Forescout Continuum Timeline

Augment compliance and risk reporting with cloud-based retention, search and historical analytics of all assets in your digital terrain

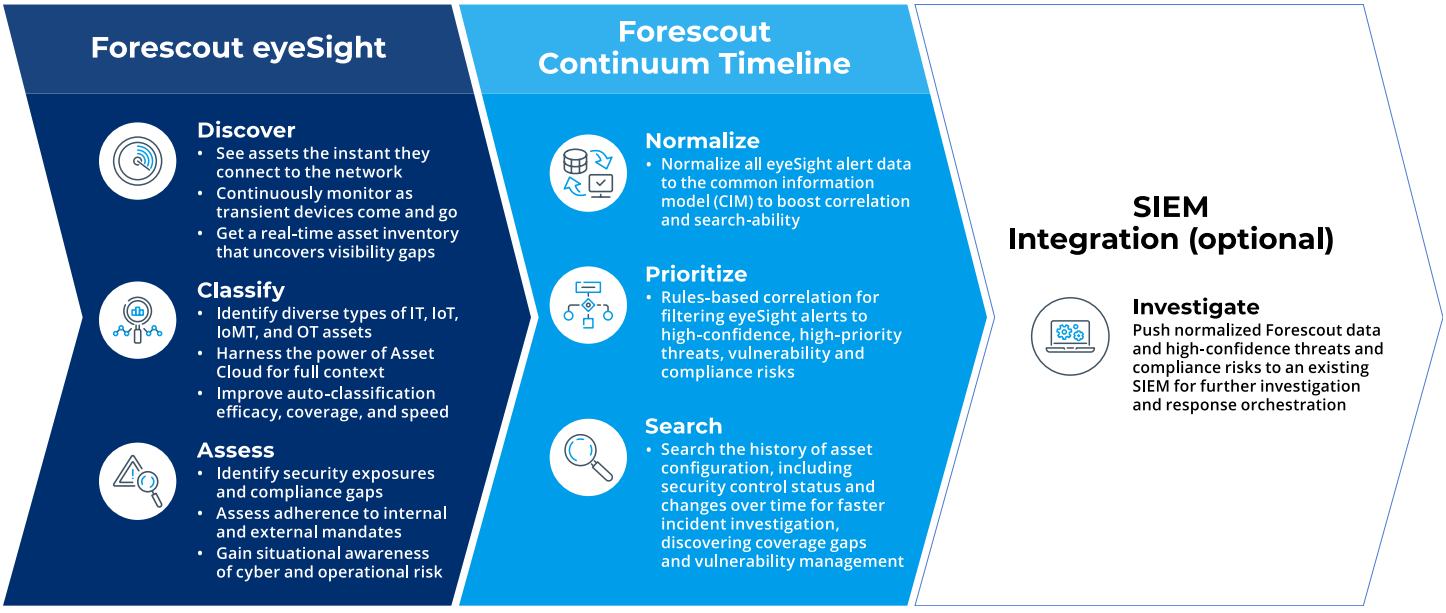
Identifying and profiling every single asset that connects to your network is essential for compliance and security reasons, and Forescout eyeSight delivers that. It provides real-time and continuous visibility across your entire digital terrain – without disrupting critical business processes – by discovering every IP-connected asset, auto-classifying it, and assessing its compliance posture and risk the instant it connects to the network. eyeSight provides continuous, real-time data for every connected asset, including:

- Location, function and type, for both managed and unmanaged assets
- Operating system and version
- Vendor and model
- Configuration state

Forescout Continuum Timeline complements and extends the value of eyeSight by providing enhanced, cloud-based data retention, search and analytics of this essential asset data to better meet compliance and audit requirements. With advanced, comprehensive security analytics and integration with SIEMs and other data aggregation solutions, Timeline can accelerate threat detection and generate significant SIEM storage-related cost savings.

The Timeline advantage

- Comprehensive SaaS solution is fast to deploy, implement and maintain
- Powerful, flexible search and investigation functions enhance SIEM value
- Data enrichment and normalization enable accurate, timely compliance and threat detection
- Highly efficient and cost-effective storage of essential asset data



Solution overview

Timeline is a cloud-native SaaS platform that operates as a seamless extension to eyeSight and has been engineered to handle the demands of the world's largest enterprises. It automatically ingests, enriches and normalizes data from eyeSight and stores it in a massively scalable data lake.

Timeline is designed for network and SecOps teams to better support compliance and threat detection and response efforts:

- **Compliance:** Quickly produce detailed, accurate, historical proof of compliance of any single asset or groups of assets, with policies, from a specific time
- **Incident investigation:** Support incident investigations with detailed, accurate asset data to help better assess threats and risks
- **Risk reduction:** Proactively identify risks and gaps to help prioritize preventive measures

Timeline key features

Advanced data pipeline: Ingested Forescout data is enriched and normalized to the common information model (CIM) to boost correlation and searchability

Asset posture history: View assets' threat, vulnerability and compliance history, and keep that history to meet 7-year compliance requirements

Security control validation: Identify missing and misconfigured security controls at any point in time. Test security control effectiveness

