
FORTINET
COLOMBIA
& ECUADOR
XPERTS26

FORTINET | COLOMBIA & ECUADOR

XPERTS26

# Shadow Applications

**Valeria Velastegui**
Sales Engineer

# Valeria Velastegui

System Engineer

# Agenda

Desafíos actuales de Shadow APP

Mitigación de los riesgos de Shadow APP

FORTINET | COLOMBIA & ECUADOR

XPERTS26

# Desafíos actuales de GenAI

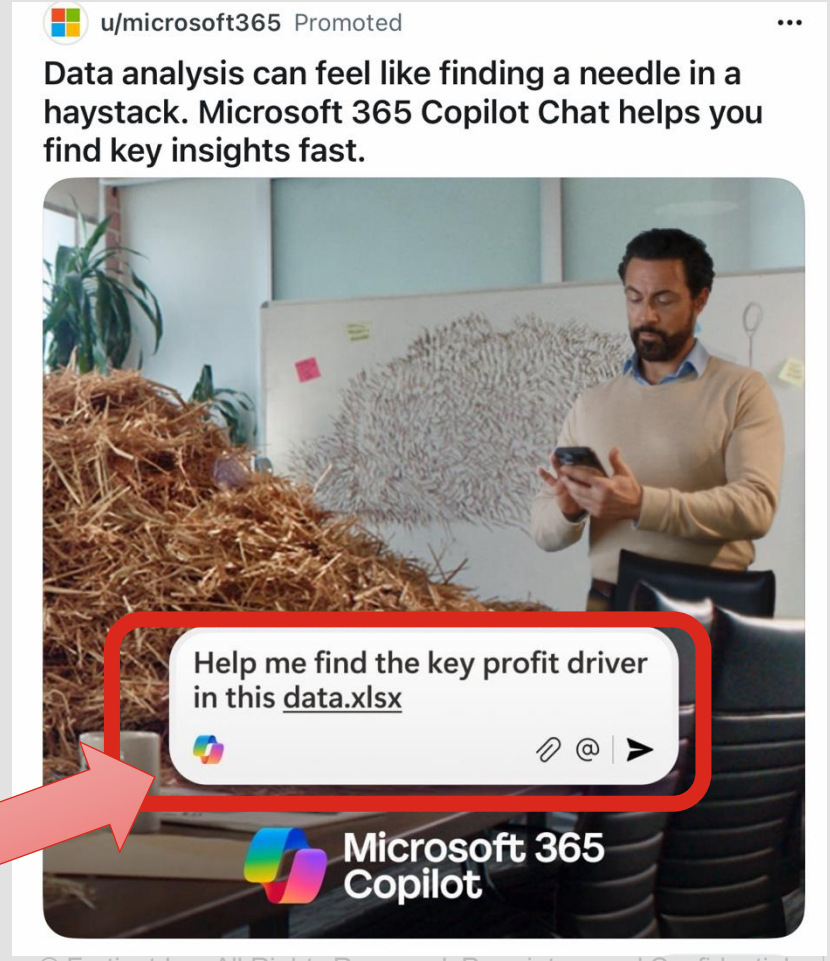
# Explosión de herramientas GenAI - Actual

# Los crecientes problemas de la AI

"By 2025, generative AI usage among enterprise employees is near-universal, with over 90–98% of knowledge workers reporting some level of AI tool usage, and a majority using it regularly in daily workflows."

1. Este crecimiento ha ido acompañado de un aumento de Shadow AI. Hoy en día, más de un tercio (38 %) de los empleados reconoce haber compartido información laboral confidencial con herramientas de IA sin el permiso de sus empleadores.

2. Shadow AI puede exponer a las empresas a diversos riesgos, como la fuga de datos, multas por incumplimiento y graves daños a su reputación.



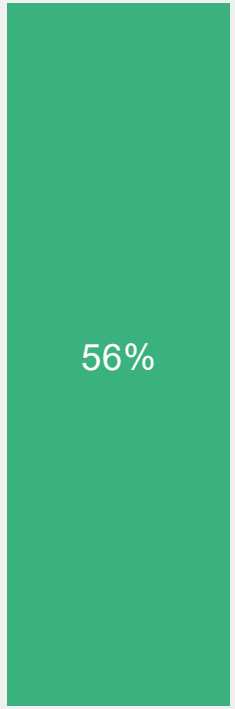

**Your Data is very Welcome!!**

based on 2025 industry reports from firms like McKinsey, Gartner, and Microsoft Work Trend Index

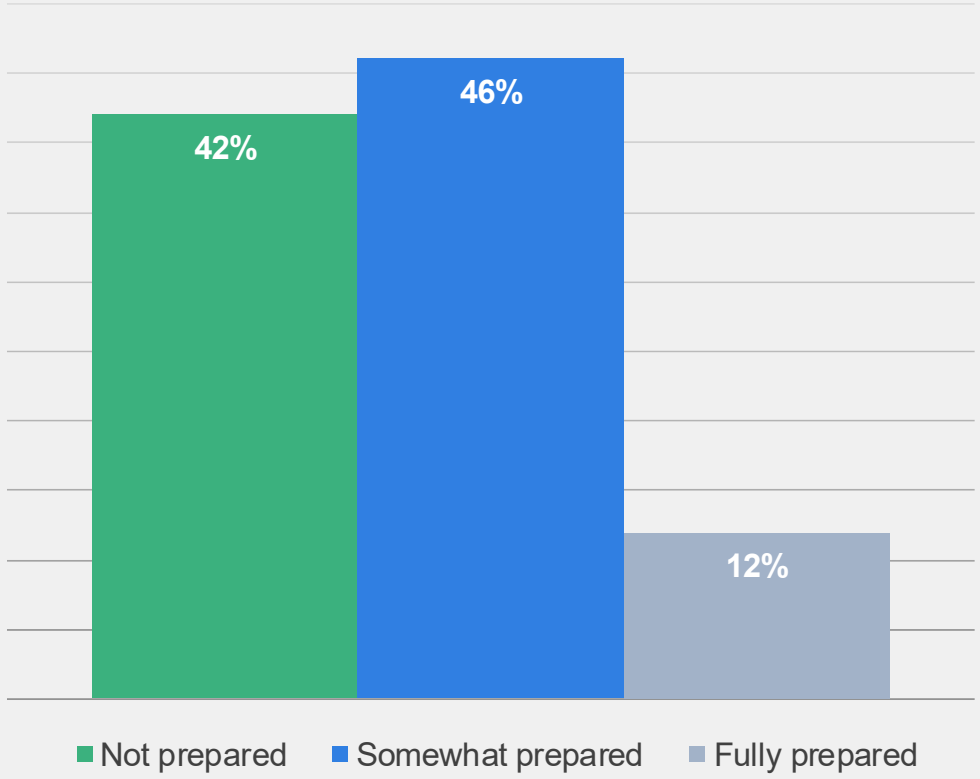
# Opiniones sobre GenAI

2025 Data/Insider Risk Reports

GenAI esta expandiendo la superficie de ataque. El 56 % están preocupados porque la data sensible pueda ser compartida por herramientas como ChatGPT




