

HOW TO – QUANTUM IOT PROTECT – ONBOARDING



Documento escrito por: Lisandro Weissheimer da Silva Security Engineering Brazil Dezembro/2023



CONTEÚDO

Sobre a solução: Quantum IoT Protect	3
Cenário atual	3
Quantum IoT Protect	3
Proteção Autonoma para dispositivos IoT	3
Perfis de rede IoT autônoma de confiança zero	4
Gerenciamento simples de IoT em um único console	4
Onboarding do Quantum IoT Protect	5
Cenário utilizado	5
Gateway	5
Manager	5
Políticas	6
Regras de Acesso	6
Ativação do serviço IoT Protect no Portal Infinity	7



Sobre a solução: Quantum IoT Protect

Cenário atual

O uso de dispositivos da Internet das Coisas (IoT) em aplicações empresariais, de saúde e industriais oferece benefícios de produtividade, mas também expõe as redes à ameaças cibernéticas em constante evolução.

De câmeras IP e elevadores inteligentes a dispositivos médicos e controladores industriais, o Quantum IoT Protect protege suas redes IoT contra ataques cibernéticos.

Quantum IoT Protect

Prevenção autônoma de ameaças para proteção de rede e no dispositivo



Proteção Autonoma para dispositivos IoT

Mais de 200 perfis autônomos por tipo de dispositivo, categoria e fornecedor





Perfis de rede IoT autônoma de confiança zero

Com o Quantum IoT Protect, você também começa a entender como os dispositivos estão se comunicando e com o que estão se comunicando. Aproveitamos técnicas de IA e aprendizado de máquina para compreender completamente os padrões e criar automaticamente regras que permitem a comunicação adequada para o dispositivo e bloquear qualquer ação não autorizada que possa servir como uma ameaça potencial à rede. É aqui que você realmente percebe a peça de prevenção.



Gerenciamento simples de IoT em um único console

Visibilidade para todos os ativos	Gening Survey	INT NETWORK PROTECTIO		EVERODED	Last 7.De		ZUNELAND KINTS			ASSETS BY 2	2408		Sertily: Quert
conectados em poucos minutos!	Auser Losses Process Process Profes	Quantitat Galensey service 107 assets (State data data Song_M1_001 of assets Differences) 11		-	19	-	165 16			9 i	86 53	D camatas D haven Pristars D hypert NAS	
Perfis autônomos de confiança zero aplicados imediatamente depois.	ана 1997 - 1997 1997 - 1997 - 1997 - 1997 1997 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977	TOP COMBUNICATING 2	DAEL	Barteri -	Last 7 De Priva Assess	yı -		I Davident	2 %		6 3 2 1	Event Kazpborius Entect Entect Event ValF devices Const Const Finant Provent	42 In loss confidence
		💇 Promete	6394.401 112,134	3303.864	27 29	1	E Parana	5	Parame 2	-	1	Diac players Dinot	
Ataques conhecidos e		Dente	B(47)	12748	25	÷	Vol? de Jose	2	Same 2		1	Papares Presert	et 11 lan gerfdange
desconhecidos de dia zero são	•	Security speen	1387,985	4.089	3		Contes		Name 1		1	Collect	
bioqueados em tempo real.	9	dia ce	1.028	122			· ·····			0	1	Smart plugs	

Uma solução abrangente de segurança de IoT é necessária para proteger sua empresa contra esses riscos e é um componente vital da estratégia de segurança cibernética de cada empresa.



Onboarding do Quantum IoT Protect

Cenário utilizado

Os próximos passos descrevem o processo de onboarding do Quantum IoT Protect bem como as características do ambiente utilizado. Neste cenário presuminos que o gateway de segurança já está operacional e sua manager devidamente conectada e ativada. Este exemplo utiliza a manager SaaS Smart-1 Cloud e o procedimento leva isto em conta.

