



F-Secure®

PORTFOLIO 2018

¿QUIEN ES F-SECURE?



F-SECURE en pocas palabras



F-Secure®

- Fundada en **1988**.
- Más de **1.000 empleados** en 25 oficinas en todo el mundo.
- Beneficios de **\$170 millones** y EBIT de \$20 millones en 2016.
- Cotizando en **NASDAQ OMX**, Helsinki.
- Negocios en más de **100 países**, trabajando con más de **200 operadores** y **miles de partners**.
- Con decenas de millones de clientes de consumo y más de **100.000 compañías** alrededor del mundo.
- Participa en **más investigaciones** sobre Ciberataques que cualquier otra compañía del mercado.

PANORAMA ACTUAL DE CIBERSEGURIDAD



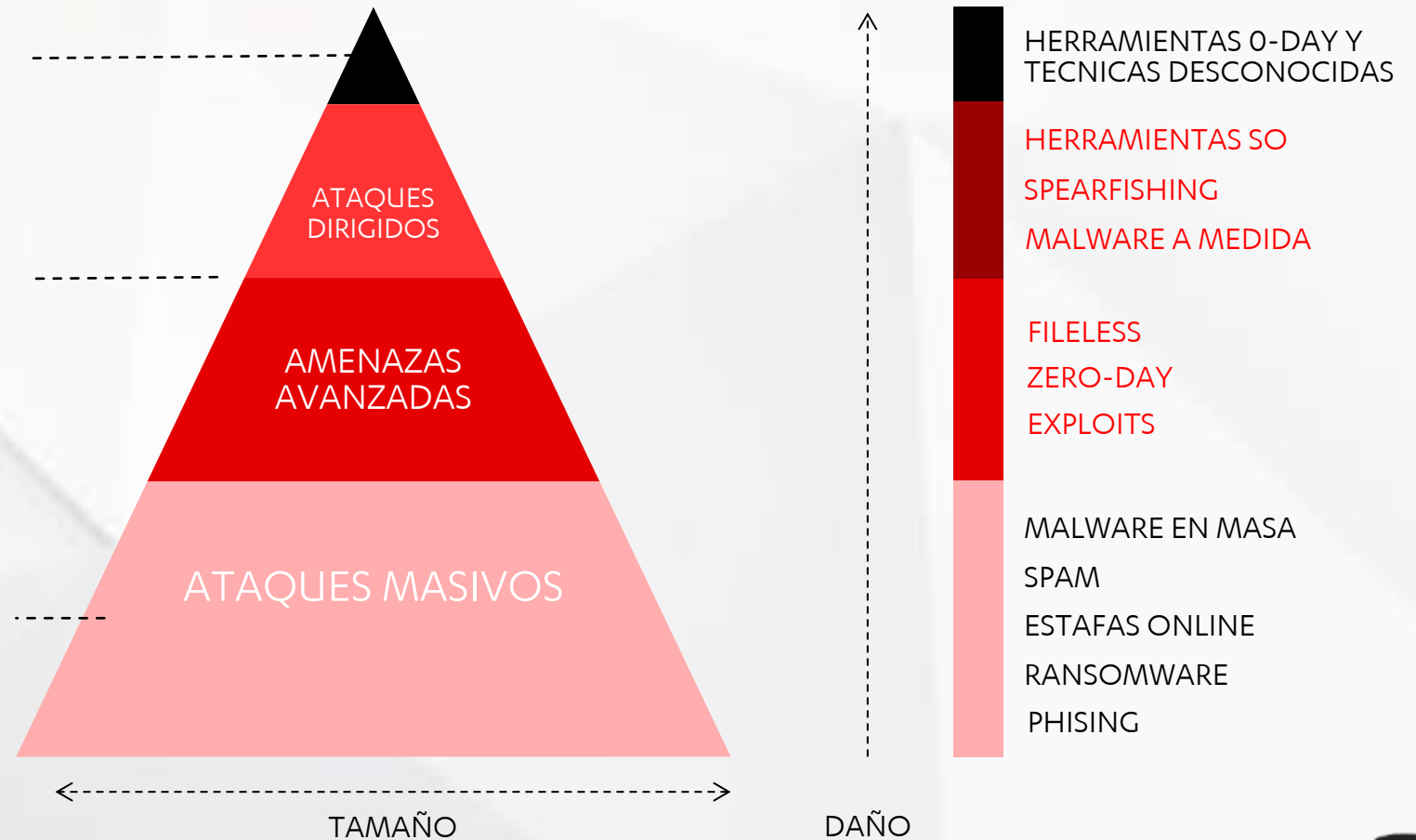
ENTENDIENDO EL ESCENARIO DE CIBERAMENAZAS

ESTADOS NACIONALES

Casi imposibles y **demasiado caros** de realizar. Aquellos que realizan estos ataques son los que no pueden permitirse no hacerlos.

Con la **mejora de las habilidades de los atacantes**, la prevalencia de **ataques sin malware** y la creciente **automatización** de los ataques avanzados, las empresas están adoptando medidas de seguridad avanzadas

Punto prioritario debido al **alto número** y al **impacto sobre las operaciones** del día a día, pero debe acotarse de la manera más eficiente y rápida posible



