How to use Dell SafeBIOS in a modern management strategy

By Sven Riebe, Dell MCSG Technical Architect team

Edited by

Gus Chavira, Dell MCSG Technical Architect team and

Amy Price, Dell MCSG Evangelist

Now that we understand what SafeBIOS is, how it works and what capabilities it brings to Dell endpoints, now we'll address some of the ways in which SafeBIOS has been integrated into the flow of client management tools.

Today's employees are working less frequently from inside the company network, spending their workdays at remote sites or working from a home office. With this increase in mobility, how is it possible to track the security status of their endpoints using corporate resources? The answer is to use cloud-based management for devices or security tools, like Microsoft Intune, VMware Workspace One and Carbon Black. In this section we will cover how to collect data from SafeBIOS using Workspace One UEM and the automation of this process based on the SafeBIOS results using Workspace One Intelligence.

Dell SafeBIOS and Workspace One: Working Together

Dell and VMware have full integrations which combine Dell's client tools with VMware Workspace One, with Dell SafeBIOS being one example. Dell devices managed by Workspace One UEM with SafeBIOS report their BIOS verification status to the management console. Previously we have shown you above a couple of features of SafeBIOS but note that Workspace One UEM (formally AirWatch) is supporting BIOS verification only directly in the Workspace One UEM UI (User Interface).



All other SafeBIOS features like Score and IoA are not shown directly in Workspace One UEM, but we can still extract this information using Workspace One Intelligence and Sensors and automate remediation workflows based on the results of SafeBIOS.

Workspace One UEM supports sensors. A sensor is a script which is run on a device and reports results back to Workspace One Intelligence. Workspace One supports sensors for Windows and MacOS. Here we will show examples of a couple of different sensors which allows collection from the full security data available from SafeBIOS that can then be used in Workspace One Intelligence.



You must supply a name for the sensor. This name you will find/use later in Workspace One Intelligence to use the data generated by the sensor.

1	Edit Sensor			\times
	1 General	Name	truster/device biosvarification	
	2 Details	Hume		
		Description (Optional)	Sensor Dell TrustedDevice for BIOS verification status	ß
			CANCEL	EXT

In this example we are using a PowerShell script in the system context to generate requested data on the devices. Example sensors are located at this GitHub repository.

SvenRiebe/SafeBIOS (github.com)

Please feel free to download for your own use and at your own risk with no warranties implied.

Edit Sensor			
1 General	Language	PowerShell	~
2 Details			
	Execution Context	System	~
	Execution	Auto	~
	Response Data	String	~
	.,,		
	Code	UPLOAD	
	12 13 Eurotion DellTrus	tadDavica SecurityAssassm	ent/) /
	14 \$ProviderNam	e = "Trusted Device Security	Assessment"
	15 \$LogName = "	Dell" # %SystemRoot%\Syste	em32\Winevt\Logs\Dell.evtx
	16		
	17 \$Result = Get-	WinEvent -ProviderName \$F	ProviderName -MaxEvents 1 # format-
	18 # Write-Host	"r'nTime: \$(\$Result.TimeCre	ated)" -NoNewline

New Assignment		×
1 Definition	Assignment Name	All Dell Devisor
2 Deployment	Select Smart Group	Start typing to add a group
		Sensor All Devices (w/o VMs)
		CANCEL

New Assignment			×
1 Definition	Select which triggers shou	ld cause this sensor to run on as	ssigned devices
2 Deployment	Trigger Event Type Event Schedule	Ť	Ę₂
	Triggers V Login Log Out Startup User Swit	ch	
		CANCEL	BACK

GETTING STARTED	Dashboard List View		Devices > Sensors (i)		
MONITOR	Device Updates Lifecycle	>	ADD - ASSIGN EDIT		
100	Profiles & Resources	>	Name	Language T	Platform T
	Compliance Policies	>	trusteddevice_meveridication	PowerShell	Windows
	Certificates	>	trusteddevice_score_fail	PowerShell	Windows
Ô	Provisioning	>	trusteddevice_diskencryption	PowerShell	Windows
ACCOUNTS	Sensors		trusteddevice_av	PowerShell	Windows
333	Peripherals	>	trusteddevice_tpm	PowerShell	Windows
APPS & BOOKS	Devices Settings	Ø	trusteddevice_firewall	PowerShell	Windows
			trusteddevice_biosverification	PowerShell	Windows
CONTENT			trusteddevice_biospassword	PowerShell	Windows
			trusteddevice_ioa	PowerShell	Windows
EMAIL			trusteddevice_score	PowerShell	Windows

