FORESCOUT

Forescout Vistaro: IA que potencia la operación

Adriana García
LATAM Director

Omar Alcalá
Channel Account Manager

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026


Because the AIs will be
more evolutionarily

EL PAÍS

Mythos, el nuevo modelo de IA de Anthropic, desata la alarma mundial

La herramienta es capaz de detectar vulnerabilidades en los sistemas informáticos que dejarían expuesta la seguridad.

hace 2 días

Nexos

Mythos, poder y riesgo en la nueva inteligencia artificial – Sociedad y poder

Las alertas han quedado encendidas desde hace meses. Las capacidades de los modelos de inteligencia artificial más avanzados superan las...

hace 1 día

Cinco Días

El Bundesbank pide a la UE que solicite el acceso a Mythos para los bancos europeos para que puedan protegerse de posibles ciberataques

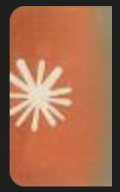
El Bundesbank ha pedido a la Unión Europea que solicite a Estados Unidos el acceso a Mythos para todos los bancos de la eurozona.

hace 6 horas

Xataka

"Tan bueno como los mejores humanos": Mozilla ha probado Claude Mythos y ha quedado tan asustada como impresionada

Las principales compañías de la IA están en la carrera por crear el mejor modelo de inteligencia artificial. Esa carrera la ha ganado...



Xataka

Zero-day para todos: la nueva IA de Anthropic ha encontrado vulnerabilidades en todos los sistemas operativos del mundo

Claude Mythos Preview ya está aquí y es tan bueno que asusta. Literalmente. Anthropic acaba de presentarlo en público, pero lo ha hecho con...

hace 3 semanas

EL PAÍS

Anthropic oculta su nuevo modelo de IA, Mythos, por ser demasiado peligroso

Para mitigar sus consecuencias potenciales, Anthropic ha creado un proyecto llamado Glasswing, una colaboración con 12 empresas que les permite...

hace 3 semanas

The New York Times

Mythos, el nuevo modelo de IA de Anthropic, activa las alarmas globales

La conmoción por Mythos se produce en un momento en el que existe una mínima cooperación internacional en materia de IA.

hace 2 días

RTVE.es

La doble cara de Mythos, el modelo de IA más avanzado de Anthropic: blindaje digital y amenaza estratégica

Diseñado para la investigación de seguridad avanzada, identifica y explota

NIST Updates NVD Operations to Address Record CVE Growth

New risk-based model will allow NIST to manage current CVE volume while modernizing the NVD for long-term sustainability.

April 15, 2026

We are working faster than ever. We enriched nearly 42,000 CVEs in 2025 — 45% more than any prior year. But this increased productivity is not enough to keep up with growing submissions. Therefore, we are instituting a new approach. The changes described below will allow us to focus on the most critical CVEs while being transparent about how we are managing our current workload. They will also allow us to stabilize the program while we develop the automated systems and workflow enhancements required for long-term sustainability.

third higher than the same period last year.

We are working faster than ever. We enriched nearly 42,000 CVEs in 2025 — 45% more than any prior year. But this increased productivity is not enough to keep up with growing submissions. Therefore, we are instituting a new approach. The changes described below will allow us to focus on the most critical CVEs while being transparent about how we are managing our current workload. They will also allow us to stabilize the

