Transformación digital segura de Cisco Campus

Nunca ha habido un mejor momento para hacer que el lugar de trabajo sea más inteligente.

Overview

El trabajo está cambiando en Cisco. En la actualidad, nuestros 72,000 empleados pueden trabajar desde cualquier ubicación: una oficina de Cisco, su hogar, la ubicación de un cliente, un lugar público, y mientras están en movimiento. Más del 50 por ciento de nuestros empleados reportan a gerentes en diferentes ciudades. Y aunque nuestra fuerza laboral ha aumentado en un 20 por ciento en los últimos cinco años, también hemos mejorado la utilización de nuestros más de 23 millones de pies cuadrados de espacio de oficinas en 94 países. Nuestro uso de las soluciones de espacio de trabajo conectadas y la arquitectura de colaboración de Cisco nos ayudó a reducir el espacio total de nuestra oficina en un 30 por ciento.

Mientras tanto, las aplicaciones que utilizamos para colaborar y comunicarse también están cambiando, proporcionando mejores experiencias de usuario, automatizando la mayoría del trabajo manual y proactivamente sugiriendo acciones a los usuarios. Los empleados de Cisco tienen acceso a estas aplicaciones desde nubes públicas, privadas e híbridas. Nuestros clientes, socios y proveedores también consumen estas aplicaciones y las utilizan para colaborar con Cisco.

Estos y otros cambios están creando impactos positivos para nuestros resultados. Como ejemplo, Cisco ha visto más de US $ 1.7 mil millones en ahorros de productividad hasta la fecha a través de nuestro uso de varias soluciones de colaboración. Y la adición de terminales de video al escritorio de cada persona de ventas ha ayudado a acelerar negocios por valor de 682 millones de dólares.

La necesidad de una infraestructura de TI ágil y segura

Más de tres cuartas partes (78 por ciento) de las empresas dijeron que lograr la transformación digital se volverá crítico para ellas en los próximos dos años, según una encuesta reciente de Capgemini Consulting y MIT Sloane Mangement Review. Para tener éxito, estas empresas deberán contar con una infraestructura de TI básica ágil y segura.

A medida que Cisco continúa transformando nuestro lugar de trabajo y nuestra forma de hacer negocios, Cisco IT debe poder responder rápidamente a las solicitudes de desarrollo y soporte de nuestras aplicaciones e infraestructura. La infraestructura ágil de TI de Cisco ya está creando nuevas experiencias de fuerza de trabajo y clientes, al tiempo que ayuda a la

empresa a innovar, mantenerse al día con las demandas de los clientes y mantener nuestro enfoque en los riesgos de seguridad.

En las siguientes secciones, exploramos cuatro áreas diferentes de infraestructura ágil que Cisco IT implementó en el campus de Cisco. También discutimos algunos de los desafíos que enfrentamos y cómo los resolvimos, y explicamos cómo Cisco continuará invirtiendo en transformación digital y disrupción.

Nuestro enfoque, se puede resumir en cuatro partes:

Parte 1. Colaboración y espacio de trabajo ágil

La colaboración es fundamental para nuestro trabajo de hoy. El aumento de las presiones competitivas, las oportunidades debido a los cambios tecnológicos (como la computación en la nube) y la adopción de procesos ágiles que permiten la entrega continua han contribuido a cambios significativos en los estilos de trabajo. Las oficinas cerradas con interacción mínima e intercambio de información han dado paso a enfoques que apoyan un mejor intercambio de información e ideas, y un trabajo dinámico e interdependiente. También vemos más equipos basados en proyectos que se forman a sí mismos, de corta duración y se centran en ofrecer soluciones rápidas e innovadoras a iniciativas muy específicas.

En resumen, las organizaciones exitosas son más ágiles y matriciales. Aprenden y responden rápidamente a través de un flujo abierto de información. Fomentan la experimentación, aprenden de forma iterativa y se organizan como una red de empleados, clientes y socios motivados por un propósito compartido.