Preparación de las organizaciones para detectar y responder a insider risks como compartición de datos por medio de herramientas de GenAI



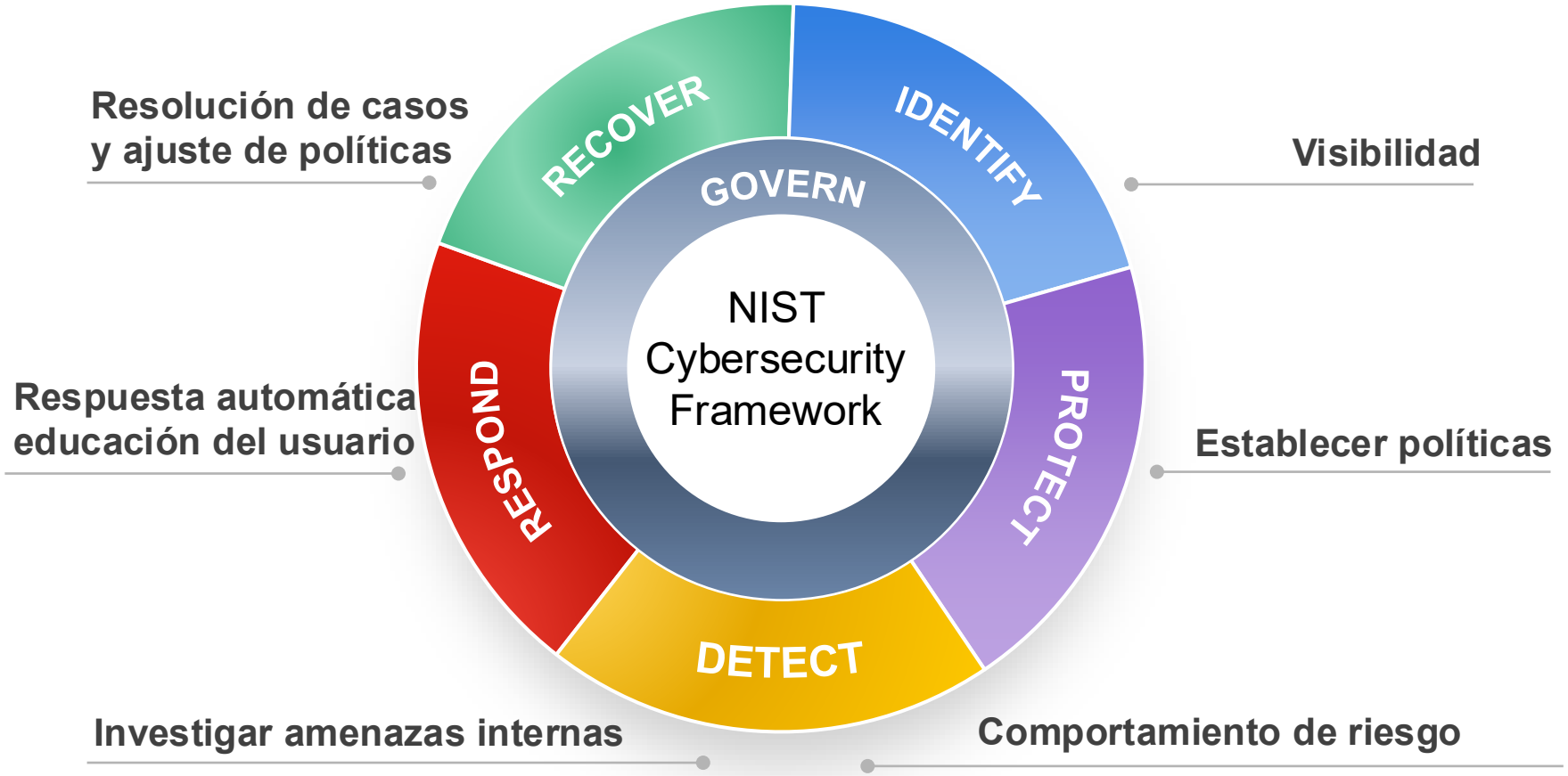
FORTINET | COLOMBIA & ECUADOR

XPERTS26

# Mitigación de riesgos Shadow AI

# Aplicando el Framework de NIST para mitigar el Riesgo GenAI

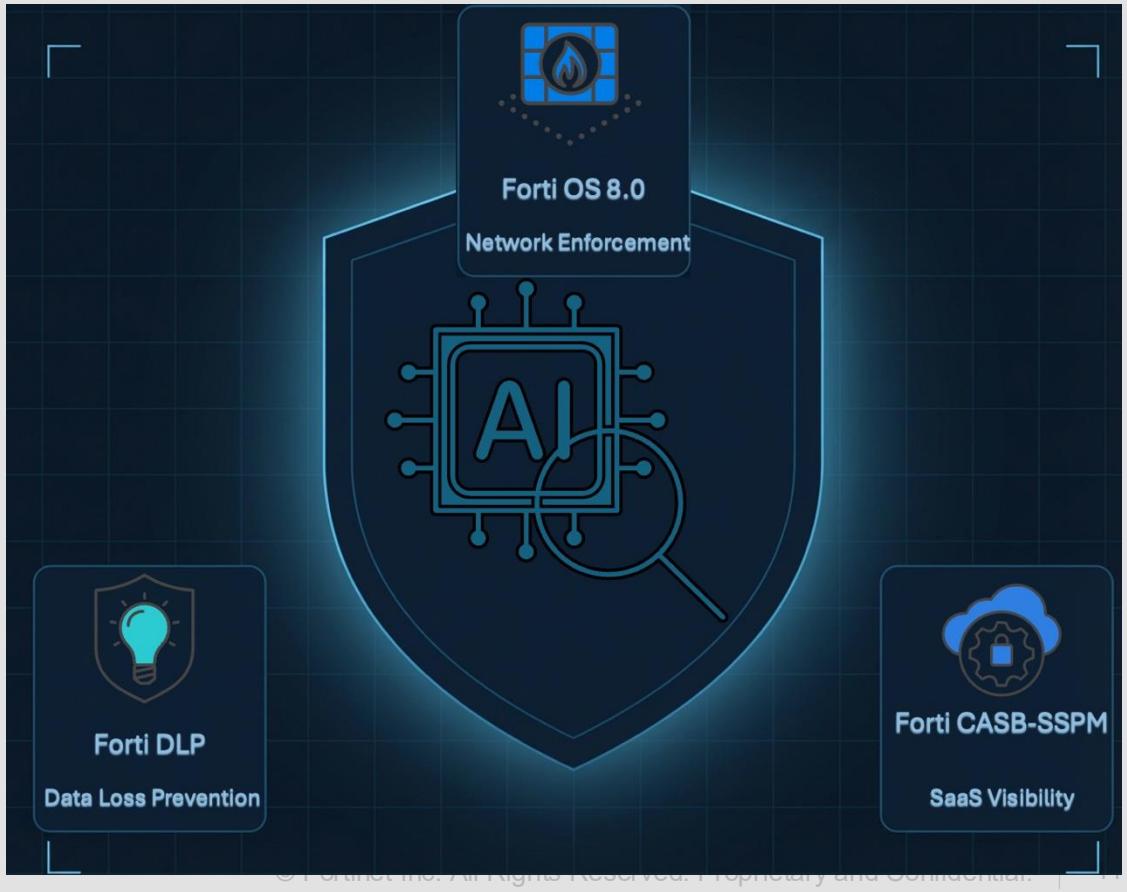
Educar a los usuarios sobre el manejo adecuado de los datos (Incluido el uso de GenAI)



# Mitigación de riesgos - Shadow AI

Para lograr una postura de seguridad sólida frente al uso de Shadow AI, es recomendable implementar una combinación de soluciones de seguridad configuradas específicamente para este caso de uso.  En este contexto, tenemos a  **Cloud Access Security Broker (CASB), Data Loss Prevention (DLP) & SaaS Posture Management (SSPM)** que son componentes fundamentales

- Visibilidad sobre las herramientas actuales de IA