ORGANIZATIONS

Information Technology Laboratory

Computer Security Division

Problema de asimetría

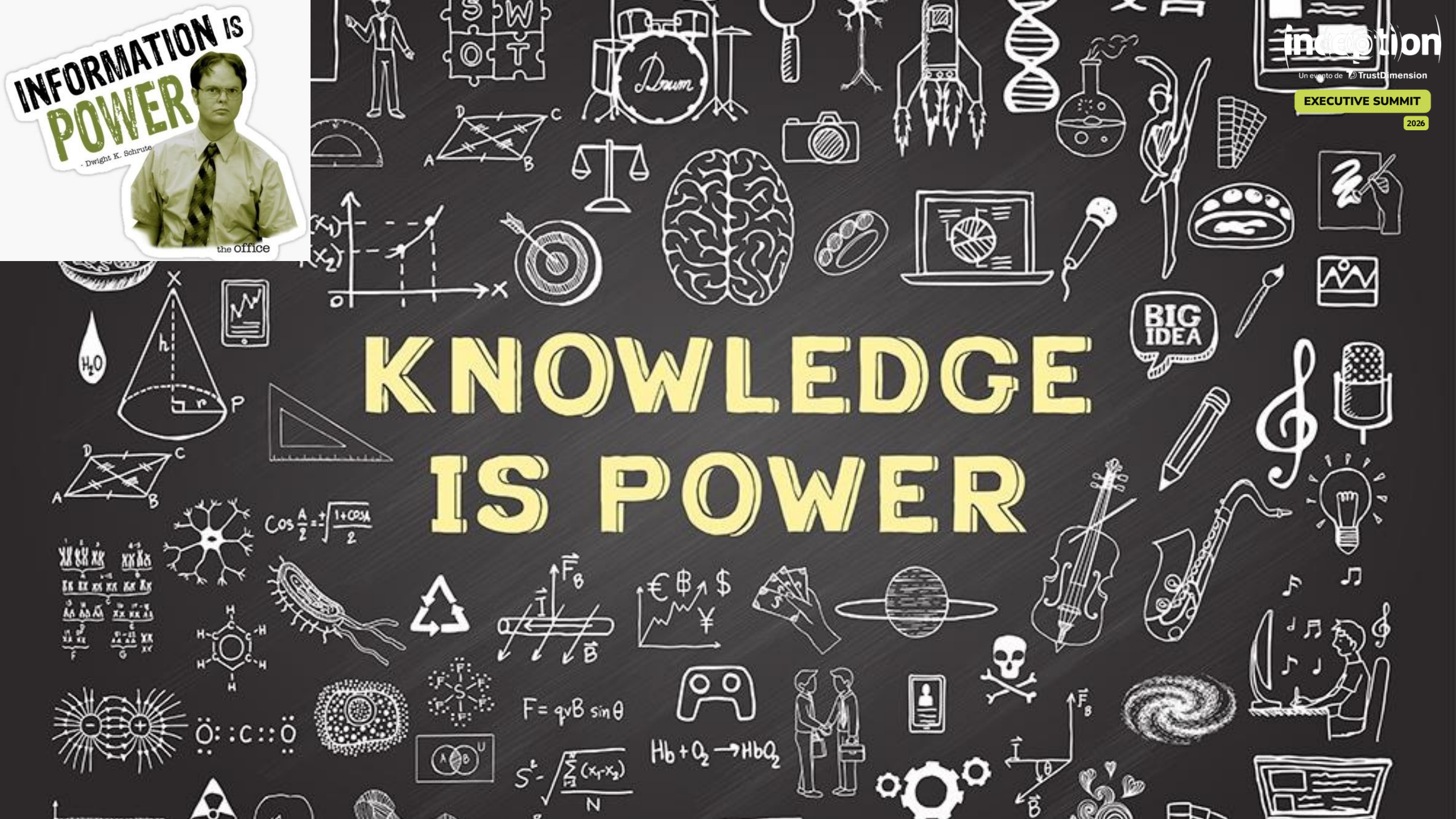
¿Cuál es mi exposici
¿Qué ha cambiado d[illegible] ayer a hoy?
¿Qué acciones debo tomar?