A medida que las organizaciones se adaptan para ser ágiles, las necesidades de colaboración se vuelven más variadas. Los empleados de todas las organizaciones están desempeñando diferentes roles y usando múltiples dispositivos a lo largo del día mientras se encuentran en diferentes ubicaciones y zonas horarias. Algunas organizaciones todavía tienen un enfoque de "talla única" para las herramientas de colaboración; Sin embargo, ese enfoque no siempre se alinea con la evolución de los entornos de trabajo o las expectativas de los trabajadores.

Cuando las herramientas corporativas no funcionan, los empleados usan su propia tecnología. Eso incluye dispositivos y aplicaciones: Android, Apple, Windows, Box, Dropbox, Skype, Facebook, SlideShare y YouTube, solo por nombrar algunos. Y al usar esos dispositivos y aplicaciones en el trabajo, los empleados esperan la misma experiencia rápida y fluida que tienen como consumidores.

Para ayudar a cumplir estas expectativas, Cisco IT implementó una experiencia de colaboración unificada y productiva. Los principios rectores son seguridad, simplicidad y facilidad de gestión. Cisco IT, junto con Cisco Workplace Resources, se centró en las siguientes tres áreas para mejorar la experiencia y la productividad del usuario final:

- **Área 1: lugar de trabajo conectado**
  Para ayudar a nuestra gente a aprovechar al máximo sus talentos innovadores, Cisco ha implementado entornos basados en actividades. Cada "vecindario"

ofrece una selección de espacios diferentes con diferentes soluciones de colaboración para apoyar la variación en las necesidades de los trabajadores, la socialización y el tiempo de inactividad. Es un enfoque ideal para nuestra fuerza de trabajo y ayuda a Cisco a reducir costos a través de un uso más eficiente del espacio de la oficina.

- **Área 2: arquitectura de colaboración**
  Traer su propio dispositivo (BYOD), acceso inalámbrico generalizado, una opción en puntos finales de video y movilidad de extensión ofrecen a nuestra fuerza de trabajo la libertad de moverse a cualquier lugar en cualquier momento con cualquier dispositivo.
  Usamos opciones de software como Cisco Spark ™, Cisco WebEx® y Cisco Jabber®, y dispositivos físicos como teléfonos IP tradicionales, dispositivos de video personales (como nuestra serie DX), dispositivos de sala de colaboración (dispositivos MX e IX)) y Spark Board para que esto suceda.

  La TI de Cisco combina estas soluciones con el estilo de trabajo del individuo y las integra firmemente con los procesos y las aplicaciones empresariales. Este enfoque integrado permite a nuestros empleados enfocarse en su trabajo en lugar de lidiar con la complejidad tecnológica.

  Asegurar BYOD

  Cisco ha empleado una política BYOD durante casi una década, y fuimos una de las compañías que lideró el camino para hacer de BYOD una opción realista para la fuerza de trabajo moderna.

  El enfoque inicial de nuestra política BYOD fue proporcionar servicios de correo electrónico y calendario en cualquier plataforma. Hoy, nuestra política permite la movilidad de la fuerza de trabajo y ayuda a que las empresas se hagan más rápido en Cisco.
  Como ejemplo, antes de BYOD, un administrador de cuenta en Cisco tendría que estar en la oficina e iniciar sesión en una herramienta para aprobar una oferta. Hoy, ese mismo gerente de cuenta puede aprobar una oferta desde cualquier lugar en cualquier dispositivo en cualquier momento.

  La omnipresencia de BYOD significaba que necesitábamos un plan integral para proteger los datos confidenciales de Cisco en dispositivos móviles confiables.

  Cisco IT utiliza un conjunto de tecnologías de Cisco para este propósito: MDM, Cisco AnyConnect® para dispositivos móviles, FireAMP para dispositivos móviles, OpenDNS®, Cisco Umbrella ™ y Cisco Identity Services Engine (ISE). Seguimos un enfoque basado en la arquitectura y nos aseguramos de que todos los

componentes de Cisco y los que no son de Cisco sean interoperables y más fáciles de soportar para TI.
TI usa Cisco ISE para autenticar usuarios y dispositivos en la red, y para permitir la cantidad correcta de acceso según el dispositivo que está usando y desde dónde podría acceder a la red. (Nota: cubrimos más detalles sobre ISE en la sección de seguridad de este estudio de caso).

iCAM y eStore

Cisco IT identificó a Box.com como una forma efectiva de compartir documentos entre dispositivos, usuarios internos y clientes. Hemos desarrollado una herramienta de análisis personalizada, llamada iCAM, para observar los perfiles de las personas y su comportamiento de red, recibir noticias de fuentes externas como Box.com y analizarlas juntas. Estamos en proceso de adoptar un enfoque más integral con el agente de seguridad de acceso a la nube Cisco Cloudlock® para proteger los datos de Cisco que residen en varias nubes públicas.

