FORCEPOINT

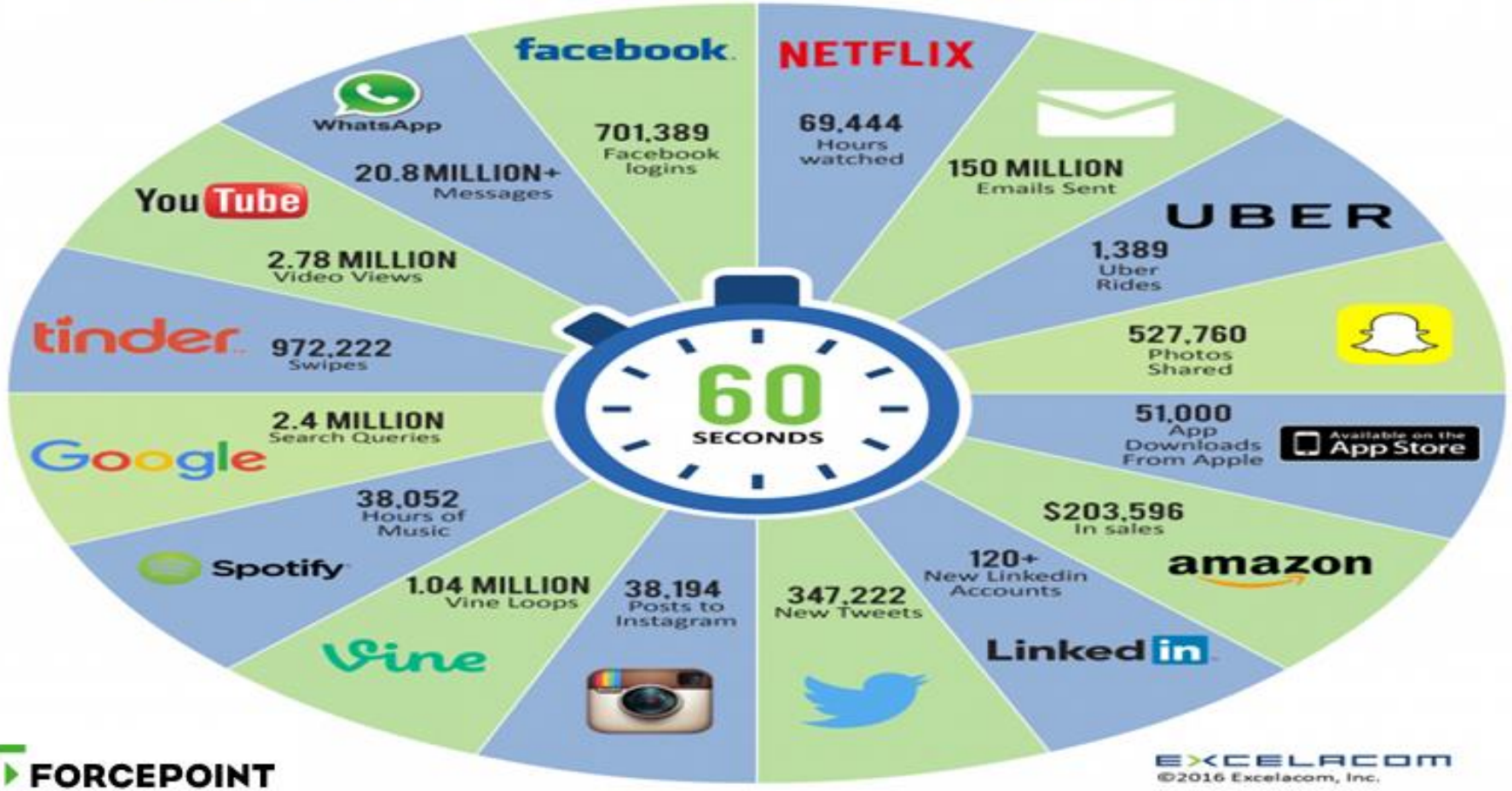
Riesgo y Amenaza Interna

Diseñando Una Seguridad Holística del Negocio basado en las personas

Pavel Orozco
Oficina del CSO
LATAM
Marzo 2017

FORCEPOINT
POWERED BY Raytheon

2016 What happens in an INTERNET MINUTE?



FORCEPOINT

EXCELACOM


La Constante del Riesgo

LA INDUSTRIA CREÓ UN ABISMO EN TORNO AL RIESGO DEL COMPORTAMIENTO DEL USUARIO

Data Loss Prevention

Insider Threat Mitigation

User Activity Monitoring

DATOS

USUARIOS

FORCEPOINT
POWERED BY Raytheon