Gateway

Modelo: 3600 Versão Gaia: R81.20 Jumbo Hotfix Take 41 Kernel: 3.10.0-1160.15.2cpx86_64 Edition: 64-bit Build: 631

HomeGate	eway	Access Blades				
IPv4 Address:	100.100.26.7	3000 Appliances	Firewall Application & URL Filtering Octated Awareness			
Access Control Policy:	Standard		Threat Blades			
	05/12/2023 14:11					
Threat Prevention Policy:	Standard	*	IPS Anti-Bot Anti-Virus			
	05/12/2023 14:11					
OS:	Gaia					
Version:	R81.20	CPU: 19%				
License Status:	📀 ОК	Memory: 49%				
Alerts:	⊘ OK					
		Device & License Information				

Manager

Modelo: Smart-1 Cloud WELCOME TO QUANTUM SMART-1 CLOUD Service Information Service Management Connect Gateways Logs Information Daily Logs (Average 30 Days): 3.12 MB Status: 1 🖳 Active Service Identifier: Entitled Daily Logs: 3 GB gateways connected Open Streamed SmartConsole + Add new Gateway Entitled Log Storage: OR R81.20 100 GB Region: oad SmartConsole for Windows US East Logs optimiz License Status: SmartConsole Connection Token: Trial (expires in 260 days) 🚯 ٦.



Políticas

Abaixo temos as políticas criadas, onde podemos notar que há apenas a layer de Controle de Acesso, no pacote de políticas Standard.

Standard	Manage Policies \times	+						
						1	🎁 Open 🗦	*
Name 🔺	Access Control	Threat Prevention	QoS	Desktop Security	Policy Targe	ets Comme	nts	
Standard	i 🗸	~			All gateways			
Policy		k			୍ ତ ×			
Stan	dard							
"General Installation Targets	Policy Types	HTTPS Inspection 🔽 🗽 Threat F	Prevention		≡			
		+						
	🕕 Custom Threat Pre	evention +			≡ -			
	🛃 Autonomous Three	at Prevention						
	HTTPS Inspection	Default Layer		■C Shared	≡ -			
	Add Tag							
				ОК	Cancel			

Regras de Acesso

As regras de acesso criadas bloqueiam acesso inboud de determinados países. Esta regra não é mandatória, mas recomenda-se como boa prática. Possui ainda uma regra que permite qualquer tráfego de saída para a Internet e uma regra de Cleanup.

								+=	.= ×	\$	*	≡ - 0
No.	Hit	s		Name			So	urce				Destin
Blocked	Countri	es (1)									
Allowed	 Allowed Outbound (2) 											
Cleanup	(3)											
Access Control				⁺≡ .= × 3	🕂 🗄 - 🕑 Install Policy 🕅	Actions • Sear			٩, ٧	^ Y		
Policy	No. Hits		Name	Source	Destination	VPN	Services & Applicatio	ns Content	Action	Time	Track	Install On
50 NAT	 Blocked Countries 	(1)										
Threat Prevention	 Allowed Outbound 	1 (2)	Allow Outbound				-		A Arrest			=
Custom Policy	2	- 106	Allow Outpound	* ADY	*** ar_Internet	₩ Any	* ADY	iπ Any	Accept	* Any	Accounting	# Policy rargets
Autonomous Policy	 Cleanup (3) 											
Exceptions	3	0	Cleanup Rule	* Any	* Any	# Any	* Any	₩ Any	Drop	* Any	Extended Log	* Policy Targets



Ativação do serviço IoT Protect no Portal Infinity

Para este exemplo iremos considerar que você já tem uma conta criada no Portal Infinity e sua instância de gerência, Smart-1 Cloud, está ativa e funcional, como mostrado nas imagens anteriores.

