Micro Focus

Administración del Acceso Autorizado a la Información Financiera

Elías Kayal
Director Comercial – CA&C
elias.kayal@microfocus.com
Septiembre, 2017

TECNASA
Es confianza

MICRO FOCUS

Agenda

- Introducción a Micro Focus
- Gestión de accesos a la información - Problemática de Seguridad
  - Indicadores empresariales de Seguridad
  - Análisis de los Ataques
  - Los Hackers han avanzado en sus técnicas
  - Relaciones de la identidad
  - Beneficios de la gestión de identidades y accesos

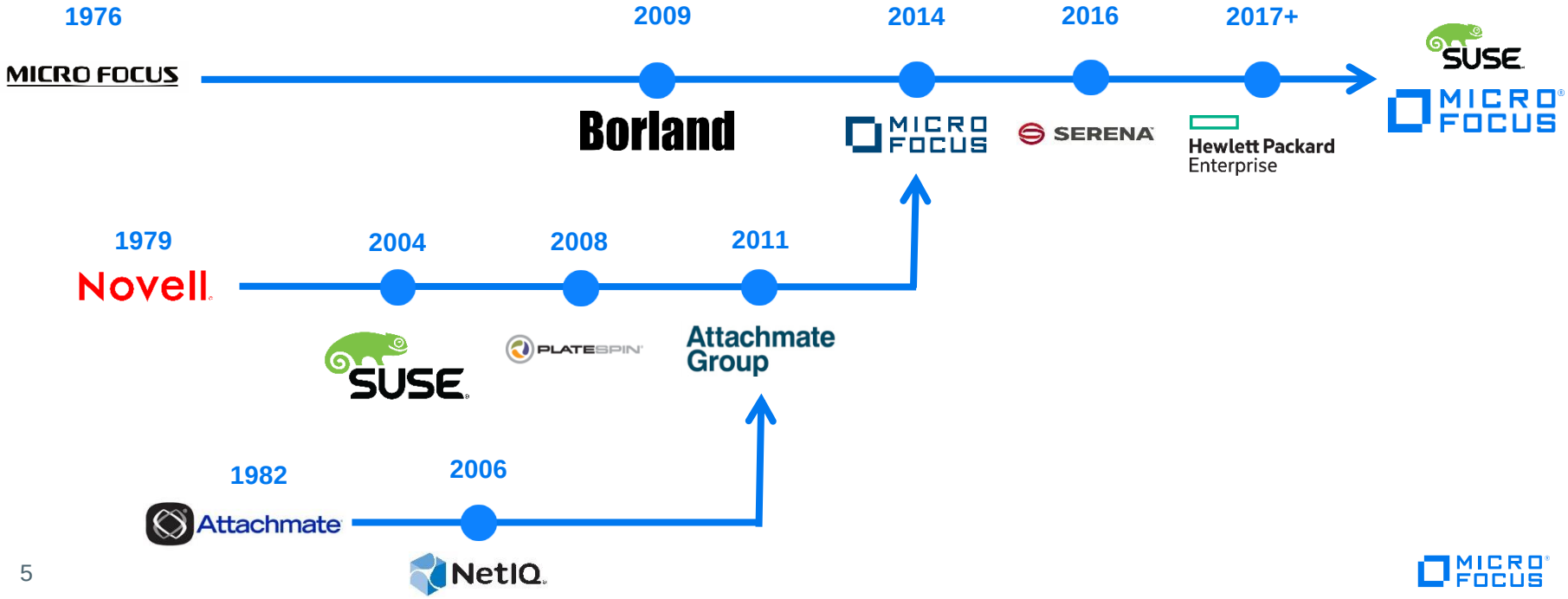
Introducción a Micro Focus

¿Quién es Micro Focus?

Micro Focus es una empresa que ofrece soluciones de software innovadoras que permiten a las compañías desarrollar, probar, desplegar, evaluar y modernizar aplicaciones empresariales vitales para el negocio.

Micro Focus es una compañía global con 40 años de experiencia en el mercado. Ayuda a todos sus clientes a innovar más rápido, con menor riesgo.

¿De dónde venimos?



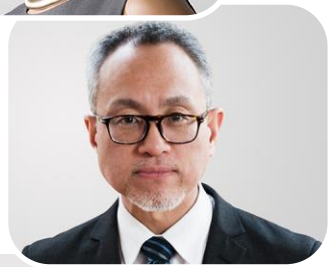
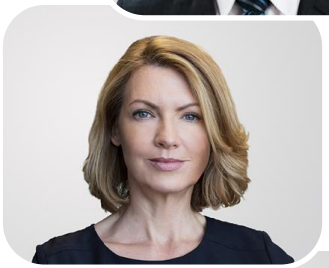
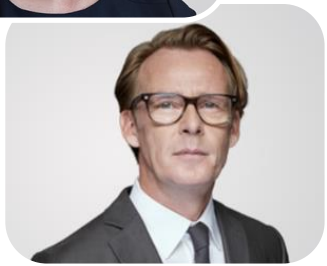
MICRO FOCUS

Gestión de accesos a la información

Problemática de Seguridad

Indicadores empresariales de Seguridad

- “Es necesario involucrar al negocio en decisiones de riesgo.”
- “La experiencia del usuario final es esencial.”
- “¿Cómo podemos reducir el pensum de cumplimiento sin incrementar el riesgo?”
- “¿Cómo ofrecemos servicios a otras partes de la organización?”
- “Debe mostrar un éxito casi inmediato…”
- “Debe contemple nuevas tecnologías basadas en la nube, la seguridad y posibles riesgos relacionados.”