AMENAZA INTERNA Y DATOS: Por que debe de interesarnos

- **Líder en Amenzas internas**
- **Líder en DLP**

FORCEPOINT

Protecting the HUMAN POINT

FORCEPOINT
POWERED BY Raytheon

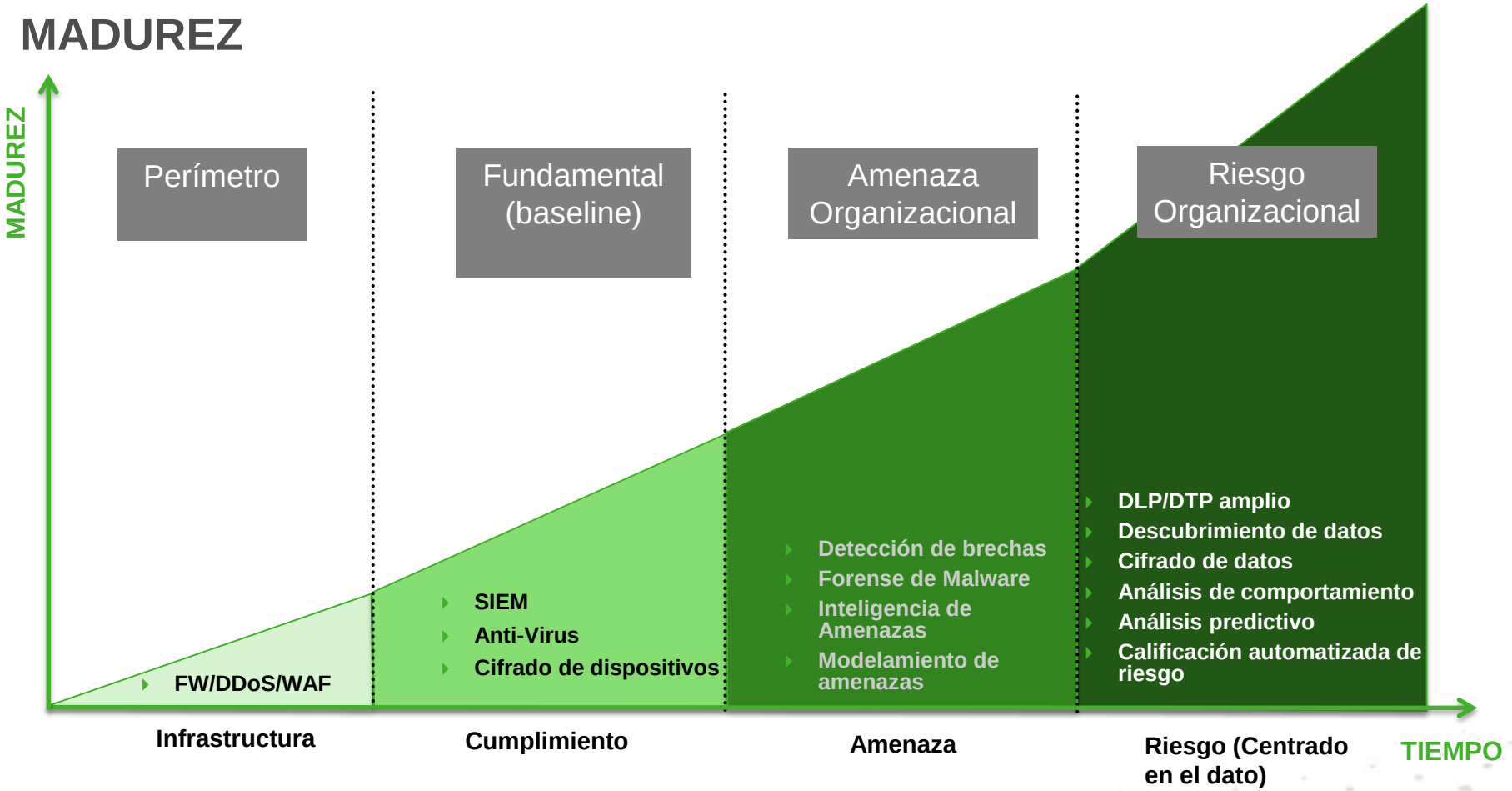
LA FUENTE MAS COMUN DE UN ATAQUE

LA IMPORTANCIA DEL CONTEXTO

Y LA VISIBILIDAD

FORCEPOINT
POWERED BY Raytheon

MADUREZ



FORCEPOINT
POWERED BY Raytheon

INSIDER THREATS

43% de las organizaciones sienten que tiene la capacidad de monitorear de manera efectiva la actividad del usuario privilegiado

