

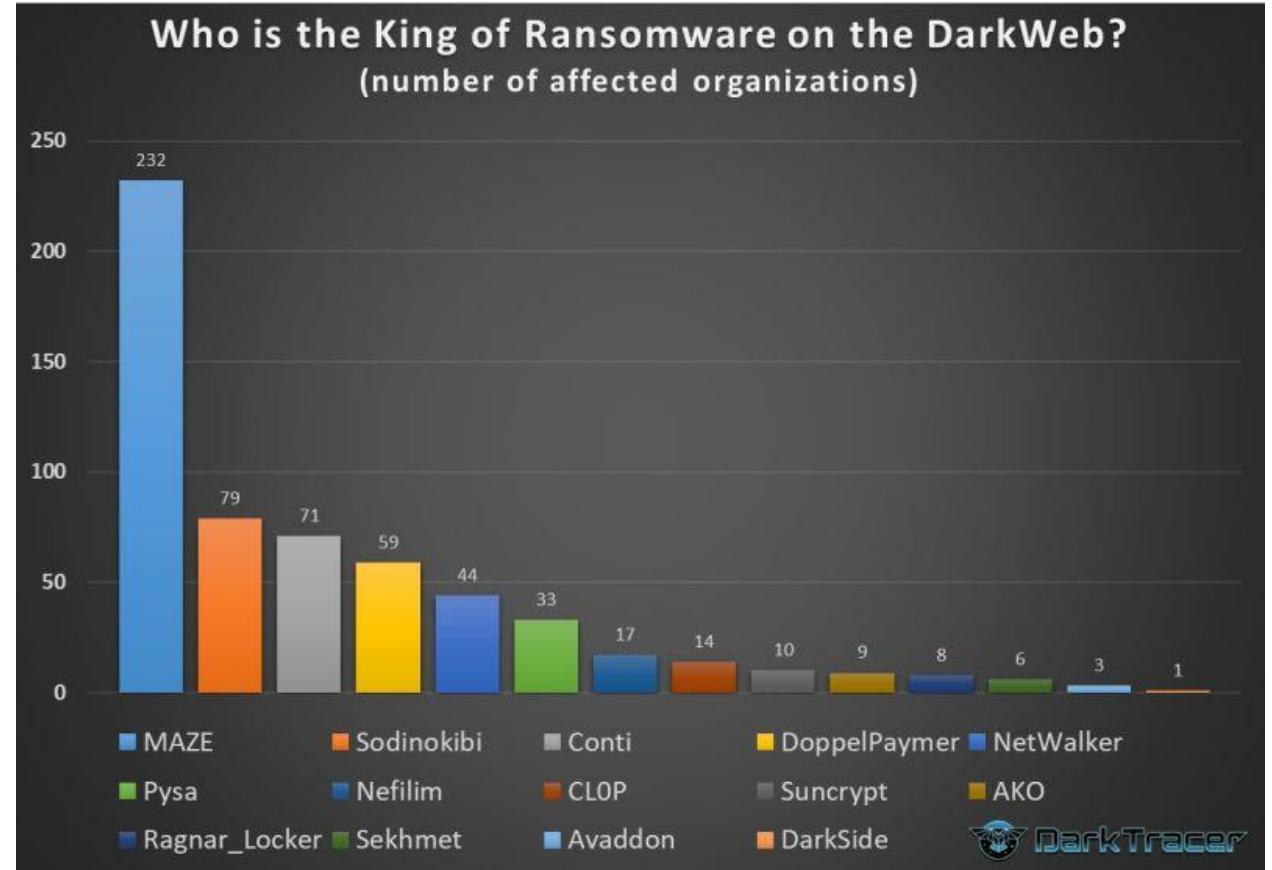


Network Endpoint Data

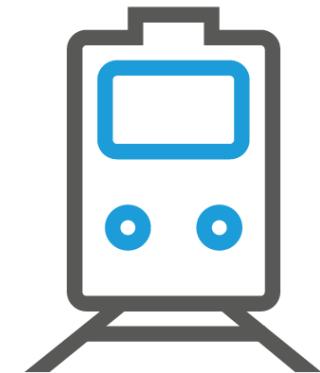
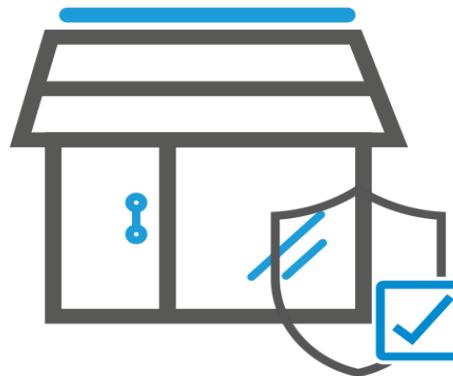
Ransomware: Más persistente y más inteligente

Evolución del Ransomware

- Antes de 2016: CryptoLocker
- 2016: Petya
- 2017: WannaCry
- 2018: Descenso. Minería de bitcoins.
