Akamai

WHITE PAPER

Mitigación de riesgos, prevención y neutralización de las intrusiones

Minimice el impacto del ransomware con Akamai Guardicore Segmentation

Descripción general

El ransomware, que en su día simplemente era una molesta cepa de malware que utilizaban los ciberdelincuentes para restringir el acceso a archivos y datos a través del cifrado, se ha convertido en algo mucho peor. Aunque la amenaza de perder datos de forma permanente ya es de por sí estremecedora, los ciberdelincuentes y los hackers de estado se han vuelto lo suficientemente sofisticados como para utilizar el ransomware para introducirse en grandes empresas, administraciones federales, infraestructuras globales u organizaciones de salud pública y paralizarlas.

El criptogusano WannaCry de 2017, que infectó 230 000 ordenadores de todo el mundo aprovechándose de una vulnerabilidad de Microsoft Windows, sirvió como señal clara de las amenazas que suponía el ransomware. Desde entonces, los atacantes se han vuelto cada vez más sofisticados y los ataques más generalizados. Por ejemplo, con la aparición del ransomware como servicio (RaaS), donde los hackers venden sus servicios. En el informe de Akamai sobre amenazas de ransomware en la primera mitad de 2022, se analizaron los patrones de ataque de Conti, famoso grupo de RaaS que se detectó por primera vez en 2020 y que aparentemente opera desde Rusia. En él se denota la necesidad de una protección eficaz contra el movimiento lateral, así como el papel fundamental que estas protecciones pueden desempeñar en la defensa contra el ransomware. Además, en el informe se descubrió que la gran mayoría de las víctimas de Conti eran empresas con ingresos de entre 10 y 250 millones de dólares.

> **La microsegmentación reduce la confianza implícita en la red, al permitir únicamente la conectividad definida explícitamente por la política, lo que permite aplicar el acceso con privilegios mínimos a todas las aplicaciones para el tráfico de máquina a máquina.**
>
> — **Forrester, Best Practices for Zero Trust Microsegmentation (Mejores prácticas para la microsegmentación Zero Trust), 27 de junio de 2022**

Es una señal clara de que las organizaciones de todos los tamaños están en riesgo debido a la combinación de tecnología obsoleta, estrategias de defensa "suficientemente buenas" centradas solo en los perímetros y los terminales, falta de formación (y protocolos de seguridad deficientes) y ausencia de una solución mágica e infalible. De hecho, según el informe de mercado sobre el ransomware en 2023 de Cybersecurity Ventures: "Se prevé que para 2031 el ransomware ataque a una empresa, un consumidor o un dispositivo cada dos segundos".

