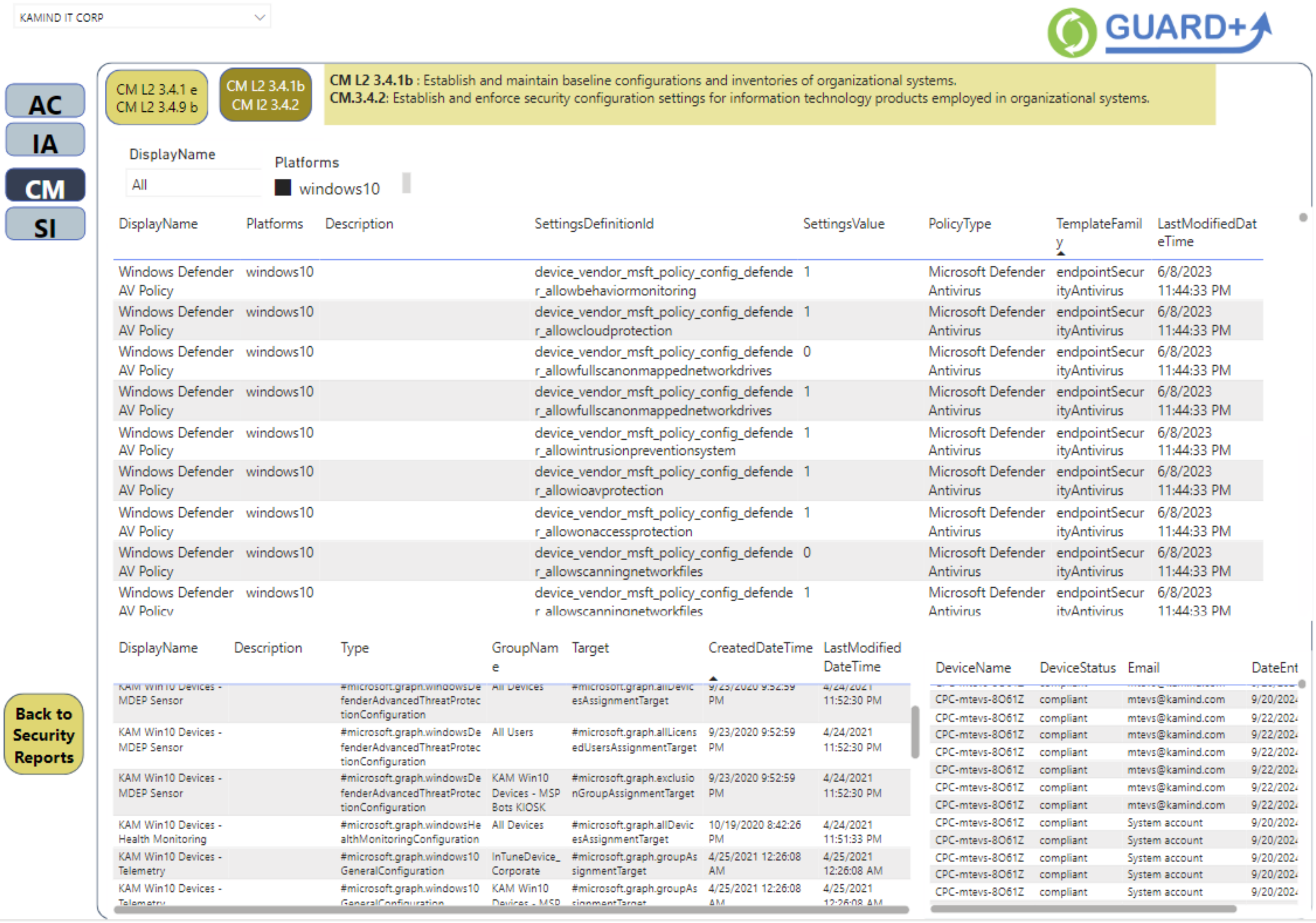
Computer Name	SoftwareName	SoftwareVendor	SoftwareVersion	DateEntered
kamind-10495	.net	microsoft		8/27/2024 10:46:30 PM
kamind-10495	.net	microsoft		8/30/2024 5:39:37 PM
kamind-10495	.net	microsoft		8/30/2024 10:42:37 PM
kamind-10495	.net_core	microsoft		8/27/2024 10:46:30 PM
kamind-10495	.net_core	microsoft		8/30/2024 5:39:36 PM
kamind-10495	.net_core	microsoft		8/30/2024 10:42:36 PM
kamind-10495	.net_core_sdk	microsoft		8/27/2024 10:46:30 PM
kamind-10495	.net_core_sdk	microsoft		8/30/2024 5:39:36 PM
kamind-10495	.net_core_sdk	microsoft		8/30/2024 10:42:36 PM
kamind-10495	.net_framework	microsoft		8/27/2024 10:46:30 PM
kamind-10495	.net_framework	microsoft		8/30/2024 5:39:37 PM
kamind-10495	.net_framework	microsoft		8/30/2024 10:42:37 PM
kamind-10495	4k_capture_utility	elgato_systems		8/27/2024 10:46:30 PM
kamind-10495	4k_capture_utility	elgato_systems		8/30/2024 5:39:36 PM
kamind-10495	4k_capture_utility	elgato_systems		8/30/2024 10:42:36 PM
kamind-10495	7-zip	7-zip		8/27/2024 10:46:30 PM
