FORTRA

Descubra Fortra

La nueva imagen de HelpSystems

Su aliado en Ciberseguridad.

Agenda

¿Quién es Fortra ?

- Portafolio y misión

Tendencias en protección de datos

- 3 casos de éxito

FORTRA

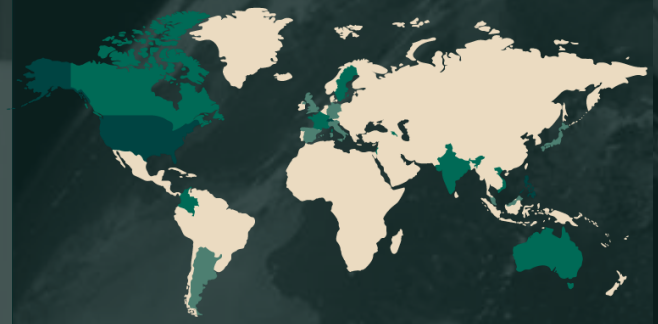
Sobre Fortra

La mayor empresa de ciberseguridad de la que tal vez no hayas oído hablar (aún)

helpsystems → FORTRA

FORTRA

Sobre Fortra



$800M+
En facturación

2,700+
Empleados
+50% en I+D

20+
Países con
presencia

30,000+
Clientes en
virtualmente todas
las industrias

FORTRA

Más de 30.000 Clientes en todas las industrias

4,6/5
SATISFACCIÓN DE NUESTROS CLIENTES
En todas las industrias

22
DE LAS 25 COMPAÑIAS TOP DE
LA LISTA FORTUNE 500

10
DE LAS 10 COMPAÑIAS TOP DE
SERVICIOS FINANCIEROS

10
DE LAS 10 COMPAÑIAS TOP DE
SECTOR DE SALUD

17
DE LAS 25 COMPAÑIAS
MÁS INNOVADORAS

IBM · MATTEL · MAYO CLINIC · Coca-Cola · Shutterfly · POLARIS · Hospital Sisters
FedEx · RICOH · STAPLES · Aflac · Borgata · nationale nederlanden · Nationwide