INTEGRATED SECURITY

VULN. MGMT

GATEWAY

EPP

EDR / MDR

TTP CATEGORIES

Recon
Delivery
Defense Bypass
Exploitation
Discovery
Migration

TTP CATEGORIES

Delivery
Defense Bypass
Phishing

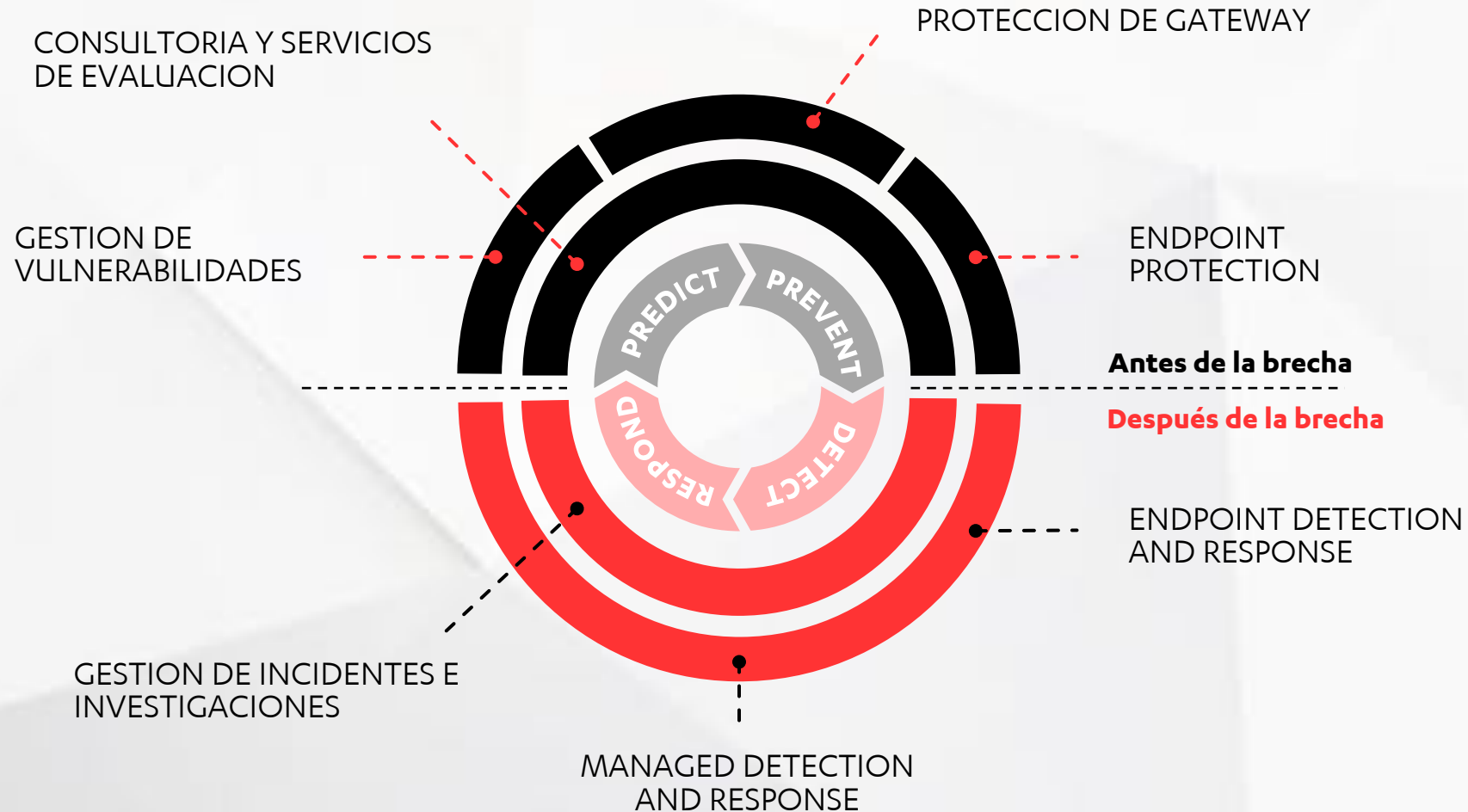
TTP CATEGORIES

| | |
|------------------|--------------|
| Recon | Exploitation |
| Delivery | Execution |
| Defense Bypass | Persistence |
| Credential Theft | Discovery |
| P. Escalation | Migration |

TTP CATEGORIES

| | |
|----------------------|------------------|
| Persistence | Discovery |
| Privilege Escalation | Lateral Movement |
| Defense Evasion | Execution |
| Credential Access | Collection |
| Exfiltration | C&C |

PORTFOLIO DE SEGURIDAD GESTIONADA



RADAR



F-Secure.

GESTIONE LAS **VULNERABILIDADES CRITICAS** DE SU NEGOCIO

F-Secure Radar es una plataforma de escaneo y **gestión de vulnerabilidades** lista para usar.

Le permite identificar y administrar amenazas **internas y externas**, informar de riesgos y cumplir con las regulaciones actuales y futuras (como **PCI DSS** y conformidad con **GDPR**).

Le permite dar visibilidad sobre el **Shadow IT**: para conocer su superficie de ataque completa y responder a las vulnerabilidades críticas asociadas con las amenazas de ciberseguridad.



DESPLIEGUE

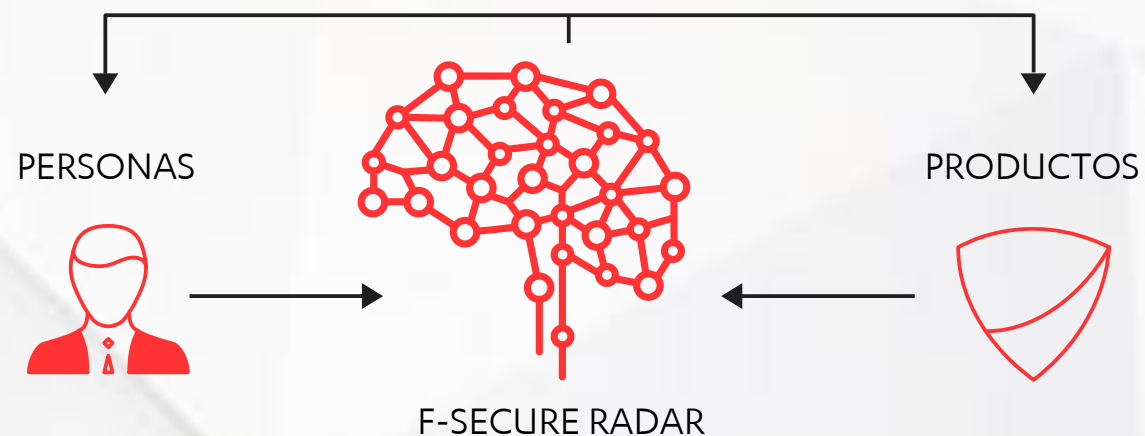
F-SECURE RADAR **CLOUD**

Lance escaneos desde la nube como un verdadero SaaS con nodos de escaneo ya incluidos

F-SECURE RADAR **PRIVATE**

Gestión completa on-premise donde todo está detrás de su firewall

TECNOLOGIA Y EXPERIENCIA DE PRIMERA CLASE



Radar no es sólo software, es la combinación de tecnología avanzada y aportes de expertos en seguridad sobre la gestión de vulnerabilidades.

Nuestros analistas trabajan 24/7 en todo el mundo para protegerlo de las amenazas más recientes.

MODELO DE VENTA SENCILLO

BENEFICIOS

- Número ilimitado de Scan Nodes
- Número ilimitado de escaneos contra los sistemas licenciados
- Número ilimitado de usuarios
- Sin restricciones de escaneos

BENEFICIOS

- Sin limitaciones de funcionalidades
- Acceso a todos los motores de escaneo
- Acceso a la API de Radar
- Sin costes ocultos

PRECIOS

- Basada en el número de IP's escaneadas
- Descuentos por volúmenes

PROTECTION SERVICE FOR BUSINESS



F-Secure.

VISION GENERAL

API DE GESTION

Integración con SIEM, RMM o cualquier otra herramienta de auditoría, gestión o informes.



PORTAL DE GESTION

Diseñado para acelerar la gestión de seguridad y para proporcionar una mejor visibilidad y control sobre todos sus endpoint.



ESTACIONES

Suite de seguridad galardonada para Windows y Mac, que incluye gestión de parches.



DISPOSITIVOS MOVILES

Seguridad y control para Dispositivos iOS & Android, Con MDM, VPN y Anti-Malware.



CONTRASEÑAS

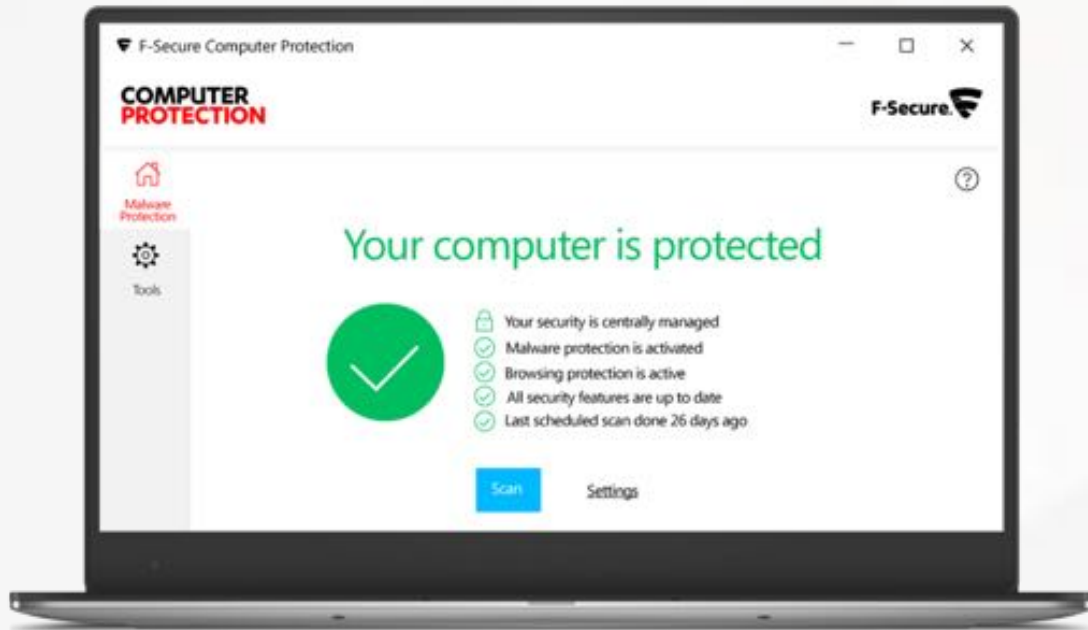
Gestor de contraseñas seguras, que ayuda a prevenir el uso de contraseñas débiles o reusadas.