Dispositivos **Amenazas** **Comunicaciones** **Accesos**

Terceros

FORESCOUT


inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

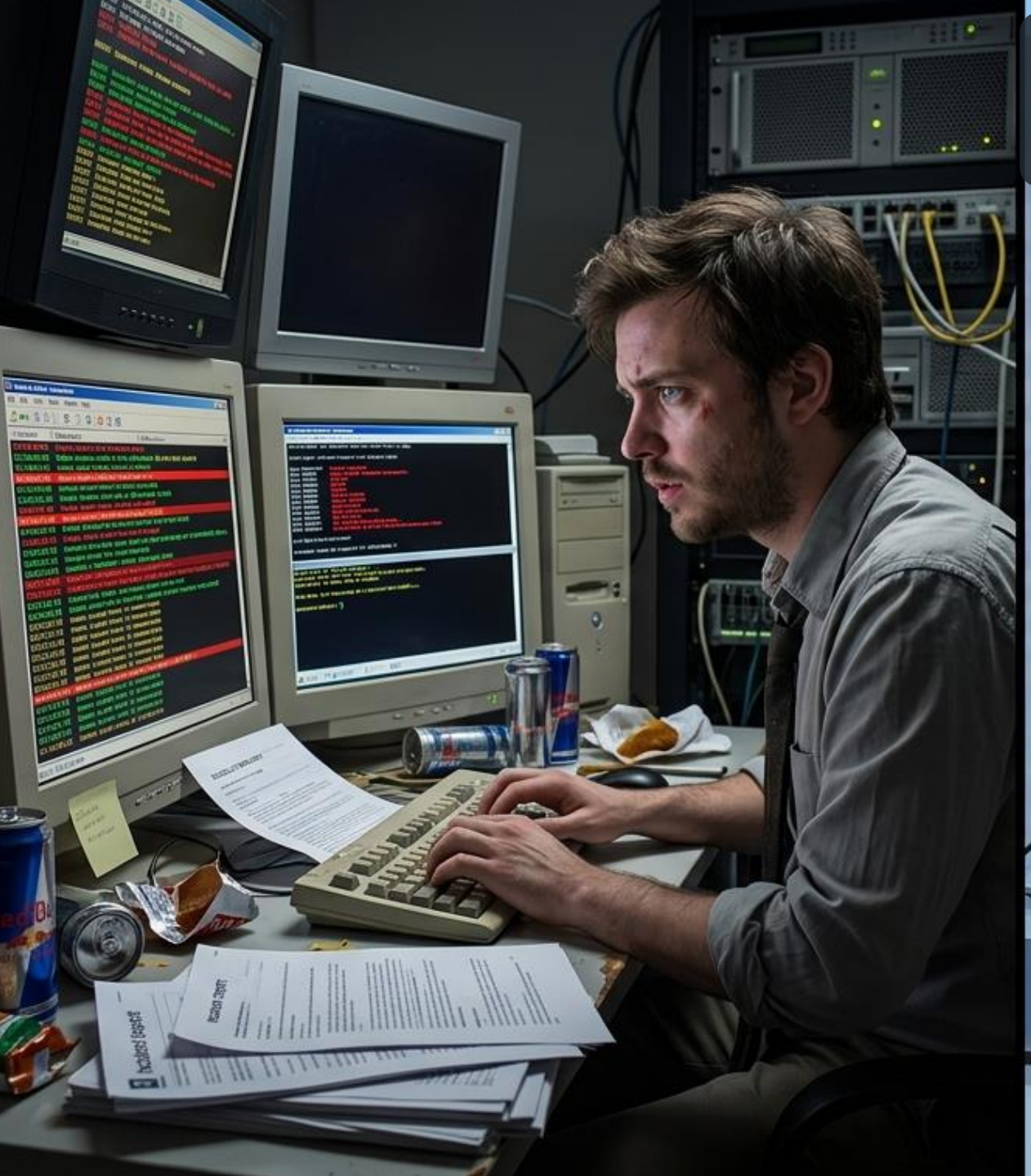


LA PROPUESTA DE FORESCOUT

Evolución de un SOC

IA CON PROPÓSITO

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026



IA

Forescout: 4D Platform™

DESCUBRIMIENTO

- Que hay realmente en tu red

EVALUACION

- Riesgos críticos, amenazas, superficie de ataque y exposición

CONTROL

- A escala para automatizar, priorizar y mitigar riesgos y amenazas

GOBIERNO

- Para lograr resultados y cumplimiento continuos

LAST UPDATE
A few seconds ago

1,833,032	1,206,720	424,656	120,672	31,952	49,032
ALL DEVICES	CAMPUS WIRED	CAMPUS WIRELESS	DATA CENTER	CLOUD	OT

FUNCTION

- 34% Employee Workstation
- 18% Mobile
- 10% Facilities
- 9% VOIP
- 8% Retail & Financial
- 6% Multimedia & Entertainment
- 3% Network Infrastructure
- 2% Wearables
- 10% Other

OPERATING SYSTEM

- 51% Windows
- 25% Linux
- 9% MacOS
- 7% iOS
- 3% Android
- 3% Cisco IOS
- 2% Unix

