This is a translation of part of the original Japanese version and is provided for reference purposes only.
In the event of any discrepancy between the Japanese original and this English translation, the Japanese original shall prevail.

April 16, 2026
HENNGE K.K.
(Securities Code: 4475, TSE Growth)

Notice Regarding the New Services

HENNGE K.K. (hereinafter the “Company”) hereby announces that the Company will begin providing the new services “HENNGE Mesh Network,” “HENNGE Password Manager,” and “HENNGE Domain Protection,” as part of its initiatives to enhance the value of “HENNGE One,” the Company’s cloud security service.

These new services are designed to enhance security capabilities in network operations, ID/password management, and domain management, respectively. In particular, “HENNGE Mesh Network” addresses the risks of existing VPN devices, which have become frequent targets of ransomware and other cyberattacks. Together with “HENNGE Endpoint & Managed Security” (released in March 2026) and the existing features of HENNGE One, we will strongly empower our customers in their implementation and operation of zero-trust security.

Please refer to the attached press releases.

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 Documents]
Press Releases:
- HENNGE Announces the Launch of "HENNGE Mesh Network," a Next-Generation Network System Achieving Zero Trust for PC Endpoints and Eliminating Traditional VPNs
- HENNGE to Offer "HENNGE Password Manager": Centralized Identity Governance for All Platforms, Including Non-SSO-compatible SaaS and Systems
- HENNGE to Launch "HENNGE Domain Protection" to Detect Spoofed Emails and Provide Guidance on Countermeasures

HENNGE Announces the Launch of "HENNGE Mesh Network," a Next-Generation Network System Achieving Zero Trust for PC Endpoints and Eliminating Traditional VPNs

— Minimizes Cyber Risk by Permitting Access Only to Necessary Resources from Authenticated Devices; Available Without Complex Configuration or Infrastructure Buildout

HENNGE K.K. (Headquarters: Shibuya-ku, Tokyo; Representative Director and CEO: Kazuhiro Ogura) is pleased to announce the upcoming launch of "HENNGE Mesh Network" within its "HENNGE One" cloud security service. Scheduled for release in October 2026 or later, the new service is designed to fundamentally eliminate traditional VPN vulnerabilities. By leveraging proprietary Peer-to-Peer (P2P) communication technology, the system secures devices such as PCs by shielding them from internet-based threats while ensuring seamless access to critical resources. The new functionality will be integrated as a feature of the HENNGE One identity management service.



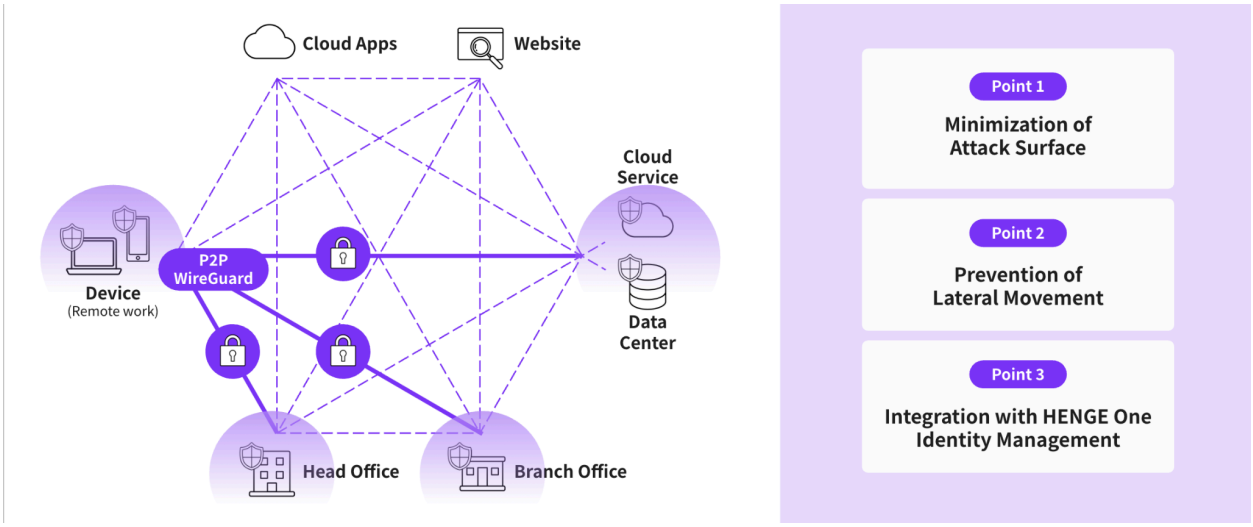
Traditional perimeter defense models are increasingly vulnerable as cyberattacks targeting VPN vulnerabilities surge. Once internal networks are breached, attackers gain access to critical resources, often resulting in significant incidents such as ransomware demands and large-scale