- Prevención de fuga de datos
- Gestión de accesos y permisos
- Cumplimiento normativo y riesgos regulatorios
- Configuración y seguridad de la postura de seguridad de las herramientas de IA aprobadas
- Aplicación de políticas a gran escala



FORTINET | COLOMBIA & ECUADOR

XPERTS26

# Mitigación de riesgos Shadow AI

# Desafíos de seguridad en aplicaciones SaaS y servicios de terceros

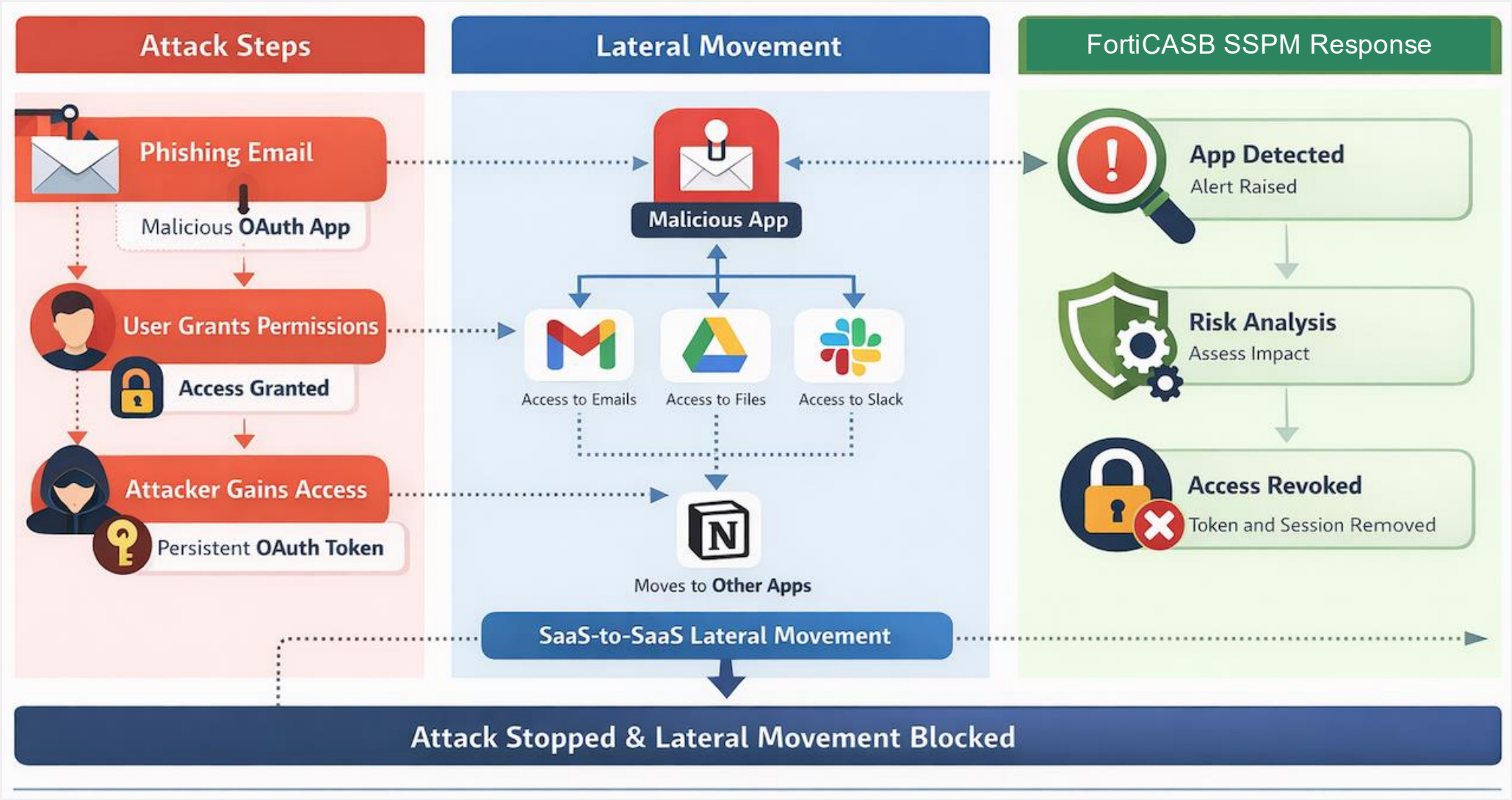
Identificar el stack de SaaS Stack

Detectar y responder a aplicaciones de terceros sospechosas

Control de identidades

Remediación automática

# Detección de ataques OAuth & Movimiento Lateral con FCASB SSPM



# FortiCASB-SSPM | Caso de uso clave

## Descubrimiento y visibilidad de aplicaciones Shadow IT y de terceros

Descubra aplicaciones SaaS desconocidas que no fueron aprobadas ni evaluadas por el área de seguridad o TI