1- Faça login no Portal Infinity (<u>https://portal.checkpoint.com</u>) com uma conta que possua direitos adminitrativos e pode ativar novos serviços:

← → C		
	S CHECK POINT	
	MY ACCOUNT	
	lisandrow@checkpoint.com	
	Region US-EU 👻	
	Don't have an account? Register here	
	Trouble logging In? Click here NEXT	INFINITY PORTAL Unified security – delivered as a service
		Help Terms

2- Após o login, vá até o canto superior esquerdo e clique no ícone do menu:



3- Selecione IoT Protect, como mostra a imagem abaixo:

RECENT (1) Smart-1 Cloud			
HORIZON Unified Management and Security Operations	Secure the Network	CLOUDGUARD Secure the Cloud	HARMONY Secure Users & Access
MDR-MPR	Smart-1 Cloud	Posture	Connect
XDR/XPR	Spark Management	Network	Endpoint
Events	IoT Protect	Workload	Mobile
Playblocks New	SD-WAN	Identity	Email & Collaboration
Policy	SASE - Internet & Private Access	ShiftLeft	Browse
SOC		Intelligence	
		Application Security	

4- Aceite os termos e clique em TRY NOW:

Quantum IoT Protect

Secure your IoT devices and secure your network from any IoT
related attack. Check Point's IoT Protect will identify, classify and
analyze every IoT device across the entire network, will
automatically apply a perfectly suited IoT policy and will prevent
loT malicious intents.
✓ I accept the Infinity Portal Terms Of Service and the Privacy Policy *
TRY NOW



5- Aguarde a ativação dos serviços:



6- Após a ativação dos serviços, é necessário realizar algumas configurações na Smart-1 Cloud. A tela abaixo indica que os serviços foram ativados mas ainda dependem de configurações para funcionarem corretamente:

	QUANTUM IOT PR	ROTECT 🏦 LWSLabs 🗸			🕾 Feedback	Publish 1 Enforce) ~~ 0	💄 🔋 Lisandro Weissheimer da Silva 🚇 🗸
*⁼	Getting Started Overview			<u>é</u>				
MONITOR	Assets Zones			WELCOME TO IOT P	ROTECTION			
O SUPPORT	Profiles Agents							
	Events							
	Firmware Scan		To discover and protect IoT devices by yo connect your Quantum Management Ser	ur Quantum gateways ver to your Infinity Portal accoun	t		How To Connect	
*			Assets Setup Inf Discovery and Assets	← • • • • • • • • • • • • •	int very	Situational Iot Desh	Visibility cord	

7- Clique em How To Connect:



8- A tela exibida traz os passos a serem executados, que faremos na sequencia:





9- Acesse a SmartConsole instalada em seu computador ou através da Streamed SmartConsole no Portal Infinity:



10- Neste exemplo usaremos a SmartConsole instalada localmente. Clique no botão Infinity Services:



11- A tela abaixo será exibida. No card Quantum IoT Protect, clique em Setup:

G I -	📦 Objects = 😍 Install Policy	🌐 Decard Sesion + 🕼 Changer 🕥 Publish							
GATEWAYS A SERVERS	INFINITY PORTAL ACCOUNT	State Ø Actor	Q. Szenh Control						
POLICES LOGS & MONITOR NUMBER SERVICES	Infinity Services Market Contemportation (Contemportation) Contemportation (Contemportation) Con	• Quantum IoT Protect • Institute Instit In	Application Company and a second and a						
C.	Copen in Browser	Ą							
UNE O WHATS NEW	Configuration Sharing Lidit Log Sharing Log Sharing Active								

12- A tela abaixo traz as duas ações a serem executadas, Configuration Sharing e Install Policy, e uma breve descrição de cada uma delas. Clique em I Agree





13- Você será direcionado ao Portal Infinity para finalizar a configuração. Certifique-se que todos os tipos de dispositivos que você deseja identificar estão selecionados e clique em NEXT:



14- Nesta tela clique em NEXT:

IOT ENVIRONMENT		×
	Practices Apply IoT Best Practice to control access of all common IoT devices	
2 PRACTICES	K IoT Best Practice 😵 Learn / Detect	
	Protect your IoT assets and control their access to the Internet by a tailored policy according to their function, manufacturer and behavior	
4 ENFORCEMENT		
5 SUMMARY		
k	BACK NEXT	