FORTRA

La Visión de Fortra

FORTRA

Fortra – adquisiciones de Ciberseguridad

Adquisiciones e innovación

2016

goanywhere by HelpSystems

Managed File Transfer

2019

clearswift by HelpSystems

Secure Email Gateway

coresecurity by HelpSystems

Penetration Testing

2020

titus by HelpSystems

boldonjames by HelpSystems

Data Classification

globalscape by HelpSystems

Managed File Transfer

vera by HelpSystems

Digital Rights Management

cobaltstrike by HelpSystems

Adversary Simulation

2021

filecatalyst by HelpSystems

File Acceleration

agari by HelpSystems

Email Security

PHISHLABS by HelpSystems

Digital Risk Protection

DIGITAL GUARDIAN by HelpSystems

Data Loss Prevention

digitaldefense by HelpSystems

beyondsecurity by HelpSystems

Vulnerability Management

2022

TERRANOVA SECURITY by HelpSystems

Security Awareness

tripwire by HelpSystems

File Integrity Monitoring

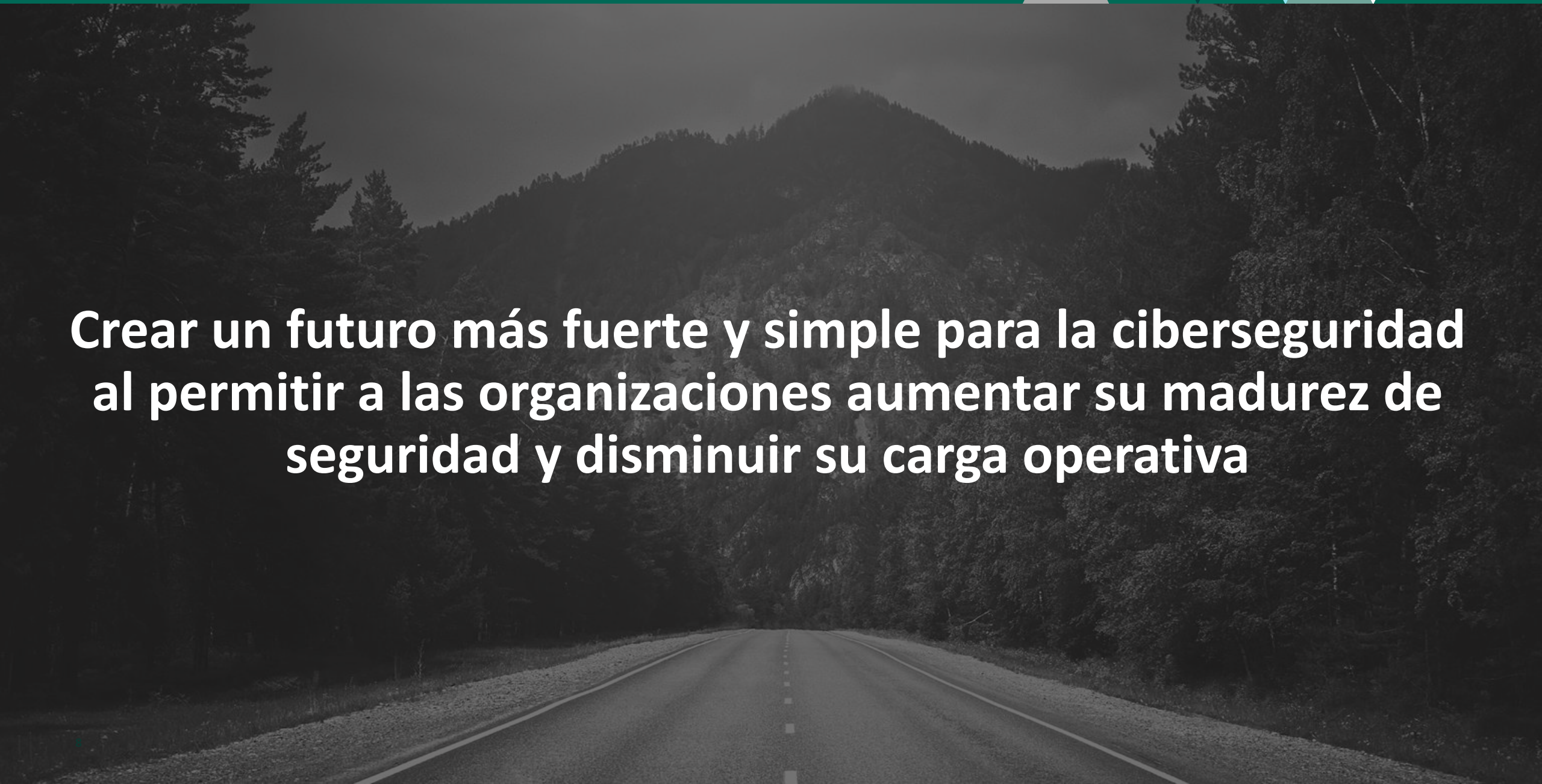
ALERT LOGIC by HelpSystems

Managed Detection & Response

OUTFLANK

Adversary Simulation

FORTRA

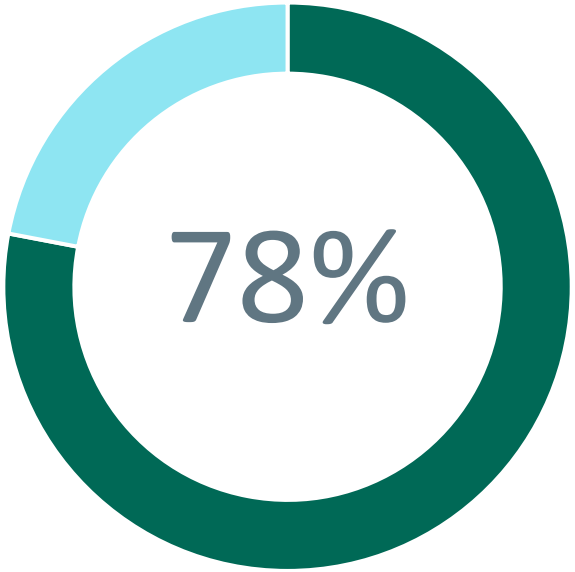


Crear un futuro más fuerte y simple para la ciberseguridad al permitir a las organizaciones aumentar su madurez de seguridad y disminuir su carga operativa

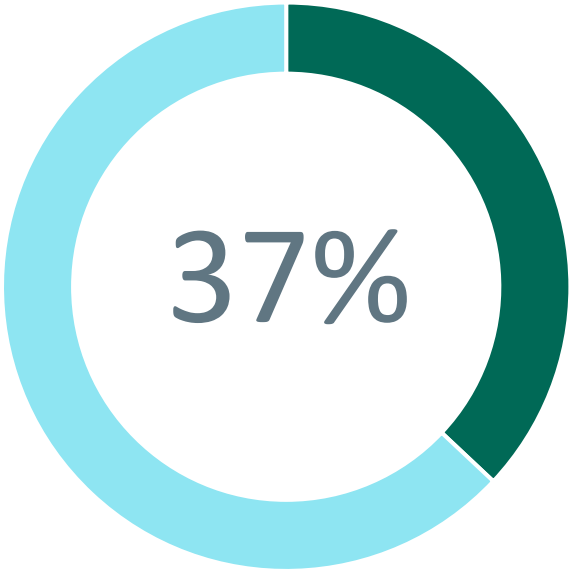
Los equipos de seguridad están sobrecargados con proveedores y productos

Esto incrementa la complejidad de gestión, y deja "huecos" que pueden ser explotados en ataques multi-vector.

Organizaciones usando 50+ Productos



Organizaciones usando 100+ Productos



Source: Security Magazine

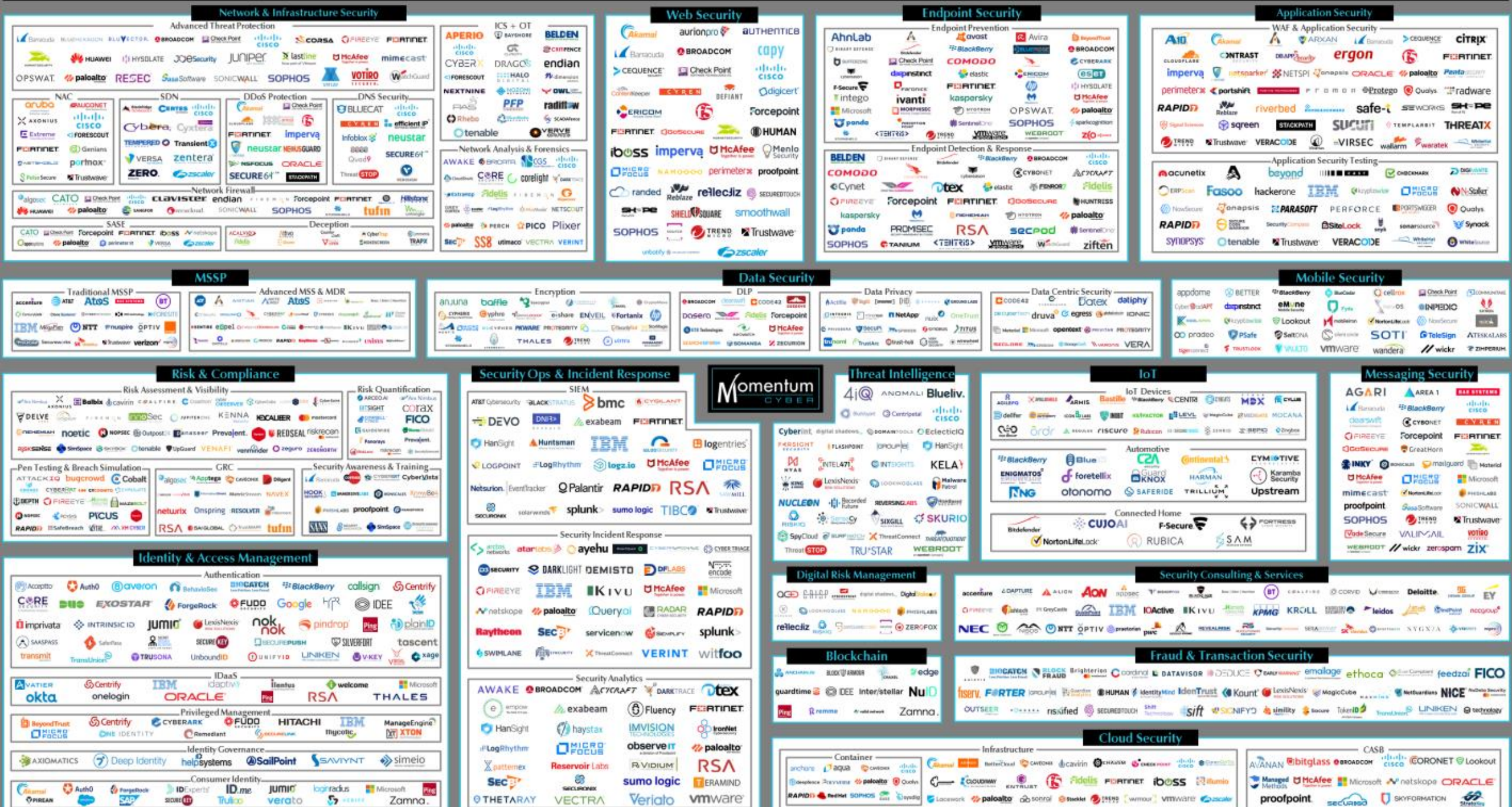
"The problem is much worse than this. ***All you need are 10 to 15 products*** *from different providers and you have a nightmare on your hands."*