- 2019: Ransom + Publicación de datos
- 2020: Tendencia al alza



Sectores más afectados por Ransomware



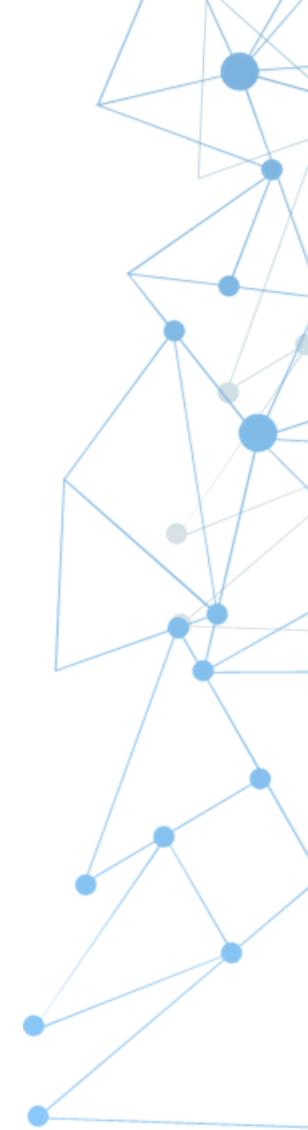


¿Cómo hacer frente al ransomware?



Medidas Antiransomware

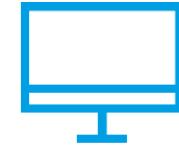
1. Backup
2. Protección del puesto de trabajo
3. Protección perimetral
4. Cifrado de datos