## Gestión de configuraciones incorrectas en aplicaciones SaaS

Identifique automáticamente configuraciones incorrectas en las aplicaciones SaaS de la organización

## Gestión de la postura de identidad

Obtenga visibilidad sobre las identidades presente en las aplicaciones SaaS

## Administración de aplicaciones de Gen-AI

Controle el uso de aplicaciones basadas en IA generativa

## Gestión de la postura de seguridad de los datos

Identifique y proteja la información sensible en todas las aplicaciones SaaS

## Remediación y automatización de flujos de trabajo

Cree flujos de trabajo para automatizar las respuestas y ejecutar acciones de remediación

# Descubrimiento y visibilidad de aplicaciones Shadow IT y de terceros

## Mejorando la visibilidad

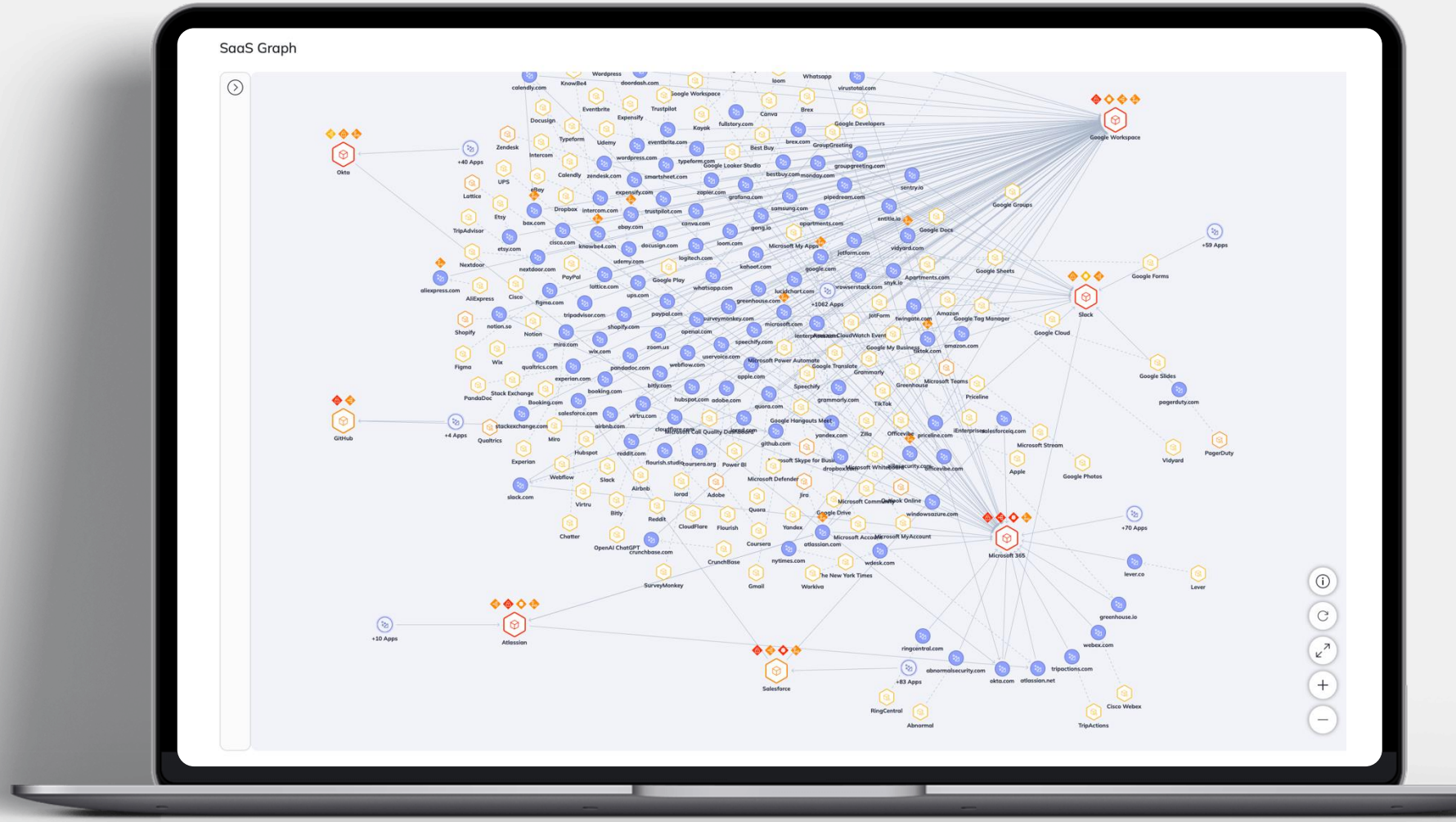
Descubra conexiones sospechosas

Detecte aplicaciones no autorizadas y aplique controles de seguridad

Elimine el acceso de aplicaciones no autorizadas o inactivas

Administre todos los complementos, extensions, API de terceros y tokens conectados

Identifique permisos otorgados a terceros y detecte riesgos de datos, uso y cumplimiento

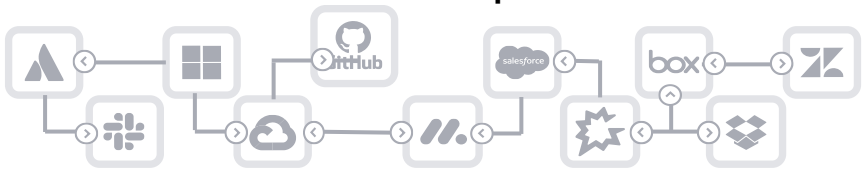


## La plataforma

Una solución sin agentes que identifica y previene la próxima brecha de seguridad originada en aplicaciones SaaS