SERVIDORES

Seguridad moderna y potente para sus servidores Windows, Linux y Citrix.





DEEPCUARD 6



DATAGUARD



THREAT INTELLIGENCE



ADVANCED WEB PROTECTION



APPLICATION CONTROL



DEVICE CONTROL



PATCH MANAGEMENT



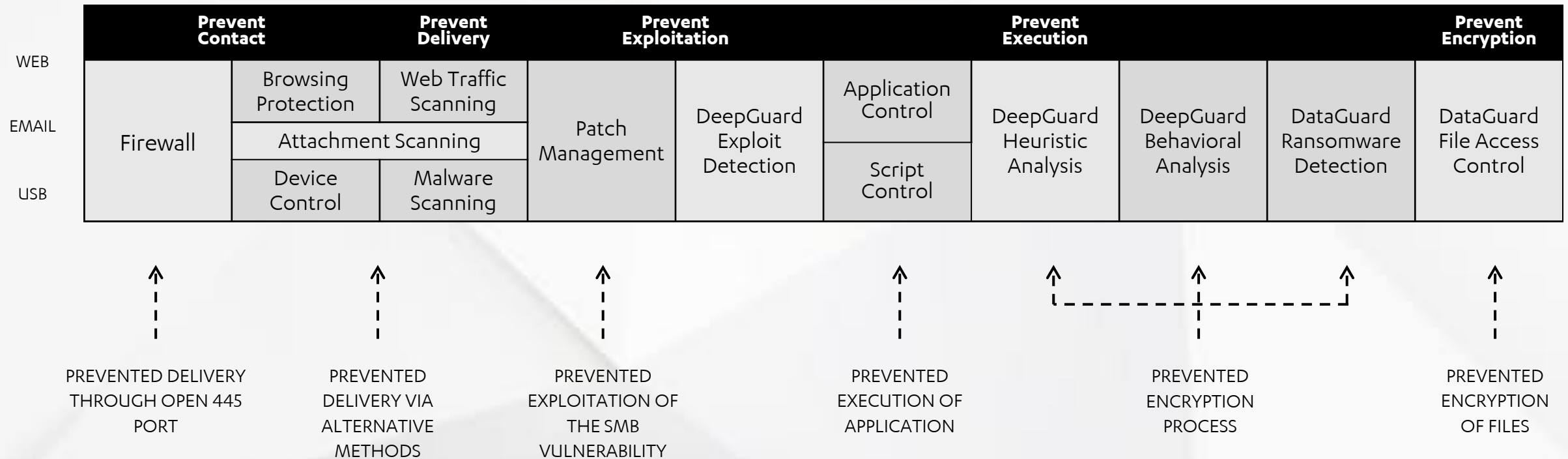
MANAGED FIREWALL



MULTI-ENGINE ANTI-MALWARE

LAYERED PROTECTION

CASE: WANNACRY





MOBILE
VPN



APPLICATION
PROTECTION



BROWSING
PROTECTION



MANAGED
ANTI-THEFT



SECURITY
MONITORING



PASSCODE
ENFORCEMENT



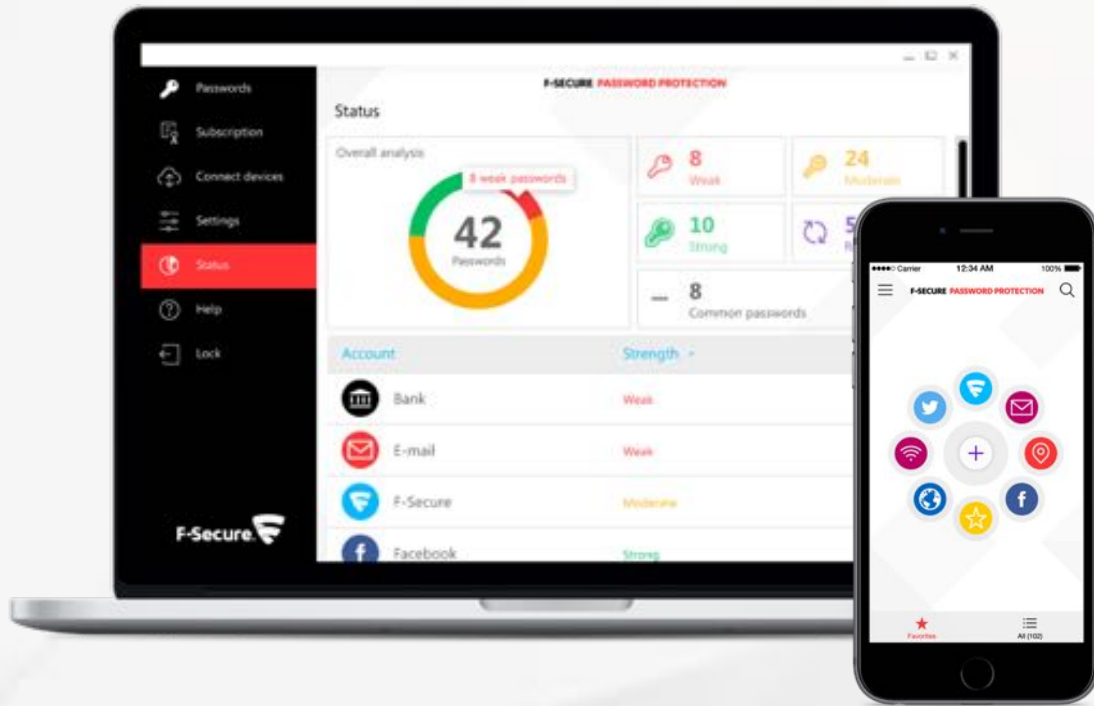
FLEET & DEVICE
INFO



TRACKING
PROTECTION



VIRTUAL
LOCATION



PASSWORD
GENERATOR



PASSWORD
MANAGER



AES-256
ENCRYPTION



PASSWORD
SYNCHRONIZATION



STRENGTH
ANALYSIS



LOCAL
STORAGE



CENTRAL
DEPLOYMENT



USER
FRIENDLY

BUSINESS SUITE



F-Secure.