How you can use these sensors with Workspace One Intelligence

We will show you in this section how to build a SafeBIOS themed Dashboard along with automation to help with the security posture of an endpoint using Workspace One Intelligence and help your security IT Team get detailed information about the Device security from Dell SafeBIOS info.

We first need to create a Dashboard. Workspace One Intelligence Administrators can make their own dashboards and widgets using the results from Sensors to make these results visible.

In this case we have created a Dashboard that is collecting all SafeBIOS Sensor info to provide a view about score, risk and security status.



You could use different data pools to generate your own Dashboard. For my example I am using my generated sensors only.

INTELLIGENCE DASHBOARDS			(e) (a) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c							
My Dashboards > Dell SafeBIOS Owner										
Headles taxed or server to be Truind General Agent Counted by its Denotebe - Lad Madified, July 23 2020 - Lad Madified Wy, to period to Middley Biol Prosent Northy										
Date Range -										
Perice Organization Group Name includes All AND Organization Group Hemarchy includes All			Ear W							
AUD WIGHTY CASTONETE			QUICK FILTERS-							
V Additor										
SafeBIOS Risk Assessment Fail	3 SafeBIOS indicators of Attack	П	SafeBIOS Risk Score							
A tusteddevice_score_ts- @ Donut -	A trusteddevice_los - B Donut -		A tusteddevice_score							
9 Your	9 Total	(10) 11	Transmission of the second sec							
VIEW 2 topp ***	VIEW	21033 ***	VEW (2193) ***							

If you want to make your own view you can add a Widget to the Dashboard, you have two options; the first option is you can use a template, or a second option is you make your own Widget like I have done.

You are free to choose output style like, Donut, Table, etc.

When devices have provided the first data, you can use your sensor and select the value for your Widget. You have the flexibility to build groups and subgroups. For my Indicators of Attack, I have grouped with the sensor only, but you can combine this with other sensors or UEM device data. You could also use filters e.g., to filter senseless values or unusual information.

SafeBIOS Indicators of Attack								
Create a widget from scr	Create a widget from scratch							
Data Visualizati	on							
SNAPSHOT HISTOR	RICAL		Ģ					
Chart Type								
HORIZONTAL	MI VERTICAL	@ DONUT	12 METRIC	₩ TABLE	TREE MAP			
Measure Count ~ of trusteddevice_ioa								
Group by (Optional) trusteddevice_joa × ADD SUBGROUP								
Results per group	10							

Automation is the key in modernization

We now have a couple of pieces of information, but I don't want to check this each time, however for my risk management I need to investigate security related-issues soon as possible.

I made an example for you, showing how you could make an automatization based on sensors.

You could go to automate or choose this option direct in the sensor Dashboard. You will guide to generate a process like *send an e-mail*, or starting processes in ServiceNow. Workspace One UEM however is using Rest-API. In my case, if Indicators of Attack is showing a risk, Workspace One UEM should run an App which made BIOS settings to solve this problem.

Option 1 over Automation



Option 2 direct from your dashboard.



If you are using the dashboard option, the filter will be the dashboard trigger - in my case the sensor indicators of attack. The automation needs a name e.g., BIOS Security Settings and you can choose if you want the automation full automatically, or manual and chosen by yourself.

Trigger (When) 🗊							
Workspace ONE UEM: Devices Data							
	Manual						
	Trigger Option	1					
AutomaticFilter (Automatically execute the workflow when incoming events match the filter							
	Schedule Define when the filtered results should execute						
Action	Action Manual Execute the workflow On-Demand (good						
		20					

The workflow now has a name and a filter to identify the right devices which are needed for this workflow. In my scenario all devices will be selected which are failing for the IoA check.