Cisco IT también construyó eStore, una tienda interna de aplicaciones de TI. eStore es un portal de autoservicio único para la entrega de servicios de TI a nuestros usuarios internos utilizando el catálogo de servicios Cisco Prime®. Los usuarios pueden buscar y acceder a cualquier servicio de TI con unos pocos clics. La mayoría de los servicios en esta plataforma están completamente automatizados y pueden configurarse en minutos. Los usuarios eligen de una lista de servicios con costos asociados y pueden elegir cualquier combinación de servicios para que coincida con sus requisitos.

- **Área 3: Integración de herramientas de colaboración en procesos de negocios**
  Incorporamos herramientas de colaboración dentro de las aplicaciones que utilizan los empleados de Cisco. Al utilizar Cisco Spark, por ejemplo, virtualizamos nuestra sala de guerra física Quarter-End. Eso llevó a una reducción del 70 por ciento en el tiempo dedicado por los ingenieros y una reducción significativa en los costos de viaje.
  Una colaboración más rápida y fácil desde cualquier lugar y en cualquier momento reunió al equipo global, mejoró la transparencia y redujo drásticamente la cantidad de tiempo necesario para las reuniones en persona.
  El Centro de comando de operaciones de TI es otro ejemplo de cómo estamos integrando Cisco Spark en el negocio. Cuando ocurre un incidente de TI, se crea una sala de reuniones virtuales de Cisco Spark. Eso le da visibilidad a los equipos de TI requeridos y reduce los esfuerzos duplicados de otros equipos.
  En caso de que un incidente se transfiera a otra zona horaria para continuar el trabajo, el historial de incidentes está fácilmente disponible. Esta capacidad ha

mejorado el tiempo de resolución de incidentes, así como el tiempo de revisión posterior al incidente.

Parte 2. Centro de datos y nube

La segunda parte de nuestro enfoque para crear una infraestructura de TI ágil implica el centro de datos y la nube, así como las aplicaciones. La digitalización acelera la velocidad de la innovación e interrumpe los modelos comerciales predominantes. Eso, a su vez, aumenta la velocidad a la que se pueden transformar las aplicaciones.

No solo ocurren cambios en aplicaciones tradicionales alojadas en centros de datos, sino que también se accede a muchas aplicaciones nuevas desde la nube pública como software como servicio (SaaS), plataforma como servicio (PaaS) o infraestructura como servicio (IaaS). Pero las empresas demandan modelos de consumo más flexibles, simples y rentables.

Hasta 2016, la visión de TI de Cisco era:

● Construir centros de datos adicionales y capacidad de infraestructura para abordar la creciente demanda del negocio. Llevamos la migración de aplicaciones a nuevos centros de datos como una oportunidad para transformar aplicaciones.

● Proporcionar flexibilidad de aplicación basada en infraestructura altamente disponible.

● Cambie a un modelo de TI como servicio (ITaaS). Como parte de este programa, construimos una clara visibilidad del costo y la calidad del servicio que entregamos a nuestros clientes internos. También pudimos construir nuevas capacidades de nube privada. Al final del turno inicial, ofrecíamos un tiempo de inactividad casi nulo para las aplicaciones críticas desde el lado de la infraestructura. También redujimos el tiempo de aprovisionamiento de infraestructura a aproximadamente 15 minutos.

El nuevo enfoque de TI de Cisco es adaptar la infraestructura a las demandas de las aplicaciones y hacer que las aplicaciones sean más inteligentes, en lugar de confiar únicamente en la infraestructura para brindar resiliencia y seguridad. Estamos logrando esto por:

● Transformar las aplicaciones al modo nativo de la nube, para que puedan adaptarse rápidamente para enfrentar los nuevos desafíos comerciales.