VENDOR & MODEL

- 53% Dell
- 20% Apple
- 9% Avaya
- 8% Cisco
- 5% Amazon
- 3% Axis
- 2% Google

DEVICES AT HIGH RISK

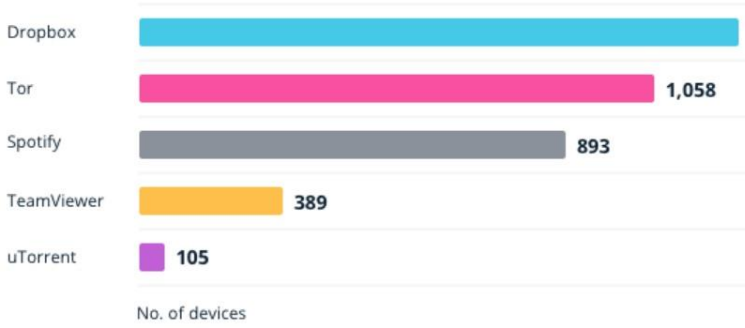
Last Hour

1,347 — 21% Devices with Weak Credentials	234 — 50% Windows Devices at Risk from WannaCry
847 — 10% OT Devices with Critical CVEs	454 — 14% Devices with Telnet (Port 23) Open

HIGHEST RISK IP CAMERAS

- 1,213 IP Cameras from Xiongmai
- 327 IP Cameras with Weak Credentials
- 214 IP Cameras with Telnet (Port 23) Open