[₽] BIOS Socurity Sottings	
blos security securitys	
Add description (optional)	
Trigger (When) 🛈	
Workspace ONE UEM: Device Sensors Data	
Manual ~ (1)	
	CLOSE
Filter (If) ①	
▼ trusteddevice_ioa includes (FAIL)	<u> </u>
	_
trusteddevice_joa 🛞 Includes v FAIL X	· + ≟ ≞

Workspace One Intelligence supporting REST-API. In my environment I have ServiceNow, Slack and Workspace One UEM/Intelligence.

In my workflow I want to push new BIOS settings to all machines where the IoA check has failed. I will do this by Workspace One UEM where my App repository is available.

Available Connectors (4)							
Workspace ONE UEM	Workspace ONE Intelligence	ServiceNow	Slack				

We have different options now like install a profile, delete device, etc. we are choosing Install Internal Application.



The device ID is managed by the workflow required to select the application. I have uploaded a PowerShell Script which makes the BIOS setting with the support of Dell Command Monitor which is installed on all my devices.

Ç	Workspace ONE UEM \rightarrow Install Internal Application ()							
	Body							
	Device ID	\$(device_id)						
	Path Variables							
		• Search for existing values						
	Application Name	BIOS_Settings {1638b388-b8f1-4e26-a9f4-1f820da7b645} v Optional						
	TEST							

If you have selected the application and tested the workflow you can enable and disable the workflow. The automatic setting is the workflow is disabled, so you need to decide whether you want to workflow to run automatically.



You can add/delete and edit your workflow as needed.

Dashbo	ards	Automations	Reports	Integrations	Sett
⊳ INT M	elligei /ork	NCE AUTOMATI flows	ONS		
A	DD ~				
\mathbf{n}	Search	name and descr	iption		
Sort by:	Enabled	~			
BIOS Last	6 Securi Run: Ne	ty Settings ver • Last Moo	dified:	Disab	led IO

Generate Security Report.

If you have security administrators or CSOs in your company it could make sense to supply a security report on a scheduled basis. In Report it is quite simple to combine different values to get a useful report. For my project I want to generate a report of all SafeBIOS Sensors and send this report on weekly basis to my security team.

The report needs a name, and if you want to select a specific device to scan, then use the filter choice.

Edit Report	CANCEL	SAVE
Dell Save BIOS Score per Device 103 starter/blark template		
Filters ()		CLOSE
T Emoly-Rule		80
	+ 14	
Report Preview ①		

We can select all fields we need for our report. We have wide options of Workspace One fields, sensors, etc.

	Edit Columns		×
osverificati	Available Columns	Normalized QSearch Image: Constraint of the second	Normalized Normalized UP DOWN CANCEL SAVE

If we are finished, we can save the report, and now we can share or automate this report for our needs.

ishboards Aut	hboards Automations Reports Integrations Settings							
Reports > De	Reports > Dell Save BIOS Score per Device Owner: Overview V					•		
T Empty R	lule							ðir,
Preview (1) This report has	9 records. 🦪 Refreshed a f	ew seconds ag	0					
Device Name	Model	OS Version	Device Organization Group Na	Domain	trusteddevice_sco_	Last Seen	trusteddevice	trusteddev
itpro-8	Latitude 7300	10.0.19042			87	Sep 27, 2021 11:04 A	PASS	PASS
itpro-8	Latitude 7400 2-in-1	10.0.19042			87	Oct 20, 2021 4:21 PM	PASS	PASS
itpro-7	Latitude 7320 Detacha	10.0.19043			87	Feb 1, 2022 1:47 PM	PASS	WARNING
itpro-9	Latitude 5300	10.0.19042		-	83	Sep 29, 2021 2:51 PM	PASS	WARNING
itpro-3	Precision 5750	10.0.19043			87	Feb 1, 2022 9:36 AM	PASS	PASS
itpro-3	Latitude 7310	10.0.19042		-	87	Sep 27, 2021 11:00 A	PASS	PASS
itpro-h	Latitude 9510	10.0.19043			83	Jan 11, 2022 2:50 PM	PASS	PASS

It does not make sense to check this report manually in a large company, so I am making a schedule of this report which I want to provide to my security team.