BUSINESS SUITE PREMIUM



SOLUCIONES DE ALTA CALIDAD





Best Solution

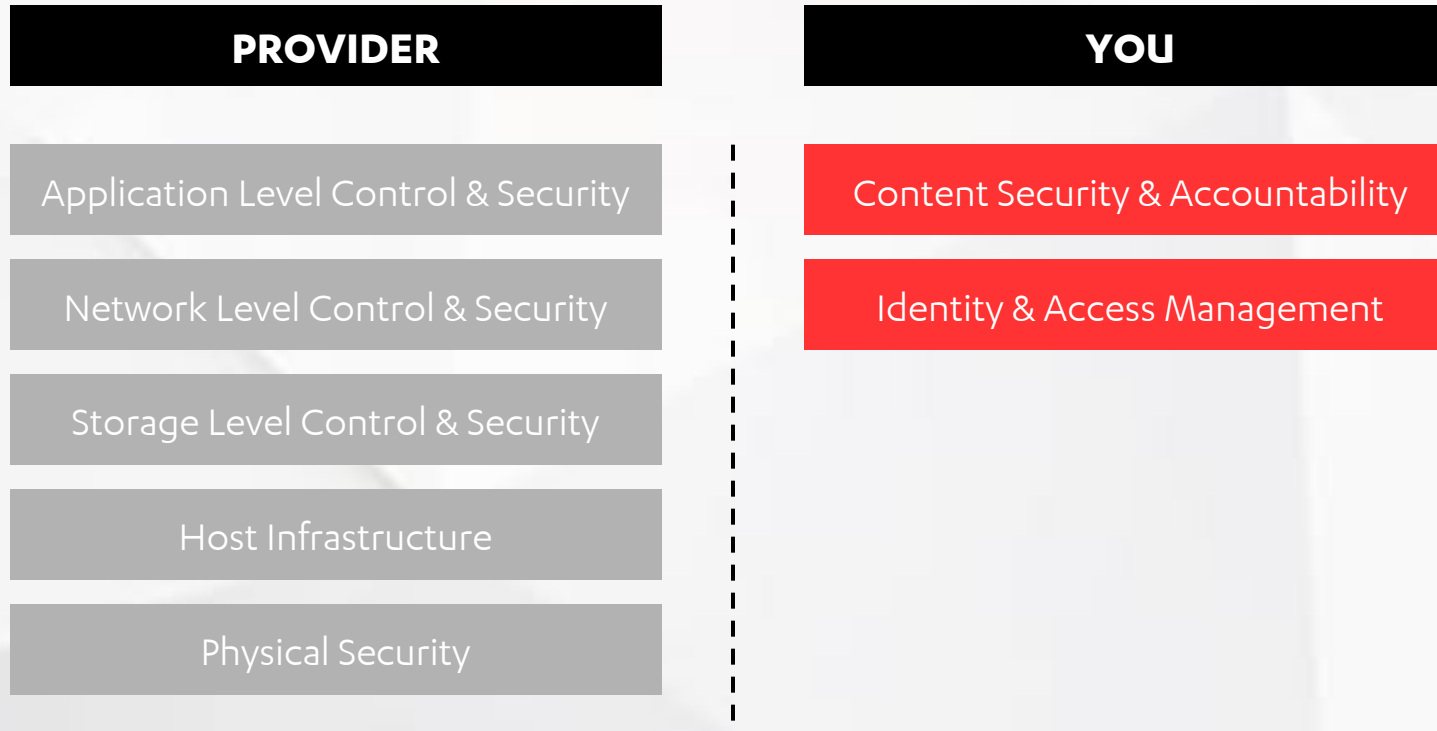
100% protection
rate against ransomware

CLOUD PROTECTION FOR **SALESFORCE**



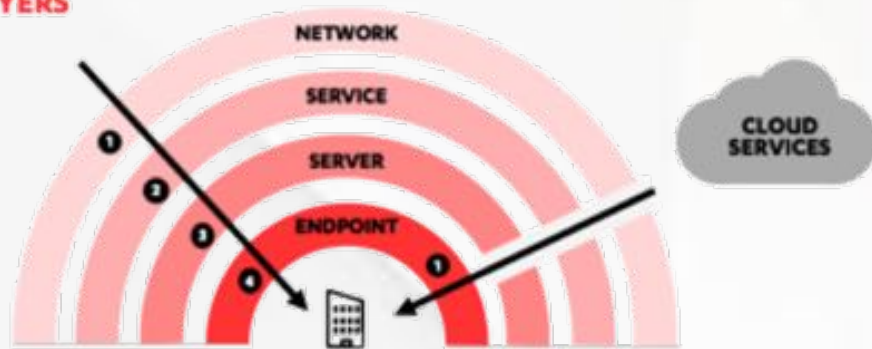
F-Secure.

SHARED RESPONSIBILITY MODEL

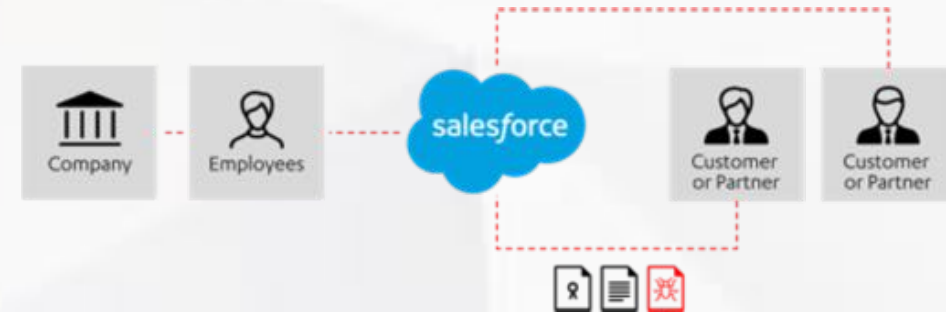


EL PROBLEMA TIENE DOS DIMENSIONES

TRADITIONAL
SECURITY LAYERS



SEGURIDAD LIMITADA
EN EL
VECTOR CLOUD



NO PUEDES GARANTIZAR
LA SEGURIDAD EN
CONTENIDOS EXTERNOS

COMPLEMENTO A LA SEGURIDAD DE SALESFORCE

F-SECURE

F-SECURE CLOUD PROTECTION

Real-Time Threat
Intelligence

Multi-Engine
Antivirus

Smart Cloud
Sandboxing

Reporting and
Auditing Service

Security Analytics
Service



SALESFORCE CLOUD

PREMIUM SERVICES

Shield
Platform Encryption

Shield
Event Monitoring

Shield
Field Audit Trail

+

PARTNER SERVICES

F-Secure
Cloud Protection

APPLICATION SERVICES

Identity & Single
Sign On

Password
Policies

Two Factor
Authentication

User Roles &
Permissions

Field & Row
Level Security

NETWORK SERVICES

HTTPS
Encryption

Penetration
Testing

Advanced
Threat Detection

Secure
Firewalls

IP Login
Restrictions

INFRASTRUCTURE SERVICES

Secure Data
Centers

Backup and
Disaster Recovery

Real-Time
Replication

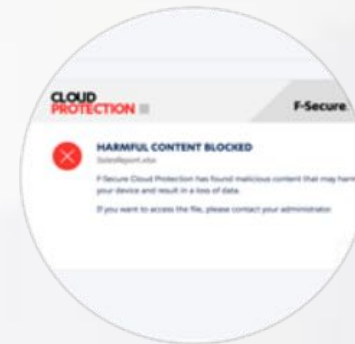
Third Party
Certifications

Customer
Audits

CLOUDPROTECTION FOR **SALESFORCE**

3. ANALIZAR

Se realiza un análisis en diferentes etapas del contenido externo, basándose en los distintos perfiles de riesgo.



1. CONTENIDO

La solución monitoriza el uso de archivos, enlaces y correos electrónicos sin obstaculizar el uso normal de Salesforce.

2. SALESFORCE CLOUD

El contenido se intercepta en Salesforce y se somete a un proceso patentado de análisis y detección de amenazas en F-Secure Security Cloud.

