BRIDGE REPORT Bridge Salon

Yasufumi Kajiura,
President CEO

# Vario Secure Inc. (4494)

## Company Information

| | |
|---|---|
| Exchange | TSE Standard |
| Industry | Information and Communications |
| President CEO | Yasufumi Kajiura |
| Address | Sumitomo Corporation Nishiki-cho Bldg., 5F, 1-6, Kanda-Nishiki-cho, Chiyoda-ku, Tokyo |
| Year-end | February |
| Homepage | https://www.variosecure.net/en/ |

## Stock Information

| Shared Price | Number of shares issued | | Total market cap | ROE (Act.) | Trading Unit |
|---|---|---|---|---|---|
| ¥703 | 4,520,053 shares | | ¥3,177 million | 6.4% | 100 shares |
| DPS (Est.) | Dividend yield (Est.) | EPS (Est.) | PER (Est.) | BPS (Act.) | PBR (Act.) |
| ¥0.00 | - | ¥74.47 | 9.4x | ¥1,227.87 | 0.6x |

*The share price is the closing price on April 9. All figures are taken from the brief financial report for the fiscal year ended February 2024.

## Earnings Trends

| Fiscal Year | Revenue | Operating Profit | Profit before tax | Profit | EPS | DPS |
|---|---|---|---|---|---|---|
| February 2021 Act. | 2,545 | 764 | 707 | 491 | 131.78 | 39.44 |
| February 2022 Act. | 2,566 | 751 | 701 | 500 | 132.29 | 40.44 |
| February 2023 Act. | 2,634 | 581 | 542 | 383 | 93.41 | 40.50 |
| February 2024 Act. | 2,640 | 520 | 509 | 347 | 76.96 | 0.00 |
| February 2025 Est. | 2,753 | 485 | 474 | 336 | 74.47 | 0.00 |

* Unit: million-yen, yen. Estimates calculated by the company. IFRS applied. Non-consolidated accounting. EPS figures are calculated based on the most recent number of shares due to the third-party allotment performed on September 27, 2022.

This Bridge Report presents Vario Secure Inc.'s earnings results for Fiscal Year Ended February 2024 and Growth Strategy etc.

## Table of Contents



## Key Points

- **The sales revenue in the fiscal year ended February 2024 was 2,640 million yen, up 0.2% year on year. While the performance of Managed Security Services, which are the mainstay, was healthy, the Integration Services business was sluggish. Operating income dropped 10.4% year on year to 520 million yen. Gross profit rose thanks to the sales growth, but it was not enough to offset the augmentation of SG&A expenses due to the active business investment, such as service plans, the recruitment of engineers and operation support staff, and the enhancement of marketing based on the medium-term management policy. Sales revenue was almost as forecast. Operating income exceeded the forecast, as they increased employees significantly through business investment, but personnel expenses fell below the forecast due to the decrease in recruitment costs and the postponement of start of working in the company.**

- **For the fiscal year ending February 2025, sales are expected to grow, but profit is projected to decline. Sales revenue is expected to increase 4.3% year on year to 2,753 million yen, while operating income is projected to decrease 6.9% year on year to 485 million yen. Managed Security Services are forecast to perform well, while the sales of the Integration Services are forecast to drop. Continuing from the previous fiscal year, the company will actively implement business investments such as hiring staff to expand its network and the security operation center (SOC), newly recruiting employees for planning new services and strengthening the sales department, marketing activities to develop new sales channels, and investment in the zero-trust security model. Until the fiscal year ending February 2027, the company will prioritize the allocation of funds to human resource investment, service development, M&A, etc., in order to realize the medium-term business plan for further growth, and refrain from paying dividends this fiscal year, too.**

- **Through its medium/long-term business investment, the company aims to achieve growth by expanding security-related areas and sales channels. In order to accomplish this aim, the company has set "expanding the areas of managed services and strengthening competitiveness," "entering the growing security market," and "strengthening the new sales system that differs from the existing sales network" as its management policies. For the fiscal year ending February 2027, the company aims for revenue of 3,763 million yen and an operating income of 920 million yen.**

