# New Additions for the Week 23 February - TOP STORIES #155

**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**

---

## Company Overview

**Nozomi Networks** is a specialist cybersecurity company focused on Operational Technology (OT), IoT, and cyber-physical systems (CPS) security, founded in 2013 and headquartered in San Francisco, California, with operations across six continents. Led by CEO Edgard Capdevielle, the company has established itself as a recognised pioneer in securing industrial control systems and critical infrastructure environments, growing from an early-stage startup to a $1 billion acquisition target. In September 2025, Mitsubishi Electric, which had already participated in Nozomi's $100 million Series E funding round in March 2024, entered into a definitive agreement to acquire Nozomi Networks as a wholly owned subsidiary, bringing its total funding raised to over $266 million.
The company was also listed on the 2025 Deloitte Technology Fast 500 as one of the fastest-growing companies in North America, underscoring its rapid commercial growth across energy, manufacturing, pharmaceuticals, transport, and other critical infrastructure sectors.

## Products and Services

**Nozomi's fully integrated**, AI-powered platform spans network monitoring, endpoint security, wireless visibility, and cloud management.

- **Nozomi Vantage**, the cloud-first SaaS platform, delivers unified security monitoring, asset risk scoring, AI-powered analytics, and centralised management of all sensor types across distributed OT, IoT, and IT networks.
- **Vantage IQ**, an AI/ML add-on to Vantage, automates threat analysis and response, replicating the expertise of senior security analysts to reduce risk at scale across large and complex operational networks.
- **Nozomi Guardian**, the core network sensor, combines automated asset discovery, network visualisation, vulnerability assessment, risk monitoring, and threat detection in a single appliance, available as edge or cloud-deployed sensors.
- **Nozomi Arc**, a host-based endpoint sensor that runs on Windows, Linux, macOS, and PLCs, providing continuous endpoint visibility, malware detection and quarantine, USB monitoring, user behaviour correlation, and automated threat prevention without disrupting OT operations.
- **Guardian Air**, a wireless sensor installed on walls or ceilings that monitors the electromagnetic spectrum for wireless devices, laptops, mobile phones, and connected sensors, integrating directly into the Vantage platform.

## Company Overview

**BeyondTrust** is a global cybersecurity company and recognised leader in Privileged Access Management (PAM) and Identity Security, headquartered in Johns Creek, Georgia, USA (near Atlanta). Founded in 1985 as Symark International, the company has evolved significantly through strategic acquisitions and mergers, most notably the 2018 merger with Bomgar Corporation, which consolidated the BeyondTrust and Bomgar product suites under a single brand. Today the company operates as a privately held organisation with approximately 1,300 to 1,700 employees worldwide and annual revenues estimated at between $315M and $400M.

BeyondTrust's mission centres on protecting what it terms "Paths to Privilege™", the access vectors that attackers exploit to gain footholds, escalate privileges, and move laterally across enterprise infrastructure. The company serves organisations across finance, healthcare, government, and critical infrastructure sectors globally, with a solution portfolio spanning endpoint privilege management, password vaulting, remote access, and AI-driven identity threat detection. Its current CEO is Janine Seebeck, supported by a leadership team with deep expertise in identity, access, and security.

## Products and Services

**BeyondTrust's portfolio** is unified under its Pathfinder Platform, an AI-driven control plane for identity and access security:

- **Pathfinder Platform**, the core AI-driven identity security platform that dynamically maps privilege relationships across human, machine, and workload identities, exposing hidden attack vectors and "Paths to Privilege™"
- **Password Safe**, unified privileged password and session management with automated credential discovery, vaulting, rotation, and threat analytics for all privileged accounts including service accounts and SSH keys
- **Endpoint Privilege Management (EPM)**, enforces least privilege dynamically across Windows, macOS, and Linux endpoints, removing unnecessary admin rights while allowing trusted application elevation without disrupting productivity
- **Privileged Remote Access**, secure, audited remote connectivity for employees, contractors, and vendors to critical systems, with automated rule-based access provisioning and no requirement for traditional VPN
- **Remote Support**, enterprise-grade remote desktop and support tooling enabling IT and service desk teams to securely access and troubleshoot end-user devices across platforms

- **Central Management Console (CMC).** which consolidates OT and IoT risk monitoring and visibility across thousands of geographically distributed sites, either on-premises or in the public cloud.
- **Threat Intelligence**, including an Expansion Pack powered by Mandiant, delivering OT-specific indicators of compromise in YARA, STIX, and SIGMA formats for faster detection and SOC efficiency.

**Your Sales Specialist is**: Taryn Fonseca

- **Identity Security Insights**, provides True Privilege Graph visualisation, mapping all entitlements, permissions, and indirect privilege paths across the identity estate
- **Identity Threat Detection & Response (ITDR)**, continuous monitoring and automated response to identity-based threats, anomalous privileged user behaviour, and entitlement drift
- **Active Directory Bridge** , extends group policy and Active Directory authentication controls to Unix and Linux environments for unified identity management
- **Cloud Infrastructure Entitlement Management (CIEM)**, governs and right-sizes access permissions across AWS, Azure, and GCP cloud environments
- **Privileged Session Management**, records, monitors, and provides real-time audit capabilities across all privileged sessions with video playback and immediate alert-and-terminate controls

**Your Sales Specialist is**: Taryn Fonseca

## Nozomi Review

**Nozomi Networks** holds a 4.9 out of 5 star rating on Gartner Peer Insights for OT Security based on 126 verified reviews as of February 2025, with 98% of users confirming they would recommend the platform. Reviewers consistently highlight its collaborative approach, highly responsive post-sales support, and forward-thinking innovation as standout qualities; one security engineer from an energy and utilities company described it as "a breath of fresh air in a stagnating space", and an OT Cybersecurity Analyst with over 20 years of experience called its support team "second to none".