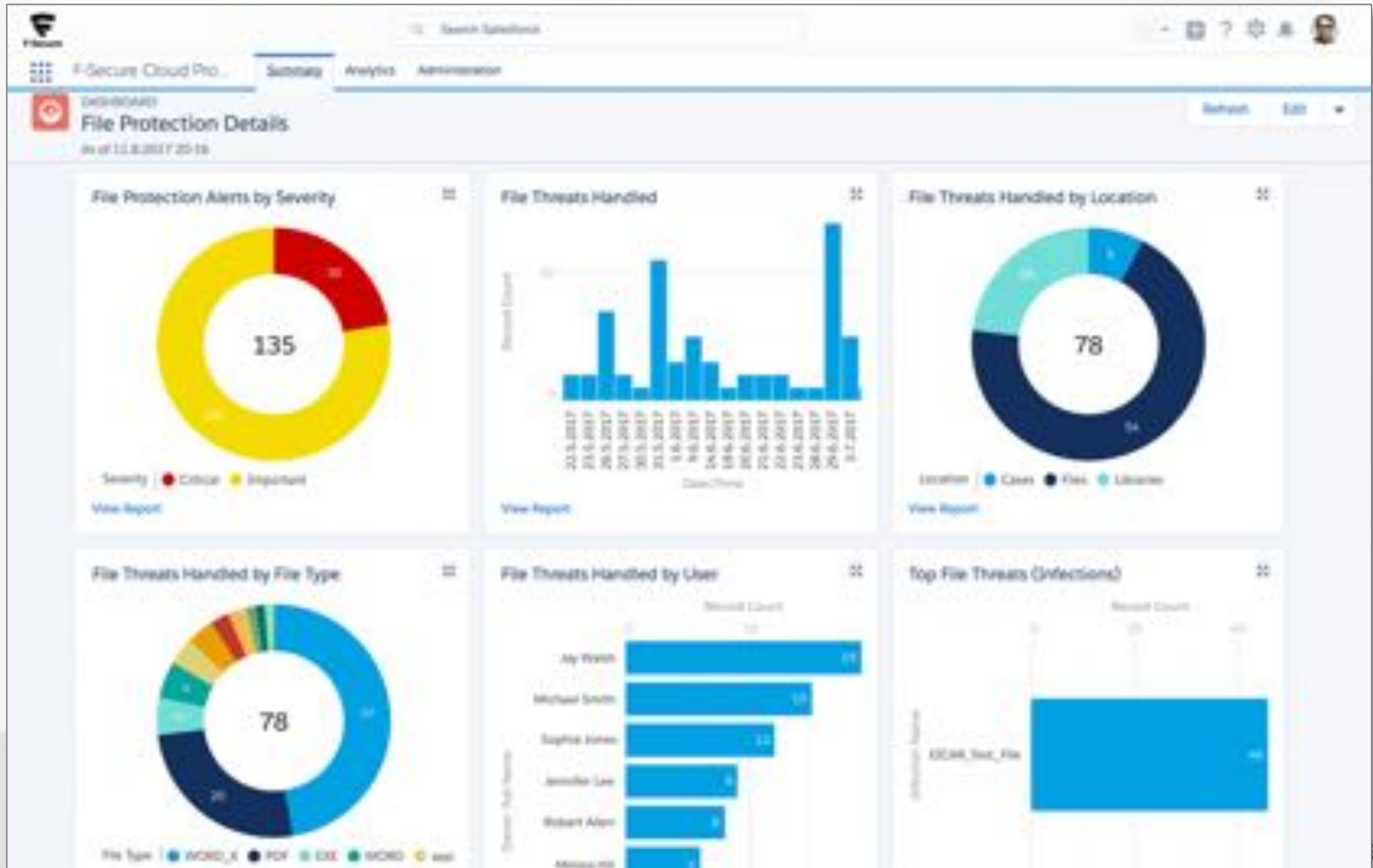
4. DETECCIÓN

El contenido malicioso se bloquea automáticamente, se evita su uso posterior y se le dice al usuario qué hacer a continuación.

5. RESPONDER

Gracias a informes completos, análisis de seguridad y huellas de auditoría completas, los administradores responden al incidente de manera eficiente.

