Publicado en NEZAHUALCOYOTL el 03/08/2017

# [Forcepoint anuncia nueva solución que detecta a los usuarios más peligrosos dentro de las empresas](http://www.notasdeprensa.es)

## La nueva analítica de comportamientos Forcepoint CASB ayuda a los equipos de seguridad de las empresas y gobiernos a reducir el tiempo de reacción al enfocarse en el impacto que los usuarios más peligrosos podrían tener en el negocio. Forcepoint Web Security y Forcepoint Email Security ofrecen nuevos controles para las aplicaciones en la nube, en tanto que el servicio Advanced Malware Detection acelera la adopción y gestión segura de la nube

 Forcepoint, líder global en seguridad cibernética, fortaleció su portafolio de seguridad en la nube para ofrecer a los equipos de seguridad nuevos controles basados en comportamientos que simplifican la protección de empleados, datos empresariales críticos y propiedad intelectual (PI). Las nuevas capacidades disponibles en Forcepoint CASB, Forcepoint Web Security y Forcepoint Email Security aseguran que los clientes de todo el mundo puedan llevar su negocio a la nube de forma segura y continuar creciendo al mismo tiempo. De acuerdo con Gartner, el tiempo promedio para detectar una brecha es de 99 días y alcanza un costo de $4 millones de dólaresi; sin embargo, las empresas pueden reducir ese tiempo usando datos y analítica. La firma espera que para el 2018, el 80% de las plataformas para la protección de dispositivos móviles incluyan capacidades para monitorear las actividades de los usuarios, así como capacidades forenses, por arriba del 5% de 2013 ii, y estima que por lo menos el 25% de las brechas empresariales auto descubiertas se localizarán mediante el uso de la analítica del comportamiento de usuarios y entidadesiii. “Ver la seguridad a través de una perspectiva centrada en las personas ayuda a las organizaciones a entender mejor los indicadores de un comportamiento cibernético normal, e identificar rápidamente la actividad y las operaciones, como el Shadow IT, que representa un mayor riesgo”, aseguró Kris Lamb, vicepresidente y director general de la unidad de Seguridad en la Nube de Forcepoint. “A medida que las empresas y agencias de gobierno cambian sus aplicaciones a los modelos SaaS y de TI en la nube, necesitan sistemas inteligentes que detectan rápidamente las anomalías, evalúen el riesgo y faciliten una solución rápida con la finalidad de proteger a los usuarios y sus datos en un mundo donde el perímetro se difumina cada vez más”. Estrategias de seguridad que se originan en la nubeForcepoint está ofreciendo hoy nuevas capacidades CASB que evalúan el riesgo existente al compartir archivos y otras aplicaciones de nube, y que protegen contra la pérdida de información empresarial crítica y de propiedad intelectual no almacenadas en una red corporativa. Ahora Forcepoint CASB analiza el comportamiento de los usuarios y las características de las aplicaciones, como datos, dispositivos y ubicaciones a los que se está teniendo acceso. Un nuevo User Risk Dashboard reporta el comportamiento de los empleados y, una característica exclusiva de Forcepoint CASB, el impacto potencial para el negocio de acuerdo con los permisos de las cuentas de los usuarios dentro de una organización. Los equipos de seguridad ahora tienen acceso más rápido a información útil con lo que logran entender completamente el riesgo a simple vista; y, cuando CASB se utiliza con Forcepoint Advanced Malware Detection potenciado por Lastline, las organizaciones pueden estar seguras de que sus datos están totalmente protegidos contra los usuarios peligrosos y el malware que se hace pasar como un usuario. Las amenazas del mundo real que enfrentan las empresas y gobiernos pueden detenerse con la analítica de comportamientos de Forcepoint CASB. Por ejemplo, los bancos que están haciendo la transición de prestar servicios financieros locales a ofrecerlos desde la nube, al igual que su infraestructura, necesitan proteger a los empleados que utilizan Microsoft Office 365 así como a los desarrolladores por contrato que utilizan las nubes públicas de Amazon o Azure para crear aplicaciones a la medida. En el sector de la salud, los doctores que terminan su turno descargan los archivos de los pacientes del sistema de expedientes médicos electrónicos al almacenamiento en la nube personal para usarlos en un nuevo consultorio, lo que elevará su nivel de riesgo como usuario y provocará que el equipo de seguridad responda rápidamente para revocar el acceso y detener el intento de exportar los datos. Forcepoint también ha mejorado sus ofertas para la nube y locales. Forcepoint Web Security y Forcepoint Email Security contienen nuevas funcionalidades y herramientas, entre las que se incluyen: Las mejoras a Forcepoint Web Security ofrecen un control más estricto de las aplicaciones de nube y bloquean el Shadow IT no autorizado. Forcepoint Web Security con nuevas herramientas de migración a la nube para Forcepoint Web Security Cloud ayuda a los clientes de dispositivos locales a migrar cuando están listos. Advanced Malware Detection (AMD) Potenciado por Lastline ya está disponible para las plataformas locales y en la nube de Forcepoint Web Security y Forcepoint Email Security. La integración de la tecnología sandbox de AMD brinda protección en tiempo real a los usuarios en cualquier lugar. Recursos adicionales: Lea los artículos Control de la analítica de comportamientos en la nube de CASB y Por qué la analítica del comportamiento es importante para proteger la nube en el blog Focepoint Insights Descargue el libro electrónico “Asegurando al personal siempre y en cualquier lugar” Descargue el Reporte de los Analistas: “El Impacto Económico Total de Forcepoint Web Security Cloud y Email Security Cloud (Forrester).” Acerca de ForcepointForcepoint está transformando la seguridad cibernética al enfocarse en lo que más importa: entender las intenciones de la gente cuando interactúa con datos críticos dondequiera que éstos residan. Nuestros sistemas robustos permiten a las compañías brindar a los empleados libre acceso a los datos confidenciales, protegiendo al mismo tiempo la propiedad intelectual y simplificando el cumplimiento. Con sede en Austin, Texas, Forcepoint soporta a más de 20,000 organizaciones en todo el mundo. Para obtener más información sobre Forcepoint, visite www.Forcepoint.com y síganos en Twitter en @ForcepointSec i Fuente: Gartner, “Smarter with Gartner The Gartner IT Security Approach for the Digital Age”, 12 de junio de 2017; http://www.gartner.com/smarterwithgartner/the-gartner-it-security-approach-for-the-digital-age/ ii Fuente: Gartner, “Designing an Adaptive Security Architecture for Protection From Advanced Attacks”, de Neil MacDonald y Peter Firstbrook, 28 de enero de 2016; https://www.gartner.com/document/2665515 iii Fuente: Gartner, Best Practices and Success Stories for User Behavior Analytics, de Avivah Litan, 13 de julio de 2016; https://www.gartner.com/document/2998124 Siga a Forcepoint en Redes SocialesFacebook: https://www.facebook.com/ForcepointLLC/LinkedIn: https://www.linkedin.com/company/forcepointTwitter: https://www.twitter.com/forcepointsecInstagram: https://www.instagram.com/forcepoint

**Datos de contacto:**

ARTURO MARTINEZ

5527680410

Nota de prensa publicada en: [https://www.mexicopress.com.mx/forcepoint-anuncia-nueva-solucion-que-detecta](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Telecomunicaciones Software Ciberseguridad Otras Industrias



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)