Depende del movimiento lateral

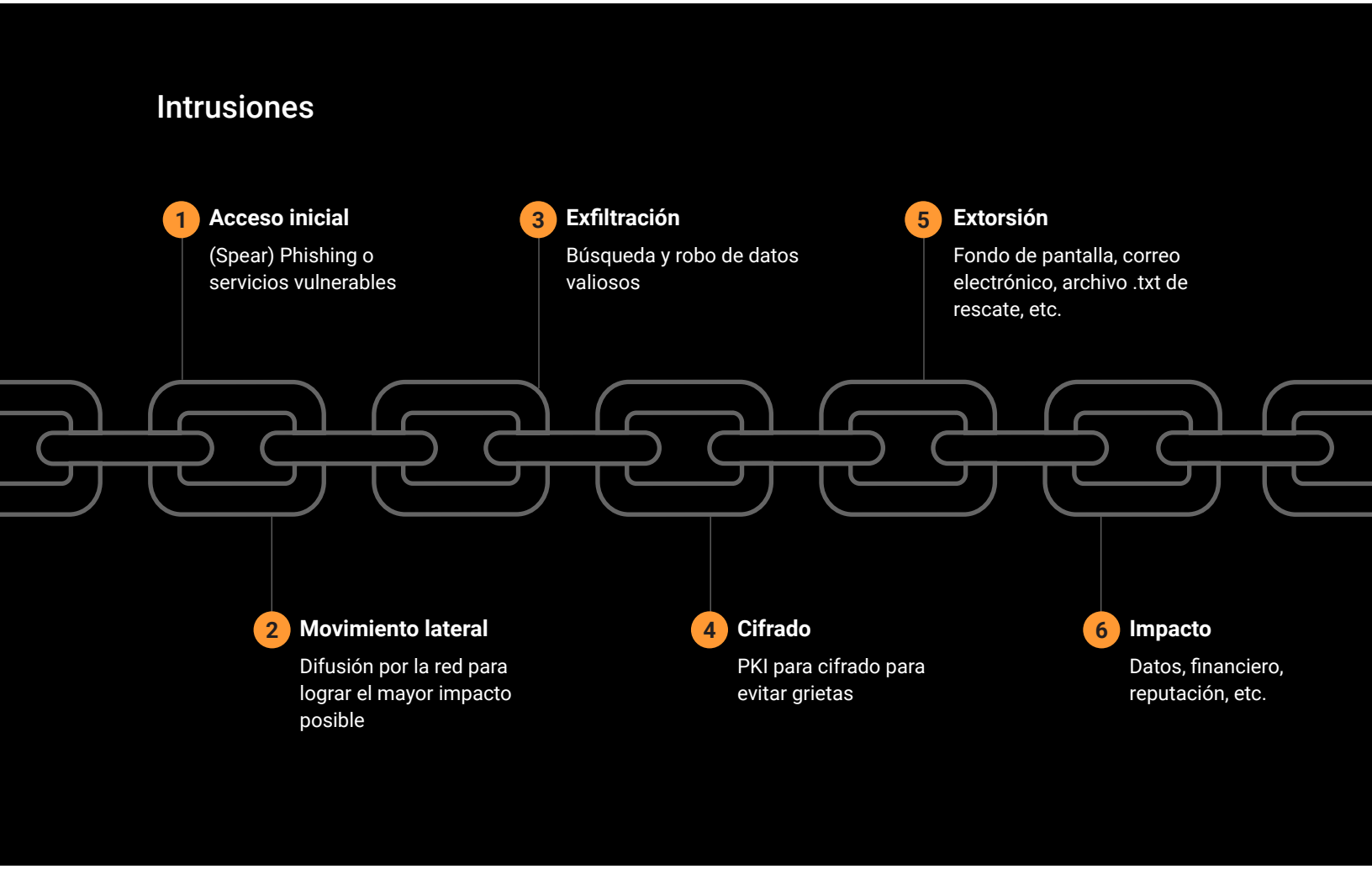
Un ataque de ransomware comienza con una filtración inicial. A menudo, esta se produce a través de un correo electrónico de phishing, una vulnerabilidad en el perímetro de la red o un ataque de fuerza bruta que abre fisuras en las defensas y distraen de la intención real del atacante. Una vez que el malware ha hecho mella en un dispositivo o aplicación, avanza mediante la derivación de privilegios y movimientos laterales a través de la red y por diferentes terminales para extender la infección y multiplicar los puntos de cifrado. Por lo general, los ciberdelincuentes se hacen con el control de un controlador de dominio, obtienen las credenciales y, a continuación, buscan y cifran la copia de seguridad para impedir que el operador pueda restaurar los servicios congelados.

El movimiento lateral es fundamental para el éxito de un ataque. Si el malware no se puede propagar más allá de su punto de entrada inicial, no es útil. Por lo tanto, evitar el movimiento lateral es clave. Las funciones de visibilidad y segmentación de una solución como Akamai Guardicore Segmentation le permiten configurar rápidamente políticas que previenen y contienen una filtración inicial. También recibirá una alerta sobre movimientos laterales y otros comportamientos sospechosos, que sirve de ayuda para detectar rápidamente el malware y así poder reaccionar de inmediato.

Parte 1: Neutralización de las intrusiones: mitigación y prevención de riesgos

El ransomware no se propaga con el ataque a un solo equipo o dispositivo. Los ciberdelincuentes utilizan el ransomware para cifrar el mayor número posible de sistemas de una red y asegurarse el pago de un rescate.