VISIBILIDAD COMPLETA





F-SECURE

**RAPID DETECTION &
RESPONSE SERVICE**

**DE MEDIA LLEVA
100 DIAS
DETECTAR UNA BRECHA**

Source: Gartner 2017

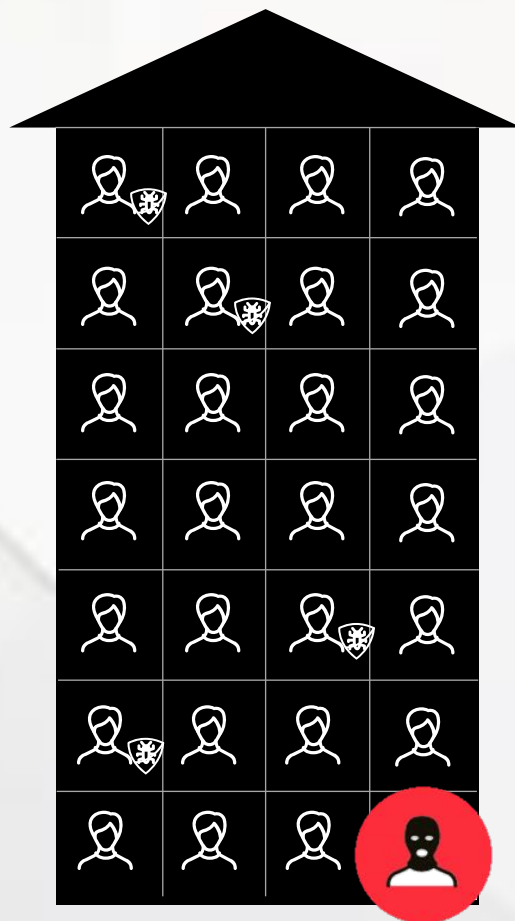
99,9 % HACEN POCO DAÑO

0,1 % GRAN IMPACTO



Habitualmente bien cubiertos

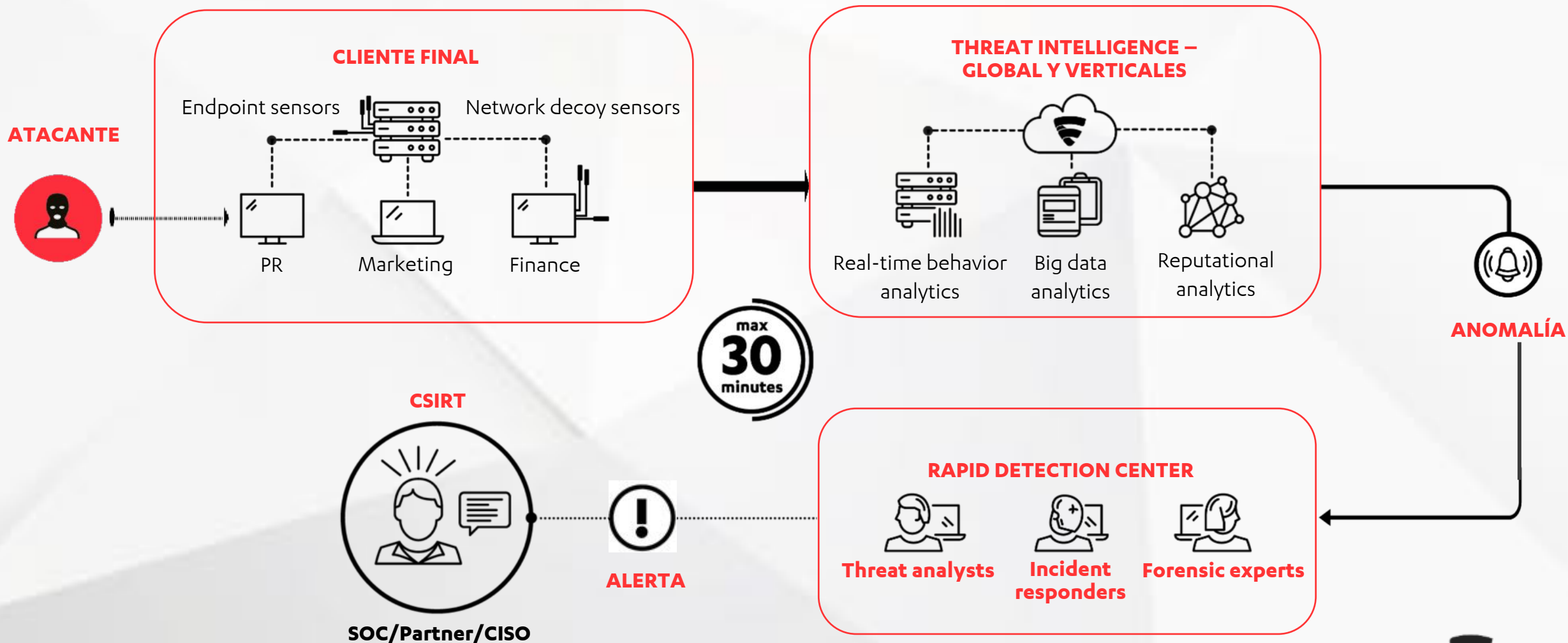
- Commodity threats
 - Machine conducted attacks
 - Malware, como ransomware etc.
 - Spam y campañas de phishing
 - >100 millones de nuevas muestras de malware cada año(AV-TEST database)
- Abordados por la seguridad preventiva:
 - Firewall
 - Email security
 - End-point protection
 - Otras soluciones preventivas



Habitualmente al descubierto

- Ciberataques avanzados y dirigidos
 - Human conducted phishing & exploit (email como vector)
 - Uso de elementos del Sistema operativo (PowerShell, WMIC, Service Commands)
 - Uso de herramientas de administración remota (RAT) y herramientas de hacking (Orcus, Litemanager, VNC, Mimikatz)
 - Tráfico oculto hacia servidores C&C (Office365, GMail, HTTPS)
- Abordados por soluciones de detección y respuesta:
 - Managed Detection and Response (MDR)
 - Endpoint Detection and Response (EDR)
 - Incident Response Services

LA COMBINACIÓN DE MAN & MACHINE



DOS ENFOQUES TOTALMENTE DIFERENTES

PREVENCION

Dilema del defensor:

Acertar siempre, el atacante sólo necesita acertar una vez.

Los productos pueden ser comprados y probados por el atacante.

DETECTION & RESPONSE

Dilema del atacante:

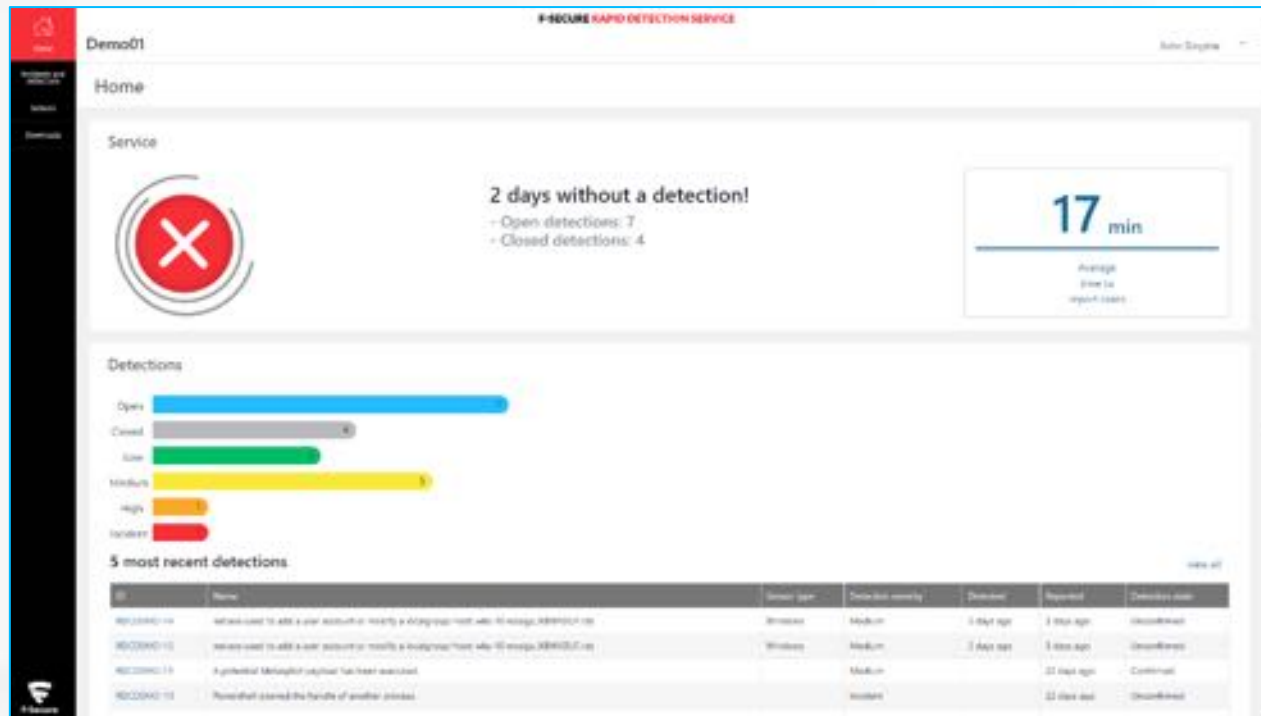
Acertar siempre, el defensor sólo necesita acertar una vez.

Los servicios no pueden ser comprados y probados por el atacante.



RAPID DETECTION SERVICE

DASHBOARD, SENSORES & ALERTAS



Thu 2017-10-19 14:46

RD Rapid Detection Center <rdc@f-secure.com>
 [RDC-4819][High][F-Secure] A process downloaded a large amount of Active Directory data

To

F-SECURE RAPID DETECTION SERVICE F-Secure

Incidents & Detections

Dear RDS Customer,

Your detection has been updated. For more information please visit RDS Portal.