Métodos de recoplicación de datos no intrusivos y sin agentes desde más de 100 fuentes

### Construcción del mapa de red SaaS



Nuestro motor de IA identifica las interconexiones entre aplicaciones y construye el mapa de relaciones del entorno SaaS

### Identificación de riesgos

Identificación de exposiciones, configuraciones incorrectas, vulnerabilidades y riesgos

### Priorización


El motor de correlación relaciona los eventos para proporcionar contexto, en lugar de generar únicamente más carga operativa

### Flujos de trabajo

Implementación de controles de protección y cumplimiento normativo

# Tipos de conectores

| | FortiAnalyzer / EDR / Proxy | Aplicaciones SaaS principales | IDP Proveedor de identidad |
|---|---|---|---|
| **Datos recopilados** | Telemetría HTTP/S y dispositivos | Configuraciones, terceras partes (NHI) e identidades | Identidades |
| **Métodos de integración** | API | API / Service Account / OAuth | API / OAuth |
| **Resultados** | Aplicaciones Shadow SaaS, Usuarios, dispositivos, e interacciones | Configuraciones incorrectas, terceros (NHI - APIs, Tokens, Service Accounts), e identidades (actividades, permisos, MFA, etc.) | Información de identidades y hallazgos de postura (SSO, MFA, permisos, aprovisionamiento y dispositivos) |
| **Alcances y permisos** | Administrador de solo lectura | Tipo A (Remediación es deshabilitada): Permisos de solo lectura para la recopilación de información* Tipo B (Remediación es habilitada): Permisos de escritura para acciones de remediación. Permisos de lectura para recopilación de información | Administrador de solo lectura |

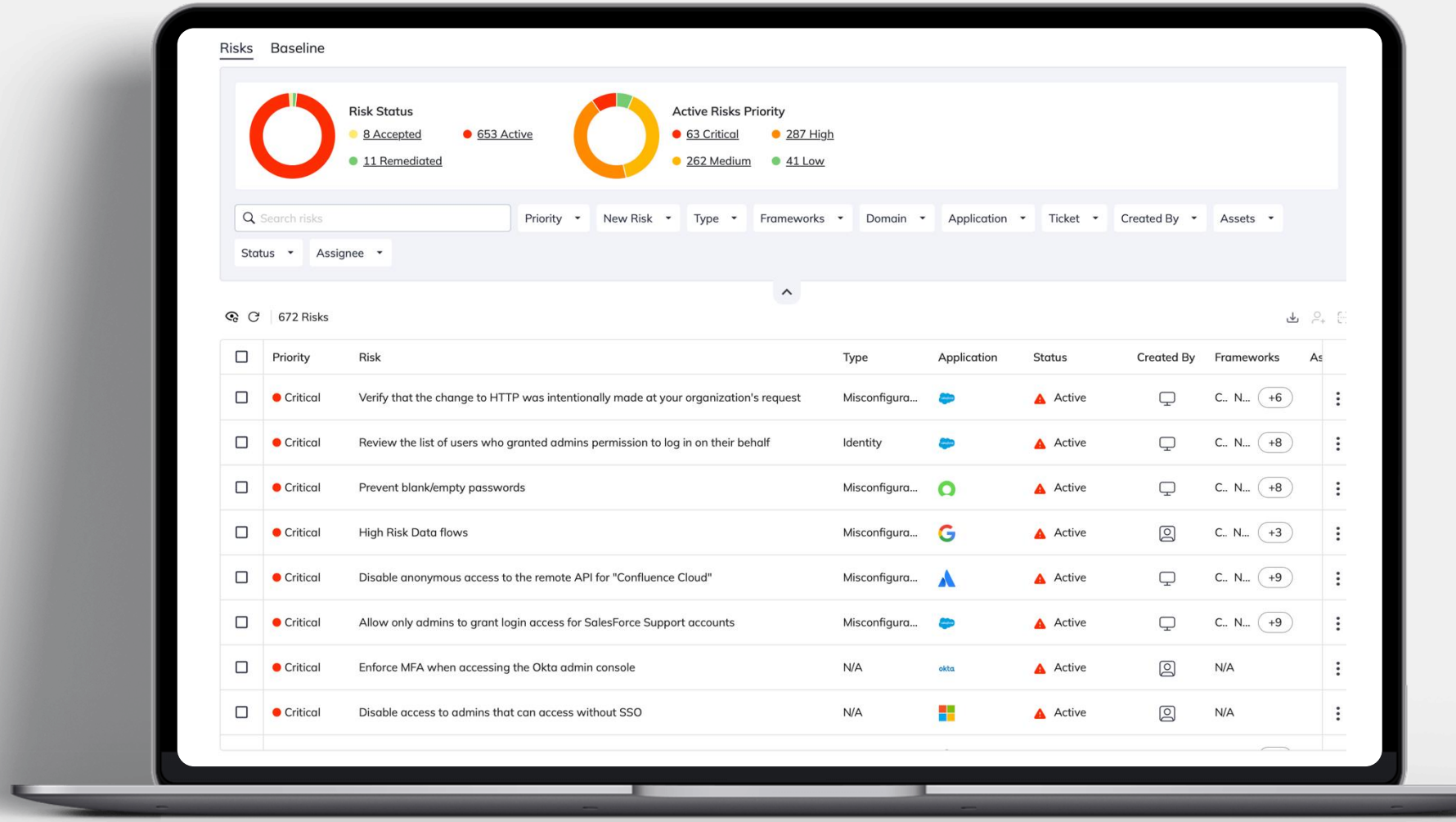
# Gestión de configuraciones erróneas SaaS (SSPM)

## Gestión de configuraciones erróneas

Detecte configuraciones incorrectas en las aplicaciones SaaS empresariales

Supervise las desviaciones en la configuración y los nuevos ajustes de seguridad

Cumpla con los requisitos de seguridad y mantenga las mejores prácticas.



