ANTE LOS ATAQUES DE RANSOMWARE

PROTEGERSE CONTRA LAS AMENAZAS HOY EN DÍA NO PERMITE BAJAR LA GUARDIA

Para ser verdaderamente eficaz, una solución de protección del Endpoint debe proporcionar prevención, detección, visibilidad e inteligencia adaptativa, antes, durante e incluso después de un ataque

Adaptive Defense integra todos esos elementos en una protección ligera en el equipo o dispositivo, soportado por una gran y escalable capacidad de procesamiento en la nube.

panda

pcnova
Total Care Computer Consulting

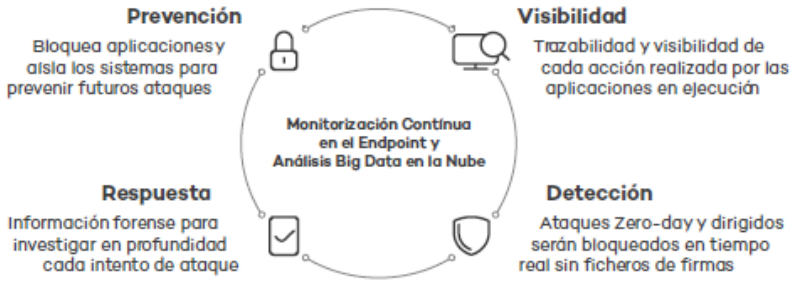
LA ÚNICA SOLUCIÓN QUE GARANTIZA LA SEGURIDAD DE TODAS LAS APLICACIONES EJECUTADAS

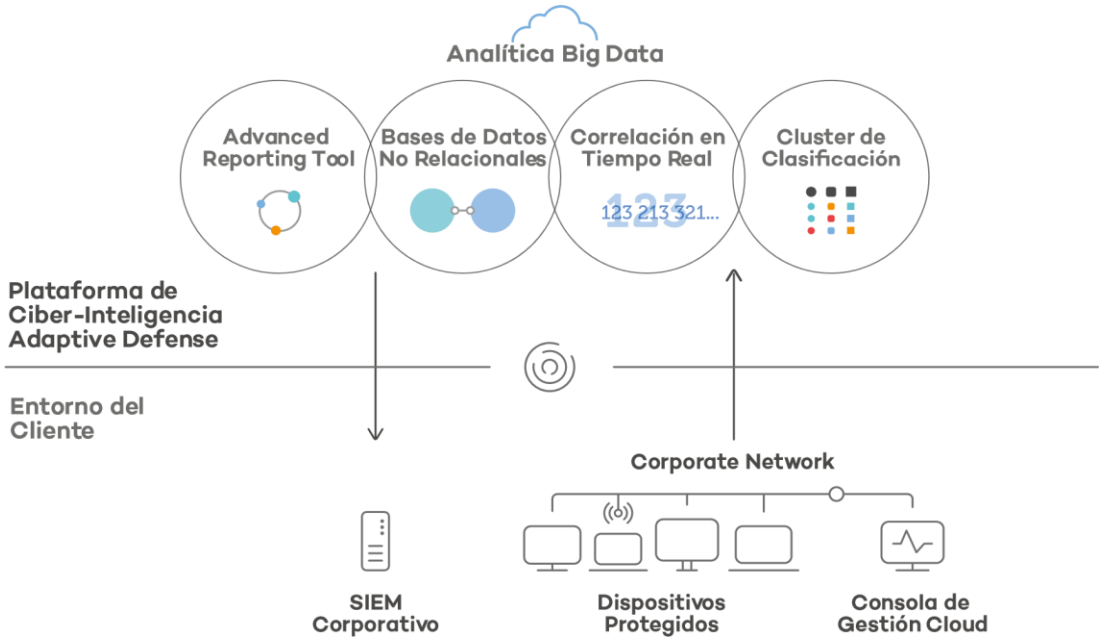
Las soluciones tradicionales antivirus resultan eficaces para bloquear malware conocido utilizando técnicas de detección basadas en ficheros de firmas y algoritmos heurísticos. Sin embargo, no son efectivas contra los ataques de día cero y ataques dirigidos, diseñados para aprovecharse de la 'ventana de oportunidad del malware' a través de herramientas, tácticas, técnicas, y procedimientos maliciosos (TTPs).

La "ventana de oportunidad" es cada vez mayor, lo que es aprovechado por los hackers para introducir virus, ransomware, troyanos y otros tipos de malware avanzado y ataques dirigidos en las empresas.

