PAESSLER
THE NETWORK MONITORING COMPANY

¿Está su seguridad realmente segura?

PRTG
NETWORK
MONITOR

PAESSLER
THE NETWORK MONITORING COMPANY

MONITORIZACIÓN DE RED COMO HERRAMIENTA DE META SEGURIDAD

Muchas tendencias de moda en TI siguen la trayectoria de un fuego artificial: una fuerte explosión, ráfaga de luz y se acabó.

La seguridad no es una de esas tendencias. Desde los primeros días de la creación de las redes, la seguridad informática ha sido un tema crítico que sigue siendo válido ahora más que nunca. En el 2015, una encuesta realizada por Paessler reveló que el **58% de todos los administradores de TI encuestados nombraron la seguridad como una de sus principales tareas y constantes desafíos**. En el pasado, un firewall y un antivirus eran suficientes para proteger la red de las PYME's, pero hoy en día, se necesitan una serie de soluciones interconectadas para contrarrestar las amenazas en constante evolución.

Todas estas herramientas de seguridad de TI sólo pueden proporcionar una completa seguridad si su funcionalidad está asegurada y si la información general sobre todas las medidas están siendo garantizadas. Esto requiere una exhaustiva estrategia de seguridad que identifique los peligros potenciales, establezca las herramientas adecuadas como protección preventiva, y que controle y observe todo ello dentro de una solución central.

PRTG NETWORK MONITOR

PRTG Network Monitor

Software de tecnología Alemana que permite:

- Monitorización unificada – todo de un solo vistazo
- Capacidad de respuesta rápida: informando y alarmando
- Planeando y optimizando el ambiente de TI
- Amigable y escalable
- +150,000 instalaciones en el mundo
- Crecimiento en América Latina
  - 2014 en 40% y 2015 en 40%

PAESSLER
THE NETWORK MONITORING COMPANY

+58% de los administradores de TI identificaron que la seguridad es una de sus importantes tareas

¿En qué nos ayuda PRTG con la **metaseguridad**?

PRTG NETWORK MONITOR

Seguridad de TI

Riesgos y potenciales amenazas

- Faltas de actualizaciones de software
- Intrusión por medio del Shadow TI
- Accesos no deseados
- Pérdida de datos corporativos
- Interrupciones potenciales
- Amenazas físicas

Seguridad de TI

Para cada amenaza existe un antídoto:

- Antivirus y Firewalls, protegen del malware
- Soluciones de Backup aseguran los datos
- Monitores ambientales verifican la idoneidad del medio ambiente
- Cámaras detectan vandalismo…

¡Si operan adecuadamente su entorno de IT estará relativamente seguro!

Seguridad de TI

¿Qué tienen en común los sistemas de seguridad de TI?

- Necesitan del apoyo de la infraestructura de red
- Poseen memoria “corta”
- Requieren de configuración de alertas en cada componente
- Ofrecen una visión encapsulada de cada componente
- Requieren continua supervisión
- Multimarca y multiprotocolo
- Registran en sus bitácoras o generan importantes alertas via snmp trap

La monitorización asegura la seguridad

Las soluciones de monitorización existen para controlar toda su infraestructura de TI y llamar la atención sobre eventuales riesgos y/o problemas.

Las soluciones inteligentes ofrecen la posibilidad de detectar comportamientos inusuales en los sistemas con el fin si es necesario de evaluar mejor el riesgo