- **President Kajiura commented, "We were able to release vulnerability diagnosis services, etc. in the fiscal year ended February 2024 as scheduled, for entering the zero-trust security field. In the fiscal year ending February 2025, we plan to release 'Vario Ultimate ZERO－Start Pack' and 'Vario Ultimate ZERO－Standard Pack' for small and medium-sized enterprises (SMEs), and in the fiscal year ending February 2026, we plan to release 'Vario Ultimate ZERO Enterprise Pack' with enhanced functions for medium or large-sized enterprises. Like this, we will enter the 'zero-trust security field' on a full-scale basis. We will continue new endeavors based on the stability of our business, and live up to the expectations from shareholders and investors, so we would appreciate your continued support."**

- **The growth of the top line is slow, but they are developing products for entering the "zero-trust security field" steadily. In addition, "AI SoC," a project for rationalizing the operation and management of network security by utilizing the AI technology of HEROZ, is progressing as planned. For this fiscal year, profit is projected to decline due to the augmentation of costs through investments, but they said that they have been offsetting the augmentation of VSR procurement costs due**

**to the global inflation and the yen depreciation so far. We would like to keep an eye on the progress of sale of "Vario Ultimate ZERO－Start Pack" and "Vario Ultimate ZERO－Standard Pack," which are to be released in this fiscal year.**

# 1. Company Overview

### [1-1 Corporate History]

In June 2001, Ambisys Inc. — the predecessor of the company — was founded with the business objectives to develop and operate information, communication, and security systems and provide consulting services on them. In May 2002, the company launched the Managed Security Services using the integrated Internet security appliance equipment. In June 2003, the company name was changed to Vario Secure Networks Inc. As an independent Internet security service company, the company steadily expanded its businesses and was listed on the Nippon New Market "Hercules" at the Osaka Securities Exchange in June 2006.

In the ensuing period, the company's growth slowed down with a higher churn rate from existing customers and the increase in service installation locations stagnating, as a result of the deterioration in corporate profits and the decline in private capital investments triggered by the bankruptcy of Lehman Brothers.
In order to make speedy management decisions and improve corporate value under a dynamic and flexible management system in the constantly changing network security market, the company realized that upfront investments were unavoidable, which might temporarily deteriorate profits. Under such a condition, the company took a decision to delist shares and concentrate on improving corporate value, and in December 2009 duly delisted the shares on Hercules.

After delisting, the company renewed its management structure amid several major shareholder reshuffles, and increased its internal cost awareness, while working to expand its businesses by strengthening the existing sales force and developing new sales agents, as well as continuously conducting R&D to improve the quality of security services. As a result, the company was able to increase corporate value, which was the purpose of delisting, by strengthening its sales structure, creating new businesses, and strengthening the service menu. The company name was changed to its current name, Vario Secure, Inc. in September 2016.
To realise a sustainable growth and corporate value enhancement, the company was convinced of the importance of securing the flexible and diverse financing methods and also that by relisting, the company could further improve social credibility, secure excellent human resources, improve employees' motivation to work, and aim for appropriate stock price formation and liquidity, the company got listed on the Second Section of the Tokyo Stock Exchange in November 2020. The company got listed on the TSE Standard Market in April 2022.

### [1-2 Corporate Philosophy, etc.]

The company's mission is **"to ensure that all enterprises using the Internet can easily and securely carry out their business, the company will offer the very best services to Japan and to the world."**

Under this mission, as a company that provides Internet-related security services, it provides comprehensive network security services to assist with the safer use of the Internet by protecting the customers' networks from attacks from the Internet, intrusions into internal networks, and various threats such as virus infections and data thefts.