data theft. These evolving threats have placed an unprecedented operational burden on IT security departments and financial costs on companies.

In response, HENNGE has partnered with Runetale Inc. to launch HENNGE Mesh Network, leveraging Runetale's advanced technology. The new service shifts the focus from location-based security, where users are, to a Zero Trust approach centered on identity, who you are. By creating a secure mesh environment, it ensures that only authenticated devices can access specific resources, all without requiring complex infrastructure or expensive system integrations.

Transitioning from Legacy VPNs: Three Core Pillars for Practical Zero Trust

HENNGE Mesh Network helps IT departments regain control of their infrastructure. Transitioning away from conventional VPN setups facilitates the implementation of a Zero Trust framework. The service offers three primary advantages.



1. Reducing Attack Surfaces and Removing VPN Vulnerabilities

By moving away from VPN gateways, which often serve as entry points for ransomware and other cyber threats, HENNGE Mesh Network enables the creation of a Zero Trust environment through mesh-style communication between endpoints. Its approach significantly minimizes the internet-exposed attack surface, thereby easing the constant pressure on IT administrators to manage and respond to vulnerabilities.

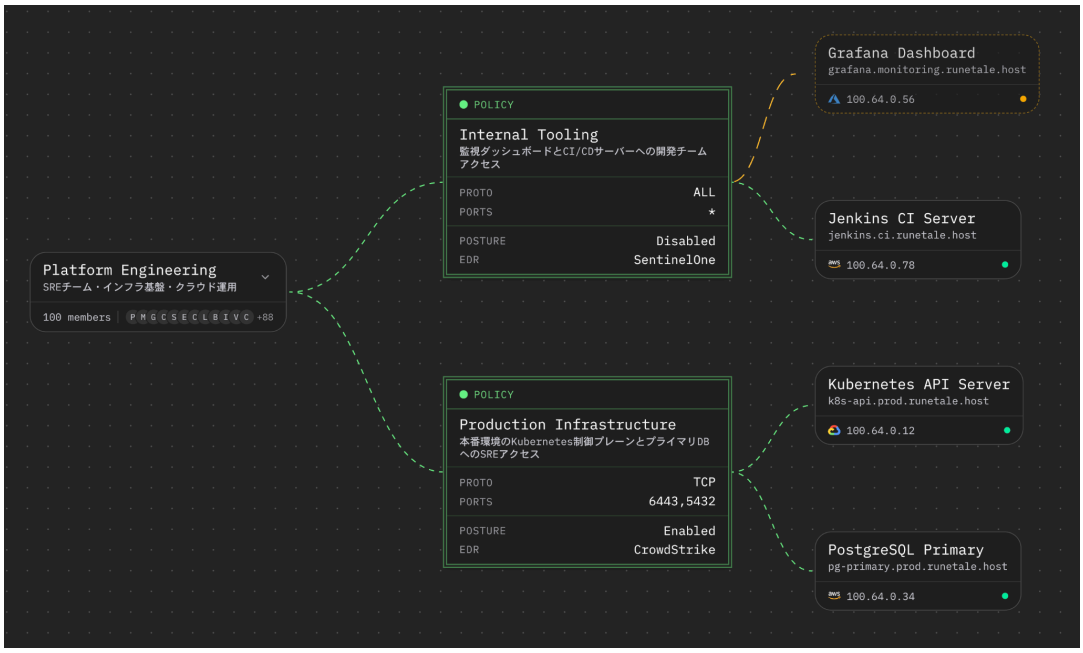
2. Preventing Lateral Movement through Micro-segmentation