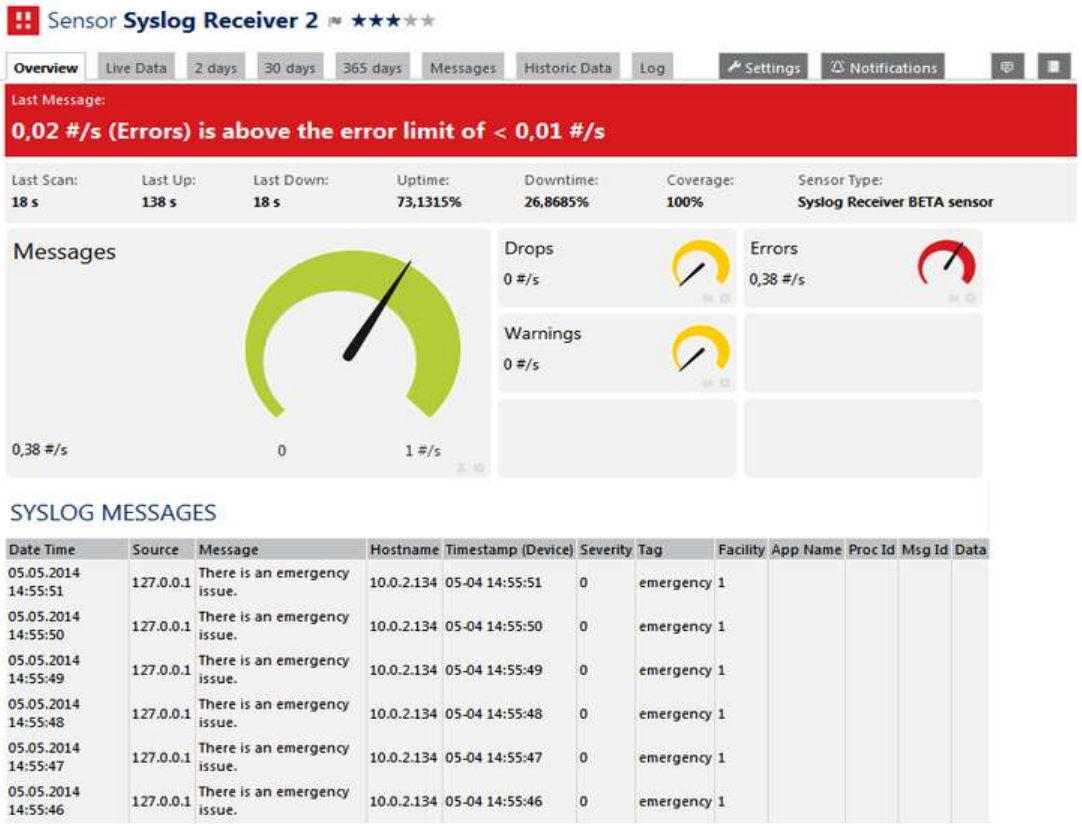
El análisis histórico de los datos permite estimar las acciones futuras requeridas

Verificación de bitácoras

PRTG monitoriza las bitácoras de los dispositivos o servicios de seguridad

Sensor ejemplo:

Syslog Receiver

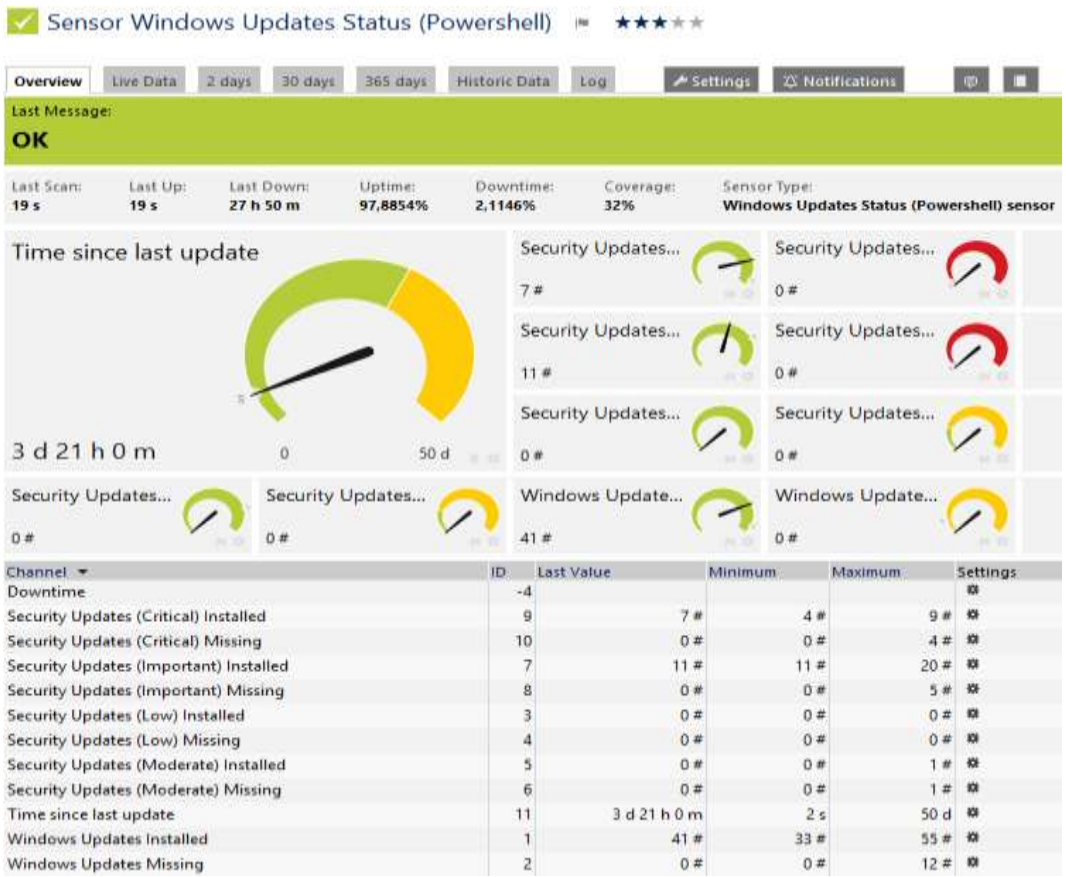


Actualización de software

PRTG monitoriza las actualizaciones de ambientes Windows

Sensor ejemplo:

Windows Update Status



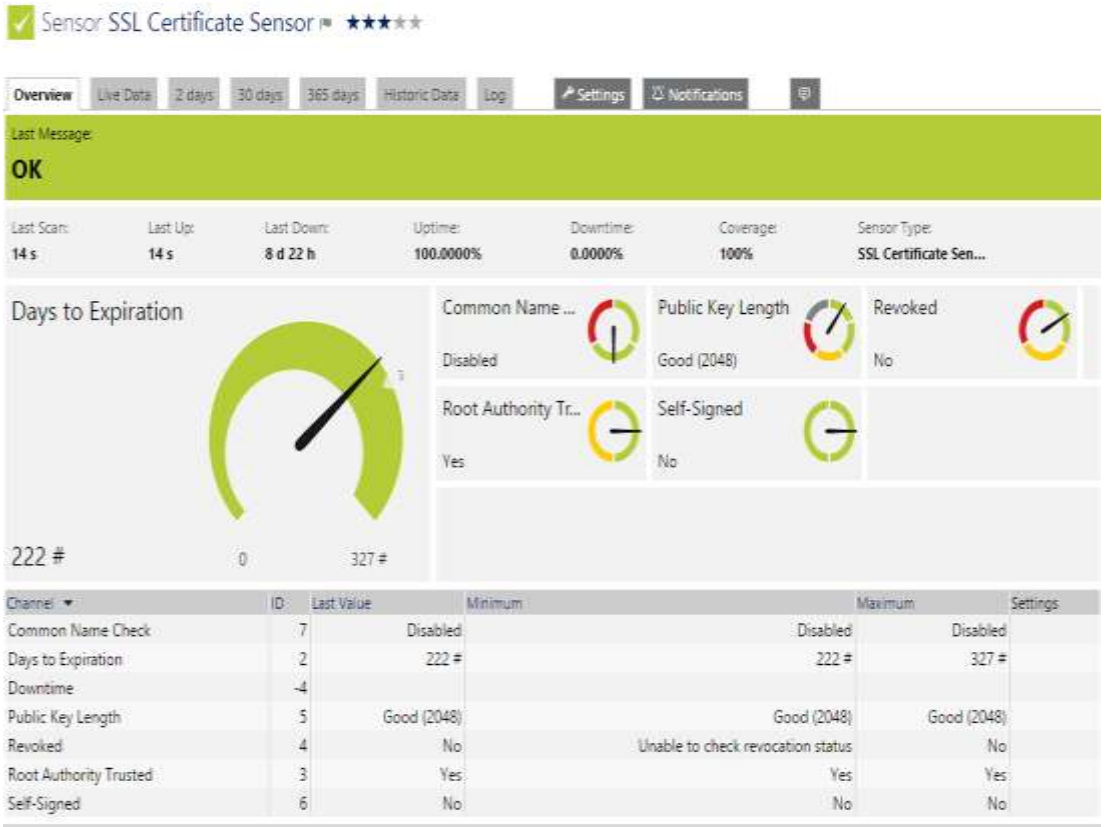
Channel	ID	Last Value	Minimum	Maximum	Settings
Downtime	-4				
Security Updates (Critical) Installed	9	7 #	4 #	9 #	
Security Updates (Critical) Missing	10	0 #	0 #	4 #	
Security Updates (Important) Installed	7	11 #	11 #	20 #	
Security Updates (Important) Missing	8	0 #	0 #	5 #	
Security Updates (Low) Installed	3	0 #	0 #	0 #	
Security Updates (Low) Missing	4	0 #	0 #	0 #	
Security Updates (Moderate) Installed	5	0 #	0 #	1 #	
Security Updates (Moderate) Missing	6	0 #	0 #	1 #	
Time since last update	11	3 d 21 h 0 m	2 s	50 d	
Windows Updates Installed	1	41 #	33 #	55 #	
Windows Updates Missing	2	0 #	0 #	12 #	

Actualización de Software

Validez de certificados SSL

Sensor ejemplo:

SSL Certificate



Channel	ID	Last Value	Minimum	Maximum	Settings
Common Name Check	7	Disabled	Disabled	Disabled	
Days to Expiration	2	222 #	222 #	327 #	
Downtime	-4				
Public Key Length	5	Good (2048)	Good (2048)	Good (2048)	
Revoked	4	No	Unable to check revocation status	No	
Root Authority Trusted	3	Yes	Yes	Yes	
Self-Signed	6	No	No	No	

Actualización de software

PRTG monitoriza las estadísticas del Windows Server Update Services (WSUS)

Sensor ejemplo:

WSUS Statistic

Intrusión por medio del Shadow-TI

Monitorización del software de seguridad

Sensor ejemplo:

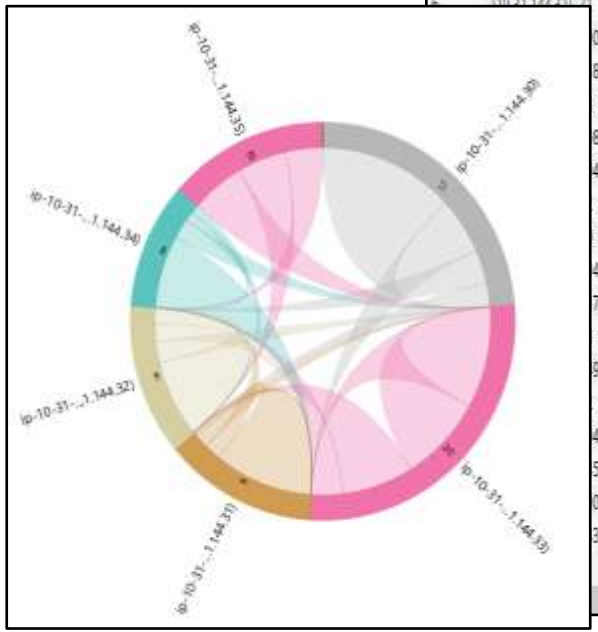
WMI Security Center

Accesos no deseados

Monitorización de firewalls, puertos, tráfico de datos, usuarios VPN, etc.