63% no tiene suficiente información contextual

61% de sus herramientas generan demasiados falsos positivos

VISIBILIDAD

62% no tienen del todo confianza de tener visibilidad amplia en el acceso de los usuarios

55% están inseguros de poder correlacionar datos de múltiples fuentes, **60%** dicen que se debe a la falta de recursos

58% no tiene confianza por que no tienen visibilidad en la empresa

18% tienen muy alta confianza en tener la visibilidad necesaria

Ingeniería Social

46% creé que la ingeniería social externa, va apuntar a usuarios privilegiados para obtener permisos de acceso

48% de los encuestados dicen que los usuarios maliciosos utilizarían ingeniería social para obtener los privilegios de alguien más

Privilegios de acceso

36%

usan monitoreo del punto final para determinar si la acción tomada por el usuario era una amenaza

64%

no tienen manera de tener contexto sobre el hecho en si

FORCEPOINT
POWERED BY Raytheon

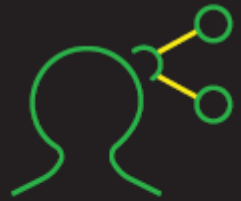
Factor Humano

74%

cree que los usuarios privilegiados tienen derecho a ver toda la información a la que tienen acceso

66%

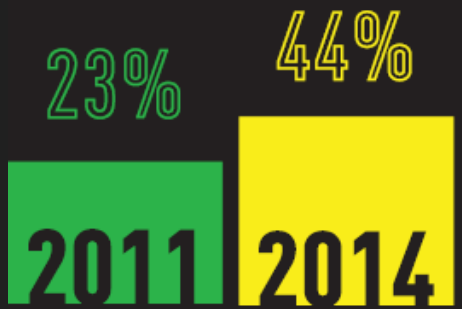
dice que el mismo personal accede a la información sensible o confidencial solo por curiosidad



58%

mencionan que las organizaciones asignan a individuos accesos mas allá de su rol y responsabilidad

PROCESO MANUAL



Utilizan procesos manuales para certificar usuarios privilegiados

VERIFICACIÓN DE ANTECEDENTES

carecen de controles de antecedentes dentro de las organizaciones antes de la emisión de credenciales con privilegios

PRESUPUESTO

59%

Tienen presupuesto asignado, pero 70% mencionan que es es igual o menor al 10% requerido

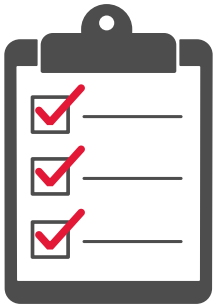
80%

de las amenazas son internas

48%

utilizan SIEM (herramientas de correlación de incidentes) para determinar si la acción es una amenaza interna

EVOLUCION DE LA PROTECCION DE LA INFORMACION



CUMPLIMIENTO

PROTECCION DE PROPIEDAD INTELECTUAL

PREVENCION DE ROBO DE INFORMACION

MITIGACION DE AMENAZA INTERNA

2003

- Data Fingerprints
- Pre-defined Compliance Policies
- Endpoint fingerprints

2010

- OCR and Cumulative (DRIP) DLP
- Apple OS X DLP endpoint
- Counter-Malicious Capabilities

2015

- Data Theft Prevention **Next Gen DLP**
- **SureView®** Insider Threat

UNA PLATAFORMA UNIFICADA, FOCO EN NUBE PARA RESGUARDAR **USUARIOS**, **DATOS** & **REDES**

- Modular
- Se integra con infraestructura
- Distribución Flexible

FORCEPOINT
POWERED BY Raytheon

PROTECTING THE HUMAN POINT

¡Gracias!

¿Preguntas?

FORCEPOINT
POWERED BY Raytheon