Fortune 500 CISO (Entertainment)

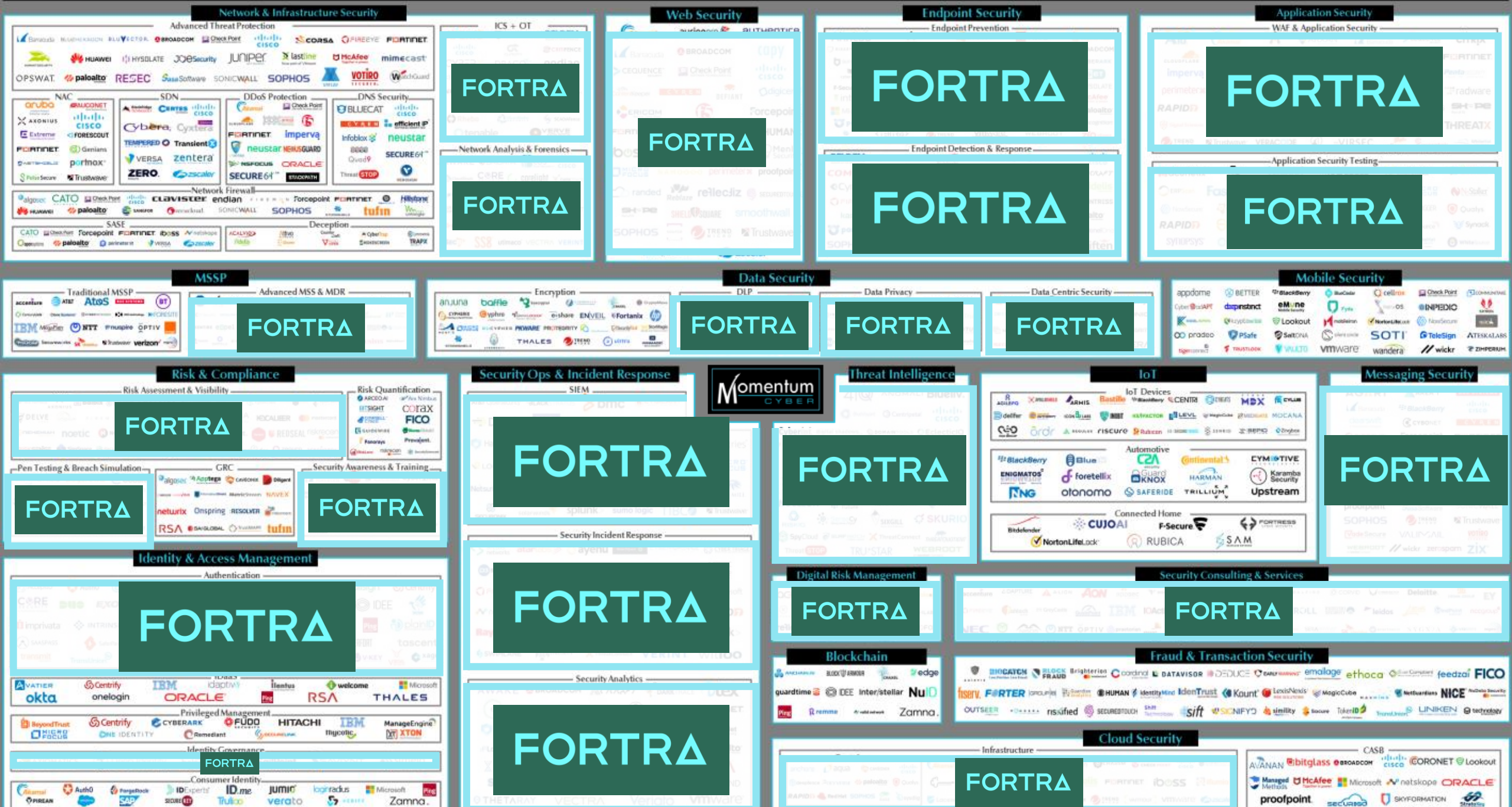
"We actually have ***over 200 security products****. Don't share this with anyone."*

Fortune 500 CISO (Manufacturing)