Medidas Antiransomware de Stormshield



**NETWORK
SECURITY**



**ENDPOINT
SECURITY**



**DATA
SECURITY**

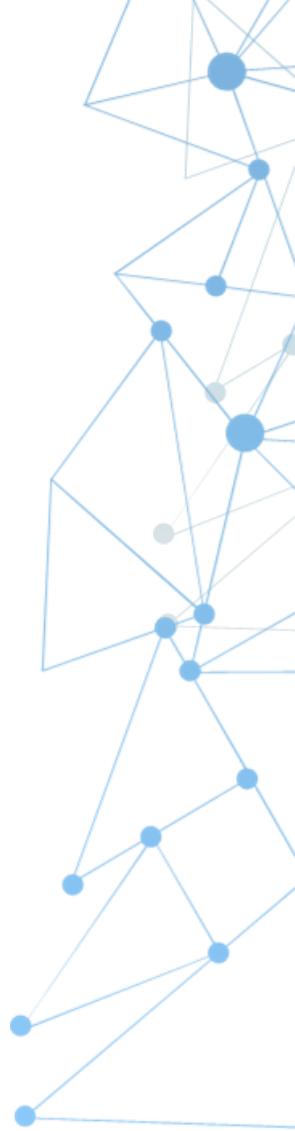
Stormshield Endpoint Security

Evolution

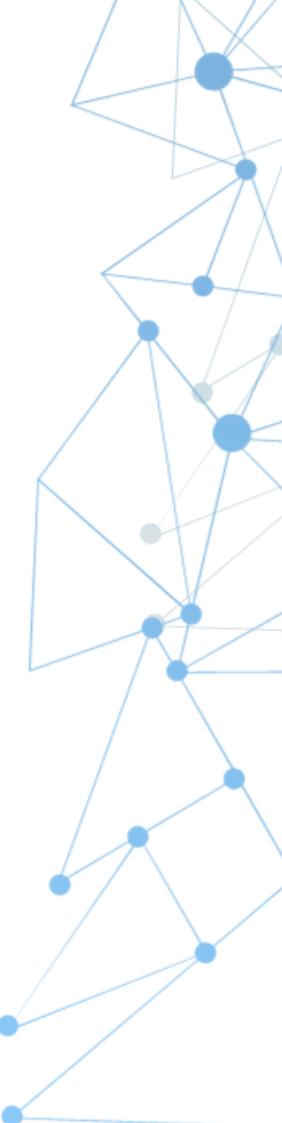
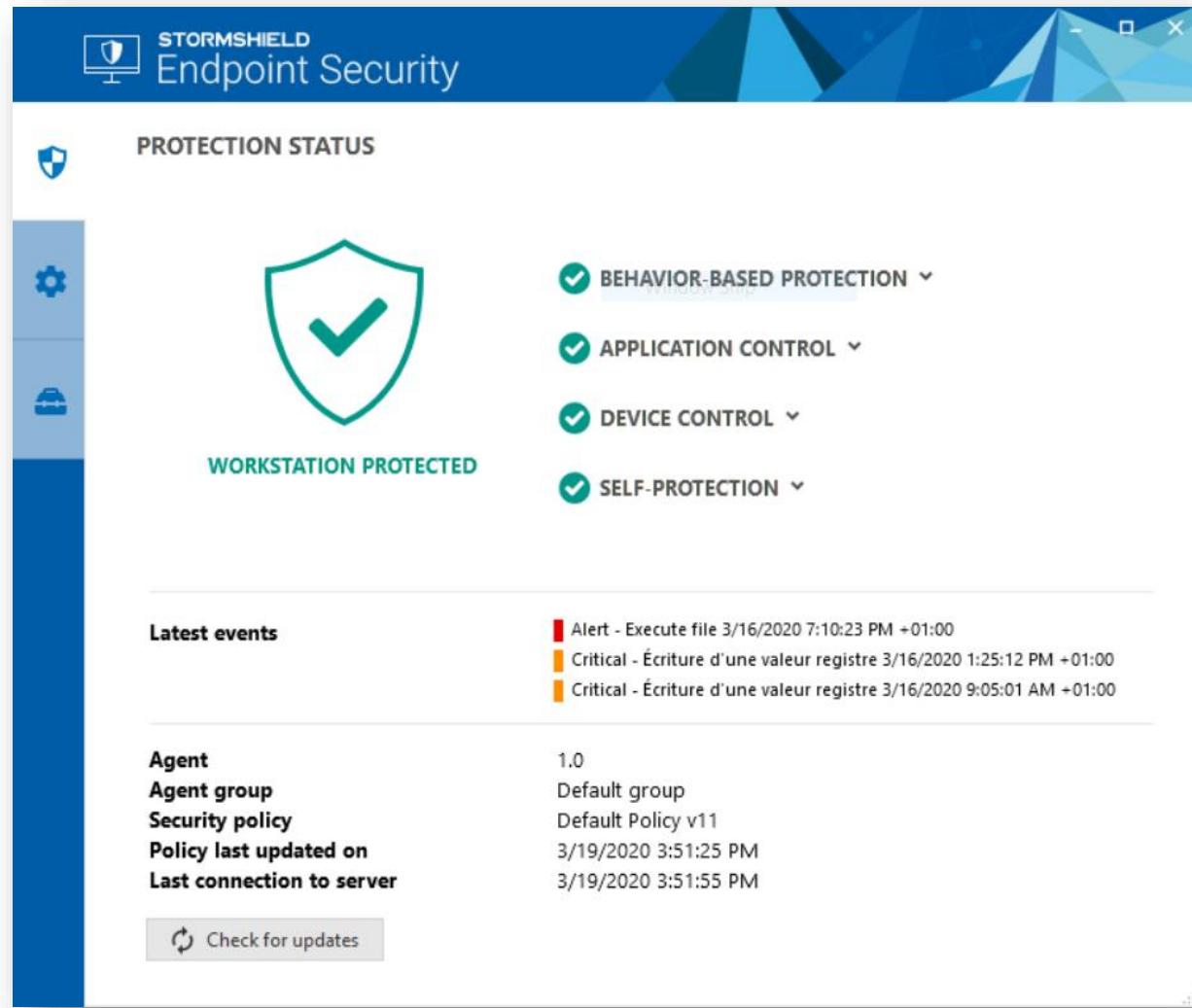
SES Evolution