15- Na tela abaixo, Discovery, selecione apenas Quantum Gateway sensors, se ainda não estiver marcado. Note que outras fontes podem ser utilizadas para descoberta. Não trataremos destas outras fontes neste documento, nosso foco é ativar os serviços de descoberta e proteção nos Gateways de Segurança Check Point:





16- Selecione a política onde serão adicionadas as regras de acesso e proteção para IoT. Após selecionar a politica, role a tela para baixo e escolha em quais Gateways você terá a layer de IoT e não equeça de marcar a última opção, abaixo dos Gateways selecionados, onde diz "Infinitiy Portal will automatically Install Policy on relevant security gateways". Clique em NEXT.

IOT ENVIRONMENT				×
	Enforcement Add IoT Layer To Polic	y Package		
	Select on which policy pa	ckages to add IoT policy as a	a layer	
	search	Q	1 of 1 items	1 selected
	Policy package Standard			
(5) SUMMARY				
	Install IoT Policy On Th	ne Following Gateways		
	Select which compatible (Duantum Gateways should	enforce the IoT policy	
			BACK	NEXT



IOT ENVIRONMENT					×				
	Select which compatible (Quantum Gateways sh	nould enforce the lo	oT policy					
	 All compatible Quantu Selected Quantum Gat 	 All compatible Quantum Gateways () Selected Quantum Gateways 							
	search	Q		1 of 1 items 1 selected					
	✓ sensor	IP address	Version	OS					
	 HomeGateway 	100.100.26.7	R81.20	Gaia					
					l				
5 SUMMARY									
	Infinity Portal w	ill automatically Instal	ll Policy on relevant	: security gateways					
				BACK NEXT					

17- Na tela final, certifique-se que as opções "Enable <u>PlayBlocks</u> Integration" e "Enforce policy and start discovering IoT Assets" estão marcadas e clique em DONE:

IOT ENVIRONMENT	×
	Summary
	System will discover: IoT assets, their properties and traffic patterns
	System will create: IOT assets and zones Discovery profiles: IOT Discovery Profile
	IoT access policy: is activated in Learn/Detect mode Policy packages: Standard
5 SUMMARY	What's next?
	Enable PlayBlocks integration
	Enforce policy and start discovering IoT assets
	Go to SmartConsole in order to install the IoT Policy
	BACK DONE

18- Será exibida a mensagem abaixo, indicando quantas alterações foram feitas nesta sessão. Clique em PUBLISH & ENFORCE POLICY:





19- Ao término do enforce, você será direcionado para este tela, indicando que houve sucesso na configuração:



20- Retorne a SmartConsole no item Infinity Services e verifique se a opção Configuration Sharing está ativa e se o card do Quantum IoT Protect está ativo também:



21- Na SmartConsole, vá em MANAGE & SETTINGS e selecione Sessions e depois Revisions. Deve haver uma sessão de enforcement do IoT, como abaixo:

<u>©:</u> -	🎲 Objects 🔹 🔮 Install Policy					
-0	** 🏘 Permissions & Administrat	Revisions	🔨 Edit Details	♥ View L Actions ▼ Q Search		12 item:
	III Blades	Publish Time 👻	Name	Publisher	Changes From Previous	Description
& SERVERS	- 🗔 Sessions	05/12/2023 16:05	La IoT Enforcement Setup	WEB_API	3	IoT Enforcement Setup
	- View Sessions	05/12/2023 16:05	<u>n</u>	WEB_API	1	
		05/12/2023 15:47	<u>C</u>	Configuration Sharing (Infinity)	1	Established secured connection with the Infinity Portal to share
SECURITY	-9 Revisions	05/12/2023 15:19	🔓 lisandrow@checkpoint.com@05/12/2023	lisandrow@checkpoint.com	1	
rocicies	Advanced 45	05/12/2023 15:06	Isandrow@checkpoint.com@05/12/2023	lisandrow@checkpoint.com	1	
<i>.</i>	🖉 Tags	05/12/2023 14:55	L lisandrow@checkpoint.com@05/12/2023	lisandrow@checkpoint.com	122	
LOGS &	🍄 Preferences	05/12/2023 14:08	L lisandrow@checkpoint.com@05/12/2023	lisandrow@checkpoint.com	1	
MONITOR	Sync with UserCenter	05/12/2023 14:07	L lisandrow@checkpoint.com@05/12/2023	lisandrow@checkpoint.com	1	
	🗔 SmartTasks	05/12/2023 13:51	L lisandrow@checkpoint.com@05/12/2023	lisandrow@checkpoint.com	2	
8	Package Repository	05/12/2023 13:44	L lisandrow@checkpoint.com@05/12/2023	lisandrow@checkpoint.com	1	
SERVICES		05/12/2023 13:44	Lisandrow@checkpoint.com@05/12/2023	lisandrow@checkpoint.com	19	
	Big Policy Settings	05/12/2023 11:24	🖳 Smart-1 Cloud	WEB_API	5	Register a new gateway: HomeGateway
يىلىر.						