Sensor ejemplo:

Netflow



1 to 23 of 23

Pos	Source IP	Source Port	Destination IP	Destination Port	Protocol	Bytes	
1.	[10.31.144.32]	137	[192.168.100.15]	80	TCP	28 KByte	8 %
2.	[10.31.144.33]	21	[192.168.100.1]	3389	TCP	28 KByte	8 %
3.	[10.31.144.35]	161	[192.168.100.2]	445	TCP	28 KByte	8 %
4.	[10.31.144.32]	194	[192.168.100.10]	80	TCP	26 KByte	7 %
5.	[10.31.144.34]	1494	[192.168.100.10]	80	TCP	25 KByte	7 %
6.	[10.31.144.31]	21	[192.168.100.16]	137	TCP	25 KByte	7 %
		00	[192.168.100.5]	1494	TCP	23 KByte	6 %
		89	[192.168.100.6]	53	TCP	22 KByte	6 %
			[192.168.100.11]	21	TCP	22 KByte	6 %
		80	[192.168.100.8]	80	TCP	19 KByte	5 %
		4	[192.168.100.7]	194	TCP	18 KByte	5 %
			[192.168.100.10]	137	TCP	17 KByte	5 %
			[192.168.100.9]	53	TCP	16 KByte	4 %
		4	[192.168.100.5]	1494	TCP	13 KByte	4 %
		7	[192.168.100.7]	3389	TCP	13 KByte	4 %
			[192.168.100.2]	53	TCP	11 KByte	3 %
		94	[192.168.100.6]	5900	TCP	11 KByte	3 %
			[192.168.100.8]	443	TCP	9,140 Byte	2 %
		4	[192.168.100.1]	25	TCP	5,780 Byte	2 %
		5	[192.168.100.3]	443	TCP	1,320 Byte	< 1 %
		00	[192.168.100.3]	1494	TCP	500 Byte	< 1 %
		3	[192.168.100.18]	22	TCP	460 Byte	< 1 %
						0 Byte	< 1 %

