iboss™
CYBERSECURITY

Seguridad de la nube bajo sus términos

ENTENDIENDO LA ARQUITECTURA DE CONTENEDORES DE NODO

Seguridad de la nube bajo sus términos

ENTENDIENDO LA ARQUITECTURA DE CONTENEDORES DE NODO

La nube ya no es una novedad. La mayoría de las compañías tienen al menos un porcentaje de su ambiente de cómputo funcionando en nube, sea de manera pública, privada o híbrida. A pesar del aumento en las inquietudes relacionadas con la seguridad y la conformidad, los beneficios en cuanto a costos y escalabilidad son genuinamente convincentes para ignorarlos.

Antes, era mucho más sencillo el monitoreo del acceso a las aplicaciones fundamentales para los negocios como la nómina, servicio a clientes y bancos de datos. Los servicios eran locales, por lo que la prevención contra pérdida de datos a base de firmas era un acercamiento viable.

No obstante, la actualidad de las empresas se encuentra frente a mayores retos en cuanto al monitoreo del acceso a sus activos. Algunos factores que hacen cada vez más compleja la gestión de saber qué es lo que está haciendo una persona y cuándo son las aplicaciones que mandan solicitudes de servicio directamente a la nube, el crecimiento de las organizaciones distribuidas y los usuarios móviles, así como las comunicaciones codificadas entre los usuarios y sistemas.

Una violación, demasiadas víctimas

Muchas nubes funcionan mediante máquinas virtuales (VM, por sus siglas en inglés). Una VM es un ambiente de software que contiene un sistema operativo y aplicaciones. Se pueden instalar múltiples VM en un mismo servidor, permitiendo que el mismo corra muchos sistemas auto-contenidos de manera simultánea; cada uno de ellos comportándose como un servidor dedicado. De esta manera es como se comparten los recursos en la mayoría de las nubes.

La organización del uso de los recursos es un tipo de software conocido como hipervisor o monitor de máquina virtual. Un hipervisor controla el procesador de un host, acomodando los recursos a cada VM según sea necesario y previniendo que una VM afecte la operación de otra.

Las complejidades generan vulnerabilidades

Las nubes son blancos valiosos para los hackers debido a que un atacante que logra ingresar a un hipervisor potencialmente cuenta con acceso a las VM y los datos (de cada cliente de la nube).

Si una nube se logra penetrar debido a una clave de acceso débil de un cliente o un PHP mal escrito, es posible que los clientes con mayor seguridad puedan recibir ataques a través del hipervisor, que se convierte en una dirección inesperada (y por lo tanto, desprotegida) para la generación de un ataque.

Los hipervisores son vulnerables porque cuentan con superficies grandes de ataque con muchos puntos de acceso. También, están formados a partir de código complejo que es difícil de diseñar, evaluar y gestionar por el simple hecho de que existe demasiado. A pesar de estos problemas, aún no existen mejores prácticas para gestionar la seguridad de los hipervisores.

Los clientes de la nube no cuentan con el control ni el conocimiento de las otras compañías que comparten su hipervisor; una compañía que se encuentra manejando datos altamente sensibles podría encontrarse en el mismo ambiente virtual que un desarrollador novato que se encuentre programando servidores con grandes vacíos de seguridad. Una simple violación puede tener como resultado la pérdida de datos, de propiedad intelectual y secretos de la industria de todas las compañías que compartan la nube. Por lo tanto, las VM que se encuentren funcionando bajo el mismo hipervisor cuentan con el mismo grado de seguridad que el vecino menos seguro.

VULNERABILIDADES DE LOS HIPERVISORES

- **Escape de VM:** Un atacante ejecuta código que permite que se escape un sistema operativo funcionando en la VM e interactúe de manera directa con el hipervisor.
- **Deficiencias en parches:** La virtualización sucede en dispositivos de red así como en servidores, generando una gran superficie que hay que parchar cada que emerge una nueva explotación.
- **Vulnerabilidades de la SSL Abierta:** Si el servidor OpenSSL comparte un hipervisor con otros clientes en la misma nube, los ataques podrían permitir que se inyecten los datos en otras sesiones o permitan la negación de los ataques de servicio.
- **Vulnerabilidades APT:** Los ataques por malware tipo *RAM scraping* pueden permitir a los atacantes ver los estados del CPU.