● Hacer que todo en el centro de datos esté definido por software.

● Automatizar la administración de la capacidad y el consumo transparente de los recursos de la nube públicos y privados.

● Incrustabilidad y seguridad en cada componente y proceso.

● Mejorar la calidad y la disponibilidad de las aplicaciones y la infraestructura con big data y análisis.

Modelo de entrega continua

Más del 70 por ciento de los equipos de aplicaciones de TI en TI de Cisco han adoptado un modelo de entrega continua, lo que ha conducido a una mejora considerable en el tiempo de entrega de nuevas capacidades comerciales y la calidad y seguridad de las aplicaciones de TI. Algunos de los beneficios clave para Cisco incluyen:

● Aumento de 2X en las capacidades entregadas

● 60% de reducción en las vulnerabilidades

● 92 por ciento de aumento en la calidad

Transformación de aplicaciones, nativo de la nube y fuente abierta

Tradicionalmente, la mayoría de las aplicaciones empresariales se utilizaban con fines comerciales y el cambio era poco frecuente. A medida que las empresas demandan nuevas capacidades en el lado de la aplicación, los equipos de TI deben transformar sus aplicaciones para que sean nativas de la nube.

En modo tolerante a la nube, las aplicaciones están estrechamente integradas durante el tiempo de diseño y no tienen la capacidad de cambiar por sí mismas, incluso si la infraestructura subyacente admite cambios dinámicos. Por ejemplo, cuando aumenta el número de usuarios que acceden a una aplicación, el rendimiento de la aplicación se degradará. El administrador de TI debe monitorear el uso, aumentar los recursos asignados y reconfigurar la aplicación para usar los recursos recientemente agregados de manera efectiva.

En el modo nativo de la nube, las aplicaciones están diseñadas para aprovechar al máximo la escalabilidad de la infraestructura subyacente. Por ejemplo, cuando la carga en la aplicación aumenta, puede detectar el aumento de la carga en comparación con la capacidad aprovisionada, y aumentar la cantidad de recursos asignados sin la intervención manual del administrador de TI.

Hoy, en Cisco, somos:

● Aprovechar al máximo la nube usando API para consumir infraestructura

● Manejar las demandas del usuario dinámicamente, sin la necesidad de recursos para monitorear el uso o realizar cambios manualmente

● Autocuración de fallas de componentes de infraestructura y software

● Reducción de costos mediante el uso de componentes de código abierto

Infraestructura del centro de datos

Cisco IT ya ha creado una excelente nube privada para nuestros usuarios internos. Admitimos más de 55,000 hosts virtuales en nuestra nube privada basada en Cisco ACI ™, servidores Cisco Unified Computing System ™ y herramientas de orquestación como Cisco Prime Service Catalog y UCS Director. Además de los componentes de Cisco, aprovechamos el hardware y el software de terceros en áreas como SAN, NAS, virtualización, PaaS e ITIL. Cisco IT también está en el proceso de agregar la capa del sistema operativo de la nube para proporcionar una completa capacidad de programación basada en API de las aplicaciones.

Data Center Analytics

En el entorno altamente virtualizado y en contenedores del centro de datos de Cisco, donde los cambios ocurren con frecuencia, las formas tradicionales de encontrar dependencias y solucionar problemas de aplicaciones no son prácticas y requieren mucho tiempo.

Cisco IT implementó Cisco Tetration Analytics ™ para inspeccionar cada paquete que fluye a la red del centro de datos. Recopilamos un gran volumen de datos y proporcionamos una vista de dependencia en tiempo casi real de las aplicaciones. La TI de Cisco puede acelerar la migración de aplicaciones de una red heredada a la nube. Los equipos de aplicaciones obtienen visibilidad para transformar las aplicaciones al modo nativo de la nube rápidamente. A su vez, los auditores pueden ver la aplicación de la política fácilmente.

El dominio de la aplicación ha sufrido una transformación radical en los últimos años. En la superficie, una aplicación puede verse muy simple; sin embargo, bajo el capó, todo el ecosistema de aplicaciones es tremendamente complejo. Hay muchos componentes, y todos deben cooperar.