Dado que el ransomware es un ataque polifacético, la implementación de varias capas de defensa puede servir para evitar daños generalizados, la pérdida de datos y el tiempo de inactividad. La primera capa de defensa sirve para prevenir la infección inicial de ransomware.



Prevención de la infección inicial

Los primeros puntos vulnerables de cualquier red son los puntos de contacto con Internet. Aunque muchos ataques de ransomware se apoyan en el spear-phishing, no hay nada que les impida infiltrarse en los servicios expuestos a Internet.

Las funciones de visibilidad de Akamai Guardicore Segmentation le permiten supervisar los servicios expuestos a Internet y limitar su exposición mediante políticas para:

- Servicios de acceso remoto (RDP, SSH, TeamViewer, AnyDesk, VPN)
- Servicios potencialmente vulnerables (Apache, IIS, Nginx)
- Equipos potencialmente vulnerables (detecte los equipos cuyo sistema operativo no esté actualizado con la función Insight adicional)
- Servicios expuestos no deseados (bases de datos, controladores de dominio, servidores de web interna o de archivos)

Neutralización de las intrusiones gracias a la segmentación

Es inevitable que una red sufra una filtración en algún momento. Podría deberse al spear-phishing, un error humano o un servidor que ejecuta servicios vulnerables y cuyos riesgos no se han mitigado correctamente. Por eso es fundamental contar con estrategias de mitigación de riesgos adecuadas.

Cuando un equipo sufre una filtración, es necesario evitar que se propague por la red. Se puede hacer de tres formas:

1. Segmentación por acordonamiento de aplicaciones

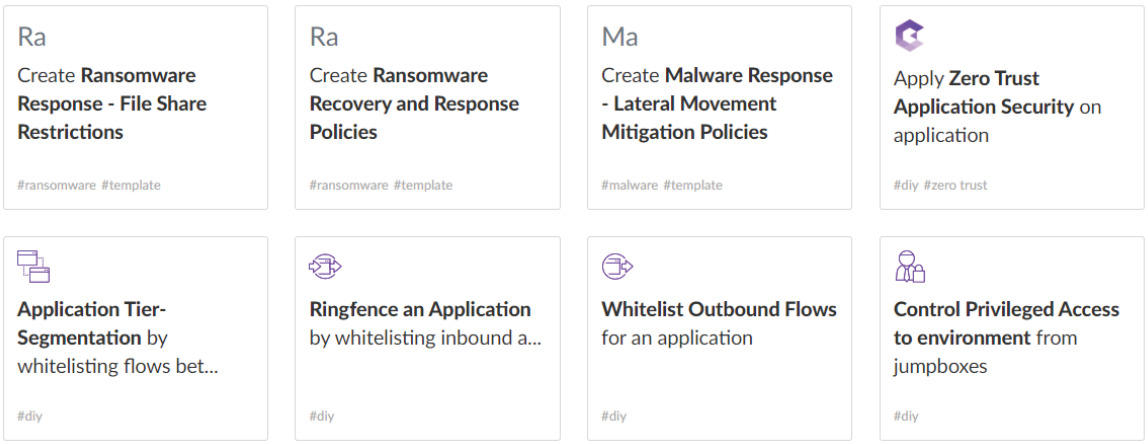
Para dividir la red en segmentos operativos (por aplicación, uso o entorno) y no permitir conexiones innecesarias entre segmentos ni dentro de estos.

Estas son cuatro pautas de segmentación que se deben tener en cuenta:

- Bloquear la comunicación entre portátiles o estaciones de trabajo.
- Bloquear la comunicación de los procesos que se ejecutan con privilegios de usuario de dominio "potentes" como, por ejemplo, administradores de dominio.
- Limitar el número de usuarios que pueden ejecutar procesos en los servidores.
- Limitar el acceso desde portátiles y estaciones de trabajo a servidores de centros de datos e instancias en la nube.