Protección avanzada basada en comportamiento capaz de bloquear amenazas desconocidas y ataques de día cero



Agente SES Evolution



Funcionalidades de Seguridad

Protecciones de prevención de amenazas



Buffer Overflow



Process Hollowing



Application Hooking

The screenshot shows the Stormshield interface with the "Stack pivoting" tab selected. The status is set to "Disabled". A note below states: "Prevents the creation of fake stacks that would allow hackers to control program execution". There is a list entry for "? Apps - Apps known to perform stack pivot..." with a delete button. At the bottom, there is a "Default behavior" section with a "Status" dropdown set to "Enabled".



Protecciones de prevención de amenazas



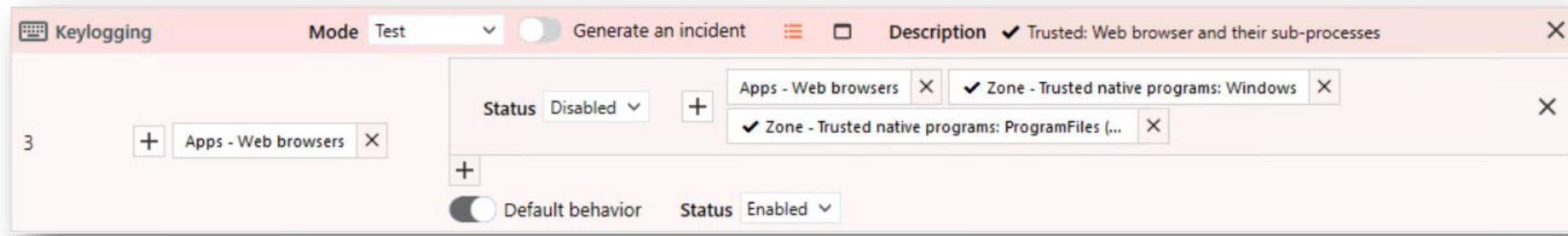
Privilege Escalation



Keylogging



Credential Theft



The screenshot shows the STORMSHIELD software interface with the 'Keylogging' tab selected. The 'Mode' dropdown is set to 'Test'. A toggle switch labeled 'Generate an incident' is turned off. The 'Description' field contains the text 'Trusted: Web browser and their sub-processes'. Below this, there are two sections: 'Status' (set to 'Disabled') and 'Default behavior' (set to 'Enabled'). Under 'Status', there are three entries: 'Apps - Web browsers' (disabled), 'Zone - Trusted native programs: Windows' (enabled), and 'Zone - Trusted native programs: ProgramFiles (...)' (disabled). A plus sign (+) button is available to add more entries.

