Notice Regarding the New Service
"HENNGE Endpoint & Managed Security"

HENNGE K.K. (hereinafter the "Company") hereby announces that the Company will begin providing the new service "HENNGE Endpoint & Managed Security," as part of its initiatives to enhance the value of "HENNGE One," the Company's cloud security service.

Please refer to the attached press release.

The impact of this matter on the Company's consolidated financial results is expected to be insignificant. However, the Company believes it will contribute to enhancing its performance and corporate value over the medium to long term. Should any matters requiring disclosure arise in the future, announcements will be made accordingly.

[Attached Document]
    Press Release:
HENNGE Expands into EDR and MDR, Streamlining Endpoint Security through Integrated Vulnerability Assessment and Threat Management

HENNGE Expands into EDR and MDR, Streamlining Endpoint Security through Integrated Vulnerability Assessment and Threat Management

—Launching in March, "HENNGE Endpoint & Managed Security" combines 24/7 expert monitoring with an industry-leading engine to provide proactive defense across PCs and Devices.

2026.02.03

HENNGE K.K. (Headquarters: Shibuya-ku, Tokyo; Representative Director and CEO: Kazuhiro Ogura; hereinafter "HENNGE") is pleased to announce the March 2026 launch of "HENNGE Endpoint & Managed Security," a new addition to its HENNGE One cloud security platform. The comprehensive solution integrates high-performance Endpoint Detection & Response (EDR), 24/7 Managed Detection and Response (MDR), vulnerability assessment, and emergency response into a single package. Designed specifically for organizations facing a shortage of security talent, it enables a robust security posture with minimal operational burden. By providing expert-led, end-to-end support—from initial threat prevention to post-incident response—as a standard offering, HENNGE delivers a uniquely integrated approach that is unparalleled in the cybersecurity industry.

Background and Challenges
While recent years have experienced increasing adoption of EDR for monitoring and mitigating device-level threats, many IT teams now face new challenges: they are overwhelmed by the constant barrage of daily alerts—commonly known as "alert fatigue"—and often lack the

specialized in-house expertise required for effective incident response once an intrusion is detected.

HENNGE Endpoint & Managed Security is specifically designed to eliminate post-deployment operational burdens, marking HENNGE's entry into the EDR/MDR markets to help customers implement zero trust within their system environments.

Built on an industry-leading Endpoint Protection Platform (EPP) and EDR technologies for advanced threat prevention and detection, the service also includes 24/7 MDR and vulnerability assessments for critical entry points, such as VPN gateways. By offering continuous monitoring and up-to-date defenses, it drastically reduces the probability of a successful attack, enabling organizations with even limited security personnel to achieve enterprise-grade safety with minimal operational effort.

Three Core Features of HENNGE Endpoint & Managed Security
The new service will be integrated into HENNGE Cybersecurity Edition, one of the three Editions that constitute HENNGE One, and is dedicated to defense against cyber attacks.
A key differentiator of this service is its scope: while typical MDR services focus solely on responding to EDR alerts, the service provides a more holistic approach. It includes daily vulnerability assessments for externally exposed IT equipment, identification of unmanaged public-facing equipment and servers, and continuous risk assessment. Specifically, it offers three core features: "Prevention," "Protection," and "Monitoring and Response," with a strong emphasis on neutralizing threats at the point of entry to complement its post-detection capabilities.
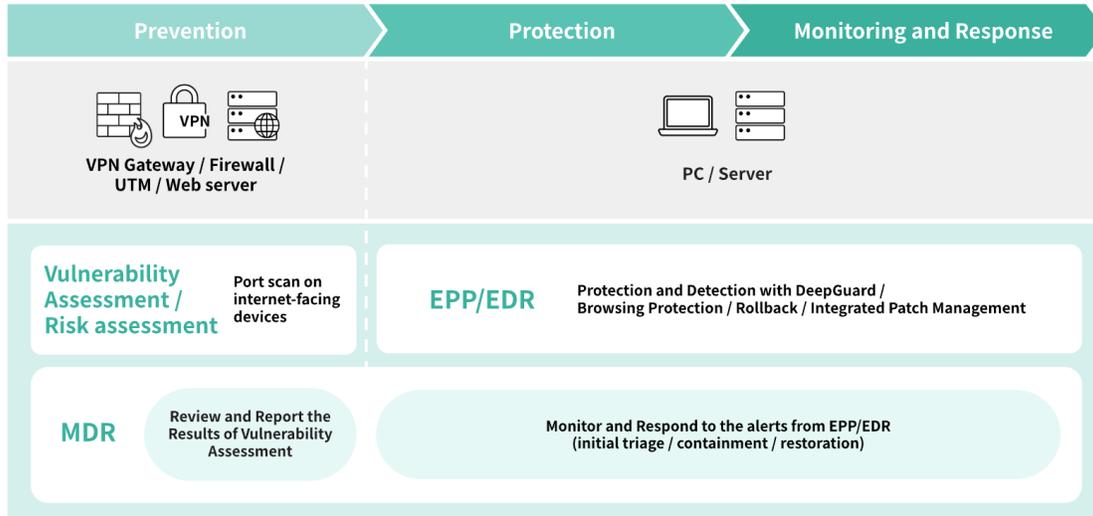
1. Prevention: Minimizing attack surfaces through vulnerability management and automated response.
This feature continuously identifies and remediates the vulnerabilities most targeted by attackers. It provides a dual-layered defense by mitigating risks across both internal and external environments.