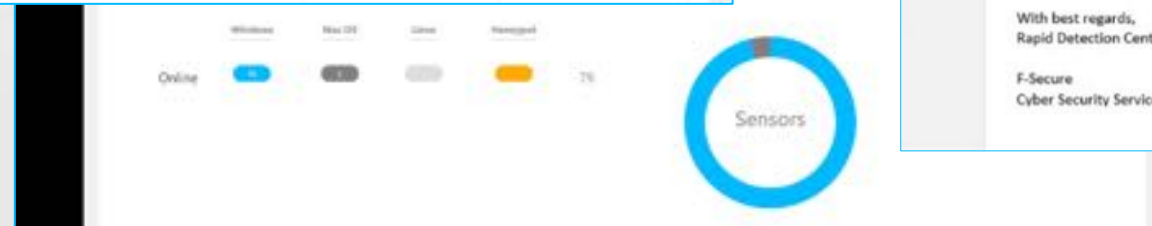
ID: RDC-4819 ([view ticket](#))

Name: [F-Secure] A process downloaded a large amount of Active Directory data, this can be an attacker mapping the network and users. Host: FS18.F-Secure.com Secure.com
Detection severity: High
Detection status: Confirmed

Detected: 2017-10-19 15:30:00.0
Reported: 2017-10-19 15:31:05.319
Host: FS18.F-Secure.com

With best regards,
 Rapid Detection Center

F-Secure
 Cyber Security Services

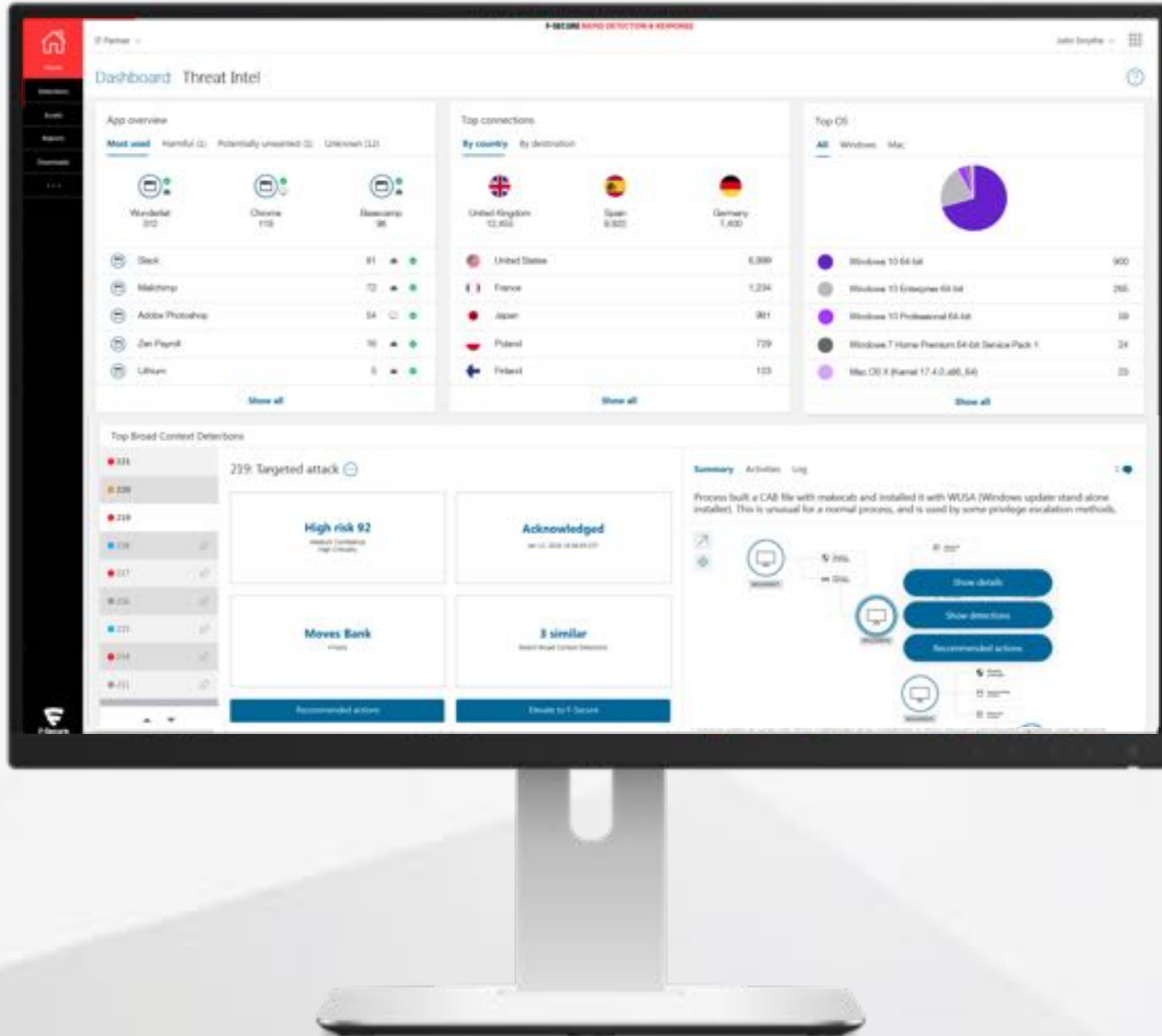




F-SECURE

**RAPID DETECTION &
RESPONSE**

INTRODUCING F-SECURE RAPID DETECTION & RESPONSE



VISIBILITY

Immediate contextual visibility into IT environment and security status

DETECTION

Protect your business and its sensitive data by detecting data breaches quickly

RESPONSE

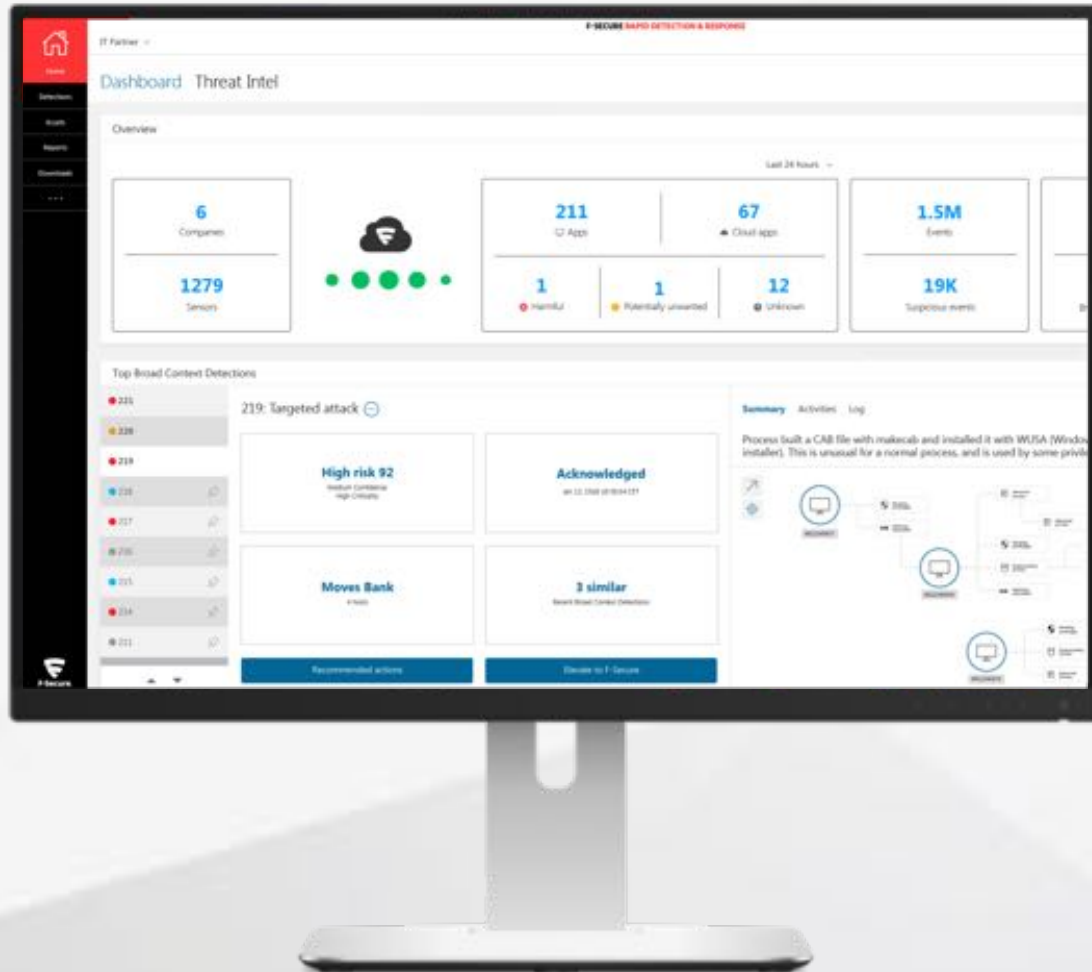
Respond swiftly with the help of automation and guidance whenever under attack

F-SECURE RAPID DETECTION & RESPONSE



F-SECURE RAPID DETECTION & RESPONSE

KEY FEATURES



BROAD CONTEXT
DETECTION™



INCIDENT
MANAGEMENT



GUIDANCE
TO RESPOND



APPLICATION
INVENTORY



CENTRALIZED
MANAGEMENT



HOST
ISOLATION



THREAT
INTELLIGENCE*



AUTOMATED
RESPONSE*



API
MANAGEMENT
INTEGRATION*

*COMING SOON

REGULACION GENERAL DE PROTECCION DE DATOS

GDPR



F-Secure.