Protección de recursos del sistema



Application Control



File Access Control



Registry Access Control

The screenshot shows the STORMSHIELD interface with two policy configurations for file access control:

Policy 1: Windows - Edge Package Installation Directory

Action	Allow	Block
Read	Allow	
Write	Allow	
Create	Allow	
Delete	Allow	

Policy 2: Windows - CustomDestinations

Action	Allow	Block
Read	Allow	
Write	Allow	
Create	Allow	
Delete	Allow	

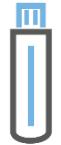
Protección de la red y control de dispositivos



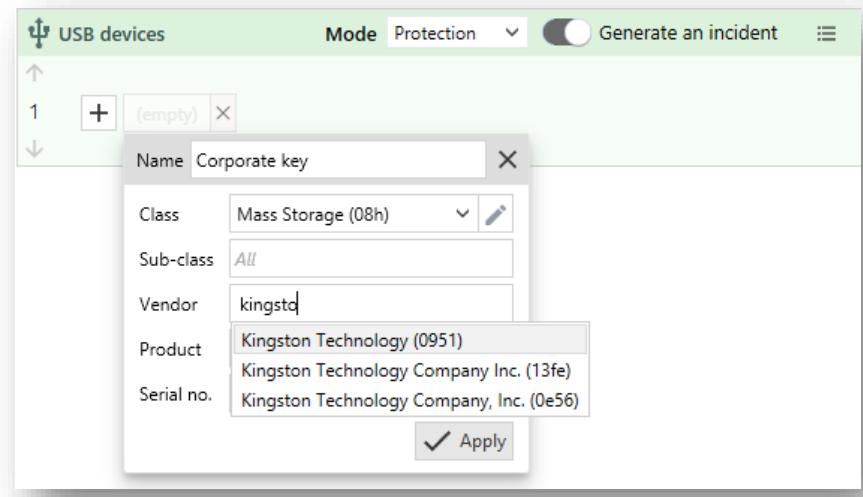
Application FireWall



WiFi and Bluetooth Protections



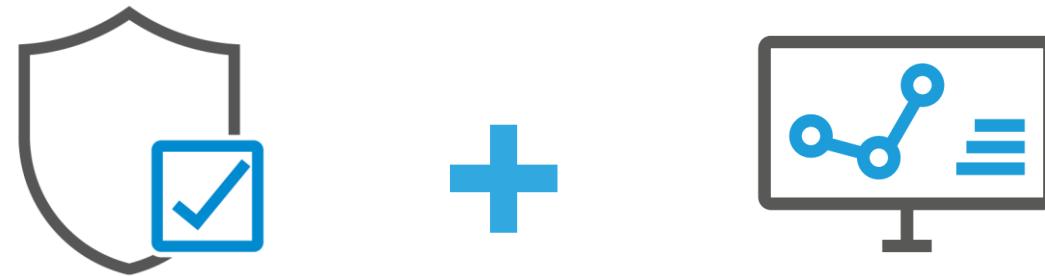
Device Control



Monitorización



SES Evolution



Solución híbrida EDR / EPP que bloquea los ataques y recopila información

Entender qué ha pasado



Gather Information

- Specific logs with common fields
- Detailed information for each protection
- Per rule override for severity and upload options



Share Information

- Syslog export for SIEM integration
- JSON format compatible with most SIEM
- SES Server used as proxy for SIEM export



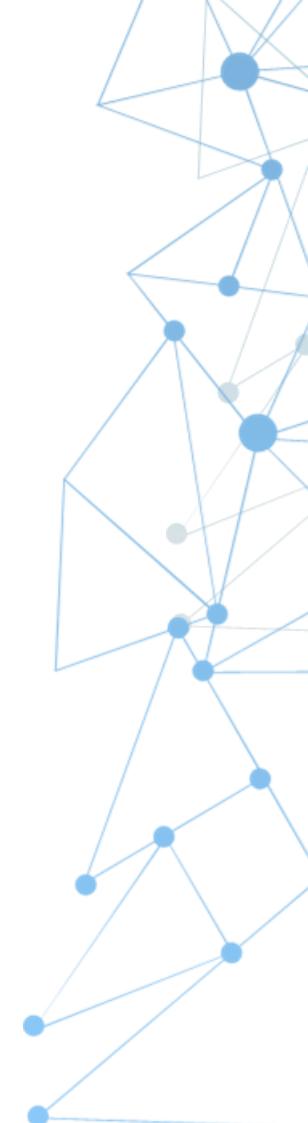
Manage Priorities

- Immediate upload of Alerts
- Less urgent logs deferred
- Easy log filtering with basic and advanced filters