### [1-3 Market Environment]

**(1) Growing demand for cybersecurity**

**◎ New types of cyberattacks receive increased attention**

In January 2023, IPA (Information-technology Promotion Agency, Japan) released the Ten Major Threats to Information Security 2023. The Ten Major Threats to Information Security 2023 were selected by IPA from information security incidents that occurred in 2022 and are considered to have had a significant impact on society. The Ten Major Threats Selection Committee, consisting of approximately 200 members, including researchers in the information security field and practitioners from companies, deliberated and voted on the threat candidates.
In terms of "organizations," "damage caused by ransomware" was the top ranking for the second consecutive year, followed by "attacks exploiting weaknesses in the supply chain," which ranked third last year. On the other hand, "attacks that target before an updated

program is released (zero-day attacks)" rose from seventh place in the previous year to sixth place, indicating that cyberattacks are becoming more diverse.

**◎ Ministry of Economy, Trade and Industry of Japan calls employers to strengthen cyber security efforts**

In December 2020, the Ministry of Economy, Trade and Industry (METI) issued a report urging business owners to strengthen cybersecurity efforts in response to the ever-increasing cyberattack entry points as well as the severities of the attacks.

This report identified the following current issues:

• In recent years, the attack entry points in the supply chain used by attackers have been constantly increasing. These include overseas bases of business partners including SMEs and companies expanding overseas, as well as gaps created by the increase in telework due to the spread of the novel coronavirus.

• In addition to demanding ransoms to recover encrypted data, ransomware that uses the so-called "double threats" — threatens to release the data that was stolen in advance before encrypting unless ransom is paid — are rapidly increasing in Japan. This is due to the establishment of an ecosystem which enables attackers to systematically provide ransomware as well as collecting ransoms systematically, allowing them to operate easily without having to be highly skilled.

• With the globalization of businesses, more and more systems that are closely linked with overseas bases are being built; however, as a result of linking the Japanese domestic systems to those of overseas without sufficient measures, the risk of intrusion is increased as this enabled the attackers to construct intrusion routes at overseas bases where security measures are insufficient.

Based on these, the report urges corporate managers to act on the following responses and initiatives:

• The severity of damage caused by cyberattacks is increasingly more serious and the damages are also more complex: management needs to be involved even more than previously.

• Responding to the damages caused by ransomware attacks is an important issue directly related to corporate trust, and sweeping management leadership is required from proactive prevention to postvention.

Under these conditions, the security service market is seeing an increase in demand.

The security service market requires advanced security measures, but companies that find it difficult to operate and manage in-house security measures tend to outsource operations and monitoring to security vendors, leading to an increase in the service usage.

The market size is expected to expand from 260.1 billion yen in the fiscal year ended 2022 to about 383.4 billion yen in the fiscal year ending 2028, with an average annual growth rate of 6.7%. (Source: Fuji Chimera Research Institute, Inc. "2023 Network Security Business Survey Overview (Market Edition)" published on December 14, 2023).

**(2) IT personnel shortage**

The METI ran a trial calculation of the output gap in IT human resources due primarily to the expansion of IT investment by companies using AI.

According to the report, if the productivity growth rate is 0.7%, the shortage in the number of IT workers in 2030 is estimated at 787,000 in the high-level scenario (3-9% growth in IT demand), 449,000 in the medium level scenario (2-5% of the same), and 164,000 in the low-level scenario (1%). Even if productivity were to rise to 2.4%, the high-level scenario still predicts a shortfall of 438,000 people.

Under these circumstances, it is difficult for companies to secure sufficient IT human resources within their companies, therefore a steady increase is expected for the demand for "managed service" that provide not only the functions but also combine the operation management as one when using IT systems.

* Gap in demand for IT personnel in 2030 (number of workers)

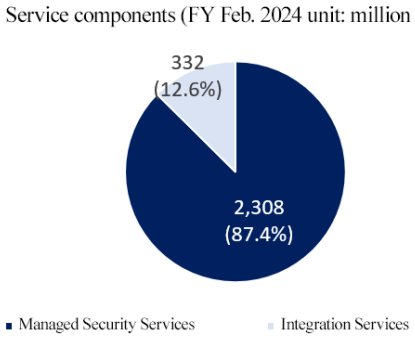
| Productivity Growth Rate | Low-level scenario | Medium-level scenario | High-level scenario |
|---|---|---|---|
| In case of 0.7% | 164,000 | 449,000 | 787,000 |
| In case of 2.4% | -72,000 | 161,000 | 438,000 |

*Created by Investment Bridge based on the Ministry of Economy, Trade and Industry's "Survey on Supply and Demand of IT Human Resource (Summary)" (April 2019).

