SOLUTION BRIEF

Forescout eyeAlert

Threat Detection & Response

FORESCOUT®

Forescout eyeAlert

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 that enhance the capabilities of security analysts through automation and threat intelligence.

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

Business Value

Reduces Business Risk

Lessens the risk and magnitude of a successful attack or data breach and eliminating virtually all alert "noise."

This enables SOC teams to more quickly and accurately detect, investigate and respond to the broadest range of advanced threats from across the entire enterprise.

In doing so, Forescout eyeAlert helps enable you to avoid business disruptions and costs resulting from a successful attack or breach.

Optimizes security operations

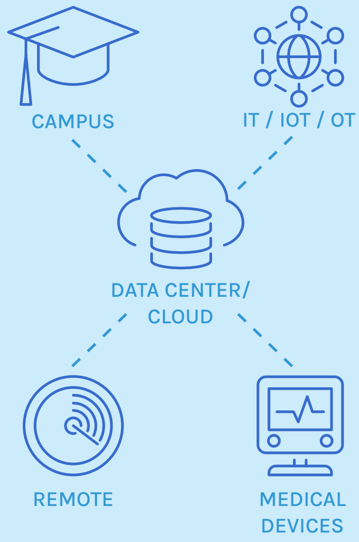
Drives SOC efficiency and effectiveness. Automatically enriches and normalizes key data and correlates signals to produce a small number of high-fidelity, high-confidence detections that truly warrant analyst investigation. It simplifies and accelerates complex investigation and threat-hunting processes with more complete, accurate information and contextual data, all from a unified console that integrates with other Forescout solutions and third- party SIEMs, case management systems and response solutions.

Forescout eyeAlert provides enhanced visibility across the entire threat lifecycle via preconfigured, customizable dashboards and reports, with key performance indicators (KPIs) tailored to analysts/IR, engineers, SOC managers, compliance/risk managers and executives. As a result, SOC teams can spend more time on higher-value security activities.

Solution Overview

Forescout converts telemetry and logs into high fidelity, SOC-actionable probable threats.

It automates the detection, investigation, hunt for and response to advanced threats across all connected assets – IT, OT/ICS, IoT and IoMT – from campus to cloud to data center to edge. Forescout combines essential SOC technologies and functions into a unified, cloud-native platform, viewable and actionable from a single console.



Forescout leverages data from across the extended enterprise, including from managed and unmanaged (agentless) devices.

Reduces Cost

Lowers SOC spending related to:

- Licensing and managing multiple SOC point solutions including data lakes; security analytics; security orchestration, automation and response (SOAR); user and entity behavior analytics (UEBA); and threat intel platforms
- Log storage
- Analyst burnout, turnover, recruiting and training
- Supporting new data sources
- Creating and tuning rules