CYBER SCAPE 2022



CYBER SCAPE 2022



FORTRA

Reconnaissance	Resource Dev.	Initial Access	Execution	Persistence	Priv Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
Active Scanning	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Acquire Infrastructure	Exploit Public-Facing Application	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spear phishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Compromise Accounts	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Credentials from Password Stores	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Compromise Infrastructure	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Develop Capabilities	Phishing	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Phishing for Information	Establish Accounts	Replication Through Removable Media	Inter-Process Communication	Compromise Client Software Binary	Domain Policy Modification	Deobfuscate/Decode files or info.	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Search Closed Sources	Obtain Capabilities	Supply Chain Compromise	Native API	Create Account	Escape to Host	Deploy Container	Input Capture	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases	Stage Capabilities	Trusted Relationship	Scheduled Task/Job	Create or Modify System Process	Event Triggered Execution	Direct Volume Access	Modify Authentication Process	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains		Valid Accounts	Serverless Execution	Event Triggered Execution	Exploitation for Privilege Escalation	Domain Policy Modification	Multi-Factor Auth. Interception	Debugger Evasion	Use Alternate Authentication Material	Data from Information Repositories	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Shared Modules	External Remote Services	Hijack Execution Flow	Execution Guardrails	Multi-Factor Auth. Request Generation	Device Driver Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service
			Software Deployment Tools	Hijack Execution Flow	Process Injection	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			System Services	Implant Internal Image	Scheduled Task/Job	File and Directory Permissions Mod.	OS Credential Dumping	File and Directory Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
			User Execution	Modify Authentication Process	Valid Accounts	Hide Artifacts	Steal Application Access Token	Group Policy Discovery		Data Staged	Proxy		System Shutdown/Reboot
			Windows Management Instrumentation	Office Application Startup		Hijack Execution Flow	Steal or Forge Auth. Certificates	Network Service Discovery		Email Collection	Remote Access Software		
				Pre-OS Boot		Impair Defenses	Steal or Forge Kerberos Tickets	Network Share Discovery		Input Capture	Traffic Signaling		
				Scheduled Task/Job		Indicator Removal	Steal Web Session Cookie	Network Sniffing		Screen Capture	Web Service		
				Server Software Component		Indirect Command Execution	Unsecured Credentials	Password Policy Discovery		Video Capture			
				Traffic Signaling		Masquerading		Peripheral Device Discovery					
				Valid Accounts		Modify Authentication Process		Permission Groups Discovery					
						Modify Cloud Compute Infrastruct.		Process Discovery					
						Modify Registry		Query Registry					
						Modify System Image		Remote System Discovery					
						Network Boundary Bridging		Software Discovery					
						Obfuscated Files or Information		System Information Discovery					
						Plist File Modification		System Location Discovery					
						Pre-OS Boot		System Network Config. Discovery					
						Process Injection		System Network Connections Discovery					
						Reflective Code Loading		System Owner/User Discovery					
						Rogue Domain Controller		System Service Discovery					
						Rootkit		System Time Discovery					
						Subvert Trust Controls		Virtualization/Sandbox Evasion					
						System Binary Proxy Execution							
						System Script Proxy Execution							
						Template Injection							
						Traffic Signaling							
						Trusted Developer Util. Proxy Exec.							
						Unused/supported Cloud Regions							
						Use Alternate Authent. Material							
						Valid Accounts							
						Virtualization/Sandbox Evasion							
						Weaken Encryption							
						XSL Script Processing							

MITRE ATT&CK®

+ FORTRA™

Risk Mitigation

Prevent the technique from being used

Risk Detection

Real-time detection of misconfigurations, policy violations and attempts/successful usage of techniques.

Risk Identification

Recurring identification of vulnerabilities, misconfigurations and policy violations.

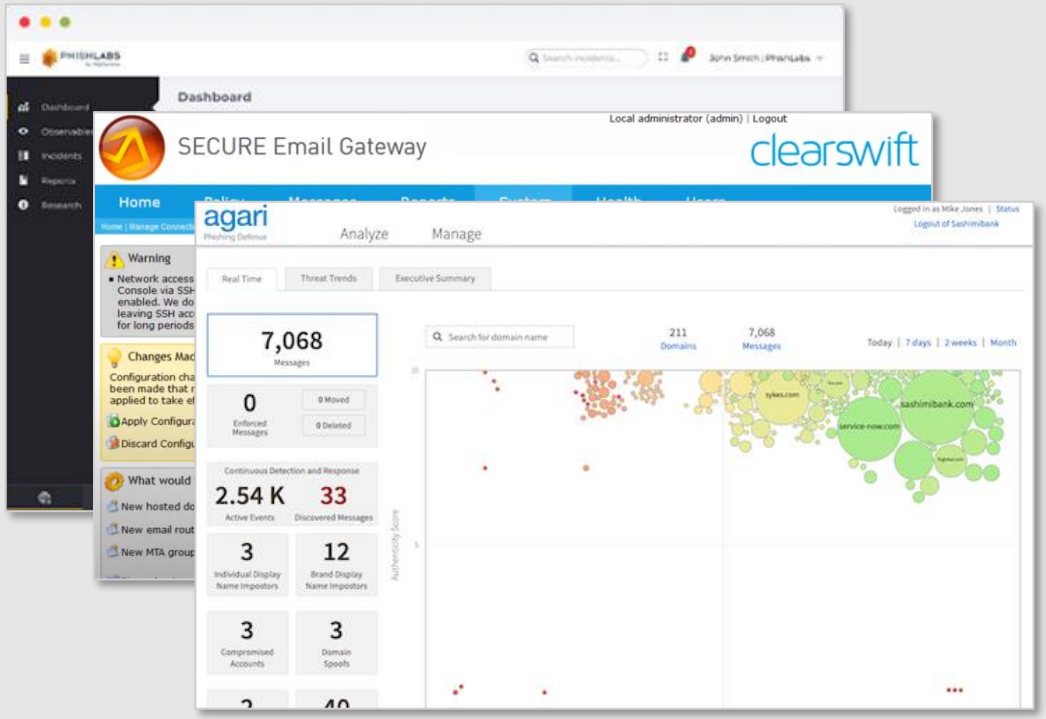
Risk Testing

Attempt to use the technique or get information to identify and quantify existing risks

