CÓMO PROTEGER SU EMPRESA - RÁPIDO - CON UNISYS DYNAMIC ISOLATION™

CÓMO PROTEGER SU EMPRESA - RÁPIDO - CON UNISYS DYNAMIC ISOLATION™

Aislamiento rápido limita el alcance

Introducción

Históricamente, las organizaciones se han centrado en defender perímetros fijos alrededor de sus operaciones. Sin embargo, este enfoque no funciona en el mundo digital actual porque los entornos empresariales son dinámicos y cambian rápidamente.

Los dispositivos conectados están en todas partes, y su adopción continúa creciendo.[1] Los asociados empresariales ya no solo usan una computadora portátil dentro de los muros de la empresa. En la era de Internet de las cosas (IoT), los asociados están utilizando múltiples puntos finales para conectarse con los recursos de la empresa de varias fuentes en todo el mundo. Y esos activos se mueven constantemente dentro y fuera de la empresa para hacer el trabajo. Eso hace que los perímetros sean más difíciles de definir, cada vez más porosos e imposibles de asegurar con el enfoque fijo anterior.

Durante esta evolución, los ciberdelincuentes también han evolucionado, volviéndose más sofisticados en sus ataques con cada día que pasa. Y a menudo los atacantes ya están al acecho en entornos empresariales, escuchando, observando y decidiendo dónde atacar a continuación.

Abordar las amenazas existentes es fundamental porque, sin su conocimiento, es probable que su empresa ya se haya visto comprometida.

Por lo tanto, es fundamental que las empresas actúen rápidamente para contener las amenazas. Eso es importante porque una vez que los ciberdelincuentes toman el control de un solo dispositivo, pueden expandir rápidamente el alcance de su ataque para comprometer otros activos. El aislamiento rápido limita el alcance de la destrucción.

Las organizaciones no pueden asumir que se puede confiar en cualquier conexión entre elementos dentro de la empresa. Deben ver sus entornos como si estos ya estuvieran comprometidos. Y necesitan las herramientas y procesos adecuados para contener esas amenazas de manera rápida y efectiva.

En este artículo, haremos lo siguiente:

- Discutir cómo el aislamiento dinámico permite a las organizaciones contener amenazas nuevas y existentes
- Aclarar cómo este enfoque es diferente y mejor que la cuarentena
- Explicar cómo el aislamiento dinámico es parte de una postura de Zero Trust, que todas las empresas deberían adoptar para abordar las amenazas de ciberseguridad de hoy

El aislamiento dinámico permite a las empresas actuar rápidamente

El aislamiento dinámico es único en comparación con otras tecnologías de ciberseguridad existentes, como la cuarentena, en lo que respecta a la operatividad y la recuperación. Dispositivos en cuarentena están fuera de servicio hasta que sean recuperados. Pero con un aislamiento dinámico, el equipo forense, el equipo de operaciones y algunos servicios críticos que son esenciales para la operación, mantienen el acceso y la operatividad.

Por lo tanto, el poder del aislamiento dinámico es tanto el aislamiento rápido como el control quirúrgico que el equipo de seguridad obtiene del punto final con una configuración mínima. El aislamiento dinámico hace un aislamiento rápido y una rápida liberación. Permite a las empresas eliminar un dispositivo (o 10.000 dispositivos, si es necesario) de la red a velocidad de malware y recuperarlo con la misma rapidez, con un solo clic o de forma completamente automática.

Otras soluciones de ciberseguridad se centran en la detección y prevención e inundan a los equipos de TI con alertas. Pero la mayoría de estas ofertas no brindan a los profesionales de TI una forma rápida y fácil de responder a esas alertas y abordar las amenazas de ciberseguridad. Eso significa que los miembros del equipo de TI tienen que invertir mucho tiempo valioso
planificando cómo responder. Mientras tanto, los hackers usan ese tiempo para expandir su alcance y el alcance de la destrucción.

1. Se espera que el crecimiento en dispositivos IoT conectados genere 79.4ZB de datos en 2025, IDC, 18 de junio de 2019

La mayoría de las soluciones son demasiado lentas para hacer frente a eventos catastróficos de seguridad cibernética. El Instituto Ponemon dice que el tiempo medio para detectar una brecha es de 197 días. Responder a una brecha típicamente toma otros 69 días.

Unisys Dynamic Isolation es diferente. Actúa a la velocidad del malware.

El aislamiento dinámico es diferente. Permite a las empresas actuar en eventos de seguridad cibernética a velocidad de malware. Unisys Dynamic Isolation™ permite a las organizaciones responder a las amenazas de ciberseguridad aplicando políticas de seguridad rápidamente, mucho más rápido que las soluciones actuales. Es mucho más rápido que el tiempo promedio de respuesta de 69 días que las empresas enfrentan al usar otras tecnologías y procesos.[2]

Cómo funciona el aislamiento dinámico

Unisys Dynamic Isolation es una solución modular que proporciona un conjunto flexible de API estándar, denominadas API de ecosistema (o ecoAPI), para integrarse con las soluciones de seguridad existentes de las empresas. El aislamiento dinámico de Unisys utiliza agentes en los puntos finales para mediar en cada conexión. Estas conexiones están preautorizadas, pre autenticadas y encriptadas sin problemas. Esto, a su vez, crea una superposición segura en cada red.