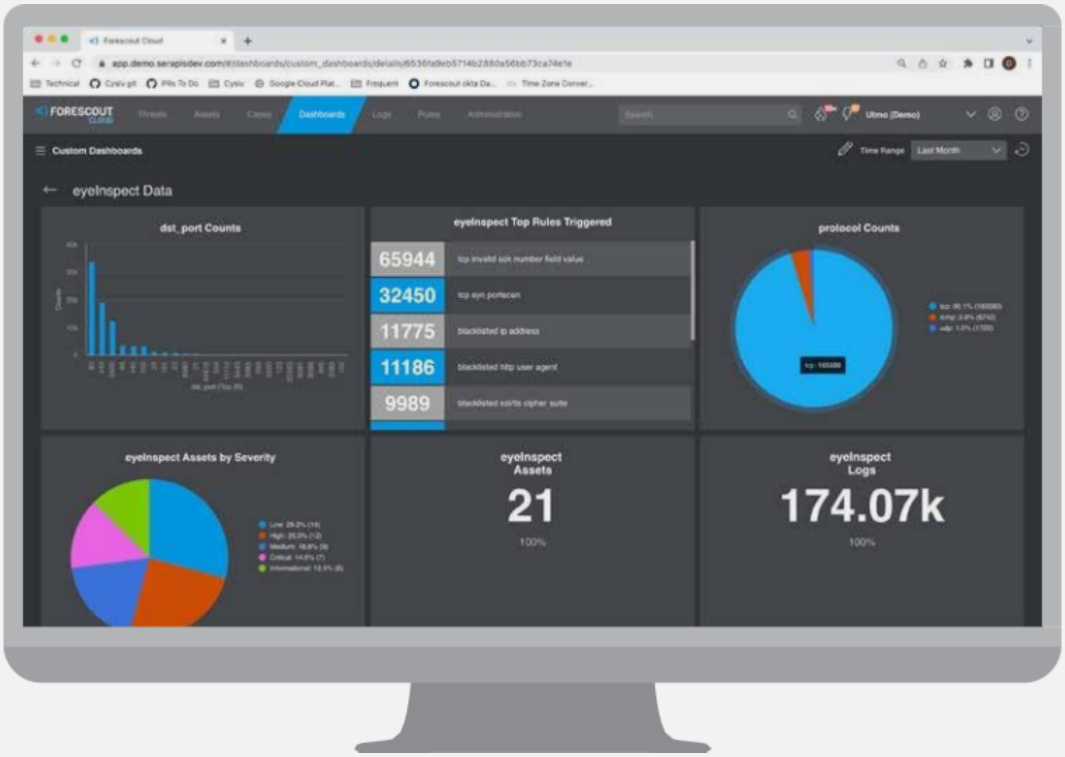
Supports compliance

Provides several hot and cold storage options, automated threat detection and threat intelligence to support compliance with key regulations and standards. This helps close the potential gap between when a breach or disruption is noticed and when a response action is taken.

Leverages existing security investments

Increases the value of your Forescout solutions as well as your network, endpoint and cloud security sensors; and enforcement points, regardless of vendor. With Forescout eyeAlert, there's no need to deploy new, vendor-specific software or hardware.

Key metrics and trends support better management of SOC performance.