Understand the attack

- Alerts uploaded with context
- Attack chart generated to visualize the events
- Create exceptions directly from logs



Gestión de logs de agentes

Filters								Default filters	Advanced filters	
Log type	Sévérité	Status	Attribute	Category of contact	Agent group	Agent	Application			
Event (16)	Très haute (8)	New (57)	Self-protection (0)	Threats (1)	Default group (57)	abr-server19 (38)	7z1900-x64.exe (24)			
Incident (12)	HIGH (33)	In progress (0)	Protection (57)	File (30)		DESKTOP-A4E5HRC (19)	dasHost.exe (12)			
	MEDIUM (16)	False positive (0)	Internal (13)	Registry (11)			wininit.exe (9)			
	Low (0)	Fixed (0)	Audit (6)	Process (1)			AgentSetup_x64.exe (7)			
		Closed (0)		Network (14)			OneDrive.exe (2)			
				Device (0)						
				Internal (0)				<input type="text" value="Enter agent name"/>		
DATE		BLOCKED	AGENT	MESSAGE			TYPE	SERVER POLICY	STATUS	ACTIONS
> 3/9/2020 1:55:30 PM			DESKTOP-A4E5HRC NT AUTHORITY\LOCA...	The 'dasHost.exe' process attempted to communicate over the network to remote address ff02::c and remote port 3702 via UDP			Outbound net...	Anti Malware P... Protection	New	
!	> 3/9/2020 1:49:30 PM	1/1	DESKTOP-A4E5HRC				Incident	Anti Malware P... Protection	New	
>	3/9/2020 1:48:48 PM		abr-server19 ABR-SERVER19\Admini...	The 'lfs.exe' process attempted to communicate over the network to remote address 185.20.49.7 and remote port 80 via TCP			Outbound net...	Anti Malware P... Protection	New	
!	> 3/9/2020 1:46:45 PM		abr-server19				Incident	Anti Malware P... Protection	New	

Gestión de alertas de agentes

ATTACK CHART

```
graph LR; explorer[explorer.exe] --> powershell[powershell.exe]; powershell --> cmd1[cmd.exe]; powershell --> ping[PING.DLL]; powershell --> malware1[Malware.2.0.exe]; cmd1 --> ping; ping --> malware1; ping --> malware2[Malware.2.0.exe];
```