HENNGE Mesh Network supports "micro-segmentation," which utilizes software to finely divide the communication range without requiring physical router adjustments. It prevents lateral movement—a common tactic in malicious attacks—based on the following principles:

- **Principle of Least Privilege:** Access rights are restricted by user ID or group, ensuring users can only reach the specific resources required for their work.
- **Containment of Damage:** If a single PC becomes infected with malware, software-based controls prevent the threat from spreading to other servers or terminals.

3. Establishing Governance through Integration with HENNGE One Identity Edition

- **Seamless Integration with ID Management:** HENNGE Mesh Network is provided as a network service within the HENNGE One Identity Edition, which is centered on Single Sign-On (SSO). ID management and network control are fully linked, ensuring IT governance.
- **Intuitive and Easy Operation:** Setting up access paths can be completed in just a few clicks from a browser-based dashboard. That allows IT system administrators to easily set up and manage the routes and services users can access, even without deep expertise in routing configurations.



Visualization of connected devices and servers (Screen image currently under development)

Feature Enhancement Plans

HENNGE plans to implement the following enhancements for HENNGE Mesh Network sequentially:

- **Further Integration with ID Management:** If an employee's departure or suspicious behavior is detected, "HENNGE Access Control," HENNGE One's ID management

function, locks the ID and immediately revokes network access rights within the Mesh Network.

- **Integration with Device Posture:** If a threat or anomaly is detected on a user terminal by client-side EPP/EDR, communication can be disconnected based on pre-set conditions.

Availability and Service Delivery

・**Release Date:** Expected in October 2026 or later.
・**Delivery Model:** Provided as a service within the HENNGE One Identity Edition.
・**Supported Platforms:** Initial support for Windows and Linux; requires the installation of dedicated client software. Support for macOS, iOS, and Android is scheduled for a post-launch update.

About HENNGE One
HENNGE One is a cloud security service with the largest market share in Japan* that helps businesses boost productivity. While leveraging new technologies like SaaS is vital for productivity gains, businesses face challenges such as implementing zero-trust security.
To address these challenges, HENNGE One offers three editions: the Identity Edition, which centralizes and protects multiple system IDs for secure and efficient work; the DLP Edition, which prevents accidental leaks of scattered organizational information; and the Cybersecurity Edition, which safeguards companies from cyber-attacks through a comprehensive approach spanning technology, people, and processes.

It achieves zero-trust security through a holistic security service, which reduces the burden of implementation and operation, thereby fulfilling the liberation of technology.
URL: https://hennge.com/global/service/one/

About HENNGE K.K.
HENNGE K.K. is a SaaS company guided by the management philosophy of “liberation of technology to change the world,” dedicated to bridging the gap between advanced technologies and practical application. It develops and sells distinctive services: a cloud security service with the largest market share in Japan, HENNGE One, which offers comprehensive security, including single sign-on (SSO), access management, email security, and secure file sharing, alongside device management and protection based on zero trust principles; a cloud email distribution service, Customers Mail Cloud. Established in November 1996, HENNGE was listed on the Tokyo Stock Exchange (TSE) Mothers (now Growth) in October 2019.
The company name “HENNGE” is a portmanteau of the Japanese word for transformation, ‘HENNKA,’ and ‘CHALLENGE,’ signifying 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/

*Ranked No. 1 for four consecutive years, from FY2021 to FY2024 (forecast), based on the 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

The names of companies, products, and services mentioned in this press release are trademarks or registered trademarks of HENNGE K.K. or other related organizations.