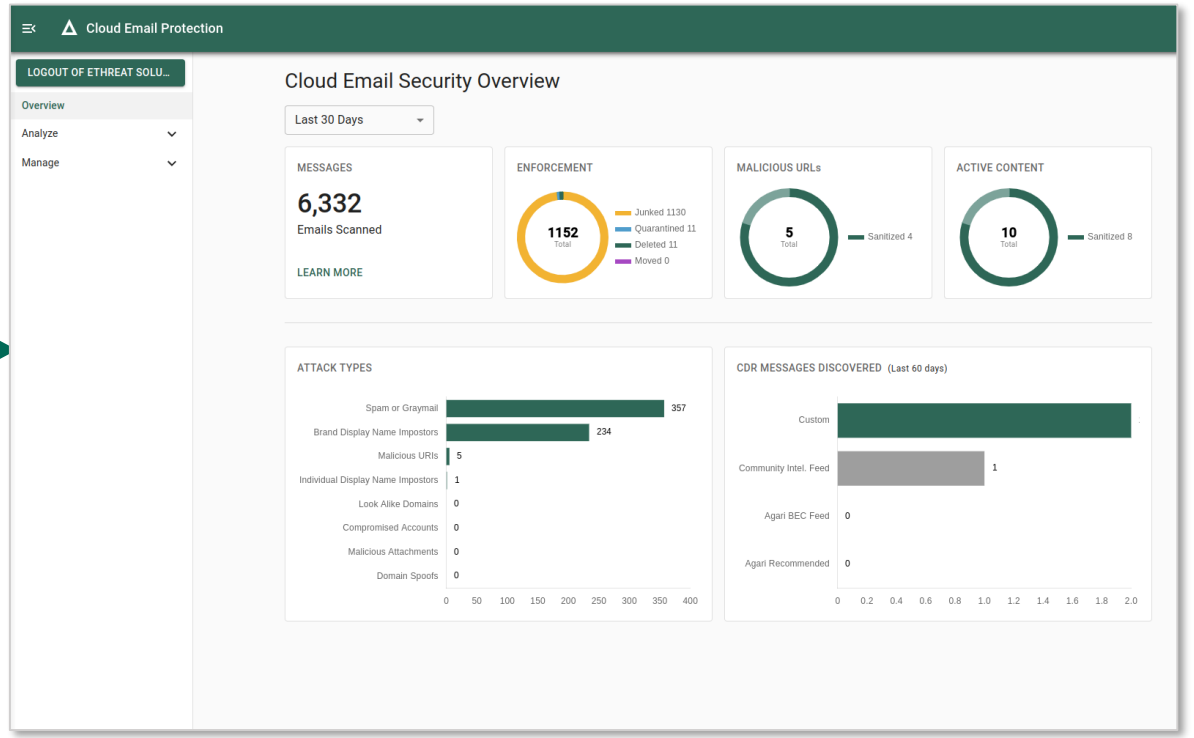
FORTRA

Estamos construyendo una Plataforma unificada para simplificar la complejidad de gestionar múltiples soluciones

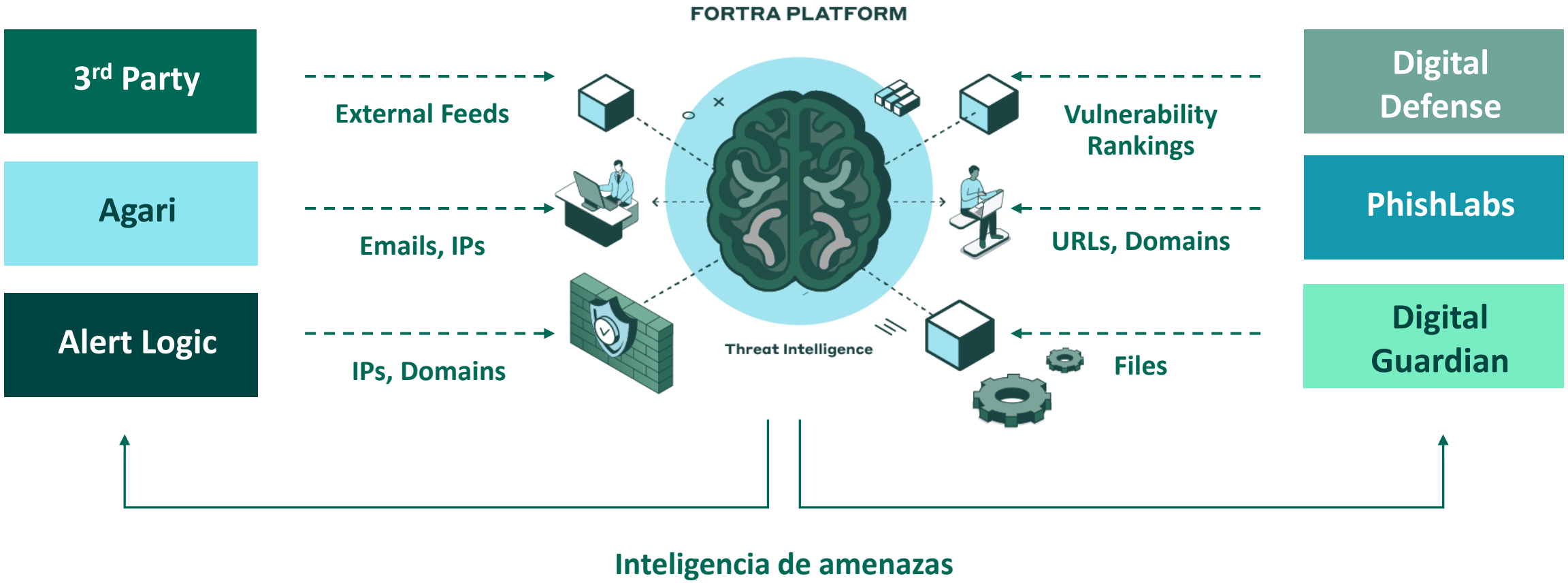
Interfaces distintas



Una interfaz con capacidades multi-vector



Y creando el Fortra Threat Brain para correlar cada riesgo e indicador de compromiso por múltiples vectores para nuestra base de clientes