Piense en los diferentes tipos de modelos de entrega: la entrega tradicional en el sitio, SaaS / basada en la nube, diferentes plataformas como la implementación de dispositivos móviles o web en todo tipo de entornos y la explosión de tipos de datos no estructurados. Desde la perspectiva del monitoreo del rendimiento de las aplicaciones, Cisco tiene la capacidad de unir todos estos tipos y fuentes de datos, y diseccionar y administrar todo a nivel de componente, manteniendo la visibilidad y optimizándolo de principio a fin.

Tres grupos se benefician de la "supervisión como servicio" de Cisco AppDynamics:

● Comunidad de desarrollo: en la fase de desarrollo, Cisco TI somete el código a pruebas de rendimiento para detectar y solucionar problemas al principio del ciclo de vida, lo que ayuda a producir código de calidad.

● Equipo de operaciones: este grupo supervisa la producción y toma medidas proactivas para corregir problemas antes de que afecten al negocio. El equipo puede identificar rápidamente la causa raíz de un problema y restaurar los servicios más rápido. El historial de los detalles

de las transacciones y los datos analíticos se utilizan para la gestión de incidentes y problemas.

● Propietarios de empresas y servicios: nuestros propietarios de servicios obtienen visibilidad en tiempo real sobre la salud y el rendimiento de su negocio y pueden aprovechar los datos para tomar decisiones más rápidas y mejores, así como para aumentar la velocidad y la estabilidad del servicio y del negocio.

Con la implementación de soluciones analíticas de centros de datos y en la nube, los desarrolladores de aplicaciones pueden autoabastecer su infraestructura en solo 15 minutos. Además, la huella del centro de datos ha disminuido en un 35 por ciento debido a una mejor utilización de la infraestructura existente.

Nuestro uso del análisis del centro de datos ha ayudado a mejorar nuestra capacidad para detectar problemas rápidamente y reducir el costo de la solución de problemas de la aplicación.

Parte 3. Red flexible y automatizada

El crecimiento exponencial en dispositivos conectados, aplicaciones entregadas a la nube y servicios, y la creciente frecuencia y severidad de los ciberataques, son algunas de las implicaciones tecnológicas clave de la digitalización. Y la forma en que los usuarios acceden a la red ha cambiado drásticamente en los últimos años. Por ejemplo:

● Los usuarios usan Wi-Fi como la forma principal de conectarse a la red de TI.

● Los usuarios usan múltiples dispositivos para acceder a la información, y necesitan la capacidad de compartir entre dispositivos.

● Los usuarios se conectan a la red desde cualquier ubicación, no solo desde oficinas.

● El tipo de tráfico en la red se ha desplazado de los datos a la mayoría de voz y video. El video no está limitado a dispositivos de colaboración dedicados; todos los dispositivos utilizados generan tráfico de video y voz.

● El dispositivo final en su mayoría encripta el tráfico.

● Los usuarios ahora están accediendo a aplicaciones complejas que están compuestas por componentes de nubes públicas y privadas, a diferencia de la forma tradicional de usar aplicaciones solo desde centros de datos administrados de TI.

● Nuevos tipos de dispositivos, como cámaras de vigilancia, sistemas de administración de edificios, luces e Internet of Things (IoT), comenzaron a aparecer en la red.

La red es el núcleo de la empresa digital y debe ser flexible. Y las organizaciones que implementan más redes digitales listas pueden aumentar los ingresos, la retención de clientes y la rentabilidad. [2]

Implementación simple, automatización y escalabilidad

Cisco IT considera seguir cuatro criterios al diseñar una red preparada para digital:

● Implementación simple, automatización y escalabilidad

● Red unificada para cargas de trabajo tradicionales y nuevas, como video, edificios inteligentes y dispositivos de IoT

● Inalámbrica ubicua

● Aplicación de políticas conscientes del contexto

Cisco Digital Network Architecture (DNA), explicada con más detalle más adelante en este documento, nos permite virtualizar los servicios de red y brinda la flexibilidad de agregar nuevos servicios sin la necesidad de aprovisionar nuevo hardware para cada servicio. La arquitectura de ADN es una arquitectura abierta y programable que permite la automatización y la administración. El número creciente de componentes de red en toda la empresa no necesita escalar los recursos de forma lineal, lo que ayuda a reducir considerablemente el costo y el tiempo necesarios para implementar nuevos servicios.