Grouper les noeuds

INFORMATION

Name	PID
powershell.exe	880

RAW LOGS

Command line

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "-Command" "if((Get-ExecutionPolicy) -ne 'AllSigned') { Set-ExecutionPolicy -Scope Process Bypass }; & 'C:\Users\test\Desktop\03-execute.ps1'"
```

Process creation date Process end date

3/9/2020 2:11:28 PM 3/9/2020 2:11:39 PM

Output code

The operation completed successfully.

Path

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Hash

MD5: CDA48FC75952AD12D99E526D0B6BF70A
SHA1: 36C5D12033B2EAF251BAE61C00690FFB17FC
SHA256: 908B64B1971A979C7E3E8CE4621945CBAE

Certificates Microsoft Windows, Microsoft Win

CONTEXT LOGS 1 / 162 log(s) Data about this incident are partial. You can request more details to the agent.

Request more data

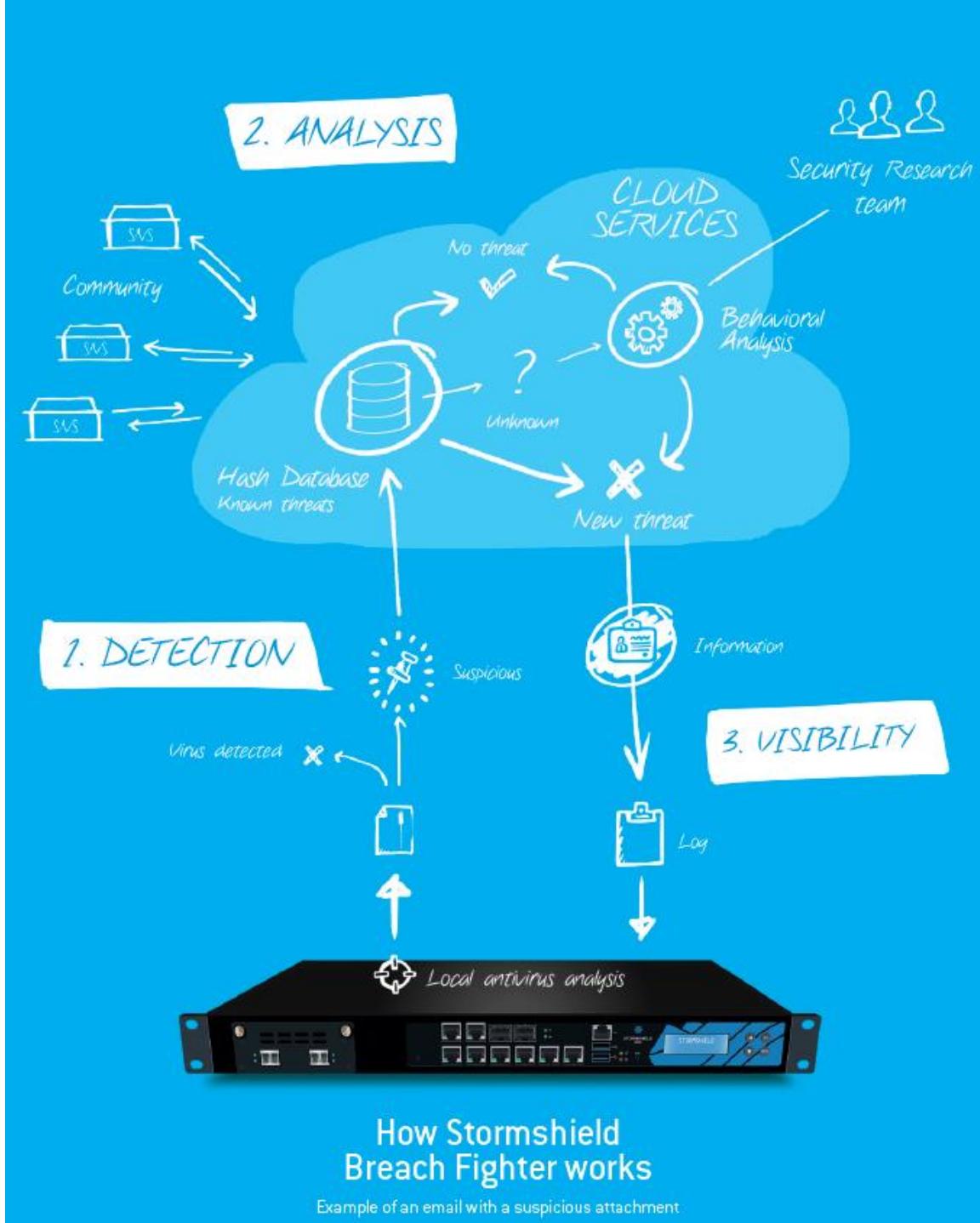