kamind-10495	7-zip	7-zip		8/30/2024 5:39:37 PM
kamind-10495	7-zip	7-zip		8/30/2024 10:42:37 PM
kamind-10495	aplicaciones_de_microsoft_365_para_empresas_-_es-es	microsoft		8/27/2024 10:46:30 PM
kamind-10495	aplicaciones_de_microsoft_365_para_empresas_-_es-es	microsoft		8/30/2024 5:39:36 PM
kamind-10495	aplicaciones_de_microsoft_365_para_empresas_-_es-es	microsoft		8/30/2024 10:42:36 PM
kamind-10495	archi_5.1.0	phillip_beauvoir_&_jean-baptiste_sarrodie	5.1.0	8/27/2024 10:46:30 PM
kamind-10495	archi_5.1.0	phillip_beauvoir_&_jean-baptiste_sarrodie	5.1.0	8/30/2024 5:39:36 PM
kamind-10495	archi_5.1.0	phillip_beauvoir_&_jean-baptiste_sarrodie	5.1.0	8/30/2024 10:42:36 PM
kamind-10495	asp.net_core	microsoft		8/27/2024 10:46:30 PM
kamind-10495	asp.net_core	microsoft		8/30/2024 5:39:37 PM
kamind-10495	asp.net_core	microsoft		8/30/2024 10:42:37 PM
kamind-10495	azure_data_studio	microsoft		8/27/2024 10:46:30 PM
kamind-10495	azure_data_studio	microsoft		8/30/2024 5:39:36 PM
kamind-10495	azure_data_studio	microsoft		8/30/2024 10:42:36 PM

