The <) FORESCOUT Platform

EXTENDED X | DETECTION D | RESPONSE R

Cyber Asset Management

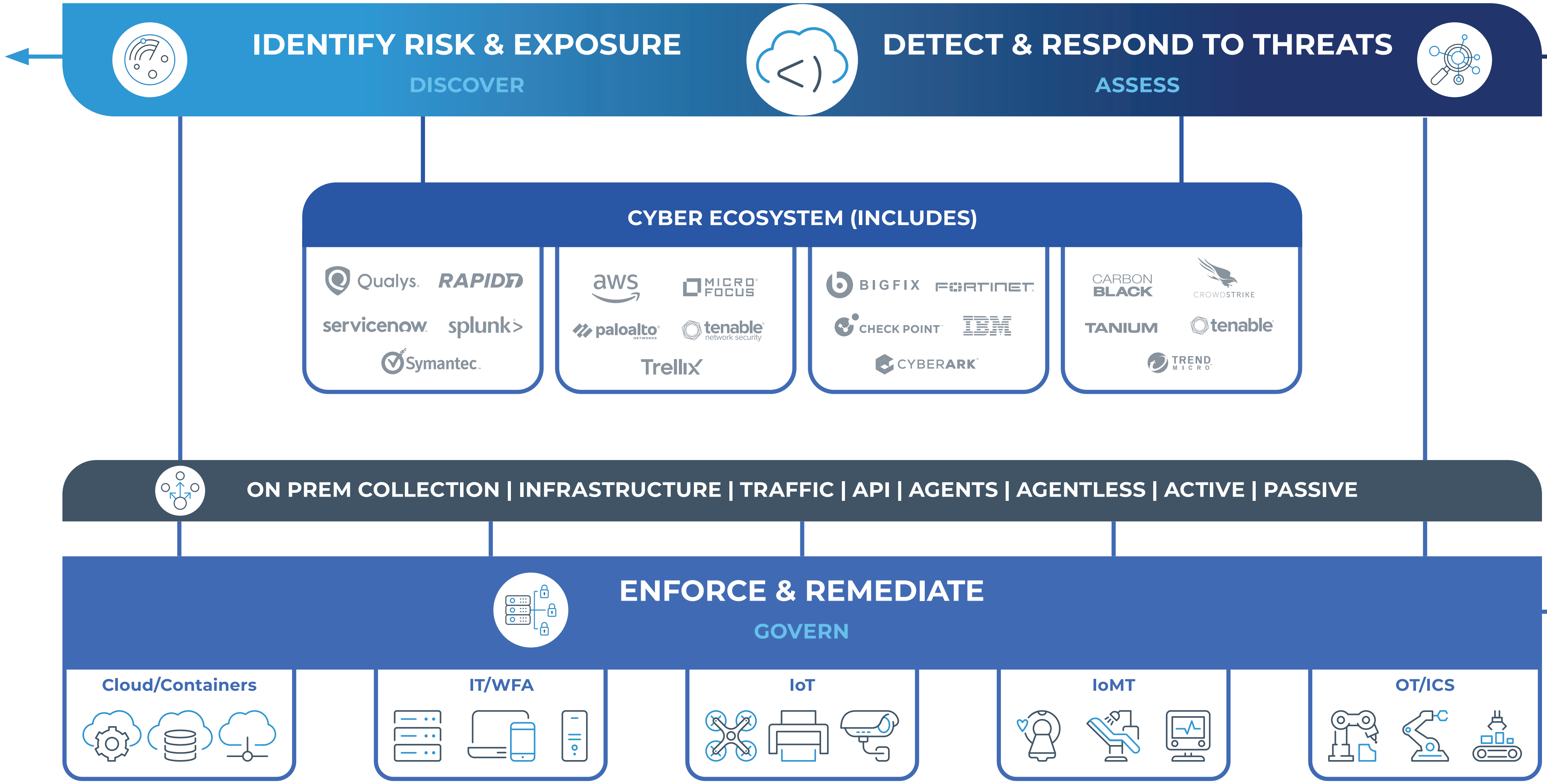
Discover and assess every connected cyber asset to provide real-time awareness of your attack surface

