Extended Detection and Response Platforms (XDR)

Creating an AI-driven Security War Room

2024 CONSTELLATION SHORTLIST

The Constellation ShortList™ presents vendors in different categories of the market relevant to early adopters. In addition, products included in this document meet the threshold criteria for this category as determined by Constellation Research.

This Constellation ShortList of vendors for a market category is compiled through conversations with early adopter clients, independent analysis and briefings with vendors and partners.

ABOUT THIS SHORTLIST

In today's complex IT environment, siloed security tools leave blind spots that attackers exploit. Traditional security solutions often operate in silos, collecting data from disparate sources like endpoints, networks, and cloud environments. This fragmented view makes it difficult to detect and respond to threats effectively, as crucial context and correlation might be missed. Extended Detection and Response (XDR) is a revolutionary approach that unifies data from diverse sources – endpoints, networks, cloud workloads, and applications – and leverages AI to deliver unprecedented threat detection, investigation, and response.

Security teams are often overwhelmed by the sheer volume of alerts generated by multiple security tools. Many of these alerts may be false positives, wasting valuable time and resources on investigation. XDR employs advanced analytics and machine learning to correlate events across different data sources, prioritize genuine threats, and reduce the noise caused by false positives. Traditional approaches to security rely on manual analysis of events, leading to delayed detection and response to threats. XDR leverages automation and machine learning to detect and respond to threats in real-time, minimizing the window of opportunity for attackers and mitigating potential damage.

The XDR market is anticipated to reach $8+ billion by 2028. This rapid growth underscores the critical need for holistic security in the face of increasingly sophisticated cyberattacks. XDR, with its unified view and AI-driven capabilities, is becoming the gold standard for modern security operations.

9 SOLUTIONS TO KNOW

Constellation evaluates more than 20 solutions categorized in this market. This Constellation ShortList is determined by client inquiries, partner conversations, customer references, vendor selection projects, market share and internal research.

- CISCO
- CROWDSTRIKE
- FORTINET
- MICROSOFT
- PALO ALTO NETWORKS
- SENTINELONE
- SOPHOS
- TRELLIX
- TREND MICRO

LIKE WHAT YOU SEE?

Consider partnering with Constellation Research on your go-to-market-strategy. Email **ShortList@ContellationR.com** for more info.

To learn more about Constellation Research Shortlists visit: **www.constellationr.com/ShortList**

THRESHOLD CRITERIA

Constellation considers the following criteria for these solutions:

- Real-time Threat Correlation: Analyzes data from all sources in real-time, correlating events and identifying complex attack patterns that individual tools might miss. This enables faster and more accurate threat detection.
- Automated Incident Response: AI-driven automated response actions based on predefined rules and threat severity, minimizing damage and downtime. This frees up security teams to focus on complex investigations.
- Predictive Threat Hunting: AI learns from past incidents and threat intelligence to predict potential attacks and prioritize vulnerabilities, enabling proactive security measures. This helps prevent breaches before they occur.
- Comprehensive Data Collection: Aggregates data from diverse sources across your IT infrastructure, providing a 360-degree view of your security posture.
- Advanced Analytics: Analyzes collected data to detect anomalies, suspicious activity, and potential threats.
- Incident Investigation: Provides tools and workflows to investigate and respond to security incidents efficiently.
- Forensics and Root Cause Analysis: Helps identify the root cause of security incidents to prevent future occurrences.
- Threat Intelligence Integration: Integrates with threat intelligence feeds to enrich analysis and stay ahead of emerging threats.
- User Behavior Analytics (UBA): Monitors user behavior across all sources to detect potential insider threats.
- Security Orchestration, Automation, and Response (SOAR): Automates incident response workflows for even faster and more efficient remediation

BUSINESS THEMES

Digital Safety & Privacy

ABOUT CONSTELLATION RESEARCH

As an award-winning Silicon Valley-based strategic advisory and futurist analyst firm, Constellation Research serves leaders and organizations navigating the challenges of digital strategy, business-model disruption and digital transformation. Constellation works closely with solution providers, partners, C-suite executives, board of directors, and its Constellation Executive Network of buy-side leaders to lead the way in research coverage and advise clients how to achieve valuable business results.

FREQUENCY OF EVALUATION

Each Constellation ShortList is updated at least once per year. Updates may occur after six months if deemed necessary.

EVALUATION SERVICES

Constellation clients can work with the analyst and the research team to conduct a more thorough discussion of this ShortList. Constellation can also provide guidance in vendor selection and contract negotiation.

Chirag Mehta
VP & Principal Analyst

Chirag Mehta is Vice President and Principal Analyst focusing on cybersecurity, next-gen application development, and product-led growth. With over 25 years of experience, he has built, shipped, marketed, and sold successful enterprise SaaS products and solutions across startups, mid-size, and large companies. As a product leader overseeing engineering, product management, and design, he has consistently driven revenue growth and product innovation. He also held key leadership roles in product marketing, corporate strategy, ecosystem partnerships, and business development, leveraging his expertise to make a significant impact on various aspects of product success.