HENNGE to Offer "HENNGE Password Manager": Centralized Identity Governance for All Platforms, Including Non-SSO-compatible SaaS and Systems

— Facilitating Individual Access Control and Log Tracking, Supporting Both Personal and Shared Credentials

HENNGE K.K. (Headquarters: Shibuya-ku, Tokyo; Representative Director and CEO: Kazuhiro Ogura) has announced the upcoming introduction of a password management feature to its cloud security service, HENNGE One. The new solution is designed to handle credentials for web services and internal systems that do not support single sign-on (SSO) integration. The upcoming "HENNGE Password Manager," set for release in October 2026 or later, offers a distinctive capability: individual-level secure management of shared credentials. By utilizing a local key on the user's PC for decryption, the service ensures that security remains uncompromised even if identy data is leaked.



As corporate infrastructure increasingly migrates to the cloud, Single Sign-On (SSO) has become common, enabling users to access multiple platforms with a single set of credentials.

However, many organizations still rely on legacy systems and SaaS solutions that lack SSO compatibility. Consequently, employees often manage these credentials independently—storing them in web browsers or recording them in spreadsheets and physical notes—placing them beyond the oversight of IT departments. Attackers exploit these weaker entry points rather than targeting robust SSO frameworks. The risks are further magnified when credentials are shared across teams or functions, as a single compromise can have a widespread impact.

Furthermore, IT teams face a significant administrative burden in managing frequent password reset requests and identity-related inquiries.

Benefits of the HENNGE Password Manager

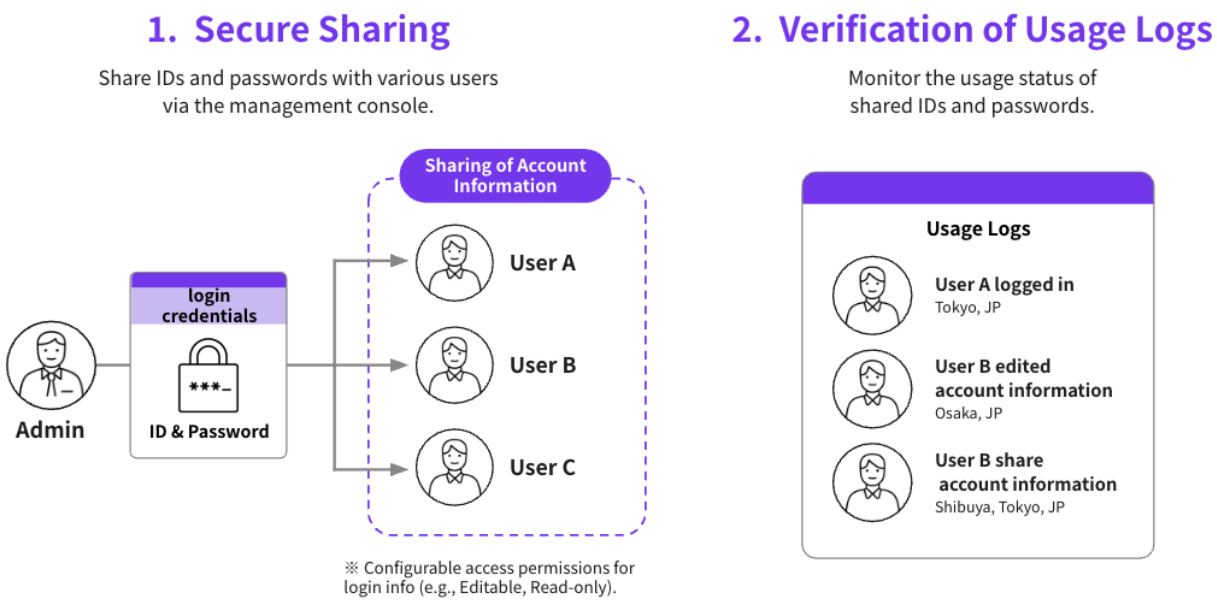
The HENNGE Password Manager solves these issues by progressively establishing an optimal identity management system that harmonizes convenience with security. A key advantage is its capacity to reliably manage shared credentials within services and systems that are incompatible with SSO. Additionally, the service is designed to accommodate organizational growth and scale accordingly.