22- Na aba SECURITY POLICIES da SmartConsole você deve encontrar agora a layer IoT Protect e as suas politicas de acesso associadas:

q : •	🛱 Objects + 🕙 Install Policy				🗑 Disant Ses	sion • 🗄	Courses Branne					StratConsole
	Standard × Manage Policies											
-						1 This Party	and the address such down to the					
GATEWAYS	Access Control					This Polic	y can be edited only from for P	rotect Appread			1001	
	- A Policy	C Shared		-		Policy No	Actions . Laurch for IP, cope			4 1 1 1		
-	C Network	Na.	Name	Source	Destination	VPN	Services & Applications	Content	Action	Track	Install On	
SECURITY	Se IoT Protect	* External Tr	raffic (1-2)									= =
	ST NAT	• 1	IoT to Outbound Traffic	By IoT Device	升 internet	* Any	H Loy	= Any	C IoT Best Practice	- N/A	H IoT Gateways	
	Threat Prevention	· Pre IoT R	lutes (1.1-1.9)									
^	ST Custom Policy	1.1	Scanners Block	E IoT Device	H Shodan	* Any	н лау	# Arty	Orop	i Log	∺ IoT Gateways	
	Autonomous Policy Exceptions HTTPS Inspection	1.2	Allowed DNS	Br IoT Device	Google Public DNS Primary Google Public DNS Secon OpenDNS Primary OpenDNS Secondary Cloudflare Public DNS Pri	* Any	🚯 domain-udp	≡ Ary	Accept	🗄 Log	₩ loT Gateways	
	2 Contraction of the second se				Cloudflare Public DNS Se							
O MARCAGE &	Shared Policies	1.3	INT DHCP	By IoT Device	# Any	# Any	dhop-request dhop-reply	# Any	Accept	E Log	3£ 107 Gateways	
	Inspection Settings	1.4	Adobe Identity Service	E: IoT Device	N: .demdex.net	# Any	😣 https	# Arty	Accept	E Log	30. IoT Gateways	
		1.5	Adobe Senice	E IoT Device	S .adobe.com	# Any	😣 https	· Any	() Accept	i top	32 IoT Gateways	
		1.00		- **** - ****	-		-	and the second		+		
			100000000000000000000000000000000000000	2003 I								1
		Summary	Details Logs	history								
		09	Q O Last 24 Hours .	Current Rule * Friter search au	ery (Ctrl+F)							=
			Showing first 50 results (1.2 sec.)	out of at least 50 results								Query Syman
		1000	Light States	Maddies Name - Annual	Destination Machine Desti		Service Audio	tion Monte A	Access Rule M. Dave	alation		
		mue	Source Source	e Madulie Name Source	Descritedon inscrime Descri	100.000	service _ Appilia	cion wante - A	Autess Male A. Desc	ripcion		
		Today, 17:23	m MAS to test	wife (76:33:21) 192.166.0.2	E23 +00	101010	https (FCP/443)		Allow Outboard			
		Teday, 17:23	ta Mil (A) s to Jack	wildi (7b: 13-21) 192 168.0.2	100 to	5 102 51 0	http:///CP/443	2	Allow Outbound			_
		Today 17:22	st M @ S to Jiel	wiji (7b-33-21) 192 168.0.2	10 10	212 122 5	domain.udo 0.009/53)	2	Alicer Outbound			
		Today 17:23	to-line	wi-fi (7b:33:21) 192.168.0.2	C 10	212.132.4	domain-udp (UDP/51)	2	Allow Outbound			
		Today, 17:21	st M 🕀 🍾 to-lini	wi-fi (7b:33:21) 192.168.0.2	4 0	88.218.28	https (FCP/443)	2	Allow Outbound			
	Access Tools	Today, 17:23	58 M 🔁 🍾 tp-lini	wi-fi (7b:33:21) 192.168.0.2	18	.213.132.5	domain-udp (UDP/S3)	2	Allow Outbound			
	K VPN Communities	Today, 17:23	58 M 😁 🍾 tp-lini	wi-fi (7b:33:21) 192.168.0.2	18	.213.132.4	domain-udp (UDP/53)	2	Allow Outbound			
	C Hadates	Today, 17:23	58 III 🔁 🍾 tp-lini	wi-fi (7b:33:21) 192.168.0.2	13	.213.132.5	domain-udp (UDP/53)	2	Allow Outbound			
	Copulation of the second secon	Today, 17:23	58 🕅 🤁 🍾 tp-lini	wi-fi (7b:33:21) 192.166.0.2	18	1.213.132.4	domain-udp (UDP/S3)	2	Allow Outbound			
COMMAND UNE	X UserCheck	Today, 17:23	:58 🕅 🔁 🍾 tp-lini	wi-fi (7b:33:21) 192.168.0.2	13	.213.132.5	domain-udp (UDP/S3)	2	Allow Outbound			
	Client Certificates	Today, 17:23	:58 🕅 🕲 🍾 tp-link	wi-fi (7b:33:21) 192.168.0.2	10	1.213.132.4	domain-udp (UDP/53)	2	Allow Outbound			
0	Application Wiki	Today, 17:23	:57 🕅 🔁 🍾 tp-lini	wi-fi (7b:33:21) 192.168.0.2	S 15	7.240.222.61	jabber (TCP/5222)	2	Allow Outbound			
	O Installation History	Today, 17:23	:57 🛛 🕅 🔁 🍾 tp-lini	wi-fi (7b:33:21) 192.166.0.2	90 44.	228.205.13	https (TCP/443)	2	Allow Outbound			

