New Additions for the Week 27 May - TOP STORIES #168

Here are the Vendors for the week, and for a full list of Vendors already transacting with us on the Marketplace, they can be found here
Click on the Vendor Logo to go to the home page for that company.

BLACK KITE

Company Overview

Black Kite is the AI-native third-party cyber risk management (TPCRM) platform trusted by over 3,000 customers globally to manage vendor risk across their extended ecosystems. Founded by certified ethical hacker and former NATO cybersecurity specialist Candan Bolukbas, the company originated from the insight that vulnerable third-party contractors are the primary stepping stones to breaching primary targets. Black Kite differentiates itself through open, standards-based risk assessments, continuous monitoring and AI-powered intelligence that goes far beyond the limitations of traditional one-off questionnaire approaches.

Products and Services

- **Black Kite Platform:** The core AI-native TPCRM platform that automates vendor monitoring, risk scoring, and assessments across technical, financial, and compliance dimensions
- **Black Kite AI Agent**: Launched November 2025, this super-agent autonomously investigates, assesses, and reports on third-party cyber risk without manual intervention
- **Cyber Risk Ratings:** Standards-based, continuously updated ratings built using MITRE's Cyber Threat Susceptibility Assessment (CTSA) methodology and passive DNS, web scanners, and OSINT sources
- **Ransomware Susceptibility Index (RSI)**: A proprietary metric that quantifies a vendor's susceptibility to ransomware attacks, unique in the TPCRM market
- **Compliance Framework Mapping:** Automated mapping of vendor risk findings to regulatory frameworks including ISO 27001, NIST, GDPR, and others
- **Financial Cyber Risk Quantification:** Translates technical cyber risk into financial exposure, enabling business-level risk decision-making
- **FocusTag Intelligence:** AI-powered alerts that surface the most critical and time-sensitive vendor threats, integrated with automation platforms such as Torq

CLAROTY

Company Overview

Claroty is a privately held cyber-physical systems (CPS) protection company founded in 2015 and headquartered in New York City, with a presence in Europe, Asia-Pacific, and Latin America. Co-founded by Amir Zilberstein, Galina Antova, and Benny Porat as the second spin-out from the Israeli cybersecurity foundry Team8, the company has grown into a recognised global leader in securing the Extended Internet of Things (XIoT) across industrial, healthcare, public sector, and commercial environments. In January 2026, Claroty raised $150 million in Series F funding led by Golub Growth, bringing its total funding to approximately $900 million at a $3 billion valuation, with strategic investors including SoftBank, Siemens, Schneider Electric, Bessemer Venture Partners, and LG.

Today, Claroty is deployed by hundreds of organisations at thousands of sites globally and was named a Leader in the 2026 Gartner® Magic Quadrant for CPS Protection Platforms. The company's platform provides deep asset visibility and a broad built-for-CPS solution set available both as a cloud-based service (xDome) and as an on-premises deployment (Continuous Threat Detection), making it the go-to choice for organisations securing operational technology (OT), IoT, building management systems (BMS), and connected medical devices..

Products and Services

- **Claroty xDome**, cloud-based (SaaS) CPS protection platform covering asset discovery, exposure management, network protection, and threat detection
- **Claroty Continuous Threat Detection (CTD)**, on-premises industrial cybersecurity solution for OT/ICS environments providing continuous threat monitoring and incident response
- **Claroty xDome for Healthcare**, purpose-built IoMT security managing medical device visibility, risk, and compliance across hospital networks
- **Exposure Management,** risk and vulnerability prioritisation across the XIoT asset estate
- **Network Protection**, segmentation and policy enforcement to restrict lateral movement across OT and IoT networks
- **Secure Remote Access,** zero-trust remote connectivity for operational staff, contractors, and vendors accessing critical systems
- **Threat Detection & Response**, AI-driven behavioural and protocol-level anomaly detection across industrial and cyber-physical environments

- **Product Analysis Module**: Launched December 2025, delivers product-level intelligence on SaaS subdomains, CPE-based software vulnerabilities, and SBOM analysis
- **Dark Web & Continuous Monitoring**: Always-on intelligence gathering from cyberspace and the dark web to detect emerging vendor risks in real time
- **Integrations:** Native integrations with ServiceNow, ProcessUnity, and other GRC and ITSM platforms

Your Sales Specialist is: Taryn Fonseca

- **Asset Intelligence**, deep OT/IoT device fingerprinting and inventory management integrated with existing SIEM, CMDB, and SOC workflows

Your Sales Specialist is: Taryn Fonseca

Black Kite Review

Black Kite has earned strong and consistent recognition from enterprise customers. The platform holds a 4.8 out of 5.0 rating on Gartner Peer Insights and a 98% willingness-to-recommend score among reviewers. It was named a Customers' Choice in the Gartner Peer Insights 'Voice of the Customer': IT Vendor Risk Management Tools report, achieving the highest overall rating in the quadrant with a 4.6 out of 5.0. In the 2023 Gartner Peer Insights Voice of the Customer report, 94% of customers who reviewed Black Kite said they would recommend the platform, the highest percentage among all vendors evaluated in the category.

On G2, customers consistently highlight Black Kite's transparency, fair pricing model, and actionable intelligence as standout qualities, with reviewers noting it as a refreshing alternative to feature-locked, tier-heavy competitors.

Black Kite G2 Reviews
Black KIte Gartner Review

Claroty Review

Claroty holds one of the strongest independent ratings in the CPS security market. On Gartner Peer Insights, the company scores 4.9 out of 5 based on 119 verified ratings in the CPS Protection Platforms category, with a 97% Would Recommend score as of March 2026, accompanying its Leader designation in the 2026 Gartner Magic Quadrant. Sample reviews highlight the platform's breadth and ease of deployment, with customers describing it as "a reliable and valuable security partner" and praising its comprehensive visibility and operational impact.