1. Role-Based Administration and Operational Visibility



The HENNGE Password Manager record view. The team feature enables secure credential sharing across customized units, such as projects or departments.

- **Detailed Access Management:** Administrators can define specific access levels for login credentials, such as "read-only" or "edit", tailored to each user's specific organizational role.
- **Comprehensive Operational Auditing:** Beyond individual login tracking, the system provides full visibility into every interaction with organizationally shared credentials. A centralized dashboard displays who performed what action—including viewing, updating, copying, or sharing—along with the exact time and location derived from IP addresses, enabling the rapid detection of potential security threats.



Sharing and Management of Credentials in HENNGE Password Manager

2. Superior Protection Against Leaked Information Misuse

By utilizing a Zero-Knowledge Architecture, HENNGE Password Manager ensures that decryption "keys" are never stored on its servers. Instead, these keys reside exclusively on the user's local device, where they are used to encrypt and decrypt sensitive data, such as passwords. This localized approach means that even in the event of a data leak from HENNGE Password Manager, the information remains inaccessible to unauthorized third parties, as the essential decryption key remains solely in the user's possession.

3. Browser Extension for Password Management

The HENNGE Password Manager offers enhanced convenience through a dedicated Chrome extension for PC and Mac users. The extension provides seamless functionality, including automatic saving of login credentials, generation of robust passwords, and automated form filling across various websites.

In addition to the browser extension, users can manage their credentials and create secure passwords directly through the HENNGE Password Manager service management console.

Target Use Cases for HENNGE Password Manager

SaaS Solutions Lacking SSO Compatibility
Centralized identity management is unattainable for SaaS platforms that do not support SSO integration. Managing individual credentials for each service can be burdensome, often leading users to share common IDs and passwords. This includes applications that lack support for authentication protocols like OIDC or SAML, which are necessary for SSO.

Non-SSO Internal and Proprietary Systems
Legacy web environments, whether custom-developed in-house or provided as vendor packages, often lack compatibility with SSO frameworks. Furthermore, organizations may be required to utilize specific systems provided by business partners. In scenarios where partners issue a restricted number of credentials, these login details are typically shared across entire departments or groups.

Availability and Service Delivery

・**Release Date:** Expected in October 2026 or later.
・**Delivery Model:** Provided as a service within the HENNGE One Identity Edition.

Detailed pricing information, along with specific Edition and Suite packages, will be disclosed at the time of the official product release.

About HENNGE One
HENNGE One is a cloud security service with the largest market share in Japan* that helps businesses boost productivity. While leveraging new technologies like SaaS is vital for productivity gains, businesses face challenges such as implementing zero-trust security.
To address these challenges, HENNGE One offers three editions: the Identity Edition, which centralizes and protects multiple system IDs for secure and efficient work; the DLP Edition, which prevents accidental leaks of scattered organizational information; and the Cybersecurity Edition, which safeguards companies from cyber-attacks through a comprehensive approach spanning technology, people, and processes.