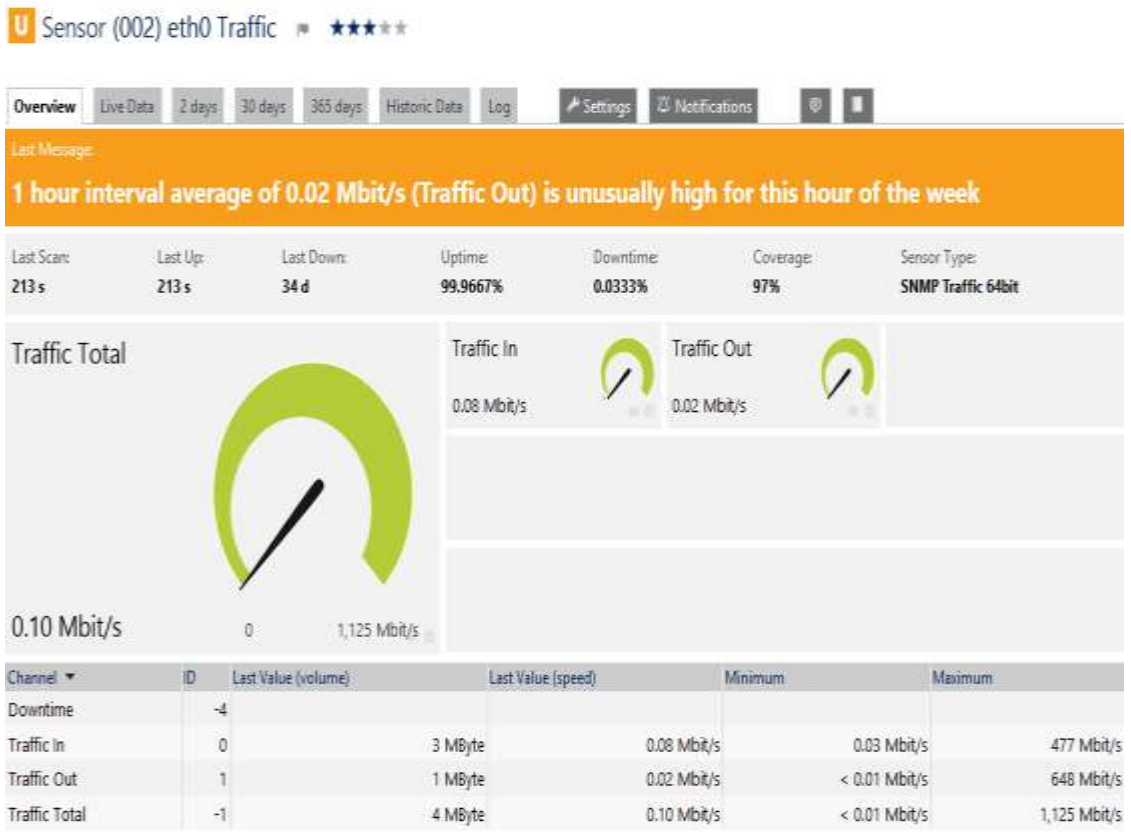
Accesos no deseados

Monitorización de tráficos inusuales:

- ¿Malware?
- ¿Extracciones de información?

Sensor ejemplo:

SNMP Traffic

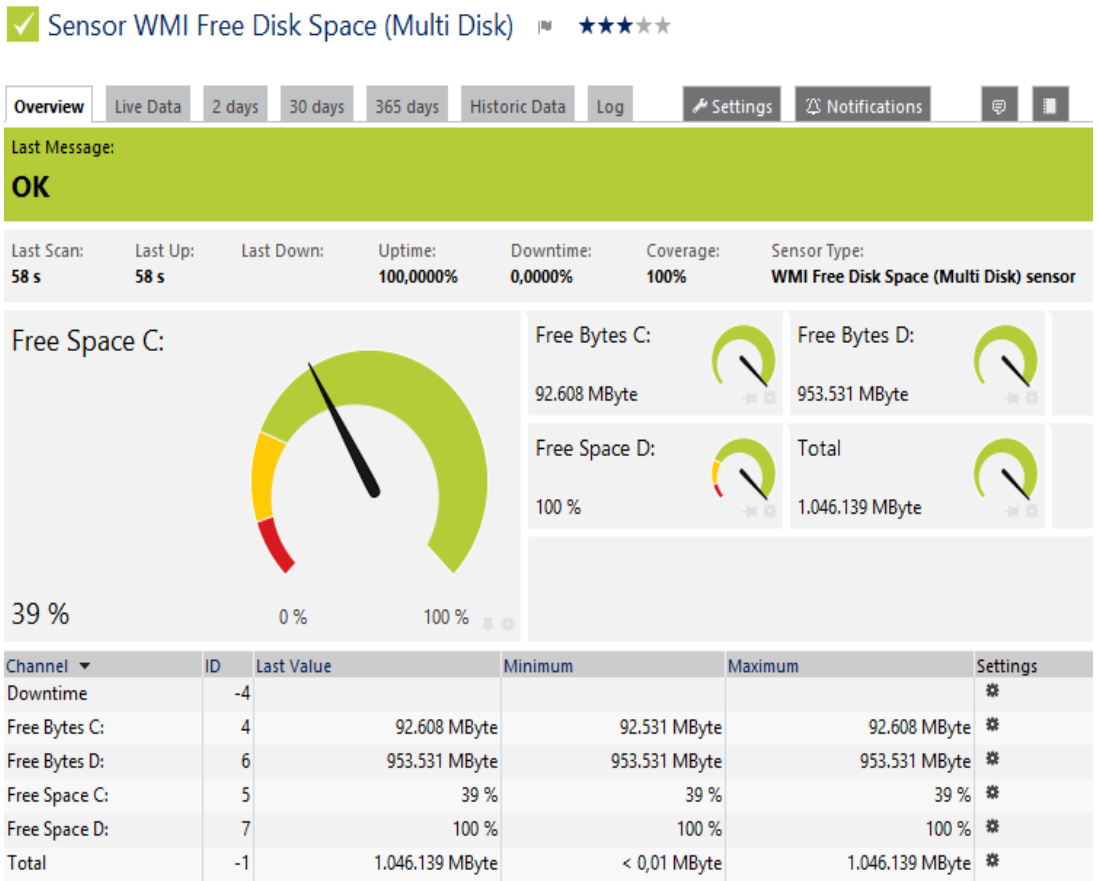


Pérdida de datos corporativos

Monitorización de discos duros y almacenamiento

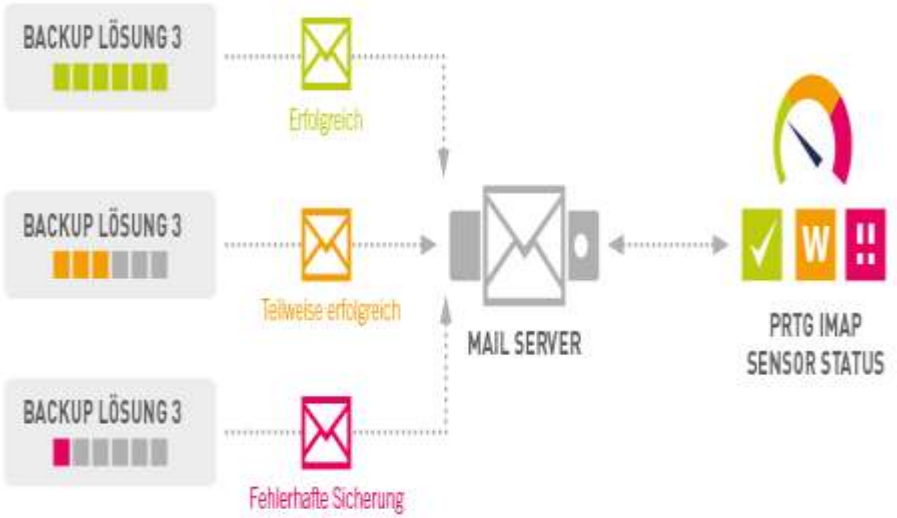
Sensor ejemplo:

WMI Free Disk Space



Pérdida de datos corporativos

Monitorización de copias de respaldo (Backup)



Sensor ejemplo:

IMAP

Pérdida de datos corporativos

Monitorización del nivel de encriptación

Sensor ejemplo:

SSL Security Check

Channel	ID	Last Value	Minimum	Maximum	Settings
Downtime	-4				
Security Rating	2	Only Strong Protocols Possible	Only Strong Protocols Possible	Only Strong Protocols Possible	
SSL 2.0 (Weak)	3	Denied	Denied	Denied	
SSL 3.0 (Weak)	4	Denied	Denied	Denied	
TLS 1.0 (Strong)	5	Accepted	Accepted	Accepted	
TLS 1.1 (Strong)	6	Accepted	Accepted	Accepted	
TLS 1.2 (Perfect)	7	Accepted	Accepted	Accepted	

Amenazas físicas

Para detectar amenazas físicas críticas en áreas sensitivas:

- Temperatura
- Vandalismo
- Fuego
- Calidad de voltaje
- Humedad
- Punto de condensación
- Nivel de C02 ...