REQUISITO DE PROCESAMIENTO SEGURO (ARTICULOS 5, 32)

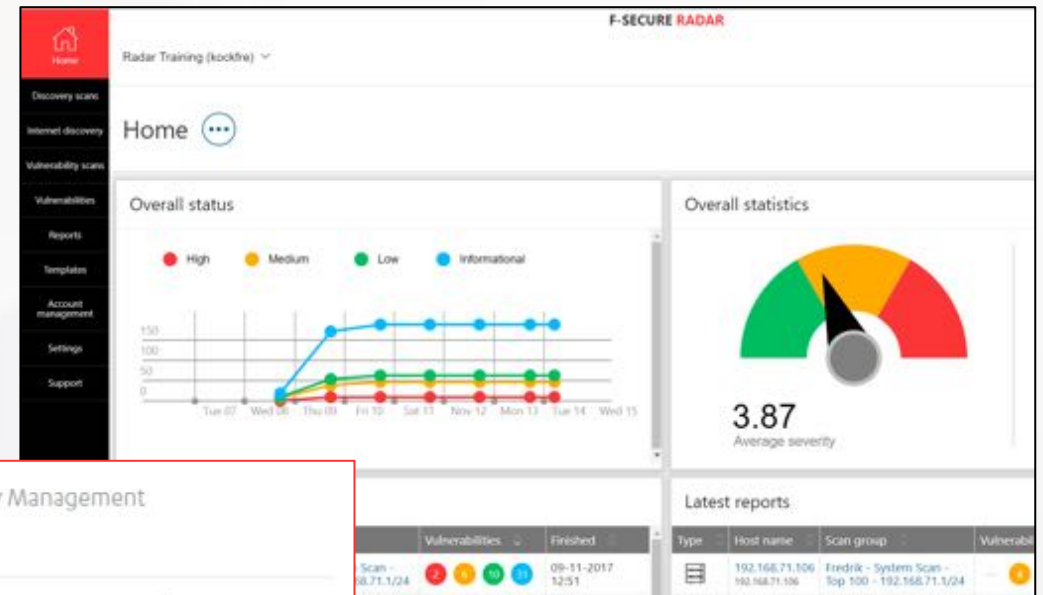
- GDPR requiere que los **datos se procesen** de una manera que **garantice la seguridad** adecuada utilizando **medidas técnicas** apropiadas.
- Esto incluye la protección contra el **procesamiento no autorizado** o **ilegal** y **contra la pérdida, destrucción o daño** accidental.


- El **Malware y Ransomware** causa destrucción no autorizada y pérdida de datos.
- **Los dispositivos móviles** son cada vez más atacados. La confidencialidad está en riesgo, **cuando usan redes públicas**. Pérdida de datos en caso de que **los dispositivos sean perdidos o robados**.
- El 63% de las brechas de datos provienen de **contraseñas débiles o robadas** (Verizon DBIR 2016).
- La pérdida accidental ocurre **fácilmente a través del correo electrónico**.



REQUISITO DE PRUEBA Y EVALUACION (ARTICULOS 32, 35)

- La **GDPR** obliga a la implementación de procesos que pongan a prueba y evalúen regularmente las medidas técnicas de seguridad.
- Debes de ser capaz de **demostrar que cumples** con los requerimientos.
- **F-Secure Radar** te permite **evaluar de manera continua el nivel de seguridad de toda la superficie de ataque**, además de la generación de informes.

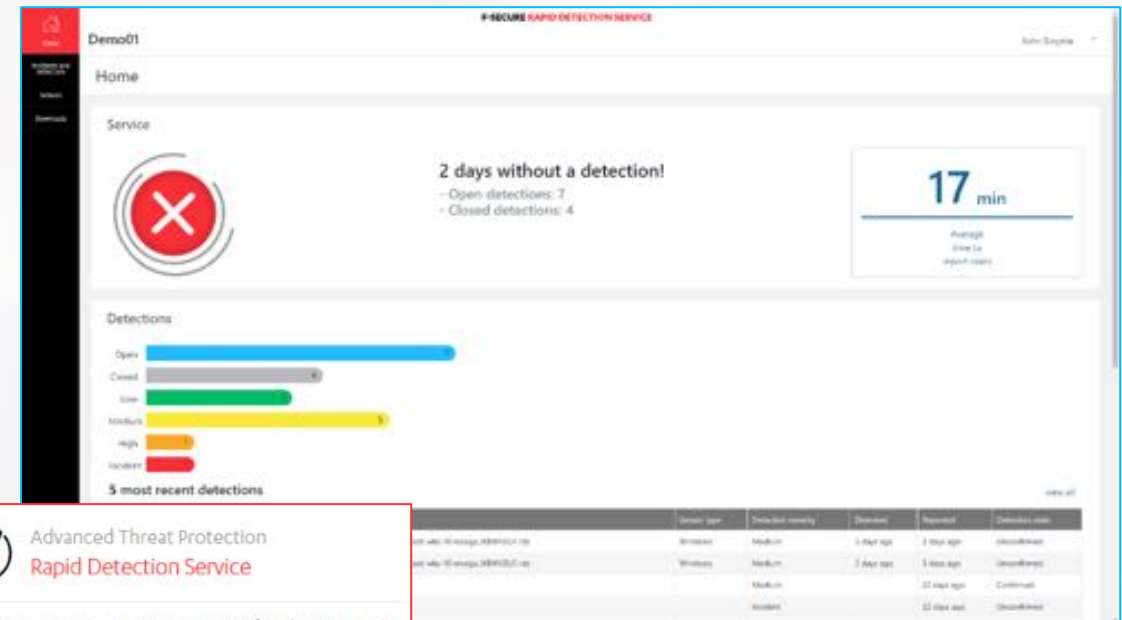


 Vulnerability Management
Radar

Turnkey vulnerability scanning and management platform.

REQUISITO DE NOTIFICACION DE BRECHAS (ARTICULOS 32, 33, 34)

- **La GDPR requiere** capacidades adecuadas de detección de violación de datos y la capacidad de notificar a DPA y sujetos de datos en un **máximo de 72 horas**.
- Debe poder **demostrar su cumplimiento** y estar preparado para las intrusiones.
- Los servicios de Detección & Respuesta de **F-Secure** se lo permiten.
- El servicio le permite saber rápidamente si el ataque implica una **violación de datos personales**.



 Advanced Threat Protection
Rapid Detection Service

Monitors your security status 24/7, alerting you of breaches within minutes with a clear action plan.



F-Secure®