La familia de productos y servicios de Adaptive Defense es la solución de Panda Security a este tipo de ataques. Como Partner Certificado de Panda Security, PCNOVA Adaptive Defense ofrece un servicio gestionado de detección y respuesta en el endpoint capaz de clasificar cada una de las aplicaciones que se ejecutan en la organización de forma precisa, permitiendo ejecutar únicamente lo que es confiable.

PCNOVA Adaptive Defense se fundamenta en un modelo de seguridad basado en tres principios: monitorización continua de las aplicaciones de los puestos y servidores de la empresa, clasificación automática mediante técnicas de Machine Learning en nuestra plataforma Big Data en la nube y, por último, el análisis en profundidad por parte de técnicos expertos de aquellas aplicaciones no clasificadas automáticamente, con el fin de conocer el comportamiento de todo aquello que se ejecuta en tu organización.



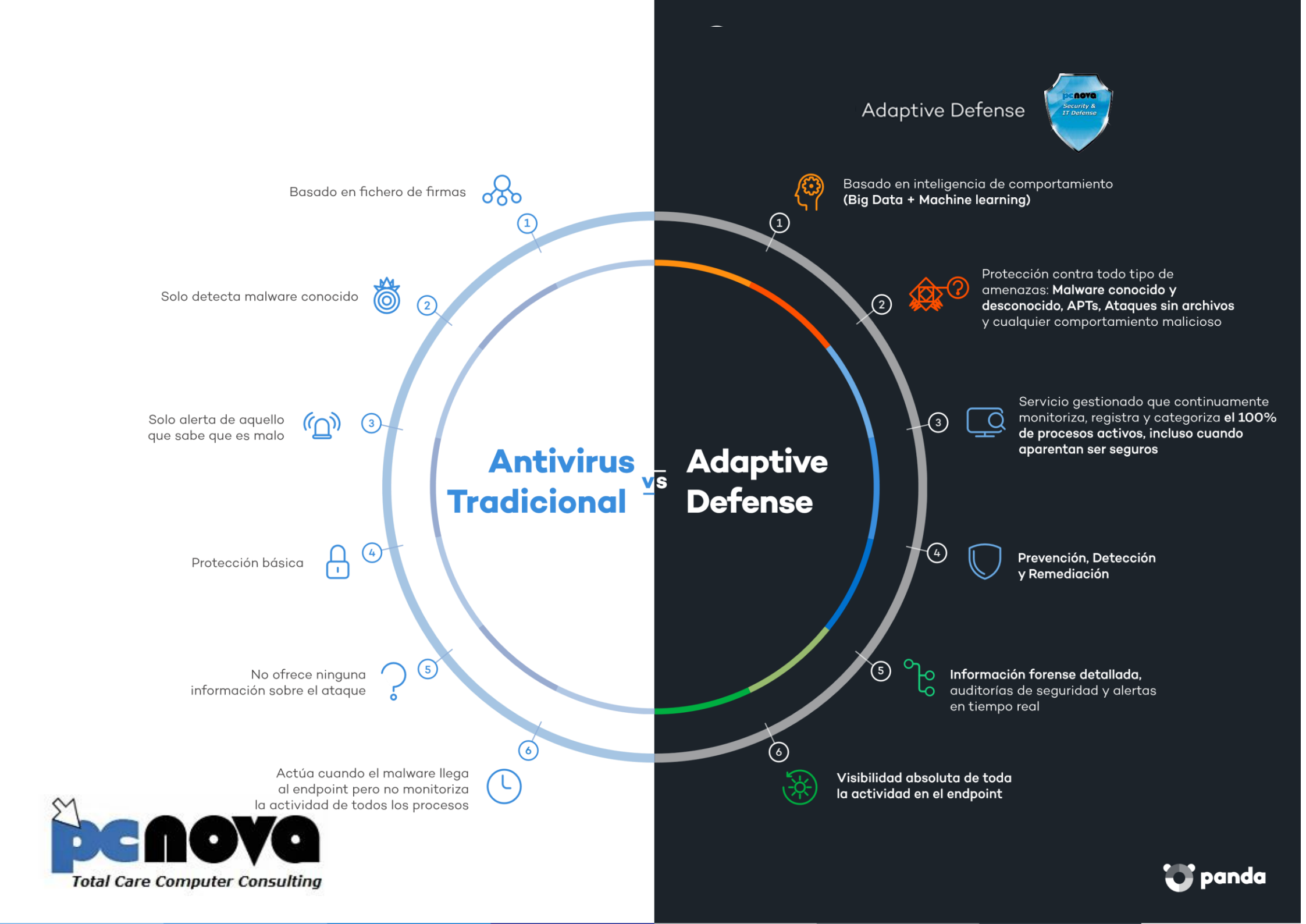


Las verdaderas soluciones de seguridad deben combinar tecnologías avanzadas e inteligencia humana y computacional, es decir, machine learning en manos de expertos en seguridad. Para que una solución de seguridad sea tomada en serio, debe ofrecer el tipo de prevención, detección, visibilidad e inteligencia que pueda detener y prevenir ciberataques de cualquier tipo de forma ininterrumpida. Creemos firmemente que los que toman decisiones deben buscar los siguientes elementos claves a la hora de decantarse por una solución de seguridad para el endpoint:

- **Monitorización continua,** mediante el registro y supervisión de toda la actividad desarrollada por los procesos en los dispositivos y equipos para detener el software no confiable en el momento de la ejecución, detectar amenazas avanzadas en tiempo real, responder en segundos y recuperarse de forma instantánea.
- **Detección de la ejecución de archivos no confiables**, que permite a tu empresa reducir la superficie de ataque en los equipos y dispositivos. Debes asegurarte de que la solución de seguridad que buscas clasifique como confiables o maliciosas todas las aplicaciones ejecutadas en tus equipos y dispositivos.
- **Automatización de la detección de amenazas**. La amenaza es más veloz que cualquier equipo o dispositivo que quieras proteger. Por tanto, no permitas que deleguen en ti la supervisión de la respuesta. Las soluciones de seguridad eficaces deben poder funcionar de forma autónoma y automatizada para adaptarse así al entorno operativo, que es único y característico de tu organización.
- **Respuesta rápida y automatizada**. Las organizaciones están saturadas con el volumen de eventos y alertas generados por los sistemas, pero una vez que el cibercriminal se infiltra, el robo de información es cuestión de segundos. Por eso, la solución de seguridad elegida debe ser capaz de identificar rápidamente un ataque en curso, establecer medidas para evitar los daños y aliviar la carga del equipo. De esta forma, se reducen costes y se automatizan tareas que antes suponían días de trabajo.

PCNOVA 2014 Total Care Computer Consulting S.L - N.I.F B-66403742
C/ Escorial 174-178, Esc.Derecha, Elo, 2da.
08024, Barcelona – España - Telf: 935.185.818
http://www.pcnova.es - atencionalcliente@pcnova.es

pcnova
Total Care Computer Consulting



pcnova
Total Care Computer Consulting

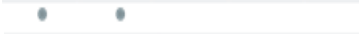
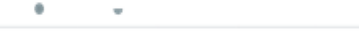
panda

Capacidades de protección crítica en los endpoints

	AD	AV	AE	AR	SB
PROTECCIÓN ANTE LAS DINÁMICAS DE ATAQUES DE SEGURIDAD ACTUALES					
Protege de malware conocido, malware no conocido y ataques de día cero, incluido ransomware y sus variantes	●	●			●
Protege de amenazas persistentes avanzada (APTs), ataques dirigidos y ciberespionaje	●				
Detecta ataques exploit conocidos o desconocidos, incluidos ataques malwareless	●		●		
Protege de ataques de botnets que convierte a los equipos y dispositivos en zombies controlados por servidores Command and Control (C&C)	●				●
MODELO DE PROTECCIÓN NEXT-GENERATION ENDPOINT PROTECTION (NGEP)					
Previene contra software malicioso, detecta durante el ataque en los equipos y previene que se repita	●	●	●	●	
Monitoriza continuamente los procesos en ejecución, clasifica las aplicaciones, evitando su ejecución si no son confiables	●				
Adaptación continua a las nuevas dinámicas de ataques mediante técnicas de machine learning en entornos Big Data	●	●			●
Se centra en el ataque a lo largo plazo, detectando y bloqueando dinámicamente herramientas, tácticas, técnicas, y procedimientos maliciosos (TTPs)	●				
DETECCIÓN, CONTENCIÓN Y RESOLUCIÓN					
Alerta en tiempo real ante una detección o un bloqueo por comportamiento con vestigios de ser malicioso	●				
Proporciona información en tiempo real sobre la actuación de un atacante: origen, causa, activos impactados y acciones realizadas	●				
Resolución automática, borrando los ficheros maliciosos, reparando cambios o matando procesos comprometidos	●	●	●	●	●
Ofrece información operativa acerca de labores posteriores de resolución y medidas de prevención frente a ataques futuros	●				
SERVICIO GESTIONADO					
Automatización con machine learning en big data, minimizando el trabajo en los equipos de seguridad y el tiempo entre detección y respuesta	●				
Expertos en descubrimiento de nuevos ataques (threats hunters) refuerzan el servicio	●	●			
Vigilancia y monitorización de la actividad de los atacantes 24/7, 365 días	●	●			●
HERRAMIENTAS DE INVESTIGACIÓN DEL INCIDENTE					
Facilita líneas de tiempo de un ataque (ficheros, registros, drivers,...) y su impacto en el negocio (activos afectados, equipos o dispositivos zombies)	●				
Acceso a la información granular, en base a perfiles de usuario, para preservar la confidencialidad Integración con otras	●				
herramientas de Investigación, en particular SIEMs	●				
PREVENCIÓN DE NUEVOS ATAQUES EXTERNOS E INTERNOS					
Visibilidad total en los equipos: software ejecutado, aplicaciones vulnerables, comportamiento de usuarios, tráfico consumido, etc. Herramientas de búsqueda de	●				
anomalías causadas por ataques externos, insiders o uso indebido de recursos empresariales	●				
Herramientas basadas en plataforma Big Data, en la nube, que minimizan la inversión, el coste operativo y en tiempo de respuesta	●				