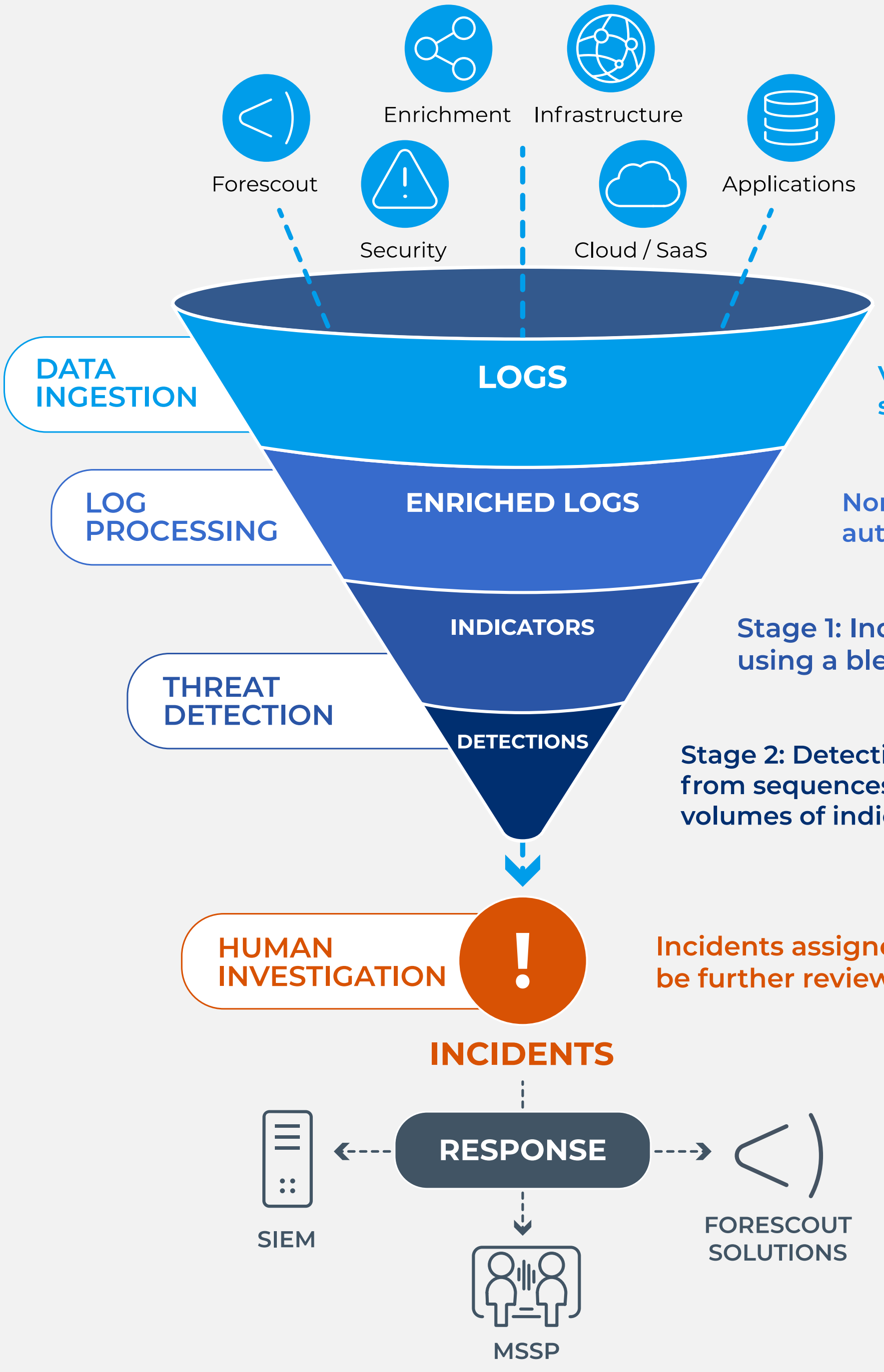
eyeInspect Top Rules Triggered

65944	tcp invalid ack number field value
32450	tcp syn portscan
11775	blacklisted ip address
11186	blacklisted http user agent
9989	blacklisted ssl/tls cipher suite

eyeInspect Assets
21
100%

eyeInspect Logs
174.07k
100%

Preconfigured and customizable persona-based dashboards and reports provide KPIs relevant to a variety of roles, including analysts/IR, engineers, SOC manager, compliance and risk managers, and executives.



Vendor-and EDR-agnostic support for 170+ data sources

Normalization to CIM and automated enrichment

Stage 1: Indicators generated using a blend of five techniques

Stage 2: Detections generated from sequences, patterns or volumes of indicators

Incidents assigned a case that can be further reviewed or acted on

Automated orchestration and response via Forescout solutions (eyeControl and eyeSight), and via SIEM and MSSPs

Why Forescout

Forescout eyeAlert, together with other Forescout solutions as part of the Forescout 4D Platform™, uniquely delivers vendor- and EDR-agnostic data ingestion and better detection, with full-spectrum response and upfront risk reduction, all with predictable and accessible pricing.

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

Better detection

- 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 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 and accessible pricing

- No penalties for sending more logs to Forescout eyeAlert, to support better detection
- License fee is based on the total number of endpoints (IP/MAC address) in your organization
- Pricing includes several hot and cold storage options to meet your business needs

Key Features

Forescout eyeAlert combines essential SOC technologies and functions into a single, unified, cloud-native console.