[1-4 Business Contents]

### (1) Service category

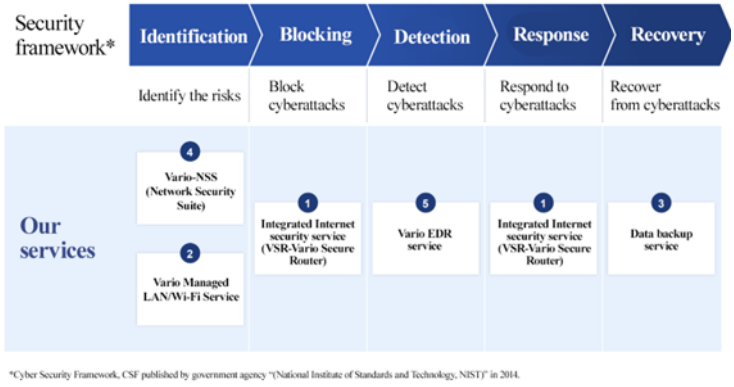
The company provides two security services: Managed Security Services and Integration Services (segment: single segment of Internet security service business).




(Source: materials provided by the company)

### ① Managed Security Services

This covers all of the processes: "identification," "blocking," "detection," "response," and "recovery" in the security framework.
Vario Secure mainly offers "integrated Internet security service" using VSR, which blocks cyberattacks, and also provides the data backup service (VDaP), the Vario EDR service that helps detect and respond to cyberattacks at lower operational costs, and Vario-NSS, which detects abnormal terminals and provides vulnerability management, etc.




(Source: the company's website)

### <Integrated Internet Security Service Using VSR>

**Overview**

This service provides comprehensive network security that protects corporate networks from the attacks from the Internet, intrusions into internal networks, and threats such as virus infections and data thefts, and enables customers to use the Internet safely.

The company's integrated Internet security service uses VSR (Vario Secure Router) — a network security device developed by the company which integrates various security functions such as firewalls, IDS (intrusion detection system), and ADS (automatic defense system) into one unit — which is installed between the Internet and customers' internal networks, and acts as a filter to remove threats such as attacks, intrusions, and viruses.

VSR is automatically managed and monitored by a proprietary operational monitoring system run by the company's data center, and operational information statistics and various alerts are processed in real time without human interventions.
Statistics and alerts are provided in real time to user company administrators over the Internet via a reporting function called, the Control Panel. In addition, the company has established a 24/7 support center, and a maintenance network covering all 47 prefectures in Japan and an operation support system such as changing the equipment settings.

Since they are manufactured at several factories in Taiwan while the core software is developed in-house, it is more cost-effective than purchasing hardware and adding services, and this is one of the reasons contributing to VSR's high operating income margin.


(Source: the company's website)

**Merits**

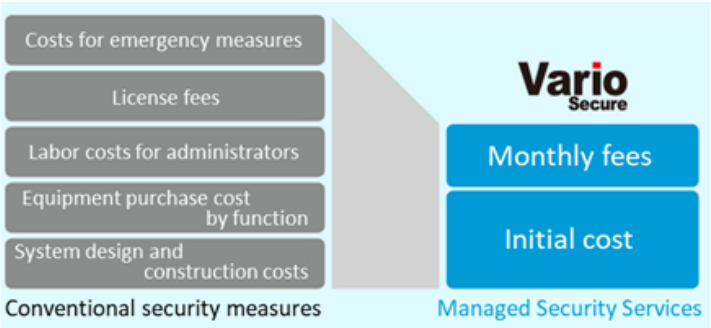
Previously, to introduce the security system such as above, it was necessary to install various security devices in-house and maintain them, making it more difficult for many companies to introduce sufficient network security measures because they required highly skilled engineers and high investments.

In addition, even after the introduction of the security system, monitoring, quick response to alerts, software updates, inquiries in the event of trouble, etc. required a great deal of effort and time, and the operational burden was extremely large.