Alerts only Épinglés uniquement

Search... ?

Time	Type	Details
3/9/2020 2:11:39 PM	Process execution	The 'powershell.exe' process attempted to run the 'C:\Users\test\Desktop\Malware.2.0.exe' process

Stormshield Network Security

BreachFighter

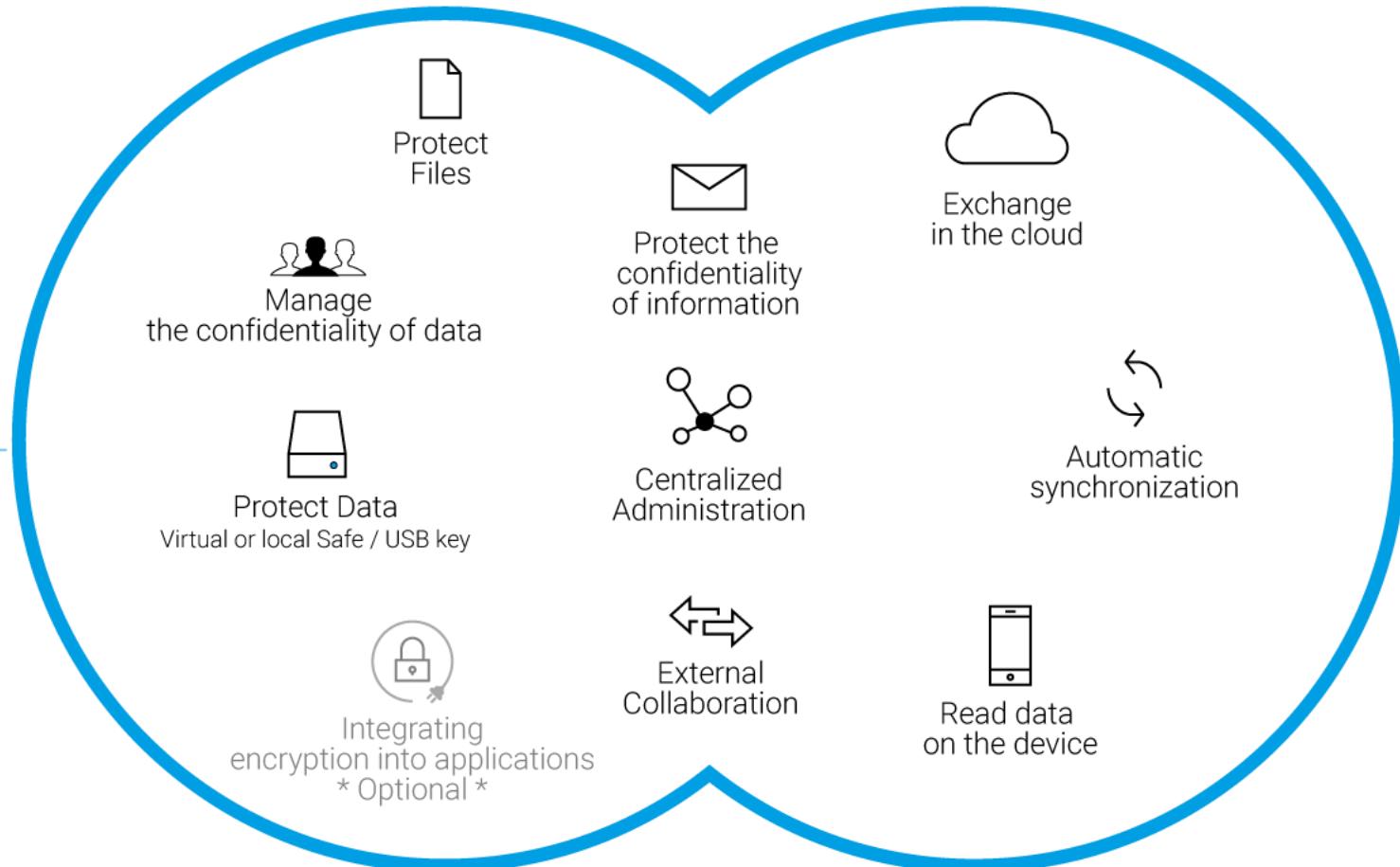


Stormshield Data Security



Stormshield Data Security

Stormshield Data
Enterprise



Stormshield Data
For Cloud & Mobility

Stormshield Data Security



Reducción del riesgo
de datos en claro



Agnóstico
Facilita soluciones colaborativas en cualquier plataforma



Integración
con las aplicaciones de negocio



Aprovechando
herramientas colaborativas de manera segura

Gracias



STORMSHIELD



Estamos en contacto

 Pº de la Castellana, 200
28046 Madrid

 +34 91 904 72 44

 iberia@stormshield.eu