Red unificada

Cada vez más dispositivos de TI e instalaciones se conectan a la red, incluidas las cámaras IP, los sistemas de administración de edificios, las luces de sobreenergía (PoE), las puertas de enlace IoT y los quioscos. La TI de Cisco trabaja estrechamente con nuestras instalaciones y equipos de seguridad física para implementar una red IP unificada en lugar de crear islas de red individuales. También es fundamental considerar las implicaciones de seguridad de la expansión de IoT y contar con herramientas y procesos adecuados para detectar incidentes relacionados con la seguridad y mitigarlos.

Pervasive inalámbrico

La demanda del usuario final para trabajar desde cualquier lugar con cualquier dispositivo requiere una implementación inalámbrica generalizada en el lugar de trabajo. A medida que los usuarios comiencen a utilizar la tecnología inalámbrica como método principal de conectividad, la red debería proporcionar estabilidad. Cisco IT ha adoptado la última generación de soluciones basadas en Cisco 802.11ac Wave2 para cumplir estos requisitos.

Los usuarios esperan el mismo nivel de disponibilidad que una red cableada. El departamento de TI de Cisco aprovecha algunas de las características únicas de la solución inalámbrica de Cisco para proporcionar funcionalidades que incluyen CleanAir®, Client Link,

cambio de estado de cliente, administración mejorada de recursos de radio, radio flexible y roaming asistido. Estas características permiten a Cisco IT proporcionar red inalámbrica a nuestros usuarios con la misma confiabilidad y rendimiento que una red cableada.

Parte 4. Seguridad

Las nuevas redes distribuidas significan nuevos desafíos de seguridad. El panorama empresarial actual ha cambiado por completo, al igual que el paisaje de amenazas. Las redes complejas y fragmentadas hacen que sea muy difícil protegerse contra las amenazas persistentes avanzadas.

Mientras tanto, Cisco continúa adquiriendo empresas innovadoras, lo que significa tratar de fusionar los sistemas de TI, los departamentos, las redes y el acceso, y las políticas y herramientas de seguridad. Agregue esto al mayor uso de los servicios en la nube y las aplicaciones en la nube, que se activan más rápido de lo que TI puede administrarlos.

Como resultado, la superficie de ataque de la empresa se ha expandido hasta el punto en que ahora es una cuestión de tiempo antes de que se vulnere una red. No si, sino cuándo.

Cisco IT no puede defenderse contra lo que no podemos ver. Es por eso que la visibilidad en la red es un componente crítico de nuestra seguridad. Capturamos lo que está sucediendo en la red a un nivel granular. Comprendemos una línea de base de cómo se ven los flujos de tráfico. Es importante ver aplicaciones, usuarios y dispositivos conocidos y desconocidos en la red para determinar si puede haber un comportamiento anómalo que requiera acción.

Cisco IT utiliza la red como sensor y Enforcer para aprovechar nuestra red existente de Cisco para realizar análisis de red y visibilidad y aplicar la política que es el elemento clave de la seguridad de la red. Estas soluciones nos ayudan a detectar flujos de tráfico y malware anómalos. También nos alertan cuando el malware intenta propagarse. Tenemos una gran visibilidad de las aplicaciones y los roles por usuario. Eso nos permite determinar si los usuarios están violando la política de acceso y detectar rápidamente dispositivos no autorizados y ponerlos en cuarentena en la red.

Un enfoque holístico de la seguridad

Solía haber un fuerte perímetro definido por los puntos finales de la red, que estaban dentro de edificios corporativos seguros o centros de datos corporativos altamente seguros. Pero en la última década, muchas cosas han cambiado. La adición de puertas de enlace de Internet requiere firewalls, IDS / IPS y más. El teletrabajo requería una mejor encriptación y seguridad VPN. La movilidad, en forma de acceso inalámbrico para computadoras portátiles, teléfonos inteligentes y almohadillas de los trabajadores móviles, disolvió el concepto de un perímetro de red y requirió una protección de dispositivos y datos significativamente mayor.