Proxy compartido, problemas compartidos

La mayoría de los proveedores de nube escanean los datos de los clientes a través de un proxy compartido en la misma. El proxy funciona como intermediario entre las partes fuera de la nube y las aplicaciones dentro de la nube. Debido a que un proxy en riesgo puede tender un puente entre la red de un cliente y otro, los proxy pueden ser una fuente de riesgo. El uso de proxy también aumenta los periodos de latencia, que implican el tiempo que toma a los datos moverse de un punto a otro. El periodo de latencia aumenta conforme transita más tráfico a través del proxy. En la programación de nube, lo anterior significa que una vez que un cliente experimenta un aumento en tráfico, otros clientes pueden experimentar retrasos en los suyos.

Conteniendo el riesgo en las organizaciones globales

Una arquitectura de nodo en la nube elimina los problemas de escalabilidad y flexibilidad mientras genera una nube mucho más segura. La arquitectura de nodo permite a las organizaciones adoptar la nube pública cuando hace sentido, ya sea para sitios remotos o usuarios móviles; mientras se generan en nubes privadas servidores de otros elementos como bancos de datos confidenciales. Lo anterior permite a las organizaciones llevar a cabo una ejecución tradicional de “aplicación en oficinas centrales” para atender los datos de las oficinas centrales, mientras se atiende de manera simultánea a sus usuarios móviles y oficinas remotas con mayor velocidad y seguridad a través de una nube distribuida de manera geográfica.

Una nube concurrida

Tradicionalmente, la seguridad de red ha funcionado con navegadores enfocándose en los puertos 80 y 443; esta práctica genera puntos ciegos dado que únicamente se observan dos puertos. Hoy en día, la seguridad de red ha evolucionado a seguridad de “Internet” que detecta los protocolos de ataque evasivos que no utilizan puertos de red. Factores como la detección de anomalías en datos, contención y ciber-analíticos avanzados pueden ayudar a identificar una violación, incluso cuando no se hayan activado ninguno de los sensores del perímetro. Lo anterior resulta crítico, pues la mayoría de los datos se roban a unos minutos del ataque, por lo que es fundamental contar con un monitoreo continuo contra infecciones dentro de una red.

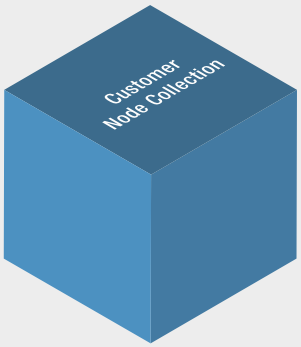
De igual manera, han evolucionado las maneras en las que se ofrece la seguridad de red. Anteriormente, las empresas tenían que escoger entre hardware in situ y seguridad de nube. Algunas organizaciones no contaban con el conocimiento ni los recursos para sentirse lo suficientemente confiados hacia su seguridad in situ; mientras que algunas organizaciones no estaban dispuestas o no podían transferir ningún aspecto de su seguridad a un tercero. Las organizaciones que se mantienen reacias a la nube cuentan con las razones para mantenerse en esa posición. Los proveedores comunes de nube a pares cuentan con un enfoque monolítico hacia su arquitectura. Sus nubes son un gran sistema, por lo que se comparten los sensores que lidian con la seguridad, escalabilidad, tiempos de latencia y requerimientos regionales. Por lo tanto, los datos de los usuarios también son potencialmente compartidos. Una arquitectura monolítica no permite una conciencia de ubicación y, por ende, si no es posible saber si los datos se encuentran en los EE.UU. o la UE, los clientes tienen la preocupación de cumplir con los requerimientos regulatorios de cada país.

Para atender estos problemas, las empresas deben considerar el alejarse de la nube monolítica y acercarse a un enfoque de nodo contenido.

