



Cibes

Organización Cibes Lift

País:
Suecia

Solución
Panda Fusion 360
+ Panda Patch
Management

Licencias
535

"Panda Systems Management 360 ha sido increíblemente importante para nosotros en Cibes".

Situación

El origen de Cibes data de 1947, cuando el inventor sueco Bertil Svedberg fundó una empresa para la fabricación de ascensores de carga. En la década de los 60, la empresa lanzó la primera generación de ascensores domésticos y poco después la primera serie de ascensores de plataforma.

Ese fue el comienzo del gran viaje que ha convertido a Cibes en lo que es hoy en día: una compañía dinámica y global, con fuertes raíces en Suecia.

En el año 2008 Cibes pasó a formar parte del grupo Cibes Lift Group, y pocos años después, en 2012, la empresa trasladó su actividad a Gävle, en lo que es actualmente el corazón de la empresa.

Cibes Lift produce entre 4000 y 5000 ascensores al año para más de 50 países. 15 de esos países cuentan con sus propias instalaciones; aun así, la mayor parte de la producción tiene lugar en la fábrica de Gävle.

La primera oficina en China fue inaugurada en el año 2015. Hoy en día, la empresa cuenta con 20 oficinas en todo el mundo y planes en marcha para construir una fábrica en China.

El traslado desde Järbo a Gävle coincidió con la incorporación a la empresa de Jonas Persson como Director de IT.

Jonas es responsable de garantizar la seguridad informática de todas las oficinas de la empresa, realizando su labor desde las oficinas centrales de la compañía en Gävle con la ayuda de Panda Fusion 360 (combinación de Panda Adaptive Defense 360 y Panda Systems Management).

Retos

Uno de los mayores desafíos a los que se enfrenta una organización como Cibes, que se encuentra en constante crecimiento, es mantener el control sobre los nuevos usuarios que se incorporan a la organización como consecuencia de la contratación de nuevos empleados. Una labor que se realiza además de forma remota, ya que Jonas realiza su trabajo desde la sede central de Gävle. Esta tarea requiere de la instalación y configuración de nuevas redes y equipos. En el caso de los usuarios ubicados en Europa, la empresa envía equipos con todas las aplicaciones necesarias instaladas desde la oficina central. En Asia, por su parte, son empleados locales los que se encargan de instalar Adaptive Defense 360 y Panda Systems Management.

Defender los dispositivos de los ataques no es sencillo. La protección debe incluir una amplia gama de mecanismos de defensa entre los que se incluya un antivirus tradicional, anti-malware, firewall personal, filtrado Web y de correo, y control de dispositivos. Además, toda protección debe proporcionar defensas adicionales contra amenazas difíciles de detectar, como son los ataques dirigidos y de día cero. Hasta ahora, los departamentos de IT se veían obligados a adquirir y mantener una serie de productos de distintos proveedores para defender sus equipos, pero esto ya es no así.

Solución

Como Jonas necesitaba una solución que facilitase el trabajo remoto, Fredrik Losman, de Panda Security le recomendó dos soluciones de seguridad en la nube: Panda Adaptive Defense 360 y Panda Systems Management.

Adaptive Defense 360 es el único producto que combina en una única solución protección (EPP) y detección y respuesta en el endpoint (EDR). Además, permite automatizar tareas, reduciendo la carga de trabajo del departamento de IT. Con Adaptive Defense 360, Panda ofrece la mejor solución EPP del mercado. El servicio incluye seguridad centralizada y fácil de administrar, acciones de remediación, monitorización e informes en tiempo real, protección por perfiles, control centralizado de dispositivos, así como filtrado y monitorización Web.

La solución se fundamenta en un modelo de seguridad basado en 3 principios: continua monitorización de las aplicaciones ejecutadas en los equipos y servidores de la empresa, clasificación automática y machine learning. Este modelo es capaz de proteger los clientes y servidores de la organización contra los ataques conocidos y desconocidos procedentes de Internet o del correo electrónico, por ejemplo.

