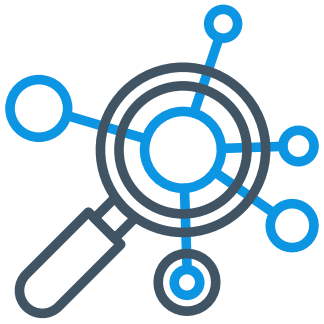
FORESCOUT

Forescout TDR

Threat Detection & Response



SOC Efficiency: Unmasking Genuine Threats

With today's ever growing threat landscape, Security Operations Center (SOC) teams are overwhelmed with daily alerts, which often leads to alert fatigue. Many of these alerts lack crucial context and accuracy, resulting in an onslaught of false positives. As a result, critical threats slip through the cracks, leaving organizations vulnerable to potential breaches.

Additionally, organizations face difficulties in acquiring and retaining the necessary security resources vital for effective SOC operations. These two challenges have prompted many companies to seek solutions for improving the capabilities of security analysts through automation and threat intelligence.

Forescout helps alleviate the burden on SOC teams, empowering them to effectively detect, investigate and respond to threats while optimizing resource utilization.

Solution Overview

Forescout TDR converts telemetry and logs into high fidelity, SOC-actionable probable threats. It automates and accelerates the process of detecting, investigating, hunting for and responding to advanced threats across the entire enterprise. From cloud, campus, remote and datacenter environments to IT, OT/ICS, IoT and IoMT devices, Forescout TDR combines essential SOC technologies and functions into a unified, cloud-native platform —and makes it viewable and actionable within a single console.

Business Value

- **Reduces the risk** of a disruptive cyber-attack or data breach
- **Optimizes security operations** and SOC efficiency by simplifying and accelerating threat detection, investigation, hunting and response processes
- **Reduces costs** related to SOC point solutions, analyst turnover, data onboarding, and rules management
- **Supports compliance** with key regulations
- **Leverages IT and security investments** while providing enhanced visibility across the entire threat lifecycle in a single pane of glass

The Forescout Advantage

Vendor- and EDR- Agnostic Data Ingestion

- Supports the products and vendors you're already invested in
- Can ingest data from any managed and unmanaged device (IT, OT/ICS, IoT, IoMT)
- Ensures more comprehensive, powerful, flexible and effective threat detection

450x Better Detections

- Advanced data pipeline enforces a common information model (CIM) to normalize ingested data and auto enrich with user info, IP attribution, geolocation, critical asset information
- Two-stage threat detection engine uses five techniques to reduce noise and improve fidelity

Full Spectrum Response

- Powerful investigation tools, and native integrations with case management solutions
- Automate responses via Forescout solutions to touch all managed and un-managed connected devices across the enterprise