El portafolio de Ciberseguridad de Fortra

FORTRA

Suites de Soluciones de ciberseguridad

PROTECCIÓN DE DATOS

- ✓ Data Loss Prevention: Endpoint, Network and Email
- ✓ Data Classification
- ✓ Data Discovery
- ✓ Secure File Sharing

Digital Guardian | Boldon James | Vera

SEGURIDAD DE EMAIL & ANTI-PHISHING

- ✓ Secure Email Gateway
- ✓ Advanced Anti Phishing (BEC)
- ✓ DMARC
- ✓ Security Awareness Training

Agari | Clearswift | Terranova

PROTECCIÓN DE RIESGOS DIGITALES

- ✓ Brand Protection
- ✓ Account Takeover Protection
- ✓ Social Media Protection
- ✓ Takedown / mitigate threats

PhishLabs

SECURE FILE TRANSFER

- ✓ Managed File Transfer
- ✓ Processes orchestration and automation
- ✓ Secure Email & Collaboration
- ✓ File Acceleration

GoAnywhere | GlobalScape | Filecatalyst | Clearswift

GESTIÓN DE VULNERABILIDADES

- ✓ Vulnerability Management
- ✓ Web Application Scanning
- ✓ Application Security Testing
- ✓ File Integrity Monitoring (FIM)
- ✓ Security Configuration Management (SCM)

Digital Defense | Beyond Security | Tripwire

SEGURIDAD OFENSIVA

- ✓ Automated Pen Testing
- ✓ Adversary Simulations
- ✓ Red Team Operations

Core Security | Cobalt Strike | Outflank

MANAGED DETECTION AND RESPONSE

- ✓ Managed Detection & Response
- ✓ Managed Web Application Firewall
- ✓ 24/7 SOC and Threat Intel Expertise

Alert Logic

IBM i SECURITY

- ✓ Compliance
- ✓ Antivirus
- ✓ Encryption
- ✓ System hardening
- ✓ High-Availability

Powertech

MANAGED SERVICES

- ✓ Digital Risk Protection
- ✓ Data Loss Prevention
- ✓ Web Application Firewall
- ✓ Managed Detection and Response
- ✓ File Integrity Monitoring

FORTRA

Suites de Soluciones de ciberseguridad

PROTECCIÓN DE DATOS

- ✓ Data Loss Prevention: Endpoint, Network and Email
- ✓ Data Classification
- ✓ Data Discovery
- ✓ Secure File Sharing

Digital Guardian | Boldon James | Vera

SEGURIDAD DE EMAIL & ANTI-PHISHING

- ✓ Secure Email Gateway
- ✓ Advanced Anti Phishing (BEC)
- ✓ DMARC
- ✓ Security Awareness Training

Agari | Clearswift | Terranova

PROTECCIÓN DE RIESGOS DIGITALES

- ✓ Brand Protection
- ✓ Account Takeover Protection
- ✓ Social Media Protection
- ✓ Takedown / mitigate threats

PhishLabs

SECURE FILE TRANSFER

- ✓ Managed File Transfer
- ✓ Processes orchestration and automation
- ✓ Secure Email & Collaboration
- ✓ File Acceleration

GoAnywhere | GlobalScape | Filecatalyst | Clearswift

GESTIÓN DE VULNERABILIDADES

- ✓ Vulnerability Management
- ✓ Web Application Scanning
- ✓ Application Security Testing
- ✓ File Integrity Monitoring (FIM)
- ✓ Security Configuration Management (SCM)

Digital Defense | Beyond Security | Tripwire

SEGURIDAD OFENSIVA

- ✓ Automated Pen Testing
- ✓ Adversary Simulations
- ✓ Red Team Operations

Core Security | Cobalt Strike | Outflank

MANAGED DETECTION AND RESPONSE

- ✓ Managed Detection & Response
- ✓ Managed Web Application Firewall
- ✓ 24/7 SOC and Threat Intel Expertise

Alert Logic

IBM i SECURITY

- ✓ Compliance
- ✓ Antivirus
- ✓ Encryption
- ✓ System hardening
- ✓ High-Availability

Powertech

MANAGED SERVICES

- ✓ Digital Risk Protection
- ✓ Data Loss Prevention
- ✓ Web Application Firewall
- ✓ Managed Detection and Response
- ✓ File Integrity Monitoring

FORTRA

Protección de datos

FORTRA

Retos en las organizaciones

Presión para asegurar los datos críticos

Presión para proteger los datos más críticos:

- Propiedad intelectual
- Datos del cliente
- Datos de los empleados
- Información financiera
- PII, PCI, PHI
- Cumplimiento: GDPR/NIST/ITAR/CCPA etc.

Despliegues largos y dolorosos de DLP

Muchos proyectos de protección de datos/DLP se vuelven largos e interminables.

Se requieren soluciones pragmáticas, de despliegue, rápido, que guíen al usuario, descubran y clasifiquen con inteligencia artificial.

Colaboración Segura

Las organizaciones deben proteger sus datos críticos y mantenerlos seguros.

Sin embargo, para que las empresas funcionen, **los datos deben compartirse** más allá de la protección corporativa.

Fortra's Data Protection

Soluciones entrelazadas que protegen sus datos a la vez que mantienen la productividad de sus usuarios.

Data Loss Prevention

Digital Guardian DLP es nuestro caballo de batalla de protección de datos, con una rápida implementación y resultados, y una mayor eficacia implementada.

Data Classification

La clasificación de datos de Fortra aumenta la eficacia de su DLP, al tiempo que reduce la fricción y aumenta la conciencia de seguridad de los empleados.

Secure Collaboration

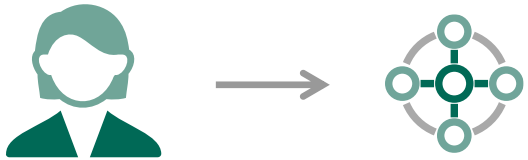
Permite compartir datos de forma segura dentro y fuera de su entorno, desde el cifrado proactivo hasta la resolución de exposiciones accidentales de datos.