In contrast, the company's Managed Security Services, which provides the one-stop solution from initial introduction to operation and maintenance of VSR, a unique in-house product, provides significant benefits to customers in the following respects:

| |
|---|
| As VSR boasts 23 different security features per unit, it eliminates the need to purchase equipment and instead provides the security system via the rental equipment. |
| A monthly fee is set for each security feature, allowing customers to choose the options they need from a variety of security features. |
| By simply paying the initial cost incurred only at the start of the contract and monthly fees, it is possible to outsource most of the man-hours required for the operation of network security, such as using the control panel, changing settings, updating software, and local maintenance through monitoring and business trip support, reducing the burden of work. |
| In addition to inquiries from customers (end-users) to the company or distributors, the company actively detects and supports problems through remote monitoring. Operation and maintenance are remotely handled as much as possible by the company's engineers, making it possible to respond more quickly compared to general on-site responses via call centers. |
| To deal with hardware failures, the company deploys inventory at warehouses of subcontractors throughout the country, and aims to replace the equipment within the target timeframe of four hours. |

The ease of introduction and the clarity of the menu are highly evaluated by mid-tier enterprises and MSEs.




(Source: materials provided by the company)

**(Number of VSR units installed)**

Most of their customers are mid-sized and small businesses who would struggle to employ IT managers with expertise on their own. As

of February 28, 2024, the number of VSR managed units was 7,796. They were installed in 47 prefectures throughout the country.
It has a high market share amongst the mid-tier enterprises and SMEs.

**<Data Backup Service (VDaP)>**

The company provides a backup service that combines VDaP, where backup data are stored on a device, and the storage in a data center. After temporarily backing up corporate digital data to VDaP, data are automatically transferred to the data center to further increase the fault resistance.
In addition, since the latest and past data are kept as version-managed backup data, it is easy to select and recover the necessary digital data by providing an interface for the customers that are easy to use when recovering data.
Utilizing its experiences in monitoring and operating services for integrated Internet security service using VSR, the company also provides the service that efficiently covers the whole country by utilizing the system for installing equipment and responding to failures.

**<Vario EDR Service>**

Vario EDR Service visualizes cyberattacks that try to penetrate through antivirus measures and avoid security incidents before they happen. It adopts highly accurate detection methods using AI and machine learning, and against the high-risk incidents, it would conduct automatic isolation of terminals and initiate investigations by security specialists. It supports clients in detecting and responding to cyberattacks with light workloads for operation.

**<Vario-NSS（Network Security Suite）>**

As the shortage of IT personnel in companies becomes more serious, the company will support the efficient operation of internal systems and promote the concept of "Information System as a Service." Vario-NSS automatically scans terminals connected to the corporate network by simply installing a dedicated terminal in the network for asset management, visualizes terminal information, and understands vulnerability response. This enables it to respond to terminals with security risks early and monitor unauthorized terminals, reducing the burden and risk on the IT asset management which tends to rely on personal operations. Through continuous updates, it can not only manage Windows terminals, but also centrally manage Red Hat Linux terminals which are widely used for internal servers, etc. reducing the burden on personnel in the information systems departments at customer companies.

**<Vario Managed LAN/Wi-Fi Service>**

It safeguards in-house LAN switches and Wi-Fi access points.

**② Integration Services**

This consists of sales of Vario Communicate Router (VCR), an integrated security device (UTM) for small and medium-sized enterprises, and Network Integration Services (IS) for procurement and construction of network equipment.

**<Sales of integrated security equipment VCR for small and medium-sized enterprises>**

The company sells VCR, a security appliance device, in response to the growing security awareness among smaller businesses and clinics with fewer than 50 employees, due to regulatory changes such as revisions of the Basic Act on Cybersecurity among others.

Unlike Managed Security Services, UTM products are imported as their own brands from overseas manufacturers and sold to end-users through distributors specializing in small and medium-sized enterprises.
Throughout the warranty period, the manufacturers provide support on sold equipment and hardware failures, through the company's and/or distributors' support desk.