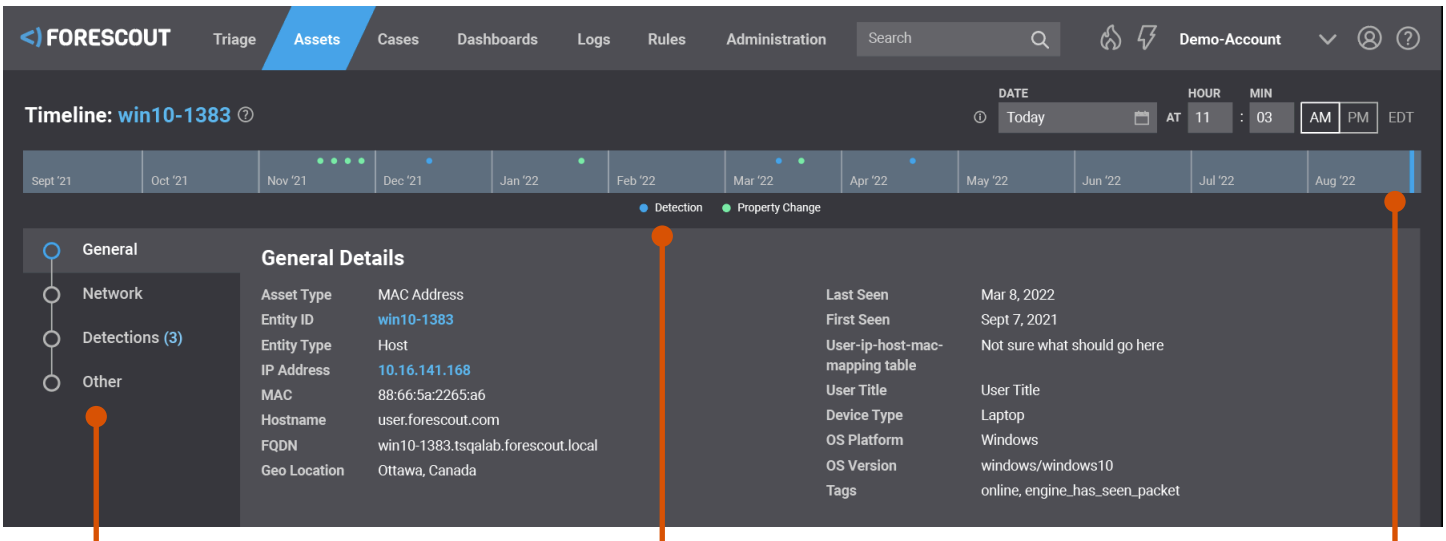
Asset configuration history: Searchable history of asset configuration changes over time for faster incident investigation, and for discovering coverage gaps and vulnerability management

Data lake retention: Massively scalable, purpose-built, indexed data lake with storage

Data analytics: Search, analyze and visualize events, alerts and telemetry. Rules-based correlation for detecting threats and compliance risks

SIEM integration: Push normalized Forescout Continuum data and high-confidence threats and compliance risks to Splunk or Microsoft Sentinel for response orchestration

Dashboard: Pre-configured and customizable dashboards provide key performance indicators relevant to a variety of roles, including analysts/IR, engineers, executives, SOC manager, and compliance/risk managers



Asset properties are logically grouped into categories to simplify search

Timeline markers highlight historical points of interest in an asset's posture or configuration

Timeline slider enables rapid access to asset properties from any point in time over the past year

Query types supported:

- Exact match
- Full text
- Wildcard
- Range
- Multiple values
- Boolean operators
- Nested queries

Benefits and use cases

Timeline enhances compliance and security by enabling network administrators and SecOps teams to query, investigate and leverage the essential data collected by eyeSight from 100% of assets in their digital terrain, across time.

For each of the use cases below, Timeline can provide asset details for a specific time (year-month-day-hour-minute-second) or a specific time period (from-to).

Compliance/audit

Quickly provides detailed, accurate historical proof of compliance of any single asset or groups of assets, with policies.

- **Asset compliance:** Provide proof that a policy, agent, service or application existed on an asset or group of assets
- **Attack surface management and security control validation:** Provide proof that security controls, such as a specific security agent or encryption, were deployed across all required assets
- **Policy violations:** Identify which asset(s) were/are in violation of a security policy

Incident investigation

Supports reactive incident investigations with detailed, accurate asset data to help assess threats and risks.

- **Asset configuration history:** Quickly determine the blast radius and scope of a compromise or incident by searching across assets to identify when a specific configuration state existed (e.g., vulnerable software) or state change occurred that introduced a vulnerable state. Quickly identify which software (such as a security agent) was running on an asset
- **Geolocation history:** Quickly identify where a specific asset is located and where it has been on the network
- **IP address history:** Quickly identify an asset's IP address history to corroborate a detected threat if the IP address changes

Risk reduction

Proactively identifies risks and gaps to help prioritize preventative measures.

- **Coverage gap discovery:** Identify entities at risk and security gaps (e.g., unpatched security vulnerabilities, high number of detected threats, or access to sensitive data or critical functions)
- **Vulnerability management:** Proactively identify state and configuration changes that would make an entity at-risk

Deployment and operation

Because Timeline is a SaaS, there's nothing to deploy on-premise, and it can be operational within weeks. Timeline eliminates the time consuming and expensive process of implementing a similar capability (search, analytics, reporting, detection, threat hunting) via a SIEM, while still leveraging the SIEM for related threat investigation and response, if desired. Timeline automatically pushes high fidelity threat detections to the SIEM for additional correlation, analysis and response. Optionally, Timeline can reduce the amount of data stored in a SIEM to generate cost savings. Once deployed, network administrators and SecOps teams can log in to query and investigate Timeline.

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