Akamai Guardicore Segmentation facilita la protección de la red contra el ransomware. Con las plantillas predefinidas, puede mitigar los ataques mediante la configuración de políticas en tres sencillos pasos:

1. **Seleccione su objetivo**, como delimitar una aplicación crítica, crear políticas de mitigación del ransomware o proteger un directorio activo.
2. **Identifique los activos relevantes que desea proteger** de la propagación del ransomware, como los activos de una aplicación de e-commerce que quiera delimitar, todas las cargas de trabajo de Active Directory en el centro de datos o los terminales. Normalmente, este paso se completa automáticamente gracias al etiquetado con inteligencia artificial (IA) de Akamai.
3. **Proteja los activos mediante la creación de políticas**. La IA de Akamai Guardicore Segmentation sugiere y recomienda automáticamente políticas basadas en el tráfico real del entorno y asimila los patrones de comunicación de las aplicaciones de cientos de redes.

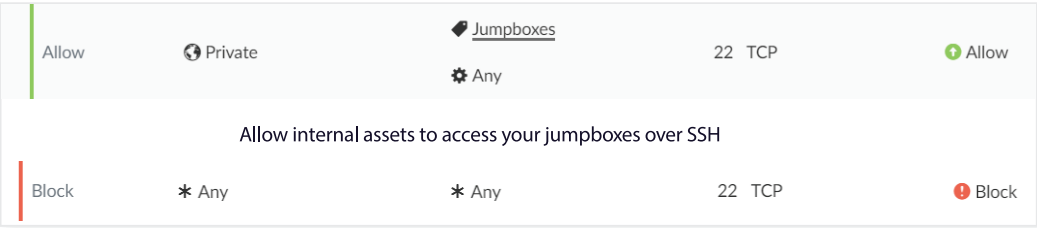


Ejemplo: Plantillas de Akamai Guardicore Segmentation

2. Prevención del movimiento lateral mediante reglas de restricción de protocolos

Existen normas generales para los protocolos y comportamientos específicos. Hay que tener cuidado a la hora de restringir algunos protocolos, ya que se utilizan de forma habitual en las operaciones cotidianas. Akamai Guardicore Segmentation elabora una visualización de todo el tráfico para crear las reglas más apropiadas para su entorno según protocolos de alto riesgo, como WinRM, SMB, RPC, RDP o SSH, entre otros.

Por ejemplo, aunque SSH es útil para la administración remota y sirve para proteger otros protocolos (como SFTP), es una herramienta que utilizan los atacantes para penetrar en los equipos y propagarse por la red. Deberá restringir todo lo posible SSH en la red mediante la creación de soluciones de salto para usuarios autorizados.



Reglas creadas en Akamai Guardicore Segmentation

3. Protección de copias de seguridad y servicios de datos críticos

Para maximizar los daños, los ataques de ransomware suelen dirigirse a los servidores de copia de seguridad de las organizaciones para cifrar los datos almacenados. De manera similar, los servicios de datos y los servidores de archivos también son objetivos del ransomware.

Utilice Akamai Guardicore Segmentation para limitar el acceso a sus servidores de copia de seguridad, bases de datos y servidores de archivos, así como para limitar el acceso desde fuera de la red y desde las regiones de su propia red que no necesitan acceso. Para minimizar la comunicación con los servidores de copia de seguridad críticos, puede utilizar Akamai Guardicore Segmentation para delimitar aplicaciones del sistema, además de bloquear la comunicación con una aplicación hasta los niveles de proceso y de usuario. Limitar la exposición de los servicios de datos al mínimo operativo reducirá el factor de riesgo y mitigará la exposición al ransomware y a las rutas de propagación.

Parte 2: Detección de ransomware y respuesta

A la hora de lidiar con ciberamenazas, como el ransomware, la previsión y la vigilancia son fundamentales. Reaccionar a tiempo ante una filtración puede minimizar el daño a la red. Las funcionalidades de Akamai Guardicore Segmentation pueden ayudarle tanto en la detección de amenazas como en la respuesta ante estas.