**<Network Integration Services (IS)>**

Their engineers cover the whole areas of designing, procuring, and building the network according to the needs of end-users, and are working to expand the business into the wider corporate network areas.
As with the VCR sales, the manufacturers provide support on sold equipment and hardware failures, through the company's and/or distributors' support desk.

### (2) Revenue model

Managed Security Services provide one-stop service from the introduction of network security to management, operation, and maintenance, and is a stacked recurring business model that collects initial costs and fixed monthly costs from users.
There is a one-time charge for the Integration Services, associated with the sale of VCRs and the procurement and construction of network equipment.

### (3) Sales channels

Sales are mainly indirect sales through distributors.
The company has signed contracts with distributors such as telecommunications carriers, Internet service providers, data center operators, etc., who are looking to provide added value to customers by attaching Vario Secure services, and has built a sales network covering the whole country. The company has established a system that can continuously create opportunities.

The company's distributors are divided into the original equipment manufacturers (OEM partners) and the reselling partners.
An OEM partner is a partner that provides security services under the distributor's own brand and enters contracts directly with the customers (end users). As of the end of February 2024, the company has signed agreements with 31 companies for all managed services such as KDDI and SoftBank.
A reselling partner is a partner that develops customers (end users) and engages in sales activities as an agent of Vario Secure, through which Vario Secure remains as the contracting entity with customers. As of the end of February 2023, the company has signed agreements with 68 companies for all managed services.
In addition to the above, to promote sales activities, Vario Secure as a security expert provides sales representatives who directly explain technical aspects to customers on behalf of distributors, and provides one-stop support from introduction to installation of services.

### (4) Total number of end users of Managed Security Services

The total number of end-user companies of the overall Managed Security Services was 3,091 as of the end of February 2024, increased 110 from the previous fiscal year.

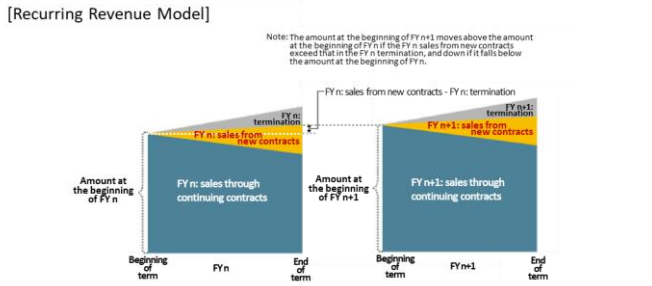
## [1-5 Characteristics and Strengths]

### (1) Unique business model

The company provides one-stop service for (1) procurement of equipment used in security services, (2) development of core software to be installed on equipment, (3) installation/setting of equipment, and (4) monitoring and operation after installation of equipment. There is no need for end-users to individually consider equipment selection and operation services, and they can quickly start using the service.
In addition, since the service is provided as one-stop, the company can easily investigate the cause of a problem and respond.
Support is available 24/7, allowing end-users to quickly receive support for inquiries and troubles.

### (2) Stable revenue model

As mentioned above, Managed Security Services are recurring business in which profits accumulate year by year due to the increase in the number of companies introduced by monthly billing, and as of the end of February 2024, Managed Security Services were provided at approximately 7,796 locations (number of VSR-installed locations) in all 47 prefectures nationwide.
In the term ended February 2024, Managed Security Services accounted for 87.4% of the company's total revenue. With a low churn rate of 0.7% (in fiscal year ended February 2024), a stable earnings model has been built, and it is possible to forecast revenues at a relatively early stage in the fiscal year.




(Source: material provided by the company)

### (3) Strong sales channels

As mentioned above, it has built strong sales channels with 31 OEM partners and 68 reselling partners, covering the whole country. It is an important asset for efficient sales for the company, which mainly targets mid-tier enterprises and MSEs.

In addition, since there are many OEM partners in the telecommunication industry and the company's services are incorporated as an option in the menu of the operating company, it is easy for users to select and introduce when the Internet connections are newly installed or altered, leading to a high order rate.