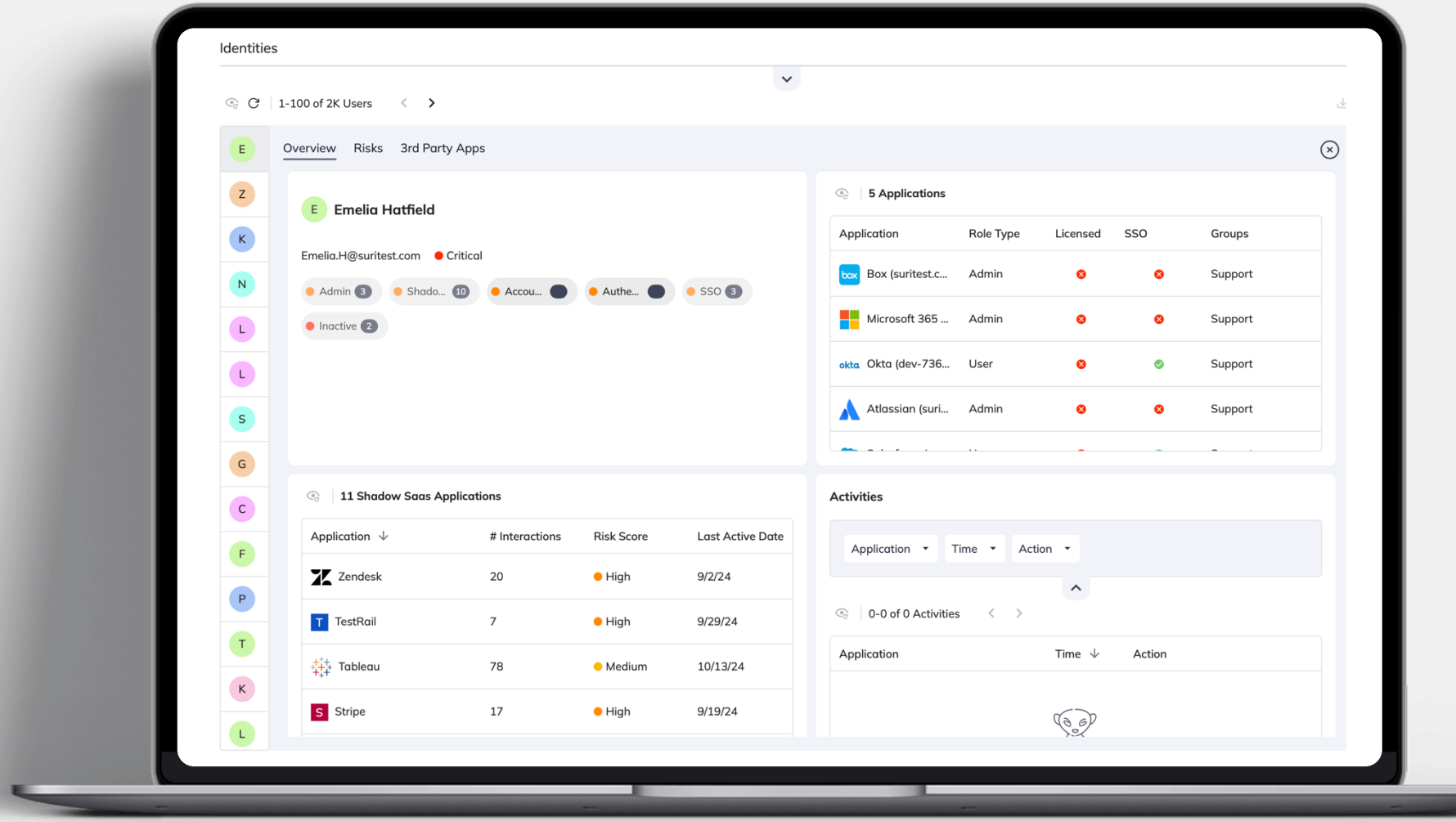
# Gestión de la postura de identidad

## Visibilidad de identidades en aplicaciones SaaS

Obtenga visibilidad de las identidades a través de multiples aplicaciones SaaS

Incorporación Segura de usuarios IDP mediante SSO y MFA

Desaprovisionamiento automático de usuarios inactivos y revocación de privilegios de acceso