Desempaquetando el contenedor

Contenedor de nube para clientes iboss

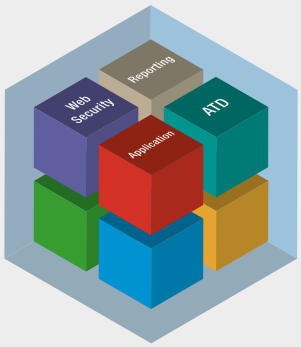
- Construido a partir de módulos individuales que trabajan simultáneamente (i.e., seguridad de red, reportes, ATD)
- Representa toda la funcionalidad de nube iboss para un cliente



CONTENEDOR CONSTRUIDO A PARTIR DE MÓDULOS

1 Contenedor = Múltiples módulos

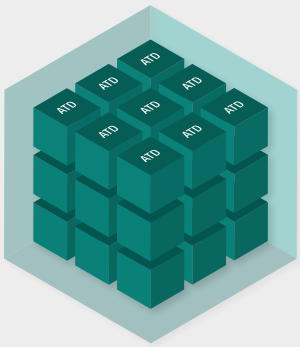
- Los módulos representan un componente (i.e. seguridad de red, reportes, ATD) y en conjunto crean un contenedor de cliente.
- Escalan de manera independiente con base en las demandas, lo cual resulta en una arquitectura de nube mucho más resistente.



MÓDULO CONSTRUIDO A PARTIR DE NODOS DE NUBE

1 Módulo = Múltiples nodos virtuales

- Se genera un cluster de una serie de múltiples nodos que llevan a cabo las mismas funciones.
- Cada nodo es una instancia virtual (VM) y puede generarse o destruirse en cuestión de segundos a través de la tela del nodo.



NODOS

Los nodos son los bloques de construcción del Contenedor de Nube de iboss. Cada nodo desempeña funciones de módulo específicas, tales como:

- Seguridad de red
- Defensa avanzada contra amenazas
- Sandboxing por comportamiento
- DLP por comportamiento
- Reportes y Registros

Se genera un cluster de múltiples nodos de nube que llevan a cabo las mismas funciones. Por ejemplo, un cluster puede estar compuesto por una colección de nodos para la Defensa contra Amenazas Avanzadas o una colección de nodos de Seguridad de Red; pero no estará compuesto de una mezcla de los dos. Cualquier nodo puede eliminarse de un módulo dado que sus funciones se replican en los nodos que se mantienen. El riesgo por pérdida de datos se minimiza gracias a que los nodos aíslan completamente las bases de datos de los clientes.

Los nodos de nube se ubican globalmente en la Nube iboss, cerca de los usuarios móviles y sitios remotos que demandan sus servicios. Los nodos de nube son virtuales por lo que pueden crearse y destruirse en segundos para entregar el nivel correcto de capacidad, redundancia y disponibilidad conforme se cargan los usuarios y cambian los conteos de clientes.

Incluso las organizaciones reacias a la nube pueden obtener beneficios a partir de los nodos para gestionar mejor a sus usuarios móviles y sitios remotos logrando evitar las dificultades de retroalimentar los datos. Los nodos de la Nube iboss pueden hostearse in situ, permitiendo a os clientes desempeñar cualquier función de la Nube iboss dentro de sus propios perímetros.

Dado que la Nube iboss no trata los nodos hosteados en sitio de manera distinta que cualquier otro nodo, estos pueden retirarse en cualquier momento sin ninguna pérdida de funcionalidad. Y considerando que los nudos pueden colocarse dentro de una red de una organización, pueden cumplirse los requerimientos del Escudo de Privacidad.

CLUSTER

Los nodos del mismo tipo forman cluster. Cada cluster tiene *un nodo nube maestro* que interactúa con nodos nube maestros de otros cluster. Cualquier nodo puede convertirse en el maestro de su cluster en cualquier momento, asegurando máxima disponibilidad y respuesta de interfaz. Dado que cada cliente cuenta con su propio contenedor, las cargas pesadas de clientes múltiples no resultan en retrasos ni interfaces no responsivas. Los cluster previenen los tiempos de inactividad y en ninguno de los casos un problema asilado tendrá efecto en todos los clientes de la nube.