Upfront Risk Reduction

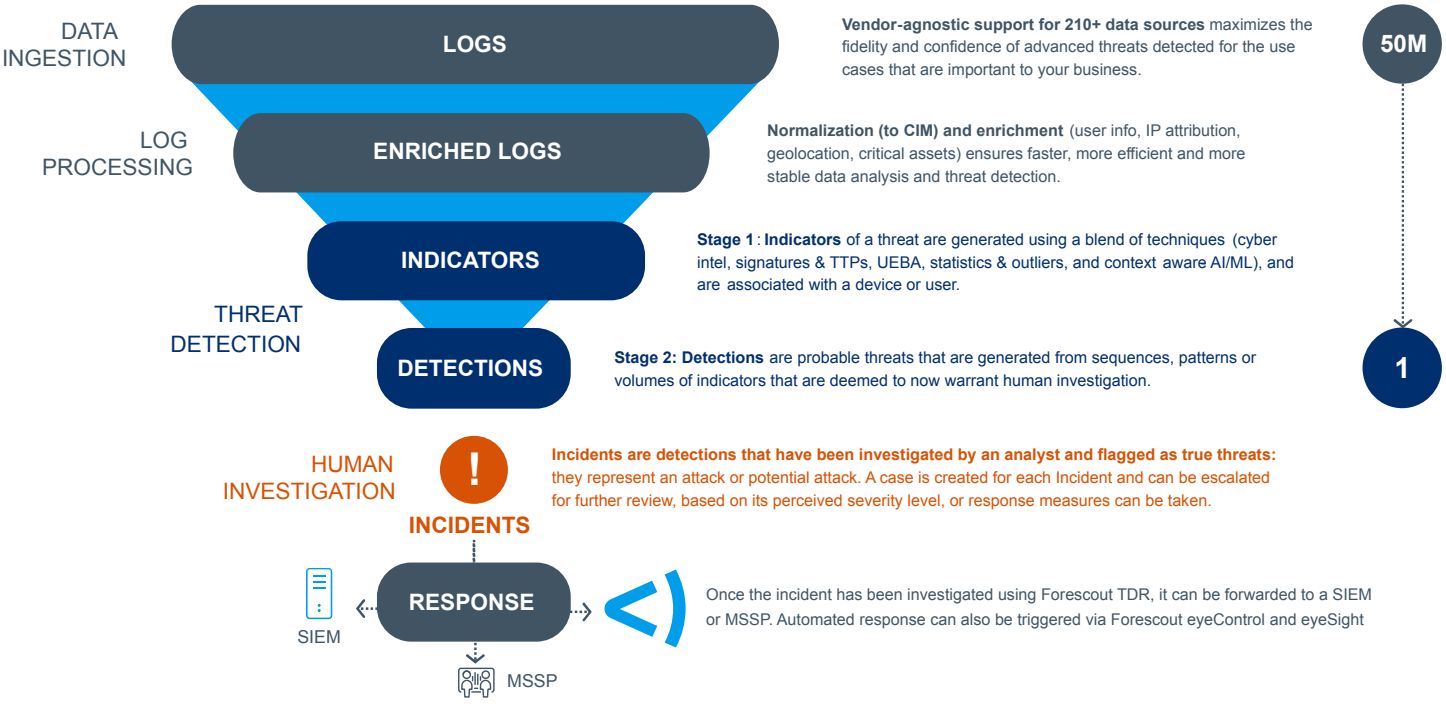
- Integration with Forescout solutions reduces the attack surface and the risk of a compromised or non-compliant device ever connecting to your network
- Continuously monitors all connected assets with dynamic access policies

Simple, Predicatible & Accessible Pricing

- No penalties for sending more logs to Forescout TDR, to support better detection
- License fee is based on the total number of endpoints (IP/MAC address) in your organization
- Pricing includes 31-day log storage, and longer-term storage options are available

1 Detection per Hour, from 50 Million Logs

Through the rigorous application of data engineering, data science and automation, Forescout TDR typically generates 1 high fidelity detection (probable threat) that warrants analyst investigation, for every 50 million logs ingested, per hour.



Key Features

- **Data Ingestion** Vendor- and EDR- agnostic support for >210 sources
- **Data Onboarding** Forescout data engineers implement data pipeline
- **MITRE ATT&CK® Integration** Prioritize data ingestion. Identify TTP blind spots
- **Data Pipeline** Normalization to CIM, and enrichment improves threat detection
- **Data Lake** Tiered storage (Hot, Warm, Cold) with rapid full-text search
- T**hreat Detection Engine** Blend of five techniques generates high-fidelity, high-confidence threats
- **Detection Rules** >1500 verified rules and models, with intuitive custom rules creation
- **Threat Intelligence** >70 global sources, and classified, corroborated & scored
- **UEBA** Behavior-based analytics detects anomalous activity
- **Dashboards** Pre-configured, customizable, persona-based
- **SOAR** Automated response via SIEMs, Forescout products and third-party solutions.
- **Case Management** Workflow, and integration with third party solutions
- **Cloud-native Solution** Nothing to deploy. New features, fixes and rules delivered seamlessly, bi-weekly
- **Multi-tenant Architecture** Create logical separations (regions, business units, etc.) while maintaining a global view
- **Global Architecture** Meet local data residency requirements with global points of presence (six as of H1 2024)
- **Artificial Intelligence** Utilizes generative AI and Machine Learning to augment and simplify security

Visit www.forescout.com/solutions/threat-detection-and-response/ to learn more.

Service and product descriptions contained herein are provide for information use only and do not constitute official documentation.

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