### (4) High market share

The company is the market leader in all following categories by employee number: 300 to 999, 100 to 299, and 0-99 in the Firewall/UTM* operational monitoring service market.

* Firewall/UTM operational monitoring service market: Sales Amount and Market Share by Employee Size (Results of FY 2022)

| | 0 – 99 employees | | 100 – 299 employees | 300 – 999 employees |
|---|---|---|---|---|
| No. 1 | Vario Secure 35.0% | | Vario Secure 22.4% | Vario Secure 20.6% |
| No. 2 | Company A 16.5% | | Company A 14.5% | Company A 8.9% |
| No. 3 | Company B 7.9% | | Company B 7.9% | Company B 8.1% |

*Source: ITR "ITR Market View: Gateway Security-Based SOC Service Market 2023" Market of Firewall/UTM operation monitoring services (FY 2022), produced by Investment Bridge with reference to the material of the company.

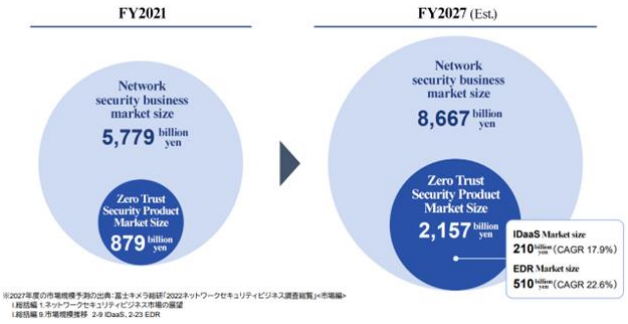
* UTM: Unified Threat Management. A network security measure operated by combining multiple security functions into one.

## 2. Medium/long-term growth strategy

### (1) Network security business market trends

Security trends have irreversibly changed from perimeter defense (no intrusion) to zero-trust (intrusion occurs) due to changes in the social environment, such as telecommuting, expanded use of cloud services, and the sophistication of cyberattacks.

In particular, the growth rate of the zero-trust security* market is expected to exceed the growth rate of the entire network security business market, and the EDR and IDaaS markets, which are specific solutions for zero-trust security, are expected to grow even higher.




(Taken from the reference material of the company)

***Zero-Trust Security**

Conventional security measures, it is assumed that the data and systems to be protected are in the internal network, however, with the spread of cloud computing, more and more data and systems that should be protected exist on the Internet, which is on the external network.

As such, the boundaries have become vague, subjects to be protected exist both inside and outside the system, thus, it is becoming increasingly difficult to take sufficient countermeasures with the conventional approach. The "Zero-Trust Security" is a security measure based on the assumption that all communications should not be trusted (Zero-Trust) when considering the security.

### (2) The company's management issues and solutions

The company acknowledges the external and internal environment and management issues in this market environment as follows.

| External environment | Internal environment |
|---|---|
| ■ The conventional perimeter defense market is expected to grow at an annual rate of around 1.3%<br>■ There is a need for multi-layered zero-trust security measures that "do not allow intrusion" and "allow intrusion"<br>■ Demand for zero trust security is expected to grow further in the future | ■ The appliance-type UTM product market for small and medium-sized enterprises has grown steadily, but the number of new installations of our VSR has remained flat recently.<br>■ Our main service is a perimeter defense type for the purpose of "not allowing newcomers"<br>■ Malware detection and prevention (Vario Endpoint Security) and ransomware-resistant backup (Vario Data Protect) show double digit growth |

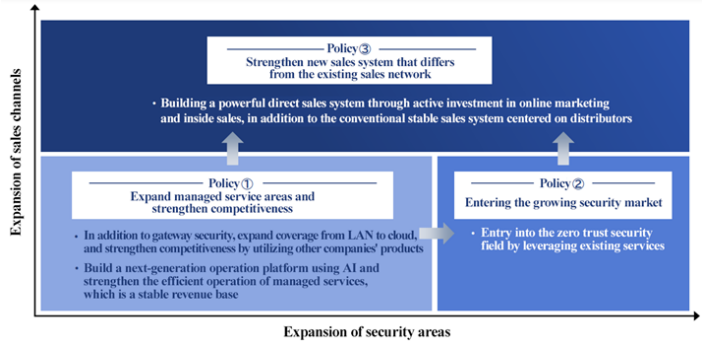
(Taken from the reference material of the company)

In order to solve these management issues, expand the zero-trust security market, and achieve sales and profit growth, the company believes it has to enhance its strengths, invest in growing markets, and strategically develop new customers.