It achieves zero-trust security through a holistic security service, which reduces the burden of implementation and operation, thereby fulfilling the liberation of technology.
URL: https://hennge.com/global/service/one/

About HENNGE K.K.
HENNGE K.K. is a SaaS company guided by the management philosophy of “liberation of technology to change the world,” dedicated to bridging the gap between advanced technologies and practical application. It develops and sells distinctive services: a cloud security service with the largest market share in Japan, HENNGE One, which offers comprehensive security, including single sign-on (SSO), access management, email security, and secure file sharing, alongside device management and protection based on zero trust principles; a cloud email

distribution service, Customers Mail Cloud. Established in November 1996, HENNGE was listed on the Tokyo Stock Exchange (TSE) Mothers (now Growth) in October 2019.
The company name “HENNGE” is a portmanteau of the Japanese word for transformation, ‘HENNKA,’ and ‘CHALLENGE,’ signifying 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/

*Ranked No. 1 for four consecutive years, from FY2021 to FY2024 (forecast), based on the 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

The names of companies, products, and services mentioned in this press release are trademarks or registered trademarks of HENNGE K.K. or other related organizations.

HENNGE to Launch "HENNGE Domain Protection" to Detect Spoofed Emails and Provide Guidance on Countermeasures

— Protecting brand integrity and preventing domain spoofing by enabling DMARC email policy configuration and status monitoring through an intuitive dashboard

HENNGE K.K. (Headquarters: Shibuya-ku, Tokyo; Representative Director and CEO: Kazuhiro Ogura) announces the launch of "HENNGE Domain Protection," a new service within its cloud security platform "HENNGE One." The new service detects and helps counter spoofed emails exploiting a company's domain, making it simple for organizations to implement and operate DMARC, the mechanism that prevents email spoofing, on their own domains. Availability is scheduled for October 2026 or later.

Compliance with DMARC also facilitates the adoption of "BIMI," which displays the company's official logo as the email sender's icon, thereby contributing to brand protection.



HENNGE Domain Protection is a crucial component of HENNGE's Zero Trust strategy. Alongside ID management, endpoint protection, and data leak prevention, it achieves the protection of email domains, which are the foundation of corporate trust.

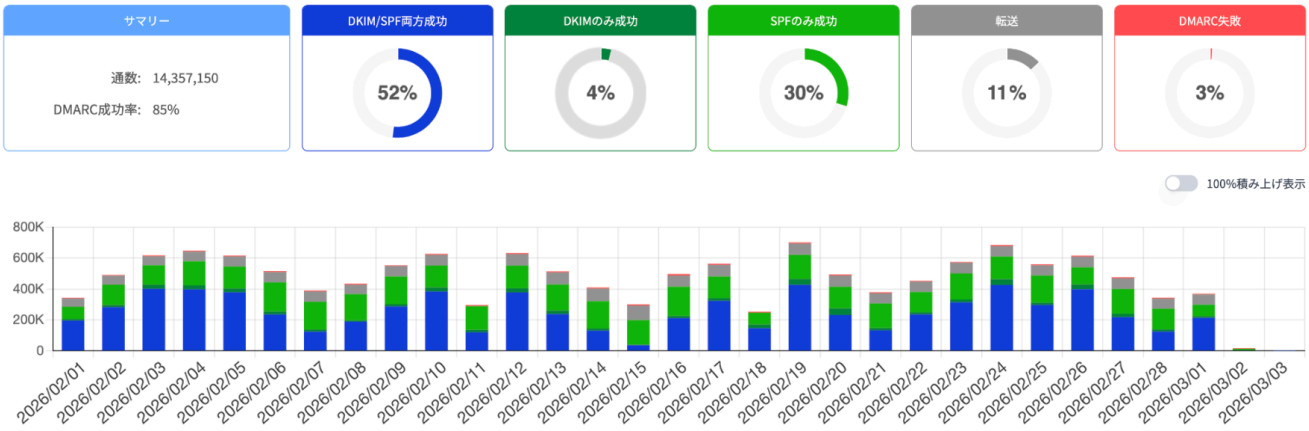
Cyber attackers leverage cutting-edge technologies, including AI, to craft highly sophisticated spoofed emails. To combat the threats, leading email service providers are tightening domain authentication requirements for both inbound and outbound traffic, strongly encouraging

organizations to eradicate fraudulent emails by implementing DMARC.
For instance, Google began enforcing strict guidelines in 2024 to reject emails from senders failing DMARC compliance. Furthermore, various Japanese regulatory frameworks—including those from the Ministry of Internal Affairs and Communications and the Financial Services Agency—now strongly advocate for DMARC adoption*.