MÓDULOS

Los módulos son colecciones de cluster diseñados para reducir la complejidad, cada uno es responsable de una función en específico que trabaja en sincronía con otros módulos en la Nube iboss. Mientras que los módulos de una plataforma de cliente trabajan de manera simultánea, están aislados de aquellos en las plataformas de otros clientes, por lo que pueden escalar bajo demanda y entregar sus funcionalidades de manera independiente. El resultado es una arquitectura mucho más resistente que facilita el uso y tiempo para comercializar las nuevas funcionalidades.

CONTENEDORES

Los contenedores abastecen toda la funcionalidad de la Nube iboss. Los contenedores son centros de datos múltiples que funcionan de una manera elástica y en periodos dinámicos para ofrecer seguridad de red bajo las necesidades geográficas de una organización, o con la finalidad de cumplir con los requerimientos regulatorios por país. La naturaleza de los datos contenidos en tránsito y reposo es que se encuentran encriptados y los contenedores se encuentran separados por fronteras OS, por lo que no existe la posibilidad de superposiciones entre organizaciones. La redundancia se lleva a cabo por completo en la nube, por lo que no es necesario realizar respaldos en cintas.

CONECTANDO LOS CONTENEDORES CON EL NÚCLEO DE LA NUBE IBOSS

La unión de los contenedores es una “fabric” subyacente que dirige el tráfico a los nodos cercanos haciendo uso de cluster de registro DNS para generar un equilibrio de carga y geolocalización de los usuarios. La autentificación de factores múltiples se incluye inicialmente a través de la autentificación SSO para los administradores que utilizan la consola de gestión. El Núcleo de Nube iboss se encarga de dirigir a los administradores hacia los contenedores adecuados.

Escalable, seguro y sensible

Conforme crecen las organizaciones necesitan más ancho de banda y más parámetros. Dado que las compañías se apilan constantemente, se forma una arquitectura enfocada a dispositivos que cada vez resulta más costosa y complicada; lo que se convierte en una mezcla de sistemas nuevos y tradicionales que potencialmente ocultan vacíos de seguridad que definitivamente absorben al capital operativo.

La arquitectura del Contenedor Elástico de Nube iboss es fundamentalmente distinta a las arquitecturas de seguridad de nube convencionales. La solución de nodo transparente de iboss permite a las organizaciones añadir usuarios u oficinas de campo sin la necesidad de negociar un proceso de planeación intensivo.

Los nodos pueden añadirse casi de manera instantánea, ya sea dentro de la base de datos del cliente, en el Núcleo de la Nube iboss, o en ambos. Dado que los nodos se acumulan de manera automática unos con los otros, la capacidad de expansión es prácticamente infinita.

Las políticas y reportes son consistentes entre todos los usuarios y se gestionan a través de una consola central de administración en un ambiente aislado y seguro. Se habilita la conciencia de ubicación, con el fin de que las organizaciones sujetas a las regulaciones por país puedan cumplir con las normas de conformidad.

La arquitectura virtual y basada en contenedores patente de iboss ofrece una nube que se puede escalar de manera infinita, dinámica y elástica, ideal para las organizaciones que necesiten responder frente a las necesidades comerciales en constante evolución mientras mantienen la seguridad de sus activos.

Acerca de la Ciberseguridad de iboss

La Ciberseguridad de iboss defiende a las organizaciones grandes y distribuidas de la actualidad contra las ciber-amenazas dirigidas que ocasionan pérdida de datos a través de la Plataforma de Portal de Red Segura de Nube de iboss, que hace uso de tecnologías patentadas para la defensa contra amenazas avanzadas dirigidas al 100% a la nube. La arquitectura única de nube de iboss ofrece a cada organización su propio contenedor, por lo que los datos de un cliente nunca se mezclan con los de otro cliente en la nube pública. Nuestras soluciones avanzadas de seguridad ofrecen una visibilidad única a través de todos los datos de entrada/salida, e incluyen armas de seguridad que revelan los puntos ciegos, detectan ataques y minimizan las consecuencias de la filtración de datos. Siendo líder en el campo de la protección contra amenazas con una capacidad de uso incomparable, iboss actualmente forma parte de miles de organizaciones y usuarios a nivel mundial.