Uno de los mayores desafíos de una organización son los usuarios. Adaptive Defense 360 minimiza el riesgo de que se produzcan incidentes de seguridad impidiendo, por ejemplo, que los usuarios puedan instalar programas considerados maliciosos o sospechosos por Panda Security.

Panda Systems Management, o PCSM, como también es llamado, permite a Jonas ejecutar, monitorizar y administrar todos los dispositivos de la empresa, independientemente de que estén en la oficina o en cualquier otro lugar.

Con PCSM, Jonas puede monitorizar los servidores de Cibes y recibir alertas en caso de que un disco duro esté a punto de fallar o los recursos de hardware de un servidor se estén agotando, por ejemplo. Además, en caso de que un empleado necesite ayuda con su equipo, Jonas puede asistirle directamente desde su equipo con las herramientas de acceso remoto.

Evaluación

Disponer de un informe completo del estado de la organización facilita al Director de IT y a la dirección de la empresa la toma de decisiones sobre las necesidades que se deben priorizar o modificar.

Siempre que Jonas habla de Adaptive Defense 360 y PCSM, destaca una y

Cibēs

Beneficios Panda Systems Management:

Tomar el control de un equipo cliente o servidor independientemente de su ubicación.

Ver el tipo de hardware y los programas instalados en los clientes y servidores.

Ver, mediante la consola, los cambios realizados en los equipos cliente, facilitando así la resolución de incidencias.

Distribuir una o varias aplicaciones de software de manera sencilla, ya sea a un cliente concreto o a toda la organización.

Disponer de un sistema de gestión de incidencias que permite la creación automática de tickets ante eventos inesperados. Por ejemplo:

caída de un servidor o fallo de un disco duro.

Panda Cloud Systems Management muestra directamente el consumo de electricidad de los clientes y servidores, así como el coste de la energía consumida. Configura reglas de consumo energético, ahorrando dinero y protegiendo el medio ambiente.

Sus informes completos sobre el estado de la organización facilitan al Director de IT y a la dirección de la empresa la toma de decisiones sobre las necesidades que deben priorizar o modificar.



otra vez los beneficios que ha supuesto para su organización disponer de dos soluciones en la nube, especialmente lo mucho que PCSM ha facilitado su trabajo gracias a poder realizar la mayor parte del mismo de forma remota..

Principales Beneficios

Panda Patch Management permite en una única solución:

Auditar, monitorizar y priorizar las actualizaciones de los sistemas operativos y aplicaciones.

Un panel único en la consola centraliza, actualizado en tiempo real, permite una visibilidad agregada del estado de los parches y actualizaciones pendientes del sistema y cientos de aplicaciones de terceros.

Prevenir incidentes, reduciendo sistemáticamente la superficie de ataque por vulnerabilidades.

La gestión de parches y actualizaciones con herramientas de gestión, fáciles e intuitivas, permiten adelantarse a la explotación de vulnerabilidades.

Contener y mitigar ataques que explotan vulnerabilidades.

Aplicando inmediatamente las actualizaciones críticas desde la consola Cloud. La consola correlaciona detecciones con vulnerabilidades, minimizando así el tiempo de respuesta, contención y remediación mediante la actualización necesaria desde la consola. Adicionalmente, permite aislar de la red los equipos afectados, mitigando así la expansión al ataque.

Reducir los costes operativos.

- No requiere ni despliegues ni actualizaciones de agente en los endpoints, simplificando la gestión son sobrecargar los equipos y servidores.
- Minimiza el esfuerzo de las actualizaciones remotas desde la consola Cloud. Además, la aplicación de parches está optimizada para minimizar errores.
- Visibilidad inmediata y desatendida de las vulnerabilidades, actualizaciones y aplicaciones en EoL3, tras la activación.

Cumplir con el principio de responsabilidad activa.

Requisito en muchas regulaciones (GDPR, HIPAA y PCI), que obliga a las organizaciones a establecer todas las medidas que garanticen la protección de datos sensibles bajo su responsabilidad.