Despite its importance, implementing DMARC presents several hurdles, such as the need to analyze complex XML report data and the risk of blocking legitimate emails when enforcement policies are strictly applied. HENNGE Domain Protection addresses these challenges by providing the following specialized features and services.

* According to the *WHITE PAPER Information and Communications in Japan*, as of September 2024, DMARC adoption for .jp domains is approximately 32.6%, and SPF (Sender Policy Framework), which authenticates by IP address, is approximately 88.4%, both showing an increasing trend.

Empowering Independent DMARC Deployment and Management Through Status Visualization



HENNGE Domain Protection Dashboard: The red "DMARC Failure" section on the far right indicates emails with a high likelihood of being spoofed.

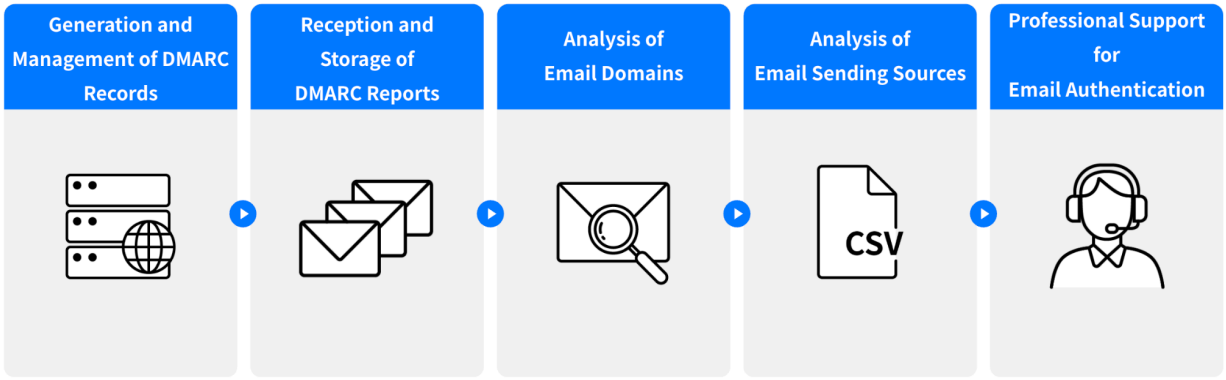
HENNGE Domain Protection supports organizations through five key stages: DMARC record generation, data accumulation, report analysis and visualization, policy enforcement, and continuous operation.

At its core is an intuitive dashboard that simplifies the analysis of DMARC reports, which are typically difficult to interpret. This tool empowers IT administrators to monitor email traffic and make informed decisions regarding security policy adjustments.

The service enables compliance through the following steps:

- **DMARC Record Generation:** Create DMARC records in just a few steps with automatic validation simply by entering the target domain into the dashboard.
- **Reporting:** Gain visibility via an intuitive dashboard that categorizes email statuses, such as legitimate, spoofed, or forwarded, and identifies all senders using the company domain by visualizing IP address data.
- **Policy Enforcement:** Implement security policies based on monitoring insights. After resolving configuration gaps, administrators can apply "quarantine" to flag suspicious emails as spam or "reject" to block them entirely. HENNGE Domain Protection supports smooth policy changes (DNS settings) for DMARC.

Professional Support for DMARC Implementation and Operation



The DMARC implementation process. Support services are also available upon request.

