JOINT SOLUTION BRIEF

Layered OT Cyber Defense for Critical Operations

Continuous asset intelligence across the network.
Probe-based detection inside the device.



FORESCOUT + CRYTICA SECURITY

FORESCOUT + CRYTICA

Layered OT Cyber Defense for Critical Operations

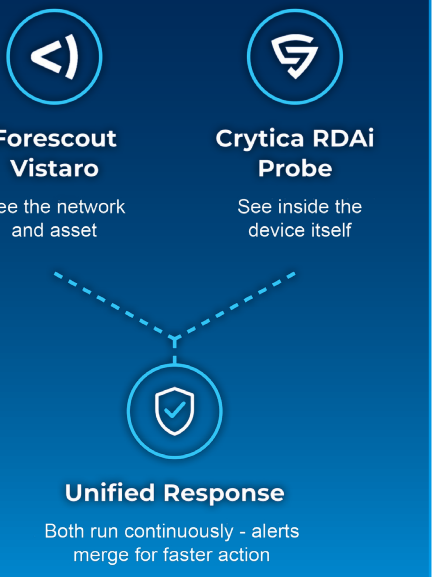
Continuous asset intelligence across the network. Probe-based detection inside the device.

CRYTICA SECURITY

BETTER TOGETHER

- Continuous integrity monitoring across OT, IoT and embedded devices where agents cannot operate.
- Deterministic Crytica alerts delivered into the Forescout Vistaro platform, enriched with asset context.
- Faster containment and support for Zero Trust, with device trust continuously verified rather than assumed.

WORKING TOGETHER



Overview

Operational technology carries the load in the sectors that cannot fail. As those environments converge with IT, the assets that matter most to the process are often the ones traditional security tooling cannot reach: teams can see the network around a controller, but not the instruction set running inside it.

Forescout closes that gap at the network and asset layer; Crytica Security closes it inside the device. The Forescout Vistaro™ platform continuously discovers, assesses, controls and governs every connected asset across IT, IoT, IoMT and OT without an agent. Crytica's patented Rapid Detection, Alert, and isolation (RDAi™) solution embeds a tiny Probe, as small as 70KB, within the device itself and detects unauthorized changes to instruction sets within seconds.

The OT Challenge

- Devices that cannot host security software. PLCs, RTUs, HMIs and embedded controllers lack the resources, operating system or change window for conventional endpoint tooling.
- Network monitoring sees traffic, not integrity. A change written into a controller's instruction set may generate no anomalous traffic until the altered logic executes against a physical process.
- Response bounded by safety and uptime. Isolating a compromised asset can halt a process, so containment requires evidence precise enough to justify the operational cost.

The Solution: Forescout + Crytica

How the Layers Fit Together

Network and asset layer
Discovery, classification, posture assessment, risk scoring, access control and zone-based segmentation across IT, OT, IoT and IoMT — *Forescout Vistaro Platform (eyeSight, eyeInspect, eyeControl, eyeSegment)*

Device layer
Deterministic detection of unauthorized changes to instruction sets, at the moment of injection and before execution — *Crytica RDAi Probe*

Operations layer
Alert enrichment with asset context, correlation across IT and OT data sources, and orchestrated response — *Forescout eyeAlert and eyeFocus, consuming Crytica Threat and Performance Alerts*

Platform Capabilities

1. Forescout Vistaro™ Platform: Core Capabilities

The platform answers what is connected, how exposed it is and what can be done about it — continuously, and without touching the endpoint.

eyeSight
Agentless discovery, classification, and posture assessment of every IP-connected asset

eyeInspect
Deep packet inspection across 350+ OT and ICS protocols, asset intelligence, change tracking, and OT threat detection

eyeControl
Policy-based network access control, automated remediation, and containment actions

eyeSegment
Design, simulation and enforcement of zone-based segmentation

eyeAlert
Alert correlation and orchestrated response across 180+ IT and OT data sources

eyeFocus
Unified cyber and operational risk metrics and executive reporting across IT and OT

© 2026 Forescout. All rights reserved.

2. Crytica RDAi: Probe-Based Change, Event and Threat Detection

Everything above observes the device from the outside. RDAi observes it from the inside. RDAi embeds a Probe, as small as 70KB, directly within the protected device. The footprint is tiny, with minimal performance impact even in constrained environments, which is what makes device-level monitoring viable on controllers, embedded systems and legacy equipment.

Detection is deterministic. RDAi detects unauthorized changes to instruction sets with certainty rather than inference, which holds false positives down and produces alerts confident enough to justify action on a live process. It detects at the moment of injection, before execution, cutting detection time from an industry average of months to seconds. Both alert types flow into the Vistaro platform, where asset context makes them actionable.

Crytica Threat Alerts

Deterministic alerts based on unauthorized changes to instruction sets, detected at the moment of injection and before execution

Crytica Performance Alerts

Actionable alerts based on measured system performance against predefined thresholds, flagging anomalies that may indicate emerging threats or operational issues

FORESCOUT

Experience the Forescout Vistaro™ platform today.

GET STARTED »

About Forescout

As AI-driven vulnerability discovery and exploitation accelerate attack velocity to machine speed, Forescout is a foundational cyber defense layer that allows organizations to segment and isolate compromised systems, block lateral movement, and automate response across IT, OT, IoT, and IoMT environments. The Forescout Vistaro™ platform, powered by agentic AI and enhanced with Vedere Labs threat intelligence, delivers a Universal Zero Trust Network Access (UZTNA) architecture that integrates seamlessly with 180+ security and IT products. With Forescout Vistaro, organizations get comprehensive inventory and classification of both managed and unmanaged assets, continuous exposure management, and real-time protection including dynamic network segmentation and automated threat response.

About Crytica Security

Crytica Security's patented technologies form the world's first Rapid Detection, Alert, and isolation (RDAi™) solution, embedding directly within Operational Technology (OT), Information Technology (IT), and Internet of Things (IoT) environments to rapidly detect unauthorized changes to instruction sets within seconds. Designed to complement and enhance existing XDR, MDR, and EDR cyberstacks, RDAi extends visibility into devices and environments where traditional tools cannot operate, delivering deterministic detection and actionable alerts for national security and mission-critical infrastructures.

FORESCOUT

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com

©2026 Forescout Technologies, Inc. All rights reserved.
Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.forescout.com/company/legal. Other brands, products, or service names may be trademarks or service marks of their respective owners.
09_26_V02