Data Ingestion

Natively supports Forescout 4D Platform™ data – and more than 210 vendor- and EDR-agnostic sources including:

- **Security**: Firewall, network IDS/IPS, EDR, endpoint protection platform (EPP), server/workload/container security, web proxy and email security
- **Infrastructure**: Windows security, AD authentication, IAM, DHCP, DNS, cloud audit trail and network metadata
- **Enrichment**: Identity (LDAP), asset inventory and classification, configuration management, vulnerability scan results, and threat intelligence (indicators of compromise, or IOCs)
- **Applications**: Database, ERP, CRM and APIs
- **Cloud/SaaS**: AWS, Microsoft Azure, Google Cloud, Microsoft 365, Google Workspace and any other SaaS application

Data Onboarding

Helps ensure that you extract maximum detection value to support your most important use cases. Forescout data engineers work alongside your team to plan and prioritize the data sources to be onboarded, then help configure the data pipeline and ensure your data is being properly parsed, cleansed, normalized and enriched.

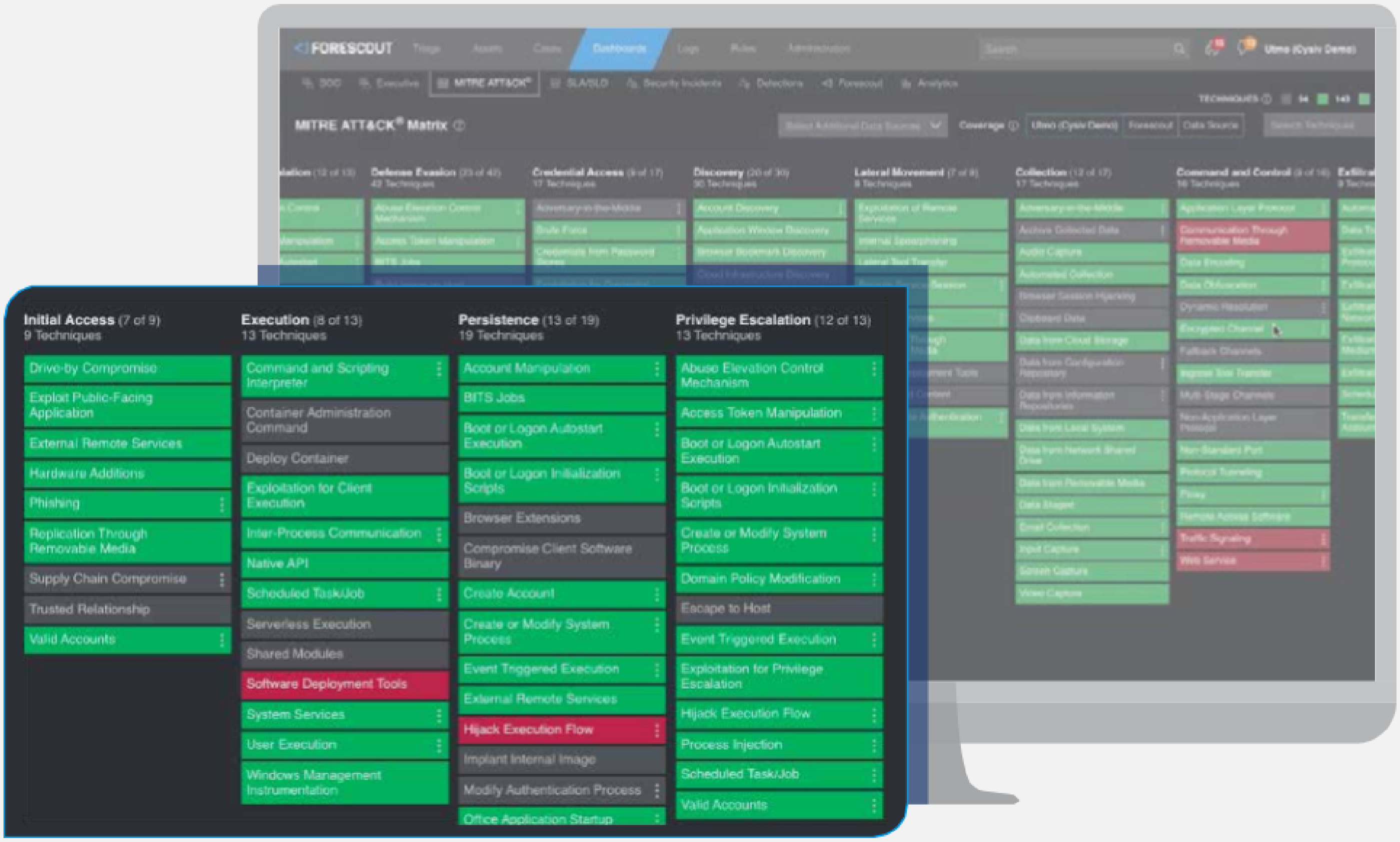
Advanced data pipeline

Applies a rigorous data science-centric approach to how it manages data flowing from enterprise-wide sources into its advanced threat detection engine. First, Forescout eyeAlert enforces a common information model (CIM) to normalize ingested data. Next, it automatically enriches that data with IP address, geolocation, ADObject properties, configuration and other contextual data for security context. This maximizes security detection value and facilitates faster correlations and threat hunting across multiple data sources. Finally, it uses an ETL (extract- transform-load) process that allows for faster, stabler, more efficient data analysis than more common ELT (extract-load-transform) processes.

MITRE ATT&CK® framework integration

The MITRE ATT&CK framework tracks cyber adversary tactics and techniques across the entire attack lifecycle. Forescout eyeAlert's integrates into this framework, to allow you to instantly see how different data sources that should be ingested for broad or specific TTP coverage, to identify potential blind spots that adversaries can exploit and to determine which additional data sources would further elevate your coverage.

MITRE ATT&CK framework integration identifies potential blind spots and opportunities to improve threat detection through the addition of other data sources.



Initial Access (7 of 9) 9 Techniques	Execution (8 of 13) 13 Techniques	Persistence (13 of 19) 19 Techniques	Privilege Escalation (12 of 13) 13 Techniques
Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism
Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation
External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution
Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts
Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process
Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification
Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host
Trusted Relationship	Serverless Execution	Create or Modify System Process	Event Triggered Execution
Valid Accounts	Shared Modules	Event Triggered Execution	Exploitation for Privilege Escalation
	Software Deployment Tools	External Remote Services	Hijack Execution Flow
	System Services	Hijack Execution Flow	Process Injection
	User Execution	Implant Internal Image	Scheduled Task/Job
	Windows Management Instrumentation	Modify Authentication Process	Valid Accounts
		Office Application Startup	

Cloud-based data lake

Massively scalable, purpose-built, indexed data lake with tiered data storage (hot, warm, cold) and rapid, full-text search. This provides cost-effective short-term and optional longer-term (7 days to 1 year+) log retention and management of either raw telemetry or enriched data, in support of security and compliance requirements.

Detection rules

Includes more than 1,500 verified, out-of-the box detection rules and models for your data sources. These rules have been tested on production data to ensure they operate effectively and deliver value on Day One. Custom detection rules give you the power and flexibility to quickly create indicator, detection and health rules that address your unique requirements, with a guided user experience.

Threat detection engine

Two-stage threat detection engine applies five detection techniques to automatically generate high-fidelity, high-confidence true threats that warrant investigation, while weeding out false positives (“noise”):

- **Signatures**: Match object attributes to a known bad object to identify threats inside raw telemetry, uncleanable malware or ransomware, for example.

- **UEBA**: Looks for abnormal behaviors that match a digital pattern, footprint, human activity or network behavior with known bad behavior. Ex: a sales rep downloading thousands of records from your CRM, unusual activity outside of normal office hours, beaconing, improbable distance traveled.

- **Statistics and outliers**: Uses clustering, grouping, stack counting, baseline and variation, outlier detection, logistic regression and other methods to detect anomalous activity. Ex: log sources going down, denial of service attacks.