TOP 5 UNAUTHORIZED WINDOWS APPLICATIONS INSTALLED

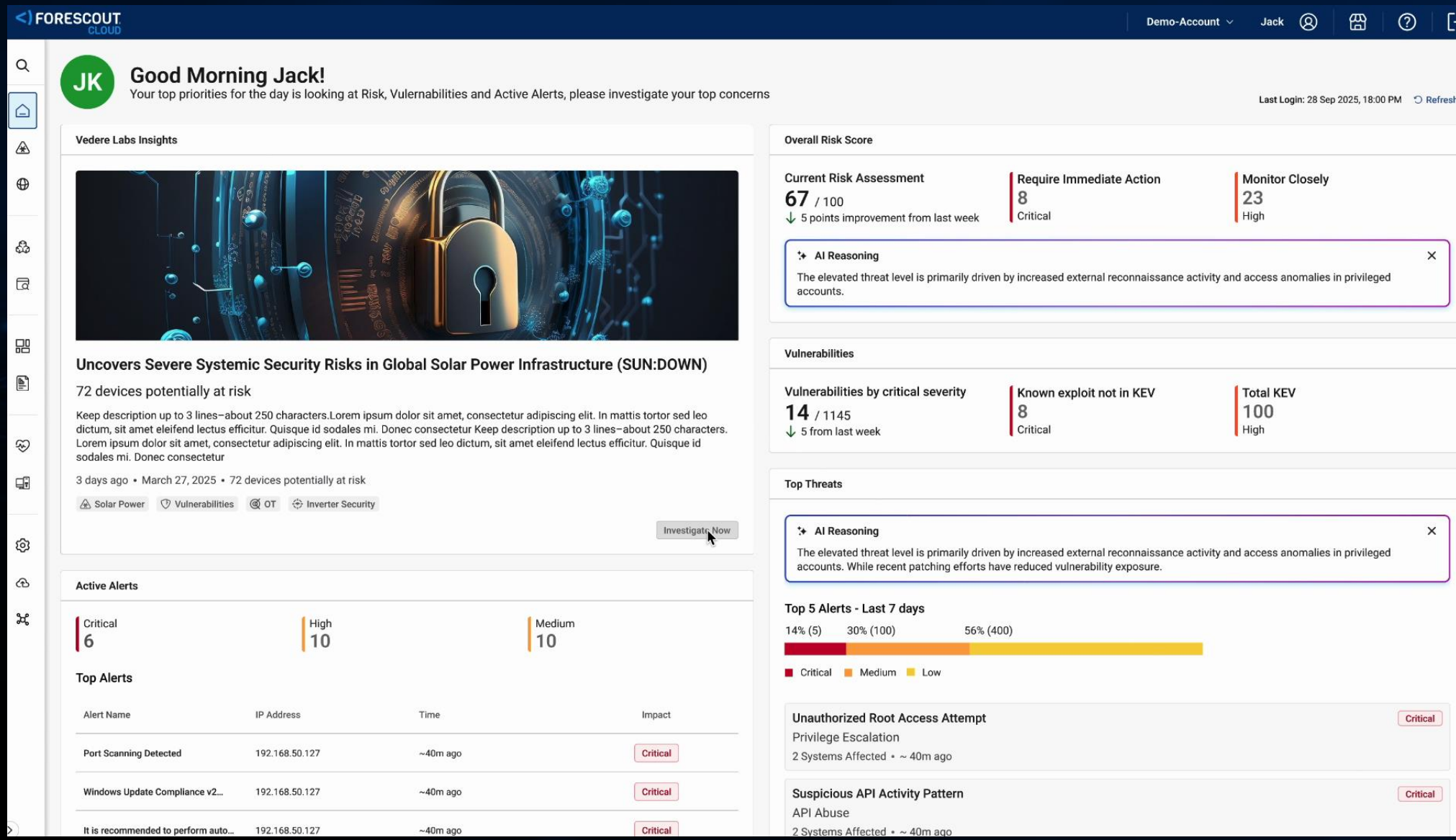


Agentic AI

- Preguntar
- Investigar
- Pensar

Forescout Vistaro AI

- Contexto
- Consecuencias
- Priorización



FORESCOUT

Fundamental Compliance

Continuous Assessment, Automated Enforcement

Forescout helps ensure fundamental compliance by providing real-time visibility and automated control across your entire network. It identifies all connected devices, including those unmanaged or unauthorized, ensuring they adhere to compliance policies

With automated policy enforcement, it can segment devices, block unauthorized access, or trigger alerts when issues arise. It simplifies compliance reporting by providing detailed audit trails and insights.

Conduct a comprehensive audit to identify compliance gaps

Generative AI

73% Investigate

Compliance Coverage

Start by reviewing the non-compliant areas and prioritizing high-risk vulnerabilities. Focus on critical assets and apply necessary controls.

82%

All Compliance

Regularly review and update compliance strategies to ensure ongoing improvement and alignment with regulatory standards.

Remediation Impact

Not Compliant	Compliant
55%	32%
	Compliant (Remediated) 13%

Maintain policies and continuous monitoring to ensure sustained compliance. Identify root causes, prioritize high-risk vulnerabilities, and initiate targeted remediation.

45% At Risk

Core Compliance

Core compliance is at 45%, indicating critical gaps. Focus on high-priority areas: identify non-compliant assets, enforce essential policies, and address vulnerabilities immediately. Leverage automated tools for efficient remediation and re-assess to track improvements toward compliance goals

92%

Endpoint Protection

Review the remaining 8% for any gaps or misconfigurations, prioritize updates or policy adjustments, and ensure continuous monitoring to maintain and improve protection levels.

20% At Risk

Encryption

This indicates significant risk. Prioritize encrypting sensitive data, starting with high-risk assets and communication channels.Implement automated encryption policies, ensure proper key management, and re-assess compliance to track progress.

79% Investigate

Firewall

Review misconfigured rules, ensure all critical assets are protected, and address identified gaps. Update policies to align with regulatory requirements, apply patches if needed, and re-assess firewall settings to enhance overall compliance and security.

10% At Risk

Extended Compliance

Extended compliance is at 10%, highlighting significant gaps that require immediate attention. Begin by identifying assets or systems currently outside the compliance scope and prioritize addressing high-risk areas with the greatest regulatory or business impact. Implement the necessary controls, applying policies, updates, or configurations, to bring these assets into compliance.

75% Investigate

Endpoint Security Compliance

79% Investigate

Encryption Standards Compliance

31% At Risk

Firewall and Network Security Compliance

96%

Data Protection and Privacy Compliance

IA que potencia y cambia nuestro trabajo

Forescout VistaroAI elimina el ruido, brinda dirección.
Inteligencia Artificial que acompaña a los expertos.

Menos tiempo

Donde comenzar

Respuestas rápidas

En cuanto se necesitan

Claridad

Táctico y estratégico
A todos los niveles

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

Lo que hacemos, importa

Gracias

Acelera la adopción de Zero Trust con IA con Forescout