Through its Customers Mail Cloud business, an email delivery platform trusted by leading institutions such as banks for critical communications, HENNGE has built extensive expertise and deep insights into corporate email operations. The new service leverages and provides the expertise of these professionals for DMARC implementation.

The key to effective DMARC deployment lies in methodically strengthening security policies. Raising the policies prematurely without adequate groundwork can disrupt the delivery of authentic business correspondence. HENNGE's specialists analyze user DMARC reports and support DMARC implementation.

Availability and Service Delivery

・**Release Date:** Expected in October 2026 or later.
・**Delivery Model:** Provided as a service within the HENNGE One DLP Edition.

HENNGE will provide the basic setup for the service at no cost.
Respective implementation and operational assistance from the specialists will be provided following a formal quote. Detailed pricing information, along with specific Edition and Suite packages, will be disclosed at the time of the official product release.

What's DMARC?

Domain-based Message Authentication, Reporting & Conformance, DMARC, is a pivotal technology for domain authentication. It enables service providers on the receiving end to verify the legitimacy of emails sent by organizations, thereby mitigating the risks posed by phishing attempts and spoofed communications. A defining feature of DMARC is that it allows administrators on the sending side to specify protocols, such as outright rejection, for emails that fail authentication.

What's BIMI?

Brand Indicators for Message Identification, BIMI, is an email standard that enables the display of a sender's trademarked brand logo as an icon within recipient inboxes for authenticated messages. By helping users visually distinguish authentic communications from fraudulent or spoofed emails, BIMI strengthens trust in the sender's identity. The mechanism works by integrating DMARC authentication with a Verified Mark Certificate (VMC) issued by a recognized authority; the logo is displayed only after a message successfully passes these security checks.

About Customers Mail Cloud
Customers Mail Cloud is a cloud-based email delivery service trusted by a diverse range of organizations, including major financial institutions like banks, credit card companies, and securities firms, as well as telecommunications carriers, government agencies, and local authorities.

It is essential for sensitive communications, such as login notifications and transaction confirmations, to comply with the latest delivery standards, including SPF, DKIM, and DMARC, while maintaining the flexibility to adapt to the evolving delivery environments of various providers.

As a specialized cloud-based SMTP relay service, Customers Mail Cloud ensures both robust security and reliable delivery for critical business emails.

About HENNGE One
HENNGE One is a cloud security service with the largest market share in Japan** that helps businesses boost productivity. While leveraging new technologies like SaaS is vital for

productivity gains, businesses face challenges such as implementing zero-trust security.
To address these challenges, HENNGE One offers three editions: the Identity Edition, which centralizes and protects multiple system IDs for secure and efficient work; the DLP Edition, which prevents accidental leaks of scattered organizational information; and the Cybersecurity Edition, which safeguards companies from cyber-attacks through a comprehensive approach spanning technology, people, and processes.

It achieves zero-trust security through a holistic security service, which reduces the burden of implementation and operation, thereby fulfilling the liberation of technology.
URL: https://hennge.com/global/service/one/

About HENNGE K.K.
HENNGE K.K. is a SaaS company guided by the management philosophy of “liberation of technology to change the world,” dedicated to bridging the gap between advanced technologies and practical application. It develops and sells distinctive services: a cloud security service with the largest market share in Japan, HENNGE One, which offers comprehensive security, including single sign-on (SSO), access management, email security, and secure file sharing, alongside device management and protection based on zero trust principles; a cloud email distribution service, Customers Mail Cloud. Established in November 1996, HENNGE was listed on the Tokyo Stock Exchange (TSE) Mothers (now Growth) in October 2019.
The company name “HENNGE” is a portmanteau of the Japanese word for transformation, ‘HENNKA,’ and ‘CHALLENGE,’ signifying 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/

*Ranked No. 1 for four consecutive years, from FY2021 to FY2024 (forecast), based on the 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

The names of companies, products, and services mentioned in this press release are trademarks or registered trademarks of HENNGE K.K. or other related organizations.