- **Algorithms**: Uses context-aware AI and ML techniques such as supervised/unsupervised learning or deep learning to detect malicious or anomalous activity or to predict attacks. Ex: identifying process paths or domain generation algorithms (DGAs).

- **Threat** intelligence: More than 70 sources of cyber intelligence leveraged to look for things like backdoors and command-and-control traffic, or people reaching out to malicious phishing sites.

Advanced Threat Detection

- Sample list of threats that can be detected with Forescout
- Application abuse
- Brute-force attacks
- Buffer overflow attacks
- Cloud resources scanning
- Cloud service misconfigurations
- Cloud: Unauthorized access
- Cloud: Unsecure storage detection
- Command & Control connection
- Compliance violations
- Cross site scripting
- Cryptojacking
- Data exfiltration
- File access failures
- Illegal resource access
- Insider threats
- Lateral movement
- Malware/outbreaks
- Network scanning
- Password cracking
- Phishing attacks
- Port and vulnerability scans
- Ransomware
- SQL injection
- Suspicious behavior
- Unauthorized access to systems
- Unauthorized changes to firewall rules
- Unauthorized service restarts
- Unauthorized service/process creation
- Vulnerability exploitation
- Web application misconfiguration
- Web-application attacks (All Layer-7 web attacks)
- Worm / virus outbreak

Threat intelligence

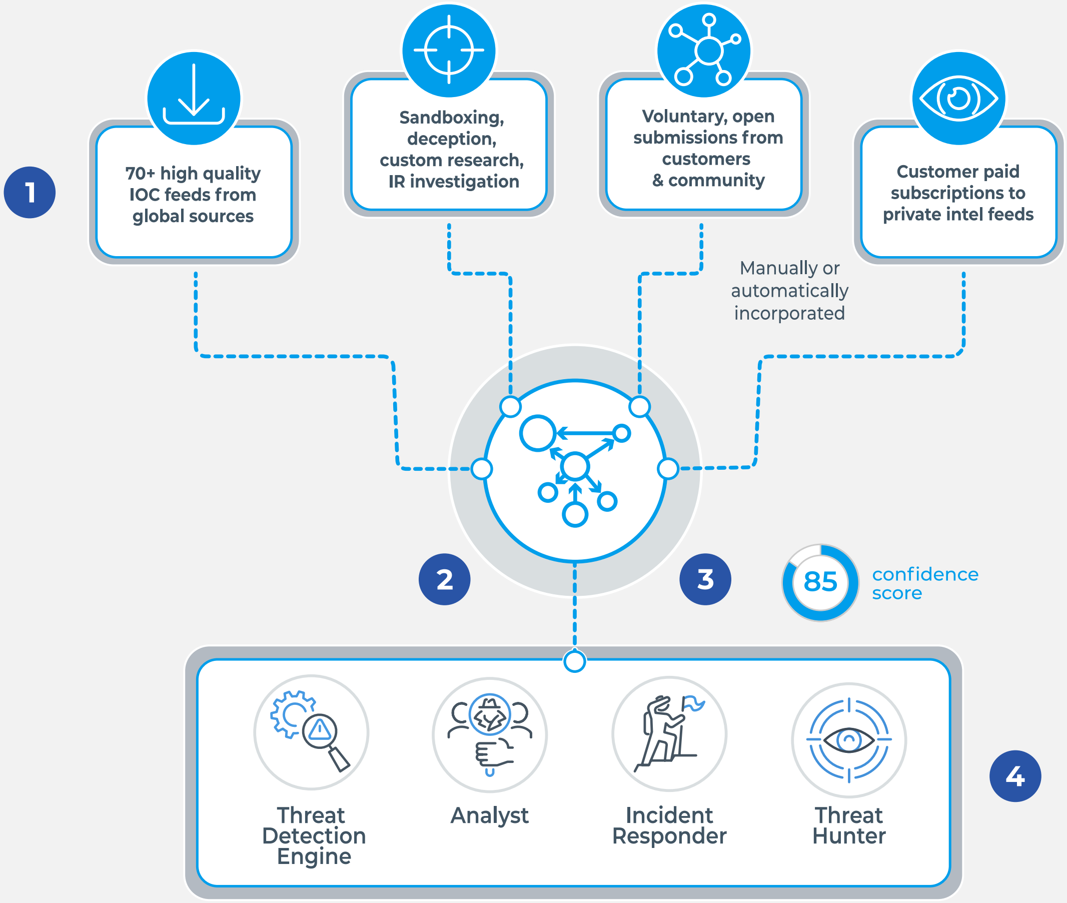
IOCs from over 70 high-quality sources worldwide, including from Vedere Labs, Forescout's team of global research experts. These IOCs are classified, corroborated and scored to provide finished intelligence that is automatically leveraged across the threat detection, hunting and investigation process. You have access to detailed threat reports from Forescout researchers that profile key threat actors and threats. Anonymized IOC data can also be shared among opt-in community members, including industry-specific ISACs, via a built-in community threat exchange.