Esa superposición controla, reduce o elimina las rutas de acceso entre las cargas de trabajo, reduciendo efectivamente la superficie de ataque. Y no requiere que los equipos de TI pierdan un tiempo precioso reconfigurando la red y obteniendo acceso físico al dispositivo.

Esta respuesta dinámica se basa en el contexto empresarial, la postura de seguridad, el nivel de amenaza, el usuario y la carga de trabajo. Permite a las empresas responder rápidamente para disminuir el tiempo medio para responder a las amenazas y reducir la superficie y la velocidad de los ataques. Si un punto final se ha visto comprometido, Unisys Dynamic Isolation puede crear un enclave seguro alrededor de ese dispositivo automáticamente. Este enclave seguro aún proporciona acceso a herramientas y equipos forenses para permitir el análisis, la respuesta a incidentes y la solución. Por lo tanto, Unisys Dynamic Isolation se puede integrar fácilmente en el libro de tácticas del equipo de respuesta a incidentes (automático o manual).

La característica de aislamiento dinámico de Unisys Stealth® permite a las organizaciones establecer roles de aislamiento global personalizados para sus propios entornos. Esas organizaciones pueden usar las API Stealth™ para mover automáticamente los puntos finales Stealth hacia o desde un rol de aislamiento global predefinido. La API Stealth Ecosystem se utiliza para crear una configuración global y roles de aislamiento global. Y la entidad a aislar se puede identificar mediante la ID de máquina del punto final o la ID de usuario utilizada por Stealth para autorizar el punto final. Los roles de aislamiento se utilizan para definir el entorno de red restringido con el que se permite operar un punto final aislado.

El aislamiento dinámico de Unisys define múltiples roles de aislamiento que pueden configurarse y modificarse globalmente. Eso simplifica las operaciones porque las empresas no tienen que escribir una regla para cada dirección IP. La función de aislamiento sirve como un modelo de política de seguridad, que define reglas generales como lo que está permitido en qué puertos. Stealth luego asigna estas reglas dinámicamente en función de la identidad del usuario definida en Active Directory o un sistema de administración de identidad similar.

Para proporcionar a las empresas una velocidad y eficiencia óptimas, Unisys Dynamic Isolation puede funcionar de forma totalmente automatizada. Las empresas también pueden optar por el control manual de Unisys Dynamic Isolation para que los equipos de TI puedan recibir y evaluar recomendaciones en su consola de administración de seguridad preferida para aprobar e iniciar el aislamiento inmediato.

[2] Encuesta revela que el descubrimiento de una brecha lleva un promedio de 197 días, Security Boulevard, 18 de julio de 2018

Por qué el aislamiento dinámico es diferente y mejor que la cuarentena

Parte de las ventajas de Unisys Dynamic Isolation es que permite que los puntos finales, y, por lo tanto, las personas y los sistemas, continúen funcionando incluso cuando están en modo de aislamiento. Eso es muy diferente a la cuarentena, que elimina completamente - o aisla - puntos finales comprometidos y vulnerables. Esta solución de Unisys también permite a los equipos de respuesta a incidentes de seguridad y operaciones acceder de forma segura al punto final y remediar el incidente de forma remota.

Como resultado, las empresas que emplean el Unisys Dynamic Isolation no sufren la disminución de la productividad y la pérdida de ingresos que ocurren comúnmente durante los esfuerzos de respuesta a eventos de seguridad cibernética. Y los socios comerciales no tienen que pasar por la frustración de permanecer inactivos mientras esperan que se restablezca el servicio en sus computadoras problemáticas u otros puntos finales.

Unisys Dynamic Isolation solo aísla el puerto o protocolo que exhibe un comportamiento anómalo, dejando el resto del sistema funcionando. Como resultado, si el servidor admitía un sistema de pago de fondo, por ejemplo, el negocio podría continuar aceptando transacciones de ventas.

Un ejemplo de aislamiento dinámico en el trabajo

Los entornos de oficina y de comercio minorista son solo un par de ejemplos de dónde Unisys Dynamic Isolation puede entrar en juego para ayudar a las empresas a moverse rápidamente para abordar las brechas y tomar medidas rápidas para contener y controlar los eventos de ciberseguridad.

La industria de la salud es otro ejemplo de cómo el aislamiento dinámico puede ayudar a abordar los puntos débiles de TI de la empresa.

Imagine una enfermera del hospital que usa múltiples escritorios y puede acceder a su cuenta de correo electrónico desde cada una de estas máquinas. Durante un turno tardío, la enfermera recibe un correo electrónico, que parece haberse originado en el departamento de TI, pidiéndole que instale una actualización de seguridad crítica.