Claroty was also recognised as a Top Performer in the 2026 Best in KLAS Awards for Healthcare IoT Security, achieving an overall score of 92.5 out of 100 across 35 unique healthcare organisation evaluations, more than any other vendor in its category.

Gartner Reviews

WatchGuard

Company Overview

WatchGuard Technologies, Inc. is an American cybersecurity company headquartered in Seattle, Washington, founded in 1996 and now celebrating over 30 years of continuous innovation in the security space. Under its new CEO Joe Smolarski, who took the helm in 2026, the company has entered what it describes as a pivotal new chapter, positioning its Unified Security Platform as the definitive tool for MSPs and SMEs navigating an increasingly complex threat landscape.

Ownership & Scale

WatchGuard is a privately held company and operates as a wholly owned subsidiary of Vector Capital, a San Francisco-based private equity firm. It serves more than 250,000 businesses worldwide, protecting in excess of 10 million endpoints, and distributes its solutions exclusively through a global network of managed service providers (MSPs) and value-added resellers. The company's partner-first philosophy is deeply embedded in its go-to-market strategy, reinforced by the launch of its new partner programme, WatchGuard IMPACT, in April 2026.

Market Position & Strategy

WatchGuard positions itself as the cybersecurity vendor of choice for SMEs and MSPs who require enterprise-grade protection without the complexity or cost of large-platform vendors such as Palo Alto Networks or Fortinet. Its Unified Security Platform integrates firewall, endpoint, identity, and SOC capabilities under a single cloud-managed console, reducing alert fatigue and simplifying multi-tenant management at scale. In 2026, the company has doubled down on AI-driven operations and platform consolidation as the market shifts decisively from point tools to integrated security platforms.

Products and Services

WatchGuard's portfolio is organised into four core pillars, all managed through the WatchGuard Cloud console:

Network Security, Firebox Platform

- **Firebox M Series,** high-performance rackmount firewalls for mid-size and enterprise branch deployments.

- **Firebox T Series,** tabletop NGFW appliances (now featuring Wi-Fi 7 and improved throughput) for small offices and remote sites.
- **FireboxV**, fully virtualised firewall for VMware, Hyper-V, and KVM environments.
- **Firebox Cloud**, cloud-native firewall instances for AWS and Microsoft Azure.
- **WatchGuard SD-WAN**, built into all Firebox platforms, enabling intelligent traffic management and failover.
- **Total Security Suite**, bundling APT Blocker, DNSWatch, IntelligentAV, Application Control, WebBlocker, spamBlocker, and Network Discovery.

Endpoint Security

- **WatchGuard EPP,** Endpoint Protection Platform with signature and behaviour-based threat prevention.
- **WatchGuard EDR,** Endpoint Detection and Response with automated threat containment.
- **WatchGuard EPDR,** combined EPP + EDR with Zero-Trust Application Service and Threat Hunting Service.
- **WatchGuard Advanced EPDR,** the top-tier endpoint tier with the most comprehensive automated response capabilities.
- **Patch Management,** automated OS and third-party application patching from the cloud console.
- **Full Encryption,** BitLocker and FileVault management for endpoint data protection.
- **DNS Filter,** cloud-based DNS-layer content and threat filtering.

Identity & Multi-Factor Authentication

- **WatchGuard AuthPoint MFA**, cloud-based multi-factor authentication with mobile DNA device binding.
- **AuthPoint Total Identity Security**, extending MFA with dark web credential monitoring and password manager capabilities.
- **Hardware Tokens**, OATH-compliant OTP tokens for environments that cannot use mobile apps.

Secure Wi-Fi

- **WatchGuard Wi-Fi 6 and Wi-Fi 7 access points**, centrally managed through WatchGuard Cloud.
- **Integrated WIPS** (Wireless Intrusion Prevention System) for rogue AP detection.
- **Wi-Fi in WatchGuard Cloud**, unified wireless visibility and reporting alongside network and endpoint telemetry.

WatchGuard Cloud & Management Services

- **WatchGuard Cloud**, single-pane-of-glass management across all product lines with multi-tenant MSP support.
- **ThreatSync**, the company's XDR engine correlating network, endpoint, and identity telemetry for unified detection and response.
- **Gold and Platinum Support plans** with 24/7 technical assistance, dedicated account management, and advanced RMA options.

Your Sales Specialist is: Taryn Fonseca

Watchguard Reviews

WatchGuard has earned consistent and strong peer recognition across the leading independent review platforms. In 2026, WatchGuard Firebox has received multiple 5/5 ratings on Gartner Peer Insights in the Hybrid Mesh Firewall and Network Firewalls markets, with verified reviewers ranging from IT Managers in the IT Services sector to CIOs in Retail.
On G2, WatchGuard holds an impressive 4.5-star rating across 514 verified reviews, with users consistently praising ease of configuration, comprehensive threat coverage, and quality of technical support.
WatchGuard also swept the 2026 TrustRadius Buyer's Choice Awards across all three of its major product lines, Network Security, Endpoint Security, and AuthPoint, meeting the rigorous threshold of 75% or more of verified reviewers selecting WatchGuard for Best Capabilities, Best Value for Price, and Best Customer Relationship. This was preceded by eight 2025 Top Rated Awards from TrustRadius, cementing its position as a consistently top-rated vendor across the MSP and SME cybersecurity segment.

Gartner WatchGuard Reviews
G2 Reviews
TrustRadius Reviews