Nozomi Gartner Reviews

## BeyondTrust Review

**BeyondTrust** enjoys strong and consistent customer ratings across verified enterprise review platforms. On Gartner Peer Insights, the company has accumulated over 650 five-star reviews and holds an overall rating of 4.5 out of 5 stars, with 87% of PAM reviewers indicating they would recommend the solution. It has earned the Gartner Peer Insights Customers' Choice distinction for Privileged Access Management on multiple occasions, as well as for Remote Desktop Software in 2024, where it achieved a 4.6 out of 5 overall rating with a 97% willingness-to-recommend score from 70 enterprise-scale reviewers.
Reviewers particularly highlight BeyondTrust's breadth of product capabilities, seamless suite integration, and the quality of its professional services and support experience. The platform has also been awarded G2's Top 50 Best Software for Enterprise Business badge based on high enterprise user satisfaction and substantial market presence.

BeyondTrust Reviews.

CROWDSTRIKE

## Company Overview

Founded in 2011 by George Kurtz (CEO), Dmitri Alperovitch (former CTO), and Gregg Marston (CFO), CrowdStrike was built from the ground up with a mission to redefine cybersecurity for the cloud era, at a time when traditional perimeter-based security was proving inadequate against sophisticated, nation-state-level threats. The company initially operated from Irvine, California, relocated to Sunnyvale, and then in December 2021 moved its corporate headquarters to Austin, Texas, adopting a predominantly remote-first model.

CrowdStrike rose to global prominence through its involvement in several landmark cybersecurity investigations, including the 2014 Sony Pictures hack and the 2015,2016 cyberattacks on the Democratic National Committee, establishing its threat intelligence credentials at the highest level. The company went public on NASDAQ in June 2019 and has grown to employ over 7,900 professionals operating in more than 170 countries, serving sectors spanning finance, healthcare, government, retail, and technology. CrowdStrike closed its 2025 fiscal year with total revenue of approximately $3.95 billion, representing a 29% year-over-year increase, underpinned by strong Annual Recurring Revenue (ARR) growth.

At the heart of CrowdStrike's offering is the Falcon Platform, a single-agent, cloud-native architecture powered by AI and a continuously updated threat graph that ingests trillions of security events per week from customers worldwide. In 2023, the company introduced Charlotte AI, a generative AI security analyst embedded in Falcon to automate threat triaging and response, and has since advanced to what it describes as an "Agentic Security Platform" built to protect enterprise environments through the AI revolution.

## Products and Services

CrowdStrike organises its Falcon platform into the following major capability areas:

### Endpoint Security

- **Falcon Prevent,** next-generation antivirus with AI-powered malware and ransomware protection
- **Falcon Insight XDR,** continuous endpoint visibility and automated threat detection and prioritisation
- **Falcon Device Control**, granular management of removable media including USB, SD card, and Thunderbolt devices
- **Falcon Firewall Management,** centralised host-based firewall policy control
- **Falcon for Mobile**, advanced threat detection for Android and iOS devices
- **Falcon Forensics**, on-demand forensic data collection and analysis at the endpoint

### Cloud Security

- Falcon Cloud Security (CNAPP), unified agent and agentless protection from code to cloud
- Cloud Security Posture Management (CSPM), continuous compliance and misconfiguration detection
- Cloud Workload Protection (CWP), runtime threat detection for containers, VMs, and serverless workloads

### Identity Protection

- **Falcon Identity Protection**, real-time detection and prevention of identity-based attacks and lateral movement
- **IT Hygiene**, continuous discovery and assessment of user and endpoint risk

### Threat Intelligence & Counter Adversary Operations

- Falcon Intelligence (Falcon X), automated threat intelligence enrichment and adversary profiling
- Falcon Overwatch, 24/7 managed threat hunting by CrowdStrike elite analysts
- Falcon Recon, digital risk monitoring of the dark web and external attack surface

### Security Operations

- **Falcon Next-Gen SIEM**, AI-driven log management, detection, and investigation across the full attack surface
- **Falcon Fusion**, native SOAR capabilities for automated orchestration and response workflows

### Data & Exposure Management

- **Falcon Data Protection,** real-time prevention of unauthorised data movement across endpoints and cloud
- **Falcon Exposure Management**, full attack surface visibility, risk prioritisation, and automated remediation

### XIoT & OT Security

- **Falcon for IoT/OT,** asset discovery and threat protection for extended IoT and operational technology environments

### Managed & Professional Services

- **Falcon Complete MDR**, fully managed detection and response combining Falcon platform with CrowdStrike expert analysts
- **Incident Response Services**, rapid breach investigation and remediation
- **Proactive Cybersecurity Advisory Services**, red team exercises, penetration testing, and security maturity assessments
- **Falcon Launch Services,** expert-led deployment and onboarding for new customers

**Your Sales Specialist is**: Taryn Fonseca

## CrowdStrike Review

**CrowdStrike** holds one of the strongest customer advocacy records in the cybersecurity industry. The company was named a Customers' Choice in the 2025 Gartner Peer Insights™ Voice of the Customer for Endpoint Protection Platforms, a recognition it has received in every single edition of the report since its inception in 2019, making it the only vendor to achieve this distinction five consecutive times. With 601 verified customer responses as of January 2025, CrowdStrike achieved a 97% willingness to recommend score and holds the highest number of 5-star ratings (450) of any Customers' Choice vendor in the endpoint protection category. Customers consistently highlight real-time threat detection, ease of deployment via the single lightweight agent, AI-driven automation, and the quality of the Overwatch managed hunting team as standout strengths.

Gartner CrowdStrike Reviews