¿ Como soporta Fortra este scenario ?

Lucas (backoffice)

Sam (negocio)

John (socio)

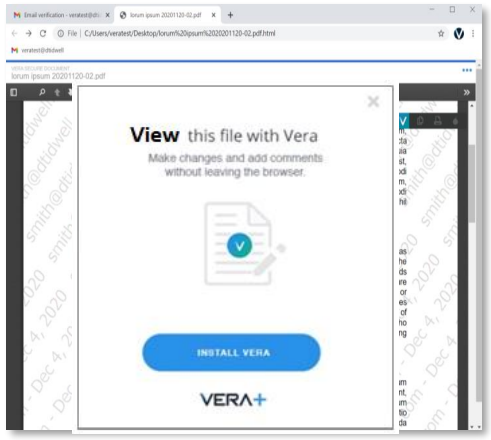


Clasificación de datos
“Confidencial – Solo interno”
País origen: España
Datos: PII, GDPR
Clasificación manual, guiada y/o con IA

Gobierno de datos
Definir política DLP
“Remediación – Bloquear o Justificar”

or…

Compartir de forma segura
“Control acceso + encriptación + marca de agua + solo lectura”



Caso real: Clasificación de datos en contratista de defensa – aero espacial

- Problema a resolver: “**Export Control**” - Con el objetivo de prevenir el desarrollo de “armas biológicas, nucleares y en general otros tipos”, la Unión Europea restringe y controla el intercambio en algunos bienes”
- **Cada “producto” debe ser clasificado** con un ECCN. Cada producto está compuesto por posiblemente cientos de otros “productos”.
- Ficheros a clasificar y proteger: diseños, planos, fotografías, etc relacionados con tecnología “controlada”

¿Por qué **Titus de Fortra** para clasificar ?

- ✓ “Asistente” para el usuario final para guiarle en la clasificación correcta.
- ✓ Añadir multitud (cientos!) de metadatos persistentes de contexto: ¿con quién se puede intercambiar un archivo? ¿En qué países? ¿Fechas expiración? ¿Sensibilidad ? ¿Qué proyecto? … para reforzar la seguridad de los datos.
- ✓ Usado por cientos de organizaciones de defensa: ministerios de defensa, policía, servicios secretos, contratistas, etc.
- ✓ Posibilidad de despliegue 100% on-premise
- ✓ Soporte para gran complejidad de niveles de clasificación, con, por ejemplo, dependencias anidadas ,selecciones múltiples.

Export Control Classification Numbers (ECCNs)

Breakdown of categories

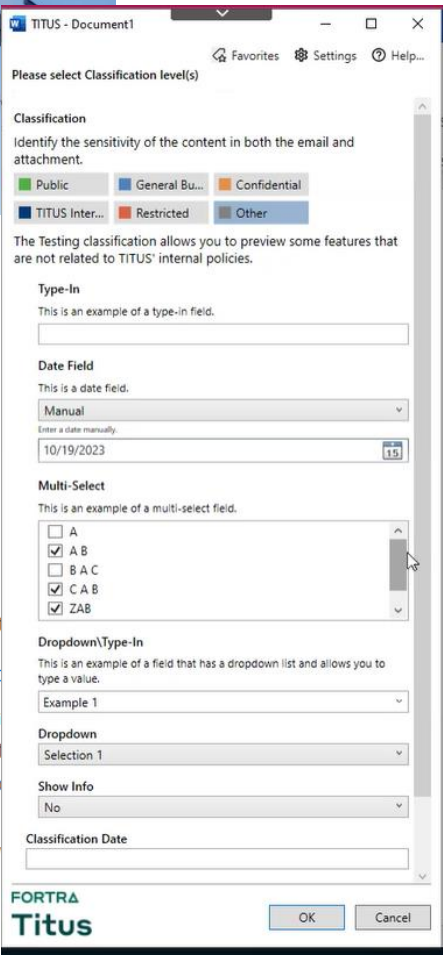
0 = Nuclear materials, facilities, and equipment
1 = Special materials and related equipment
2 = Materials processing
3 = Elect
4 = Com
5 = Telec
6 = Sens
7 = Navi
8 = Mari
9 = Aero

Breakdown of product groups

- A = Systems, equipment, and components
- B = Test, inspection, and production equipment
- C = M
- D = S
- E = T

Breakdown of reasons for control (cat

- - 001 - 099 = Wassenaar Arrangemen
- - 101 - 199 = Missile Technology Cont
- - 201 - 299 = Nuclear Suppliers Group
- - 301 - 399 = Australian Group
- - 401 - 499 = Chemical Weapons Con
- - 501 - 899 = (reserved)
- - 901 - 999 = National controls



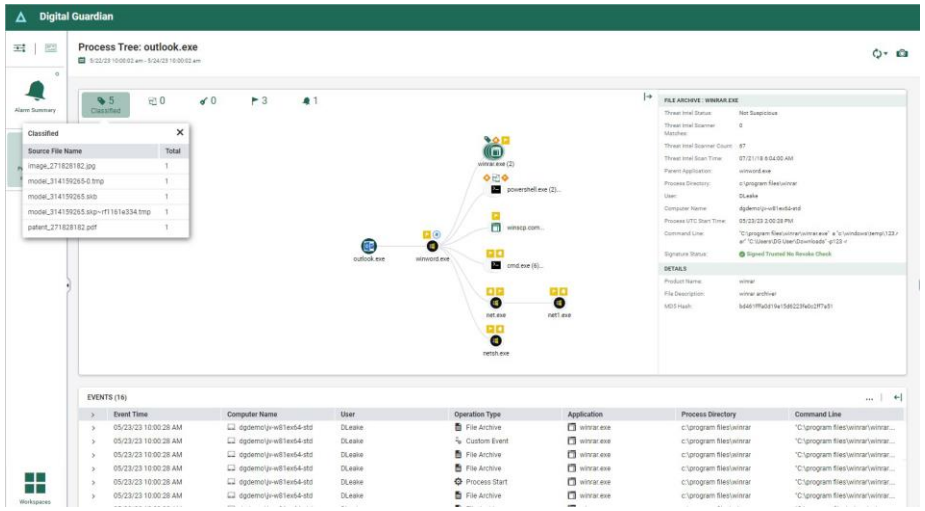
Caso real: DLP en una de las Consultoras top mundiales

- Situación inicial: **+600.000 end points**, usando un DLP conocido de terceros. Difícil de gestionar. Muchos falsos positivos. Mala integración con clasificación. Deciden reemplazar.