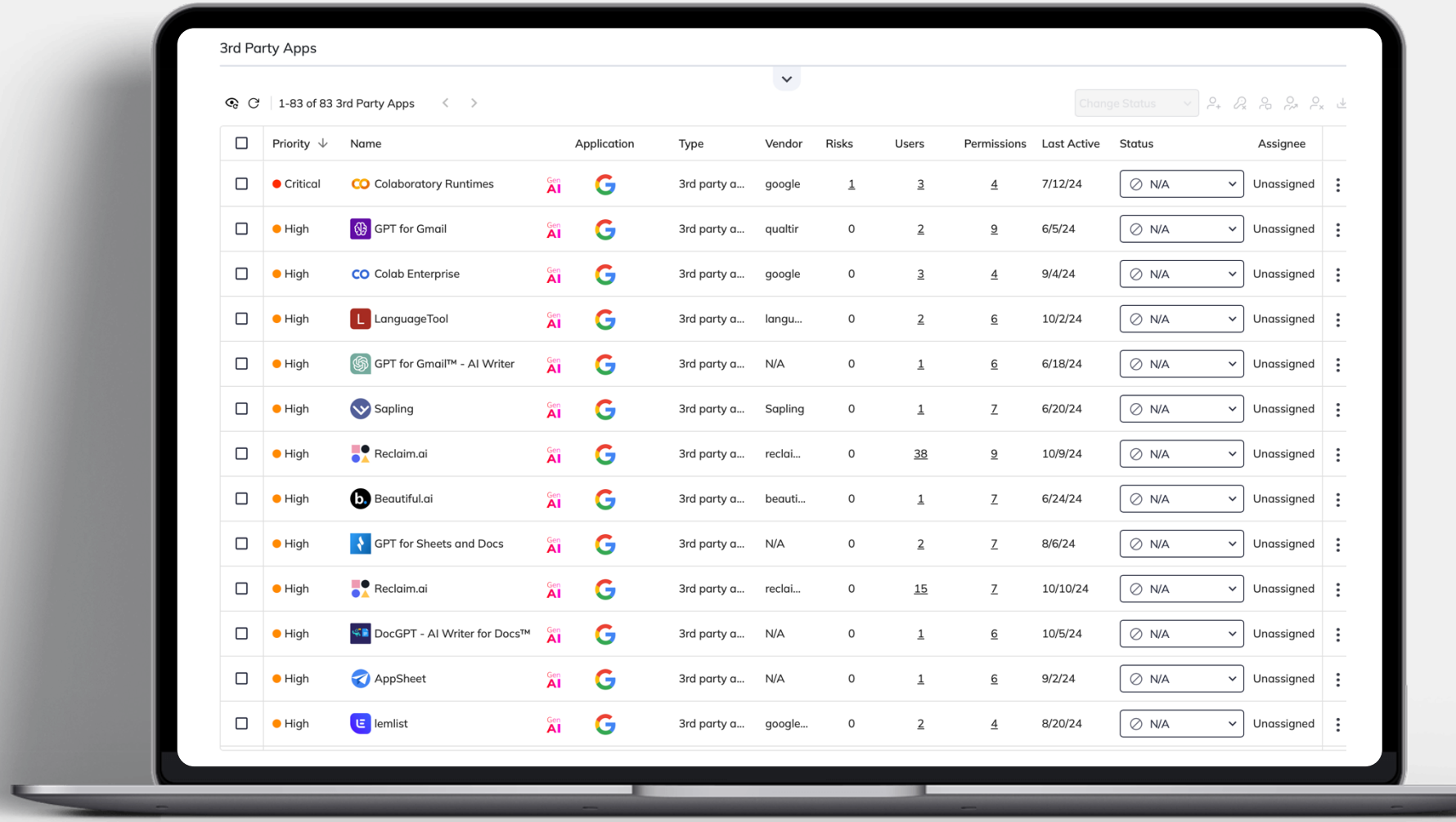
# Administración de aplicaciones GenAI

## Control de aplicaciones de IA generativa

Controle el uso de aplicaciones de GenAI en toda la organización

Revoque el acceso a aplicaciones de terceros no autorizados

Utilice flujos de trabajo sin Código para automatizar el análisis de seguridad y el control de herramientas de GenAI



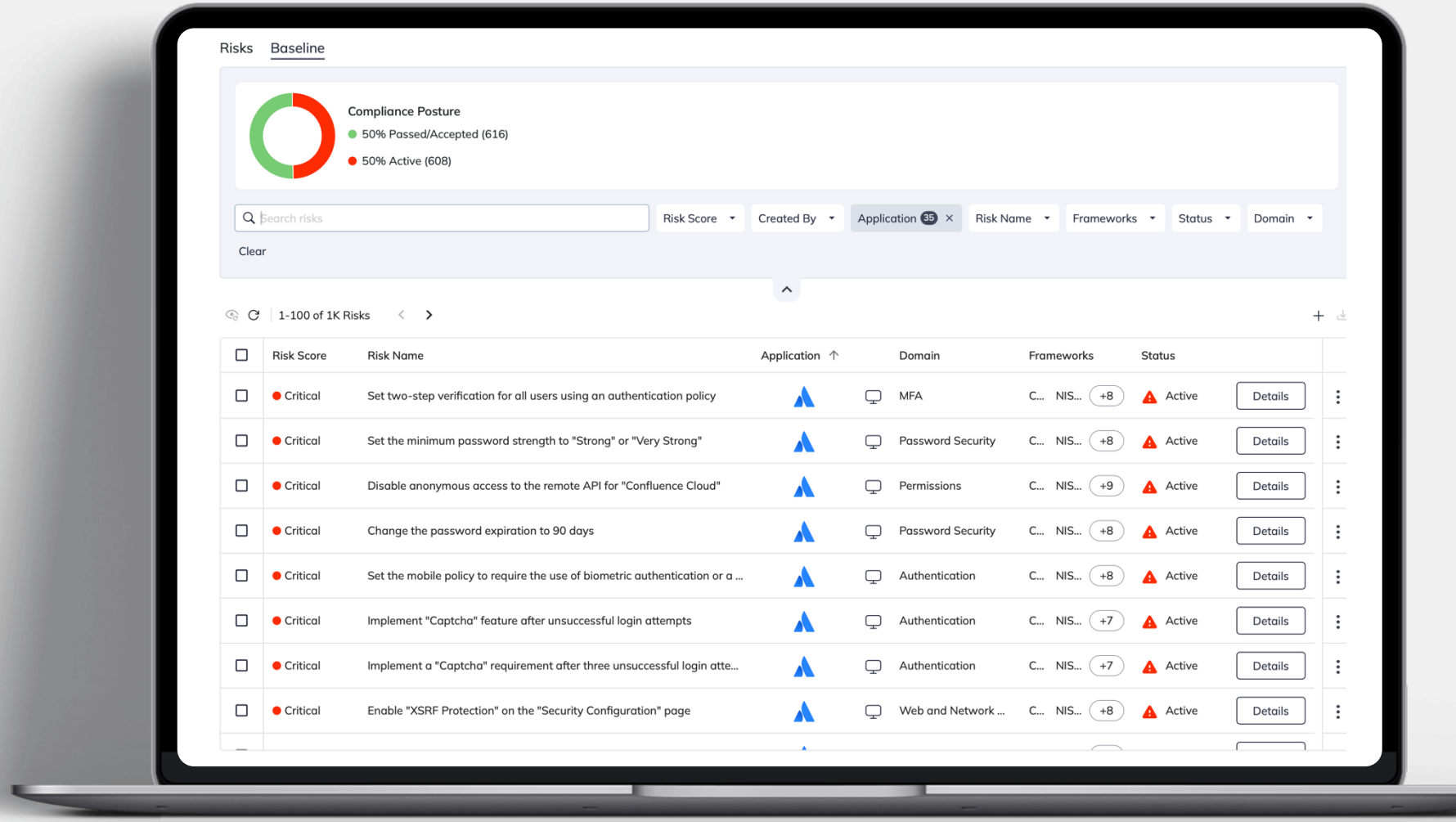
# Gestión de la postura de seguridad de los datos y protección contra malware

## Datos y cumplimiento normativo

Cobertura y alineación completa con más de 12 marcos de seguridad (NIST, SOC-2, MITRE, ISO, etc.

Monitoreo de la compartición y descarga de datos sensibles PII y evaluación continua de riesgos de seguridad de la información

Cumplimiento continuo mediante la gestion y supervisión centralizada de riesgos a nivel corporativo.