- **Automated Patch Management (Software Updater):** Many cyberattacks exploit unpatched vulnerabilities in operating systems and applications. This service centrally

automates updates, ensuring endpoints remain in a perpetually secure state. (Currently available for Windows).
- **Attack Surface Management (ASM):** This function identifies blind spots—such as inadequately managed internet-facing servers and VPN devices—and visualizes critical vulnerabilities that require immediate action, accompanied by a comprehensive risk assessment.

2. Protection: Preventing intrusions with a 100% protection score technology of a "Best Protection" award-winning engine.

At the core of this protection is WithSecure™ Elements, the recipient of the AV-TEST "Best Protection Award" for 2024. With a proven track record of achieving a 100% protection score* against over 90,000 malware samples, the engine effectively blocks the execution of unknown threats and ransomware.

- **"DeepGuard" for neutralizing unknown threats:** This feature blocks unknown attacks and ransomware execution using proprietary behavior-based detection technology that does not rely on traditional signature files.
- **"Browsing Protection" for blocking web-based threats:** This function prevents infection by proactively blocking connections, even if a user accidentally attempts to access a malicious or high-risk website.
- **"Rollback" for rapid recovery:** In the event of ransomware encryption, this feature enables near-instant restoration of data and OS configurations, minimizing overall impact and downtime.

* https://prtimes.jp/main/html/rd/p/000000391.000001340.html

3. Monitoring and Response: Visualizing invisible threats through 24/7 MDR and dedicated dashboards.
Against sophisticated threats that may bypass even the most robust defenses, the expert analysts maintain round-the-clock vigilance through a hybrid 24/7/365 monitoring system.
- **Expert-led initial response:** Analysts filter through massive EDR log volumes to conduct initial triage. By notifying the user's team only of "actionable incidents," the service eliminates the burden of unnecessary alerts.
  Our experts handle critical tasks, including removing malicious files, advising on required software updates, and managing technical inquiries with manufacturers.
- **"User Portal" for operational transparency:** An intuitive dashboard provides real-time visibility into alert response statuses and daily vulnerability assessment results, transforming security management from a black box into a transparent, easily manageable process.
- **Monthly reports:** Beyond monthly operational summaries, these reports provide comprehensive insights into device health (security posture) and risk assessments, supporting the ongoing maturity and improvement of the user's organization's security.

Availability and Pricing

- **Launch Date:** March 2026 (Scheduled)
- **Pricing (Excluding tax):** 950 JPY per month per device

- o All-inclusive price including the MDR service (24/7 monitoring and reporting), ASM (vulnerability assessment and risk evaluation), and EPP/EDR licensing.
- o For detailed plan configurations and volume discount inquiries, please contact our sales team.

Comment from Tsuyoshi Fujioka, Japan Country Manager of WithSecure
"We are honored that our award-winning WithSecure™ Elements has been selected as a core component of HENNGE's new service. By integrating our cutting-edge security capabilities—including proprietary behavior-based detection, ransomware protection, and web threat blocking—with HENNGE's sophisticated operational management, we can provide organizations with robust, multi-layered protection for their IT environments. Through our continued collaboration with HENNGE, the recipient of our 'WithSecure Japan Partner of the Year 2024' award, I am confident that we will empower even more organizations to drive their businesses forward with peace of mind, securely protected against today's rapidly evolving cyber threats."

About HENNGE K.K.
Established in November 1996, HENNGE K.K. is a SaaS company guided by the philosophy of "liberation of technology to change the world." It develops and sells unique services that bridge the gap between technology and reality: a cloud security service with the largest share in Japan**, HENNGE One, which offers comprehensive security including single sign-on (SSO), access management, email security, and secure file sharing; a cloud email distribution service, Customers Mail Cloud. Since October 2019, HENNGE has been listed on the TSE Growth (ex Mothers) in the Tokyo Stock Exchange (TSE).

The company name "HENNGE" originated from the Japanese character for transformation, 'HENNKA' and 'CHALLENGE' representing its commitment to embracing every change as an opportunity.

Company name: HENNGE K.K. (securities code: 4475)
Address: Daiwa Shibuya Square, 16-28 Nampeidaicho, Shibuya-ku, Tokyo
Representative: Kazuhiro Ogura (Representative Director, President and CEO)
URL: https://hennge.com/

**ITR Market View: Identity and Access Management/Personal Authentication Cybersecurity Market 2025 IDaaS Market: Sales and Share by Vendor (ITR)

- Press Contact
HENNGE K.K.
Corporate Communication Division
Email: hennge-pr@hennge.com
TEL: 03-6415-3660
Person in charge: Ichishima, Yano