pcnova
Total Care Computer Consulting

PCNOVA 2014 Total Care Computer Consulting S.L - N.I.F B-66403742
C/ Escorial 174-178, Esc.Derecha, Elo, 2da.
08024, Barcelona – España - Telf: 935.185.818
http://www.pcnova.es - atencionalcliente@pcnova.es

FACILIDAD DE DESPLIEGUE, GESTIÓN Y USO	
Facilidad de despliegue, actualización y administración desde la nube, que permite proteger sistemas remotos como si estuvieran en la red	
Despliegue masivo, sin interrupción del servicio, con autoaprendizaje y adaptación a la empresa de forma transparente (up & running en horas)	
Multi-tecnologías perfectamente integradas, evitando consumos indebidos y potenciando sinergias entre ellas	
Inapreciable impacto en la red y en los equipos protegidos, con un impacto máximo del 5% en el rendimiento del sistema	
Mínimo inconveniente para los usuarios, evitando sobrecarga de trabajo en los equipos de operaciones que se pueden centrar en la investigación de incidentes	
CAPACIDAD DE PROCESAMIENTO EN TIEMPO REAL	
Tecnología de Machine Learning sobre entornos de Big Data como única vía para la clasificación de los procesos en tiempo real	
La nube y el procesamiento Big Data posibilitan la extensión, compartición y crecimiento exponencial del conocimiento, en tiempo real	
La nube y la minería de datos sin limitación computacional, reducen la complejidad de los sistemas y favorece una eficiente gestión del riesgo	

LEYENDA:

AD: Adaptive Defense

AV: Anti Virus

AE: Anti Exploit

AR: Anti Ransomware

SB: Sand Boxing

REQUISITOS DEL SISTEMA PARA LA INSTALACION DE ADAPTIVE DEFENSE

Instalación del Agente:

- Equipos: Desde **Windows XP SP2 a Windows 10** (plataformas de 32/64 bits). (Próximamente MAC OSX, Linux y Android)
- Servidores: Desde **Windows 2003 a 2012** (bajo cualquier configuración o arquitectura).

Requisitos de Software:

El agente del servicio Adaptive Defense es una aplicación que requiere la instalación de los siguientes componentes estándar:

Windows:

- **.NET Framework, versión 2.0 SP2 o posterior**. Por ejemplo .NET Framework 3.5 SP1. El instalador comprobará si se encuentra instalado o no, pero no lo instalará en caso de que no lo encuentre.
- **Visual C++ 2008 Redistributable Package**. El instalador comprobará si está instalado o no, y lo instalará en caso necesario: (http://www.microsoft.com/es-es/download/details. aspx?id=5582).
- **Certificados Raiz Windows Actualizados.**

Requisitos de Conexión:

El agente se comunica por defecto vía HTTPS con el front-end del servicio, por lo que necesitará acceso a Internet a través del **puerto 443**. Debe estar permitido el acceso a las siguientes URLs:

- https://paps.pandasecurity.com
- https://rpuws.pandasecurity.com
- https://rpkws.pandasecurity.com

Se debe permitir la comunicación, así como la descarga de comprimidos desde dichas URL:

- Para permitir la comunicación por SSL **se deben tener los Certificados raíz actualizados** http://download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/rootsupd.exe
- En caso de que se utilice un proxy, deberá estar configurado, al igual que las claves correspondientes, en el portal Web **ANTES** de que se descargue el instalador. **Se debe utilizar unas credenciales de proxy que no caduquen.**
- En caso de que se utilicen varios proxies distintos, se generará un archivo MSI personalizado para cada uno, que deberá desplegarse en la red correspondiente.