Visibility & Compliance

Forescout provides data that enables the most accurate CMDB and full asset history

Risk Prioritization

Identify high risk cyber assets to prioritize response actions and minimize exposure caused by vulnerabilities and misconfiguration



IDENTIFY RISK & EXPOSURE

DISCOVER

DETECT & RESPOND TO THREATS

ASSESS

CYBER ECOSYSTEM (INCLUDES)

Qualys. RAPID7 servicenow splunk> Symantec.

aws MICRO FOCUS paloalto tenable Trellix

BIGFIX FORTINET CHECK POINT IBM CYBERARK

CARBON BLACK CROWDSTRIKE TANIUM tenable TREND MICRO

ON PREM COLLECTION | INFRASTRUCTURE | TRAFFIC | API | AGENTS | AGENTLESS | ACTIVE | PASSIVE

ENFORCE & REMEDIATE

GOVERN

Cloud/Containers | IT/WFA | IoT | IoMT | OT/ICS

True Threat Correlation

Eliminate alert noise to better detect advanced threats, and provide automated responses across your entire enterprise

Optimize Security Operations

Automate, simplify and accelerate TDIR processes, and eliminate alert fatigue, from a single console

SecOps Visibility

Get comprehensive visibility into a broad range of critical SOC performance metrics, via persona-based dashboards and reports

Network Access Control

Continuously monitors all connected assets to govern access to the enterprise-wide network infrastructure, through flexible and dynamic network access policies

Risk & Threat Containment

Reduce your blast radius with real-time pinpoint network controls giving you the time to properly mitigate or remediate security concerns

Segmentation Management

Remove the complexity of deploying network segmentation. Monitor and maintain your network controls with real-time traffic visibility to avoid gaps and misconfigurations

THE FORESCOUT ADVANTAGE

- Vendor / Device Agnostic
- Real-Time & Continuous
- Managed & Unmanaged Devices
- Deployment Flexibility
- Converged Platform
- Proven at Scale

<) FORESCOUT®

FORESCOUT

EXTENDED
X

DETECTION
D

RESPONSE
R

OPEN (VENDOR AGNOSTIC)

- **Native support for 180+ sources:**
  - 12 EDRs
  - Security
  - Infrastructure
  - Enrichment
  - Applications
  - Cloud
- **1500+ verified rules**
- **New data sources and rules continuously added**

★ **Device state & configuration data**

≤ 1 TRUE THREAT PER HR*

- **450x better than typical SOC**
- **2-stage detection engine leverages 5 detection techniques:**
  - Cyber intel
  - Signatures
  - UEBA
  - Stats/outliers
  - Algorithms (context-aware AI/ML)
- **MITRE ATT&CK® integration**

★ **Device state & configuration data**

*Average, based on ~50M logs ingested per hour

FULL SPECTRUM RESPONSE

- **Powerful threat investigation features**
- **Integrations with case mgt, SIEM**
- **Touch every connected device (managed & unmanaged)**

★ **Network & host responses include:**
  - Restricting rogue assets/infrastructure
  - Quarantining assets
  - Turning off ports
  - Restricting access
  - Starting mandatory apps & processes
  - Updating agents/Applying patches
  - Terminating unauthorized applications
  - Disabling peripheral devices

MANAGED & UNMANAGED

CLOUD/CONTAINERS | IT/WFA | IoT | IoMT | OT/ICS

- **Integrated feature-set improves SOC efficiency & effectiveness:**
  - Advanced data pipeline
  - Threat detection engine
  - SOAR
  - UEBA
  - Threat intel platform: 70 sources
  - Custom rules
  - Case mgt & SIEM integrations
  - Persona-based dashboards
- **Cloud data lake included:** Cost-effective, tiered log storage (Hot, Warm, Cold):
  - 31-day
  - 365-day
  - Custom periods
- **Enterprise grade:**
  - Cloud native
  - Multi-tenant
  - Global architecture
- **Pricing:** Predictable, simple & accessible. Based on # of endpoints, not log volumes
- **Data onboarding included:** Helps ensure rapid time-to-value (days, not months)

★ **Proactive risk reduction:** Reduce attack surface via integration with other Forescout solutions

★ Provided through other Forescout solutions