Learn more about KAMIND Guard™ and KAMIND Guard+ at http://www.kamind.com

CM.L2-3.4.1 – SYSTEM BASELINING (continued)

Configuration per Device: Guard+ pulls the Device Configurations and Policies.

device configuration policy is a set of rules and settings applied to devices managed by Microsoft Intune to ensure compliance and security standards across an organization. These policies allow administrators to control various aspects of device behavior, including security settings, WiFi configurations, VPN access, and encryption requirements. Through these policies, IT teams can configure operating system features, manage applications, enforce password complexity, and deploy security baselines.



CM L2 3.4.1b : Establish and maintain baseline configurations and inventories of organizational systems.
CM.3.4.2: Establish and enforce security configuration settings for information technology products employed in organizational systems.

DisplayName: All
Platforms: ■ windows10

DisplayName	Platforms	Description	SettingsDefinitionId	SettingsValue	PolicyType	TemplateFamily	LastModifiedDateTime
Windows Defender AV Policy	windows10		device_vendor_msft_policy_config_defender_allowbehaviormonitoring	1	Microsoft Defender Antivirus	endpointSecurityAntivirus	6/8/2023 11:44:33 PM
Windows Defender AV Policy	windows10		device_vendor_msft_policy_config_defender_allowcloudprotection	1	Microsoft Defender Antivirus	endpointSecurityAntivirus	6/8/2023 11:44:33 PM
Windows Defender AV Policy	windows10		device_vendor_msft_policy_config_defender_allowfullscanonmappednetworkdrives	0	Microsoft Defender Antivirus	endpointSecurityAntivirus	6/8/2023 11:44:33 PM
Windows Defender AV Policy	windows10		device_vendor_msft_policy_config_defender_allowfullscanonmappednetworkdrives	1	Microsoft Defender Antivirus	endpointSecurityAntivirus	6/8/2023 11:44:33 PM
Windows Defender AV Policy	windows10		device_vendor_msft_policy_config_defender_allowintrusionpreventionsystem	1	Microsoft Defender Antivirus	endpointSecurityAntivirus	6/8/2023 11:44:33 PM
Windows Defender AV Policy	windows10		device_vendor_msft_policy_config_defender_allowioavprotection	1	Microsoft Defender Antivirus	endpointSecurityAntivirus	6/8/2023 11:44:33 PM
Windows Defender AV Policy	windows10		device_vendor_msft_policy_config_defender_allowonaccessprotection	1	Microsoft Defender Antivirus	endpointSecurityAntivirus	6/8/2023 11:44:33 PM
Windows Defender AV Policy	windows10		device_vendor_msft_policy_config_defender_allowscanningnetworkfiles	0	Microsoft Defender Antivirus	endpointSecurityAntivirus	6/8/2023 11:44:33 PM
Windows Defender AV Policy	windows10		device_vendor_msft_policy_config_defender_allowscanningnetworkfiles	1	Microsoft Defender Antivirus	endpointSecurityAntivirus	6/8/2023 11:44:33 PM

DisplayName	Description	Type	GroupName	Target	CreatedDateTime	LastModifiedDateTime
KAM Win10 Devices - MDEP Sensor		#microsoft.graph.windowsDefenderAdvancedThreatProtectionConfiguration	All Devices	#microsoft.graph.allDevicesAssignmentTarget	9/23/2020 9:52:59 PM	4/24/2021 11:52:30 PM
KAM Win10 Devices - MDEP Sensor		#microsoft.graph.windowsDefenderAdvancedThreatProtectionConfiguration	All Users	#microsoft.graph.allLicensedUsersAssignmentTarget	9/23/2020 9:52:59 PM	4/24/2021 11:52:30 PM
KAM Win10 Devices - MDEP Sensor		#microsoft.graph.windowsDefenderAdvancedThreatProtectionConfiguration	KAM Win10 Devices - MSP Bots KIOSK	#microsoft.graph.exclusionGroupAssignmentTarget	9/23/2020 9:52:59 PM	4/24/2021 11:52:30 PM
KAM Win10 Devices - Health Monitoring		#microsoft.graph.windowsHealthMonitoringConfiguration	All Devices	#microsoft.graph.allDevicesAssignmentTarget	10/19/2020 8:42:26 PM	4/24/2021 11:51:33 PM
KAM Win10 Devices - Telemetry		#microsoft.graph.windows10GeneralConfiguration	InTuneDevice_Corporate	#microsoft.graph.groupAssignmentTarget	4/25/2021 12:26:08 AM	4/25/2021 12:26:08 AM
KAM Win10 Devices - Telemetry		#microsoft.graph.windows10GeneralConfiguration	KAM Win10 Devices - MSP	#microsoft.graph.groupAssignmentTarget	4/25/2021 12:26:08 AM	4/25/2021 12:26:08 AM

DeviceName	DeviceStatus	Email	DateEnt
CPC-mtevs-8O61Z	compliant	mtevs@kamind.com	9/20/202
CPC-mtevs-8O61Z	compliant	mtevs@kamind.com	9/22/202
CPC-mtevs-8O61Z	compliant	mtevs@kamind.com	9/22/202
CPC-mtevs-8O61Z	compliant	mtevs@kamind.com	9/22/202
CPC-mtevs-8O61Z	compliant	mtevs@kamind.com	9/22/202
CPC-mtevs-8O61Z	compliant	mtevs@kamind.com	9/22/202
CPC-mtevs-8O61Z	compliant	mtevs@kamind.com	9/22/202
CPC-mtevs-8O61Z	compliant	System account	9/20/202
CPC-mtevs-8O61Z	compliant	System account	9/20/202
CPC-mtevs-8O61Z	compliant	System account	9/20/202
CPC-mtevs-8O61Z	compliant	System account	9/20/202
CPC-mtevs-8O61Z	compliant	System account	9/20/202