4 de las 5 consultoras top tienen proyectos de DLP con Digital Guardian

¿ Por qué eligieron Digital Guardian de Fortra?

- ✓ PoCs con virtualmente todos los DLP Enterprise
- ✓ Posibilidad de mapear su complejidad en políticas de protección de datos
  - ✓ Política global + políticas geográficas + políticas por vertical para más de medio millón de empleados
- ✓ Clasificación basada por **contexto**: usuarios, grupo de usuarios, ubicación de los ficheros, etc + Clasificación basada en **contenido**
- ✓ Integración bidireccional con MIP (Purview)
- ✓ Ejemplo: usuario hace captura de pantalla, y comprime en zip. DG sigue los datos y aplica etiqueta Purview en cada paso, asumiendo que es una captura de una aplicación que contiene datos sensibles.
- ✓ Visibilidad total en portal único (reporting big data)

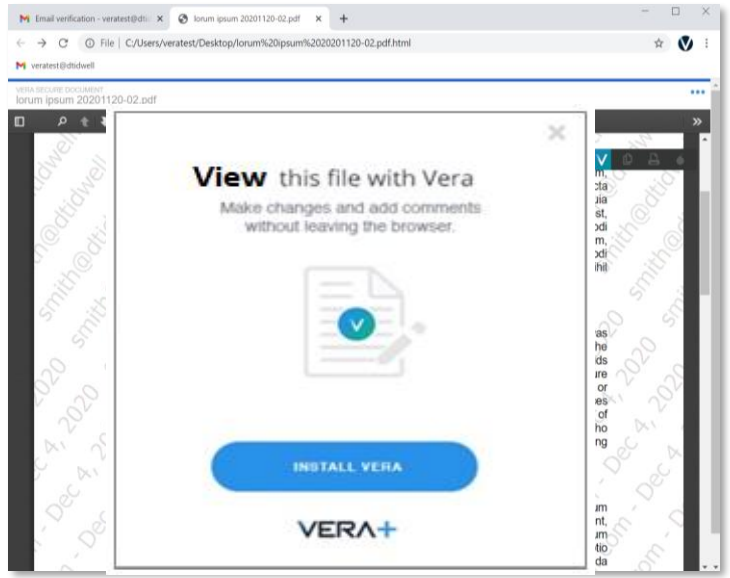


Caso real: Compartición Segura de datos en empresa de ropa deportiva

- ❑ Problema a resolver: **Proteger diseños** (propiedad intelectual)
- ❑ Los diseños se comparten con socios que los fabrican en múltiples países, principalmente en Asia.
- ❑ **“Clones” aparecen a la venta antes del lanzamiento del producto original -> Los diseños se filtran/venden a terceros.**

¿Por qué **Vera de Fortra** para proteger los datos ?

- ✓ Seguridad que viaja con los ficheros, encriptación
- ✓ Posibilidad de revocar permisos cuando ya no son necesarios
- ✓ Imposible compartir originales (ie, Autocad) con terceros
- ✓ Auditoría de quien accede a los ficheros, cuando, desde dónde.
- ✓ Granularidad de políticas:
  - ✓ solo lectura, modificación, copiar, pegar, imprimir, marca de agua, etc.



FORTRA

Suites de Soluciones de ciberseguridad

PROTECCIÓN DE DATOS

- ✓ Data Loss Prevention: Endpoint, Network and Email
- ✓ Data Classification
- ✓ Data Discovery
- ✓ Secure File Sharing

Digital Guardian | Boldon James | Vera

SEGURIDAD DE EMAIL & ANTI-PHISHING

- ✓ Secure Email Gateway
- ✓ Advanced Business Email Compromise (BEC)
- ✓ DMARC
- ✓ Security Awareness Training

Agari | Clearswift | Terranova

PROTECCIÓN DE RIESGOS DIGITALES

- ✓ Brand Protection
- ✓ Account Takeover Protection
- ✓ Social Media Protection
- ✓ Takedown / mitigate threats

PhishLabs

SECURE FILE TRANSFER

- ✓ Managed File Transfer
- ✓ Processes orchestration and automation
- ✓ Secure Email & Collaboration
- ✓ File Acceleration

GoAnywhere | GlobalScape | Filecatalyst | Clearswift

GESTIÓN DE VULNERABILIDADES

- ✓ Vulnerability Management
- ✓ Web Application Scanning
- ✓ Application Security Testing
- ✓ File Integrity Monitoring (FIM)
- ✓ Security Configuration Management (SCM)

Digital Defense | Beyond Security | Tripwire

SEGURIDAD OFENSIVA

- ✓ Automated Pen Testing
- ✓ Adversary Simulations
- ✓ Red Team Operations

Core Security | Cobalt Strike | Outflank

MANAGED DETECTION AND RESPONSE

- ✓ Managed Detection & Response
- ✓ Managed Web Application Firewall
- ✓ 24/7 SOC and Threat Intel Expertise

Alert Logic

IBM i SECURITY

- ✓ Compliance
- ✓ Antivirus
- ✓ Encryption
- ✓ System hardening
- ✓ High-Availability

Powertech

MANAGED SERVICES

- ✓ Digital Risk Protection
- ✓ Data Loss Prevention
- ✓ Web Application Firewall
- ✓ Managed Detection and Response
- ✓ File Integrity Monitoring

FORTRA

Gracias!