Los servicios en la nube han expandido el centro de datos corporativo altamente seguro hacia centros de datos de proveedores que proporcionan niveles de seguridad y cumplimiento normativo variables ya menudo desconocidos. Mientras tanto, la seguridad cibernética de la infraestructura ahora es tan avanzada que, siempre que la infraestructura esté bien reparada y actualizada, se pueden detener casi todos los ataques estándar.

En la actualidad, la mayoría de los ataques exitosos rodean las defensas estándar del perímetro al encontrar personas de confianza que les permiten (y su malware) ingresar a la red a través del correo electrónico y la nube. Como ejemplo, los empleados de Cisco visitan 350 millones de sitios web por día, y cerca del 2 por ciento de esos sitios están bloqueados. Evitamos más de 500,000 descargas de malware por día. También recibimos alrededor de 4,5 millones de correos electrónicos por día desde fuera de la compañía. Algunos apuntan a sitios web infectados y alrededor de 200 correos electrónicos por día llevan archivos adjuntos de carga de virus.

A la luz de estas dinámicas, la TI de Cisco está adoptando un enfoque más holístico de la seguridad al centrarse en la configuración de políticas y prácticas que ayudan a proteger los activos, los datos y la propiedad intelectual de Cisco de forma proactiva y reactiva. Si bien la tecnología es una gran parte de la arquitectura de seguridad de Cisco, un ojo vigilante en las tendencias dentro del entorno empresarial y el impacto en los usuarios también son importantes para nuestro plan integral.

El enfoque de seguridad de TI de Cisco es utilizar una combinación de tecnologías, procesos y conocimiento y capacitación para educar a todos en Cisco. Todas estas áreas se extienden a través del continuum de tres ataques de antes, durante y después.

Cisco Talos ™ ha neutralizado con éxito la infraestructura maliciosa en la naturaleza, contrarrestando a los atacantes en su propio terreno. Talos es la organización de inteligencia de amenazas líder en la industria con más de 250 investigadores. [3]

Veamos cómo las soluciones de seguridad de Cisco nos ayudan en las diferentes fases de un ataque. Cuando los atacantes realizan un reconocimiento, investigan a los empleados en línea (tal vez a través de las redes sociales) e intentan mapear la red. Los atacantes necesitan preparar su propia infraestructura, por ejemplo, servidores de botnets.

Los atacantes pueden usar un correo electrónico de phishing, publicidad maliciosa (publicidad maliciosa) u otra técnica para lanzar su ataque. Independientemente de cuán legítimo sea el correo electrónico de phishing, Cisco Email Security bloqueará el mensaje malicioso. Al bloquear en la capa DNS desde la nube, Cisco Umbrella ™ protege a los usuarios de acceder a dominios, direcciones IP y URL maliciosos. Los usuarios también pueden usar Cisco Web Security para bloquear sitios web HTTP y HTTP maliciosos.

Después de un lanzamiento inicial, los atacantes explotan las vulnerabilidades en la red para obtener un punto de apoyo. El firewall de próxima generación de Cisco (o NGFW) y Cisco Meraki ™ MX protegen los activos críticos de que se acceda a través de aplicaciones comprometidas en el borde, la sucursal y el centro de datos. El Sistema de Prevención de Intrusos de Nueva Generación (o NGIPS) de Cisco identifica y bloquea exploits con una eficacia líder en la industria.

Los atacantes quieren instalar malware para llevar a cabo tareas complejas, por ejemplo, el registro de teclas. Advanced Malware Protection (o AMP) bloquea los archivos maliciosos antes de que puedan ingresar a su red y monitorea continuamente la actividad de archivos y

procesos. Los archivos desconocidos se analizan en ThreatGRID® y, cuando se consideren maliciosos, AMP emitirá una alerta retrospectiva.