23- Volte ao Portal Infinity e verifique se existem dados na aba Overview:

Getting Started	Supervision V16 initiated by Lisandro Weissheimer da Silva finished successful	By.	
Overview	IOT NETWORK PROTECTION IOT EMBEDDED		
Assets Zones	DISCOVERY SOURCES Last 7 Days 👻 -	ENFORCEMENT MODES -	ASSETS BY ZONE Sort by: Quantity
Practices Triggers	New discovery source (profile) IoT Discovery Profile	Assets Zones 1 1	1 👷
Profiles Agents	IoT assets 1 (out of 1 devices)		
Events		Internet access practice modes	
Firmware Scan		Risk mitigation practice modes	
Þ			
		Prevent Learn/Detect Disabled	
	TOP COMMUNICATING ZONES Last 7 Days 👻 -	ASSETS AT RISK -	
	Zone O Active A O Connecti O Blocked Q	By Level By Indicator	
	Wi-Fis 1/1 8,623 1 >		
			THINGS TO DD
		No data found	
			National
			140 0808 100110



24- Na aba Assets você terá a lista dos ativos descobertos até o momento:



Deste ponto em frente, novos ativos serão descobertos e adicionados ao Quantum IoT Protect.

Para saber mais sobre Quantum IoT Protect, clique aqui.

Para saber mais sobre Smart-1 Cloud, clique aqui.