Incidentes de seguridad relacionados a tecnologías, junto con el continuo aumento en la sofisticación de la delincuencia cibernética, está impulsando la demanda de mejoramiento de la gestión de identidades y accesos, además de nuevas soluciones de seguridad

CUMPLIMIENTO REGULATORIO

68% de los los líderes en seguridad consideran que "lograr y mantener el cumplimiento normativo" es una prioridad crítica. (Forrester 2017)

ADOPCION DE LA NUBE

59% adaptación a modelos de negocio basado en nube híbrida. (Forrester 2017)

TRANSFOR-MACIÓN DIGITAL

48% de los CIO esperan un mayor negocio a través de canales digitales. (Gartner 2016)

DELINCUENCIA CIBERNÉTICA

38% de aumento en crímenes cibernéticos (IDG 2015 v 2014)

TECNOLOGÍA DE CONSUMO

“Aunque las tecnologías de consumo crean nuevos riesgos para la empresa, eliminar su uso es cada vez más difícil e impráctico ", dijo Rich Mogull, Vicepresidente de Investigación de Gartner.

¿Qué es la violación de datos?

La violación de datos indica un incumplimiento de la seguridad que conduce a la destrucción, pérdida, alteración, divulgación no autorizada o acceso a datos personales transmitidos, almacenados o procesados. Es decir, una violación es algo más que la pérdida de datos personales

Por ejemplo:

Un hospital podría ser responsable de un incumplimiento de datos personales si el registro de salud de un paciente se accede inapropiadamente debido a la falta de controles internos apropiados.

ico.
Information Commissioner's Office

Cumplimiento

¿Estamos cumpliendo con todos los mandatos aplicables? ¿Cómo reducimos el costo del cumplimiento?

Violación de datos

¿Estamos haciendo lo suficiente para controlar el acceso a la información sensible? ¿Entendemos nuestro entorno de amenazas?

Nube

¿Cómo se está gestionando el riesgo de esquemas en la nube?

Riesgo

Internet de las cosas (IoT)

¿Cómo aprovechamos de forma segura el IoT?

Móvil

¿Es seguro el uso de dispositivos móviles?

Riesgo de terceros

¿Estamos haciendo lo suficiente para gestionar el acceso de socios, contratistas y clientes?

Entrega de Servicios

¿Estamos haciendo lo suficiente para garantizar la disponibilidad y la seguridad de los datos?

Red

¿Estamos asegurando la seguridad de la red?

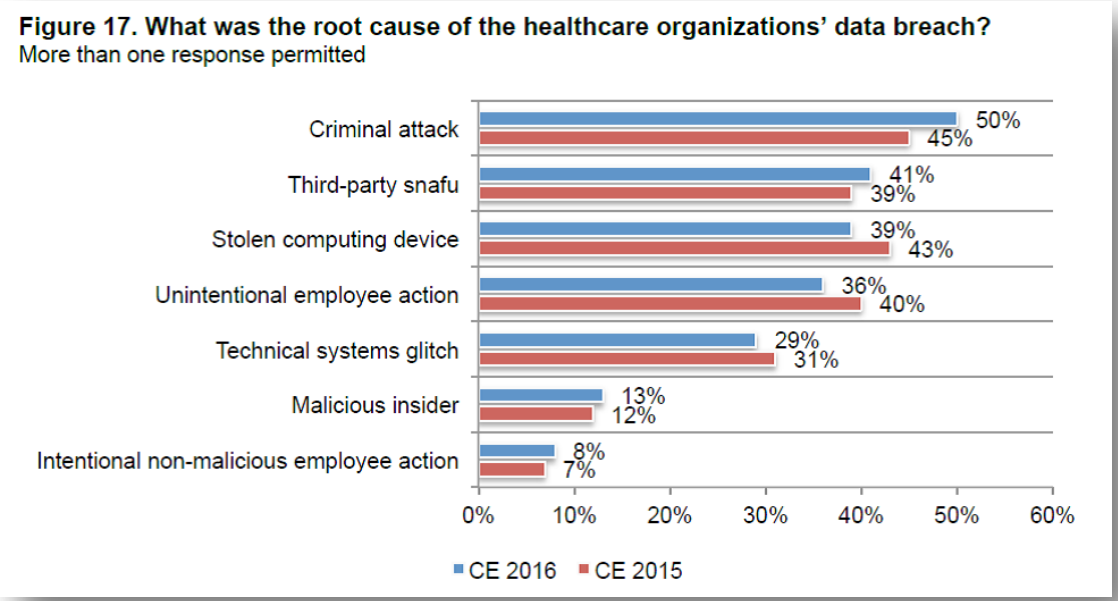
MICRO FOCUS

40%

De las violaciones de seguridad y robo de datos han sido a causa de usuarios internos

Fuente: Forrester Research, “Understand the State of Data Security and Privacy: 2015 - 2106 ”

Análisis de los Ataques



Robos de:

Archivos | Estados Financieros | Datos de Asegurados | Pagos | Calendarios | Correos | Análisis Mensual | Nómina | Estatus Mensual

Fuente: Ponemon Institute, "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data", May 2016.