Detección de amenazas con Akamai Guardicore Segmentation

Entre las incidencias encontramos:

- **Engaño**: que detecta e intercepta intentos de movimientos laterales sospechosos y los redirige a señuelos dinámicos para que se puedan supervisar y analizar sus acciones. Las incidencias de engaño son muy fiables y proporcionan información detallada sobre las actividades malintencionadas y la siguiente fase de ataque de los ciberdelincuentes.
- **Análisis de red**: los ciberdelincuentes recopilan información una vez que están dentro de una red. Utilizan análisis de red como método de reconocimiento para detectar puertos o servicios abiertos por los que otros servidores están esperando. Akamai Guardicore Segmentation detecta automáticamente los análisis de red y alerta a los usuarios de inmediato.
- **Detección basada en políticas**: las políticas de seguridad en niveles de red y de procesos permiten reconocer de forma instantánea comunicaciones no autorizadas y tráfico que incumple los estándares.

Akamai Guardicore Segmentation presenta la función Insight

Akamai Guardicore Segmentation facilita la consulta de los activos individuales aprovechando una función adicional basada en osquery. El marco de consulta que ofrece permite detectar rápidamente actividades anómalas, como las instantáneas de volumen, la acción previa al cifrado más común del ransomware. También detecta troyanos utilizados para distribuir el ransomware al reconocer una técnica de camuflaje común que oculta malware en el archivo svchost.exe, un proceso legítimo de Windows.

Búsqueda gestionada de amenazas

El servicio gestionado de búsqueda de amenazas de Akamai alerta a los usuarios de cualquier comportamiento anómalo en la red. Se utilizan técnicas como el análisis de conexiones entrantes y salientes de Internet y sus GeoIP asociadas, la búsqueda de nuevos ejecutables que tengan una presencia creciente en la red (lo que puede indicar que se está produciendo una propagación) y el análisis de conexiones de activos para encontrar indicios de movimientos laterales a través de anomalías en el recuento de los pares.

Respuesta inmediata

Una vez que se haya detectado una amenaza en la red, como el ransomware, puede implementar cuanto antes medidas de mitigación. Para ello, deberá aplicar políticas en los niveles de proceso y de usuario a fin de bloquear o aislar las actividades malintencionadas.

Visibilidad incremental de las infecciones

Con su pista o indicador de riesgo (IOC) inicial, puede empezar a buscar indicadores adicionales, como patrones de comunicación, procesos, puertos utilizados o activos infectados, entre otros. Akamai Guardicore Segmentation puede ayudarle a encontrar todos los activos con este indicador (todos los activos que se comunican con C2, que se comunican con un puerto único o que ejecutan un proceso malicioso). Además, con un mapa visual de su entorno, puede buscar similitudes con otros equipos infectados o rastros de una propagación.

Parte 3: Desinfección y recuperación

Cuando tenga una lista de todos los equipos infectados y de todos los IoC, puede comenzar la desinfección. Divida los equipos en tres grupos con las siguientes etiquetas: **aislado**, **monitorizado** y **limpio**.

Aislado

- Contiene activos **infectados** por el malware.
- Mantenga estos activos **en cuarentena** hasta que se haya eliminado el malware.

Monitorizado

- Contiene activos que pueden **estar infectados** o no.
- **Supervise** estos activos hasta que se haya asegurado de que el malware se ha **eliminado**.