La enfermera abre el archivo adjunto e instala lo que cree que es una actualización de seguridad. Pero el archivo adjunto es en realidad WannaCry.[3]

Una vez que la computadora portátil de la enfermera está infectada, WannaCry lanza un servicio que escanea la red local e Internet en busca de máquinas accesibles con puertos expuestos. Todas estas actividades suceden muy rápidamente y el ataque puede penetrar todos los dispositivos en una LAN típica en cuestión de minutos.

Después del primer escaneo de la red, un signo revelador de comportamiento anómalo, el aislamiento dinámico aísla la máquina y la cuenta de correo electrónico, evitando que el malware se propague. Y si la enfermera intenta acceder a otra computadora para ejecutar el mismo archivo adjunto, el aislamiento dinámico aísla las cuentas de la enfermera, o limita su acceso a un puerto específico o servicios particulares, en cada punto final en el que puede iniciar sesión.

Unisys Dynamic Isolation permite que los puntos finales - y, por lo tanto, las personas y los sistemas - sigan funcionando incluso cuando están en modo

[3] ¿Qué es WannaCry Ransomware, cómo infecta y quién fue responsable?, OSC, 30 de agosto de 2018

Unisys Dynamic Isolation también puede bloquear el puerto en todo el entorno hasta que se libere y se implemente una solución de seguridad. En ese punto, el aislamiento dinámico restaura la funcionalidad completa de la cuenta y la computadora portátil.

Cómo el aislamiento dinámico admite una postura de ciberseguridad de Zero Trust

Unisys Dynamic Isolation es un gran ejemplo de Zero Trust en el trabajo.

Zero Trust es una postura de seguridad cibernética que las empresas inteligentes están adoptando para proteger sus activos críticos donde sea que se encuentren. Las empresas que adoptan Zero Trust nunca asumen que pueden confiar en cualquier aplicación, dispositivo, paquete o usuario. Y actúan en consecuencia al establecer microperímetros que compartimentan diferentes segmentos de red, protegen la propiedad intelectual y otros datos confidenciales de aplicaciones y usuarios no autorizados y reducen la exposición de sistemas críticos o vulnerables al prevenir ataques laterales.

La arquitectura Zero Trust otorga acceso solo a dispositivos y usuarios que han sido debidamente autenticados y autorizados. Y emplea una superposición de cifrado para permitir conexiones solo entre puntos finales que han pasado por ese proceso de verificación.

Construyendo un modelo Zero Trust en la nube

Zero Trust define primero la superficie que necesita protección. Entiende los gateways, hosts, red y los servidores y el valor de los datos. Y sabe dónde se almacenan los datos y asigna flujos de datos.

Se alienta a las empresas que adoptan la arquitectura Zero Trust a hacer que las zonas protegidas y las políticas de seguridad relacionadas con ellas sean lo más detalladas posible para reducir la superficie de ataque a la red tanto como sea posible. Estas empresas crean sus políticas de seguridad basadas en patrones de comportamiento, políticas configurables, estado del dispositivo, geolocalización y controles basados en el tiempo, membresía de grupo, granularidad de reglas y tiempo para otorgar y denegar el acceso.

Con una arquitectura Zero Trust, las empresas obtienen la inteligencia sobre el tráfico y los patrones de usuario que necesitan para anticipar posibles problemas y actuar rápidamente sobre los eventos de seguridad cibernética.

Conclusión

La acción rápida es de suma importancia en el entorno de TI empresarial actual, en el que los ciberdelincuentes se mueven rápidamente para comprender y atacar los entornos de TI y los medios de vida de las empresas.

Cuanto más tiempo les tome a las empresas identificar y mitigar los eventos de seguridad cibernética, más tiempo tendrán los hackers para crear estragos y ampliar el alcance de la destrucción.

Claramente, las empresas están bajo ataque, y están en una carrera contra el tiempo. La mayoría de las herramientas y procesos de ciberseguridad actuales no abordan adecuadamente la necesidad de Zero Trust, visibilidad completa, acción rápida y continuidad empresarial. Unisys Dynamic Isolation es la excepción.

Con Unisys Dynamic Isolation, un servicio de extremo a extremo impulsado por Stealth, las empresas pueden responder a eventos de ciberseguridad y aplicar políticas de seguridad a la velocidad del malware.

Esto es importante, porque cuando se trata de abordar las amenazas de ciberseguridad, el tiempo es esencial. Y para las empresas que trabajan para proteger sus entornos de TI para que puedan mantener el negocio en movimiento, el tiempo es dinero

Por primera vez, el Unisys Dynamic Isolation permite a las empresas abordar tanto el imperativo de seguridad de neutralizar las amenazas como el imperativo empresarial de mantener el negocio en movimiento.

Por primera vez, el Unisys Dynamic Isolation permite a las empresas abordar tanto el imperativo de seguridad de neutralizar las amenazas como el imperativo empresarial de mantener las operaciones en movimiento.

Para obtener más información sobre cómo su organización puede beneficiarse de una ciberseguridad más rápida y dinámica utilizando el Unisys Dynamic Isolation, visite www.unisys.com/security.

Para más información visite www.unisys.com

12/19

19-0746