Los Hackers han avanzado en sus técnicas

Los Hackers quieren adueñarse de sistemas importantes y de credenciales privilegiadas. Y lo logran principalmente por medio de:

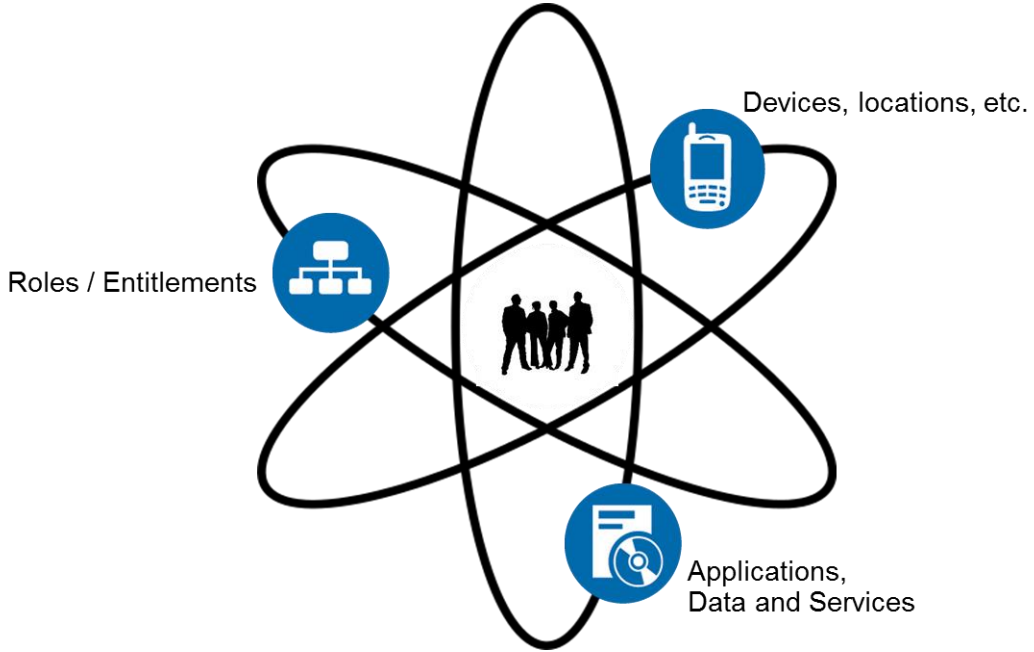
Spearfishing
Usando correos para robar datos y son dirigidos específicamente a un usuario

Ingeniería Social
Son preguntas o trucos para obtener información confidencial en una conversación.

Malware Personalizado | APT
Crear software malicioso específico para una empresa o una red. Puede estar “dormido” mucho tiempo

Relaciones de la identidad

¡Más importante que nunca!



Conoces…

- ¿Quién tiene acceso a qué en su organización?
- ¿Cuál es el propósito, valor y riesgo de aplicaciones, cuentas, grupos y permisos?
- ¿En qué usuarios o aplicaciones debe centrarse?
- ¿Si tienen los usuarios accesos adecuados?
- ¿Cómo identifica oportunamente a usuarios que estén violentando políticas de segregación de funciones?
- ¿Si existen cuentas huérfanas?
- ¿Si las cuentas privilegiadas son mal utilizadas?

Crecimiento de la inversión proyectada en Seguridad

- IAM (Identity and Access Management), 6% CAGR (Tasa Compuesta de Crecimiento Anual) hasta 2019 (Gartner)
- Identity Governance & Administration, 7% CAGR hasta 2019 (Gartner)
- SIEM (Security Information and Event Monitoring), 8% CAGR hasta 2019 (Gartner)
- Análisis de comportamiento de las identidades, USD $200 millones para 2017.
- Privileged Account Management (Identidades Privilegiadas) - USD $500 millones en 2014, con un crecimiento anual aproximado del 32% (Gartner)
- Active Directory Management, USD $100 millones, con un crecimiento anual aproximado del 20% (Forrester)
- Advanced Authentication, 19%-30% CAGR

MICRO FOCUS

Beneficios de la Gestión de Identidades y Accesos

- Tener conocimiento de quién tiene accesos a qué aplicativos o recursos en la organización.
- Asegurar el cumplimiento.
- Mitigar el riesgo de accesos descontrolados o excesivos.
- Empoderamiento del negocio en la governanza de usuarios y accesos.
- Reducción del tiempo en el cumplimiento regulatorio a través de la mitigación oportuna de posibles riesgos que comprometan la información.
- Eliminar la penalización por incumplimiento de la normativa.
- Reducir o eliminar los procesos manuales propensos a errores y aumentar la eficiencia.

www.microfocus.com