Sensor ejemplo:

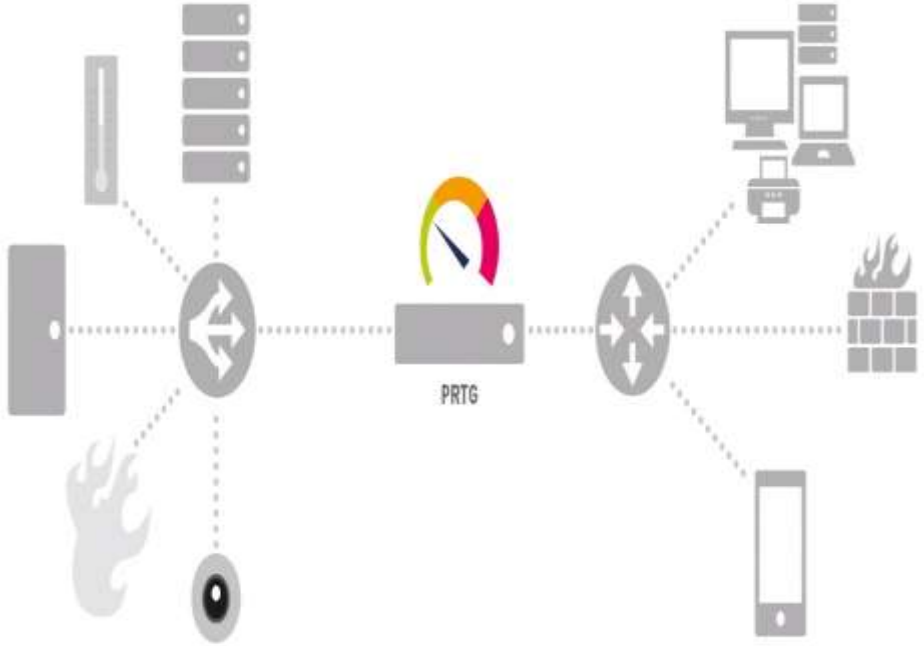
SNMP Library

Disponibilidad y Rendimiento

Hardware | Aplicaciones | Servicios

- Evita interrupciones de los sistemas de producción y sistemas de seguridad
- Reconoce ataques y eventos inusuales

¡Ningún punto ciego dentro de TI¡



¡Rápida Reacción!

Alertas y notificaciones

- Notificaciones vía Email
- Envía Push-Notifications
- Envía SMS/Pager-Message
- Envía Event Logs
- Envía Syslog-Message
- Envía SNMP-Trap
- Ejecuta Acciones HTTP
- Ejecuta Programas
- Envía Amazon Simple Notification Service Message
- Asigna Tickets
- Activa una alarma audible

¿Acciones futuras requeridas?

Prácticamente, para todas las amenazas se encuentra el "antídoto" correcto.

1. Los antivirus y los firewalls protegen contra el malware,
2. Las copias de seguridad aseguran datos,
3. Los sensores ambientales controlan la humedad y la temperatura, y
4. Las cámaras de vigilancia tienen a la vista a los intrusos no deseados.

Mientras todos estos sistemas funcionen de forma confiable, su ambiente de TI estará relativamente seguro.

Pero, ¿cómo puede asegurarse de que todo funciona adecuadamente? Y sobre todo, ¿cómo se mantiene un registro del número de sistemas que son esenciales para la seguridad de su TI?

Para un concepto de seguridad integral usted necesita una solución de monitorización de todos los componentes de seguridad, como una especie de herramienta de seguridad meta para la monitorización y control de todos los componentes claves.

Informes

Almacenamiento de datos sin sumarización

Exportación de datos

Generación automática de informes

Presentación visual

¡Gracias!

¿Preguntas?

¡No dude en contactarnos si necesita más información!