1. Forescout leverages IOC data from a broad range of reliable sources

2. IOC intel is correlated into a searchable graph model database of "known bad" domains, URLs and IPv4 & IPv6 addresses

3. Each IOC is dynamically assigned a confidence score based on an assessment of the quality of the source

4. This confidence-scored IOC intel is then leveraged by the threat detection engine, and by customer SOC teams, to accelerate and improve the threat detection and investigation process


1
70+ high quality IOC feeds from global sources
Sandboxing, deception, custom research, IR investigation
Voluntary, open submissions from customers & community
Customer paid subscriptions to private intel feeds
Manually or automatically incorporated
2
3
85
confidence score
Threat Detection Engine
Analyst
Incident Responder
Threat Hunter
4

UEBA

Behavior-based analytics are used to detect significant changes to behavior or anomalous activity for an entity. Standard profiles and behaviors are built for users and hosts across time, and any activity that is anomalous to these standard baselines is triggered as suspicious.

Dashboards and reports

Preconfigured and customizable persona-based dashboards provide KPIs relevant to a variety of roles, including analysts/IR, engineers, SOC manager, compliance and risk managers, and executives. Proactive dissemination and sharing of reports and/or metric delivers insight into the hands of those responsible for managing SOC operations as well as executive team members.

SOAR

Orchestrates the SOC process from detection through investigation and response with built-in case management and notifications. Forescout eyeAlert automates security through enrichment sources such as IP geolocation, user and asset information, and correlation to multiple intelligence sources. It leverages the Forescout 4D Platform™ for automated orchestration and response workflows that can touch every managed and unmanaged (un-agentable) device across your enterprise. You can also continue through integration with 3rd party solutions such as Microsoft ExtraID, Microsoft Defender ATP, Trendmicro, VisionOne, Service Now, Crowdstrike Falcon, and the list is growing.

SIEM integration

True threats identified by Forescout eyeAlert can be fed to an existing SIEM for centralized orchestration and incident response.

Continuous software and content updates

New features, functionality and fixes, along with new detection rules and models, are seamlessly delivered every few weeks, without requiring any operational support or causing disruption.

Multi-tenant architecture

Logical separations (or tenants) easily created based on country, office location or business unit, for example. You can also generate aggregate views and perform queries and analyses across tenants and business units, right up to the global level. This is particularly beneficial for large enterprises, multinationals, MSSPs and organizations with regional SOCs.

Unified global architecture

Data residency and compliance requirements readily met, with cost-effective support for regional security operations. Specify where you want your logs to be stored among 25 regions across the Americas, Europe and Asia-Pacific – while still being able to view and query your data globally.

Cloud-native

Nothing to deploy, with new features, fixes and rules delivered seamlessly, bi-weekly.

Artificial Intelligence

Empowers cybersecurity operators to make timely, informed decisions with a greater degree of confidence.

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