Forescout XDR

eXtended Detection and Response

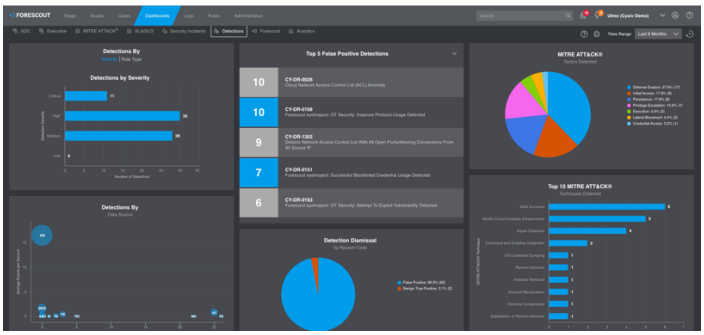
Improve SOC efficiency by 450x with better detection and response of true threats

Security operations center (SOC) teams face a daily barrage of incomplete and inaccurate alerts that lack vital contextual information, many of them false positives. As a result, analysts miss critical threats and take longer to investigate and respond to them, increasing the risk of a breach. In fact, the typical SOC receives an estimated 11,000 alerts per day, or 450 alerts per hour[1] – most of them low fidelity, low confidence alerts, and false positives.

With Forescout® XDR, that number is reduced to one SOC-actionable detection an hour – or one probable threat that warrants human investigation.[2]

Solution Overview

Forescout XDR 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 including cloud, campus, remote and datacenter environments, and from IT, OT/ICS, IoT and IoMT devices by combining essential SOC technologies and functions into a unified, cloud-native platform, viewable and actionable from a single console.



Business Value

- **Reduces the risk** of a disruptive cyber-attack or data breach
- **Optimizes security operations** 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've 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
- 2-stage threat detection engine uses a blend of 5 techniques to reduce noise & improve fidelity

Full Spectrum Response

- Powerful investigation tools
- Native integrations with case management solutions
- Automate responses via Forescout solutions to touch all managed & un-managed devices

Upfront Risk Reduction

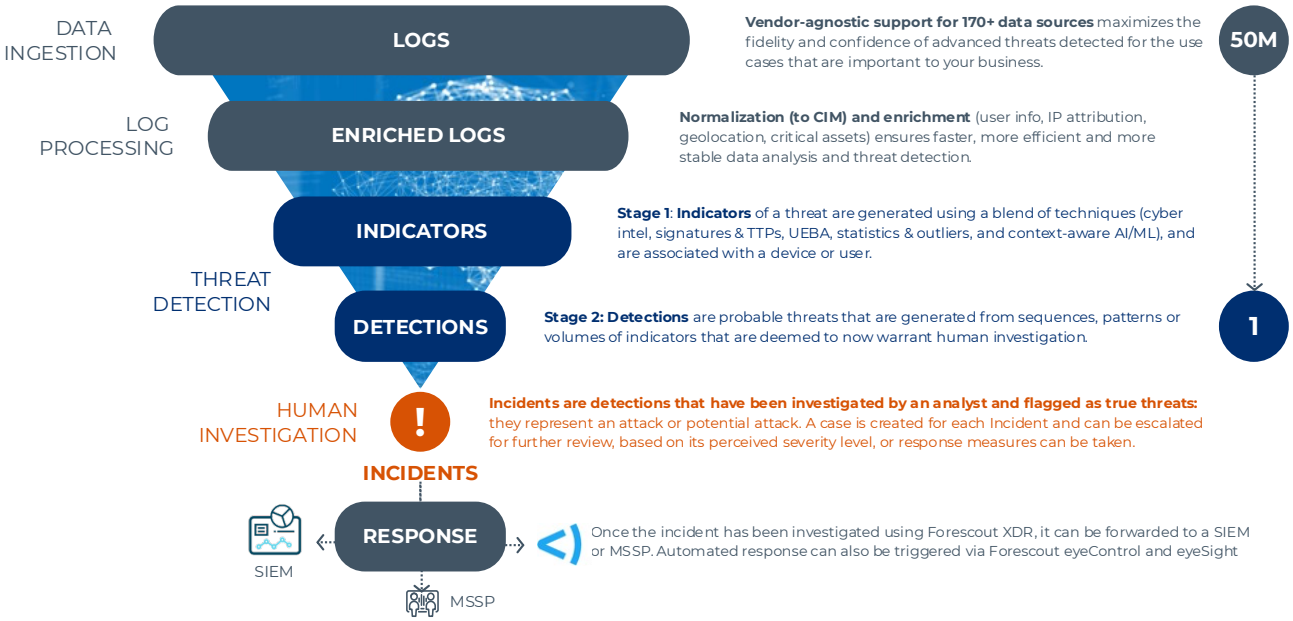
- Integration with other Forescout solutions reduces the attack surface, and the risk of a compromised or non-compliant device connecting to your network in the first place
- Continuously monitors all connected assets with dynamic access policies

Simple, Predictable & Accessible Pricing

- No penalties for sending more logs to Forescout XDR, 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 XDR typically generates 1 high fidelity detection (probable threat) that warrants analyst investigation, for every 50 million logs ingested, per hour.[2]



Key Features

Data Ingestion	Vendor- and EDR- agnostic support for >170 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
Threat Detection Engine	Blend of 5 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
Case Management	Workflow, and integration with 3rd 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…) while maintaining a global view
Global Architecture	Meet local data residency requirements, with global query

Visit www.forescout.com/xdr to learn more (March 2023).

[1] "The2020 State of Security Operations", Forrester Consulting
[2] Based on aggregate Forescout client data from a 1-year period (Dec 2021-2022) across 30 enterprises, representing a range of company sizes and industries.

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