Los atacantes usan el tráfico de comando y control para comunicarse con la infraestructura maliciosa. Cisco Umbrella ™ bloquea este tráfico sobre cualquier puerto o protocolo cuando los usuarios están dentro o fuera de la red corporativa. Esto es cierto incluso cuando la VPN está desconectada.

Si un atacante ha penetrado exitosamente en una red, persistirá hasta que logre sus objetivos. Cisco Identity Services Engine (o ISE) mitiga las amenazas actuales al limitar el acceso a la red en función del quién, qué, cuándo y dónde de las personas y los dispositivos conectados a la red corporativa. La tecnología Cisco TrustSec® está integrada en los dispositivos de Cisco, que trabajan con ISE para aplicar políticas a través de la segmentación definida por software.

Para detectar intrusiones en una red, StealthWatch® establece una línea de base de actividad y detecta anomalías, analizando datos históricos y en tiempo real del flujo neto. Y Cisco Cloudlock® bloquea el uso indebido de credenciales y el movimiento de datos confidenciales dentro de las aplicaciones en la nube cuando esto es lo que persiguen los atacantes.

Simple, abierto y automatizado

Los productos de Cisco se comunican entre sí porque están abiertos. Al automatizar y simplificar los procesos, la seguridad es más efectiva. Por ejemplo, los eventos de AMP para puntos finales se integran con las soluciones de seguridad Web, correo electrónico, Cisco Umbrella ™, NGFW y Cisco Meraki ™ de Cisco para detectar amenazas rápidamente.

La información de la política también se comparte entre los productos. Si StealthWatch identifica a un usuario comprometido, ISE y TrustSec cambiarán la etiqueta de grupo seguro y la política de seguridad web para ese usuario cambia automáticamente.

Los productos de seguridad de Cisco comparten inteligencia de amenazas ampliamente, especialmente a través de Cisco Talos. Si una implementación de AMP en una ubicación detecta una nueva variante de ransomware de día cero, otras implementaciones de AMP en todo el mundo se actualizan a través de Talos. Con la inteligencia de amenazas de Talos, un cliente podría bloquear una variante de día cero incluso si nunca antes había estado expuesta a ella.

Por último, el intercambio de información contextual simplifica los flujos de trabajo. El contexto en ISE se puede aplicar al establecer políticas dentro de NGFW y es tan fácil como crear cualquier otra política de NGFW. Las API en toda la cartera de seguridad de Cisco permiten la integración con soluciones de terceros en su red.

Resultados

Cisco es el líder mundial en redes que transforma la forma en que las personas se conectan, se comunican y colaboran de forma segura. También somos, como resultado, un objetivo principal para los ciberataques.

Al utilizar una combinación de soluciones de seguridad de nuestra compañía, así como de terceros confiables, la TI de Cisco ha podido reducir la tasa de infección del host en un 48 por ciento y evitar incidentes importantes como el ataque de ransomware que afecta a WannaCry en nuestros sistemas.

Resumen

La TI de Cisco continúa impulsando innovaciones en el lugar de trabajo para atraer nuevos talentos, mejorar la productividad y reducir costos. Estamos trabajando en estrecha colaboración con los equipos de seguridad e instalaciones para crear una arquitectura unificada para el espacio de trabajo digitalizado. A través de nuestra colaboración y ayudando a nuestros clientes a través de sus viajes de transformación digital, hemos aprendido que:

- El diseño para el lugar de trabajo moderno debe considerar cambiar las preferencias del usuario y las nuevas y emergentes herramientas de colaboración y comunicación.
- Esas herramientas deberían ser interoperables e integradas en procesos y aplicaciones empresariales.
- Las empresas también deben enfocarse en crear las políticas correctas y crear conciencia entre los usuarios sobre los riesgos de seguridad. Además, las políticas deben basarse en el contexto y no estar vinculadas a una ubicación o dispositivo específico.

También entendemos que la red debe estar altamente visualizada y automatizada para responder rápidamente a las cambiantes necesidades comerciales. También debe ser flexible para acomodar nuevos dispositivos y crecer. Y, por último, las empresas deben diseñar su red para que sirva de sensor y ejecutor de políticas para que puedan enfrentar los desafíos del entorno de amenazas cibernéticas cada vez más complejo de la actualidad.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.