Schedules	
	1
	Schedules
VIEW ADD SCHEDULE	

We have a couple of options for report scheduling. I am configuring the report on weekly basis at 12pm. I am now getting an email each Monday with a link to my new report. The reports will also be stored so I will have a history of my reports in the future.

Schedule: Dell Sav	ve BIOS S	icore p	er Dev	ice				×
Schedule Name	Dell Trusted	d Device Re	eport for Se	curity Team	1			
Recurrence	Weekly							~
Day(s) of the week	М	т	w	т	F	S	S	
Starts At	12:00							CET (j)
Ends		NO EN	ND DATE				END BY	
							CANCEL	SCHEDULE

Carbon Black integration

VMware security products have a full integration of Dell Safe BIOS, so it is very simple to use this feature. Dell Device with SafeBios can be also be monitored by Carbon Black. The chapter Live Query provides a standard Query to check the status of Dell Safe BIOS, which allows Carbon Black Administrators to take actions based on the results. An example could be to disconnect device if the BIOS is looking affected by an attack to secure the Company environment.

vm Carbon B	lack Cloud	Notification ³⁰⁰ Help > Sve	en Riebe (nfr-complete.delltechnologies) >
N nfr-complete.dellte	NEW QUERY Run a recommended query or create your own with custom SQL Learn more		
Dashboard	Recommended SQL Query		Visit the Query Exchange
▲ Alerts ♦ Investigate	All IT Hygiene Vu (95) (26)	Inerability Mgmt Threat Hunting (17) (30)	Compliance (22)
Live Query			
New Query	Q Search		os 🗸
Query Results			
⊘ Enforce >	Queries run against all endpoints by default. However, you can select a specific polit	y or endpoints.	
🏳 Harden 🔰 🗲	Description: On Windows XP and later operating systems, credential theft tools credentials to certain applications. By default, Windows stores the should be disabled. Learn more: https://atack.mitre.org/technique	such as Mimikatz) can access the WDigest protocol that se e credentials in the Isass.exe process for user convenience s/T1003/	ends plain text
🗗 Inventory >	Results: Lists 0 for all systems that have UseLogonCredential disabled. If no to protect against credential theft. If results are 1 for Windows 10 of	results are returned, CB recommends deploying this IT Hy r Windows 2016, CB recommends conducting an immedia	ygiene policy via GPO ite investigation.
In the settings →	+	Carbon Black recom	nmends that you run this query daily
	IT HYGIENE		
	Dell SafeBIOS Verification Status 曲		Schedule Run
	Description: Reports the BIOS verification status for supported Dell platforms ru more: https://www.dell.com/support/manuals/us/en/04/trusted-de	inning Windows 10 (Latitude, OptiPlex, Precision, and selection wice/trusted_device/introduction	ct XPS). Learn
	Results: Displays the BIOS verification status for Dell endpoints running the recommends policy hardening, guarantine of endpoints that displa	Dell Trusted Device agent (PASSED, FAILED, or NOT AVAIL v a FAILED status, or further investigation via Live Respon:	ABLE). Carbon Black se.
	-	Carbon Black recom	nmends that you run this query daily
	WITH b1 AS (SELET COUNT(*) AS cmt, 1 AS one		Edit SQL
« Collapse	ERM PASICIPU		

After running the query, the Carbon Black Agent on the local machines reports the device Safe BIOS status to the Carbon Black Console.

If you have Workspace One Intelligence in place you can use the Carbon Black integration. This integration gives you the same availabilities as I am using above in my Workspace One scenario.

🕼 Workspace ONE Intellige	nce Q APPS - Search for app name or package ID	
Home Getting Started Solutions	Dashboards Automations Reports Integrations Setting	15
~	Integrations	
(b) Integrations	Integration	Status: 🥝 Authorized
	SET UP	VIEW
	Netskope Set up your Netskope connector to get the most out of our Workspace ONE Intelligence and Netskope integration.	Carbon Black Set up your Carbon Black connector to get the most out of our Workspace ONE Intelligence and Carbon Black Integration.
	Trust Network	Trust Network
	SET UP	SET UP