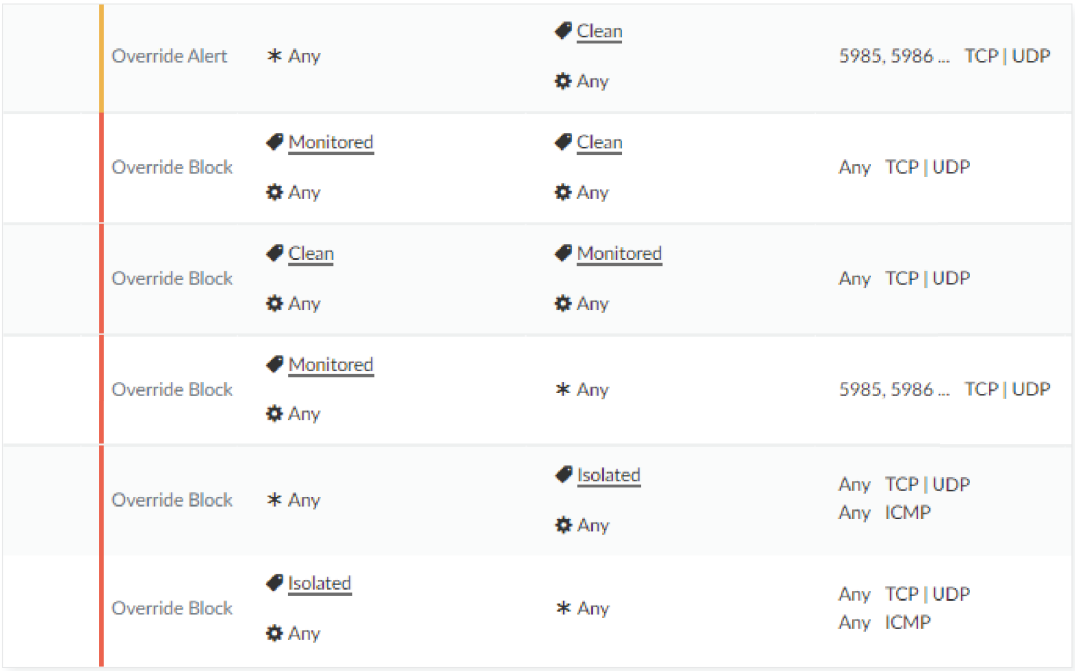
Limpio

- Contiene activos que se ha confirmado que **no están infectados** y que pueden **funcionar con normalidad**.

Directrices de segmentación para la recuperación

Después de definir los tres grupos, puede empezar a agregar políticas para segmentar la red creando cuatro niveles de comunicación:

- **Bloquear** todas las comunicaciones entrantes y salientes con los equipos **aislados**.
- **Bloquear** la comunicación del protocolo de administración remota con los equipos **monitorizados**.
- **Alertar** sobre la comunicación del protocolo de administración remota con los equipos **limpios**.
- **Bloquear** todas las comunicaciones entre los tres grupos.