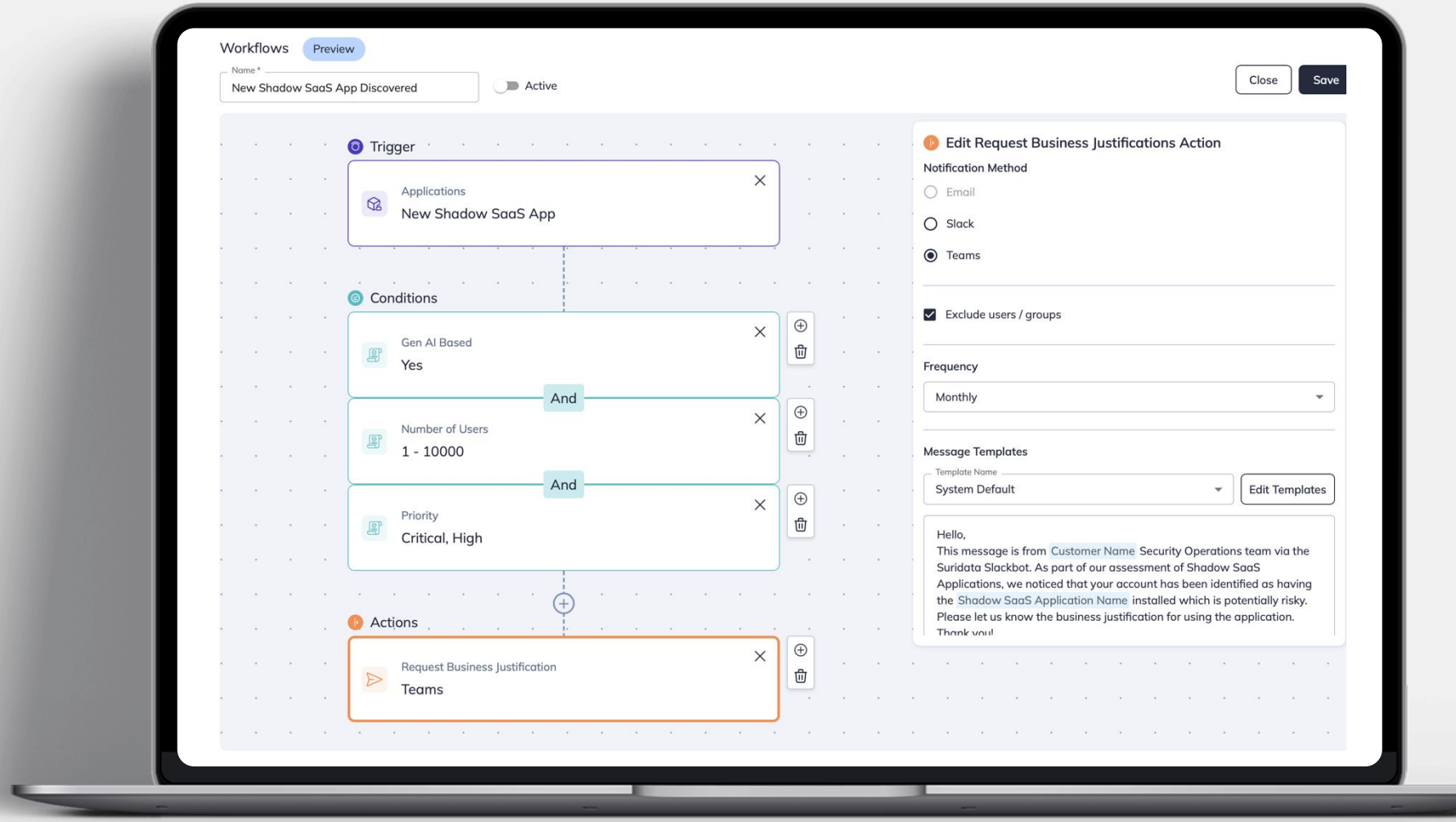
# Remediación y flujos de trabajo

## Automatización de flujos de trabajo

Validación y justificación de negocio por parte de los responsables y usuarios autorizados

Automatización de tickets, alertas y asignación de riesgos entre las áreas de negocio, ciberseguridad y TI

Revocación de accesos y desaprovisionamiento eficiente de usuarios



FORTINET | COLOMBIA & ECUADOR
XPERTS26

# CRITERIOS

# Critero de éxitos que se puede recomendar

| Valor | Caso de Uso | Criterio de éxito |
|---|---|---|
| Descubrimiento Shadow SaaS | Identificar y priorizar aplicaciones Shadow SaaS | Las aplicaciones Shadow SaaS serán identifcadas y priorizadas, y el sistema proporcionará información sobre los riesgos, el uso y los usuarios asociados. |
| Integraciones SaaS | Proporcionar un amplio catálogo de aplicaciones | El sistema contará con una amplia selección de aplicaciones SaaS clave y permitirá un proceso de integración simple y rápido |
| Eliminación de configuraciones incorrectas | Identificar, priorizar y corregir configuraciones incorrectas que introducen vulnerabilidades en las aplicaciones SaaS conectadas | El sistema identificará y priorizará correctamente las configuraciones incorrectas de acuerdo con las mejores prácticas de los proveedores SaaS, estándares de seguridad y certificaciones, proporcionando pasos de remediación accionables |
| Reducción del Riesgo de aplicaciones de terceros | Identificar, priorizar y mitigar los riesgos asociados con aplicaciones de terceros. | Al analizar los riesgos asociados con las aplicaciones de terceros conectadas a los activos SaaS, el Sistema recomendará acciones de control y priorizará las aplicaciones que requieren atención. |
| Gestión de la postura de identidad | Obtener visibilidad de las identidades en las aplicaciones SaaS, aplicar SSO y MFA para usuarios activos y retirar usuarios inactivos | Identificar administradores y usuarios que se conectan mediante cuentas locales, así como usuarios inactivos que deber ser desactivados. |
| Reducción de riesgos de acceso a archivos | Identificar, priorizar y corregir problemas de acceso en archivos almacenados en aplicaciones SaaS | El Sistema identificará archivos compartidos externamente, enlaces anónimos y descargas excesivas, y permitirá ejecutar acciones de remediación |
| Flujos de trabajo de tickets y colaboración | Integrarse con herramientas de gestión de tickets y colaboración para mejorar la eficiencia y la comunicación durante la remediación de riesgos. | Reducir el tiempo de resolución de incidents y aumentar la productividad mediante flujos de trabajo optimizados. |

FORTINET | COLOMBIA & ECUADOR

XPERTS26

# Tiempo de práctica


FORTINET
COLOMBIA
& ECUADOR
XPERTS26