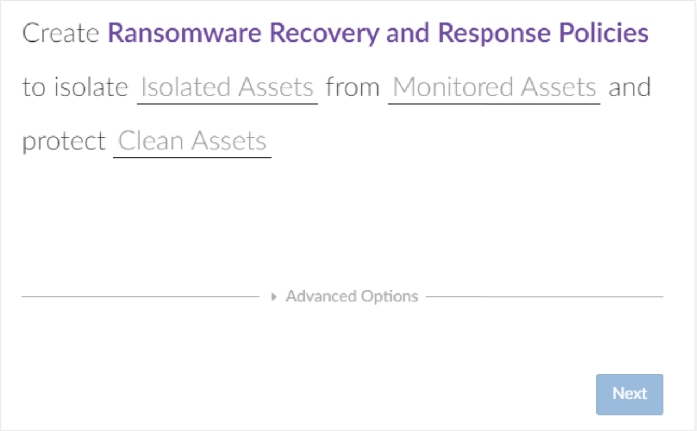


Reglas de bloqueo y alertas de Akamai Guardicore Segmentation

Plantilla de recuperación y respuesta ante el ransomware

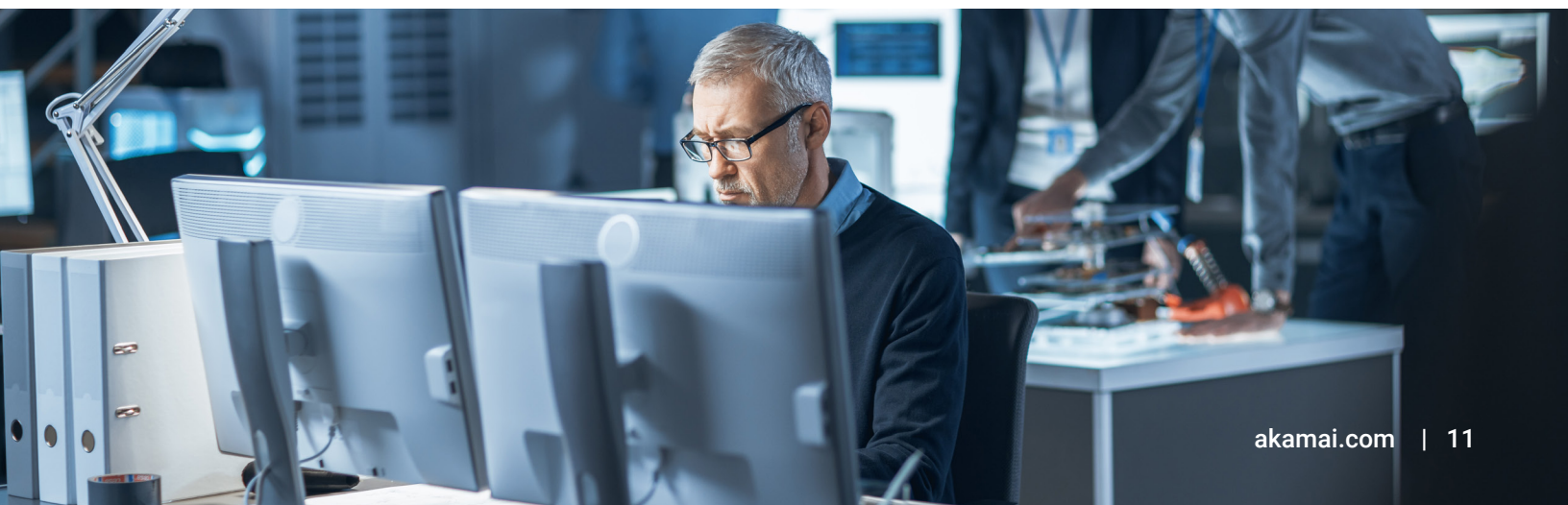
La plantilla de políticas de recuperación y respuesta ante el ransomware incluida en Akamai Guardicore Segmentation proporciona una política prediseñada y fácil de usar para restringir el acceso a los grupos de recursos con las etiquetas **Aislado, Monitorizado** y **Limpio**.

Esta plantilla le permitirá mantener fácilmente la continuidad operativa de los equipos **limpios** sin tener que preocuparse por la (re)infección de los equipos **aislados**.



Conclusión

Si confía en los firewalls heredados o en la defensa exclusivamente perimetral, no podrá evitar que el ransomware se extienda por su red y bloquee las aplicaciones e infraestructuras fundamentales. La realidad es que las filtraciones son inevitables y debe estar preparado. Akamai Guardicore Segmentation puede ayudarle a detectar amenazas en el tráfico este-oeste del centro de datos y bloquear el movimiento lateral del que depende el ransomware para cifrar y pedir tomar como rehén sus activos más importantes.



Cinco pasos para mitigar el impacto de un ataque de ransomware con Akamai Guardicore Segmentation

Preparación mediante la identificación de todas las aplicaciones y activos que se ejecutan en su entorno de TI.

Prevención mediante la creación de reglas para bloquear las técnicas más comunes de propagación de ransomware.

Detección mediante la recepción de alertas sobre cualquier intento de obtener acceso a las aplicaciones segmentadas y las copias de seguridad.

Corrección mediante la activación de medidas de cuarentena y contención de amenazas cuando se detecta un ataque.

Recuperación mediante capacidades de visualización con estrategias de recuperación por fases.

Detenga el movimiento lateral del ransomware en su red. ¿No nos cree? Compruébelo personalmente. akamai.com/guardicore

Akamai protege la experiencia de sus clientes, su personal, sus sistemas y sus datos, ayudándole a integrar la seguridad en todo lo que crea, dondequiera que lo cree o distribuya. La visibilidad de las amenazas globales que ofrece nuestra plataforma nos permite adaptar y desarrollar su estrategia de seguridad para integrar el enfoque Zero Trust, detener el ransomware, proteger las aplicaciones y las API o combatir los ataques DDoS, y le proporciona la confianza necesaria para innovar, crecer y transformar todo su entorno. Para obtener más información acerca de las soluciones de seguridad, informática y distribución de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en Twitter y LinkedIn. Publicado en mayo de 2023.