### (3) Medium-term management policy

In order to achieve growth by expanding security areas and sales channels through medium/long-term business investment, the company will promote the following three management policies.

Policy 1 Expanding managed service areas and strengthening competitiveness
Policy 2 Entering the growing security market
Policy 3 Strengthening the new sales system that differs from the existing sales network




(Taken from the reference material of the company)

**＊Policy 1: Expanding managed service areas and strengthening competitiveness**

In addition to gateway security, the company will expand the scope of managed services from LAN to cloud services and strengthen competitiveness by utilizing other companies' products.

Moreover, the company will build a next-generation operation platform using AI through an alliance with HEROZ and strengthen the efficient operation of managed services, which is a stable revenue base.

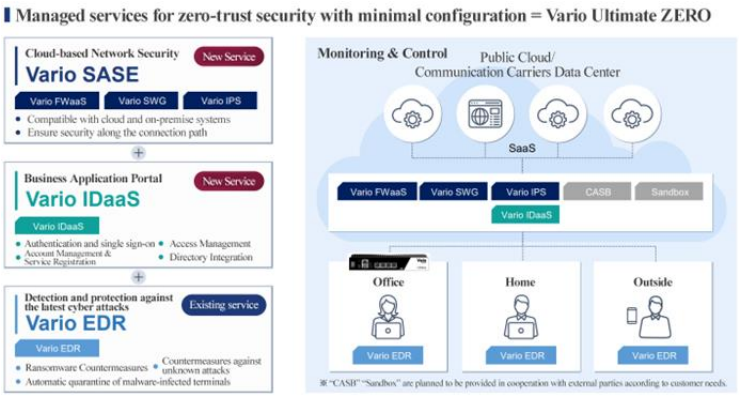
| |
|---|
| Progress in the fiscal year ended February 2024<br><br>An option for vulnerability diagnosis was released. They found 8 new distributors, which have marketing capabilities, for managed services. The effects of the organizational restructuring for marketing have been exerted steadily. |

**＊Policy 2: Entering the growing security market**

Utilizing existing services, the company will enter the zero-trust security field.

They will offer security services suited for the scale of small and medium-sized enterprises, which are targeted by the company, for protecting the cloud and office environments, and provide “Vario Ultimate ZERO” for ensuring security and saving labor for operation

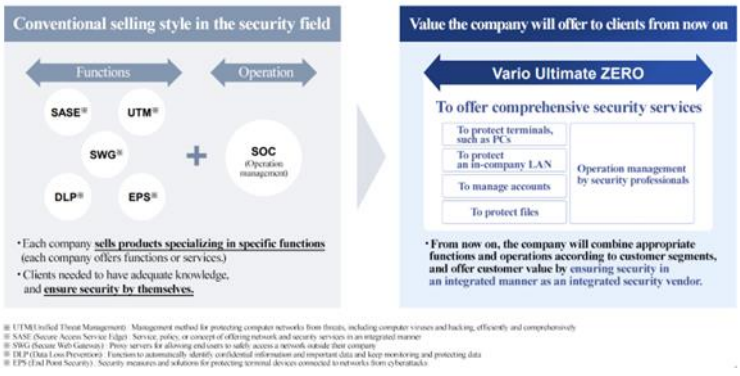
and management.




(Taken from the reference material of the company)

| |
|---|
| Progress in the fiscal year ended February 2024<br><br>They developed the cloud management function and the single sign-on (SSO) function.<br>While providing existing products, the company made preparations for the release of zero-trust security MSS, which protects on-premise systems, cloud systems, and SaaS in a cross-sectoral manner. |

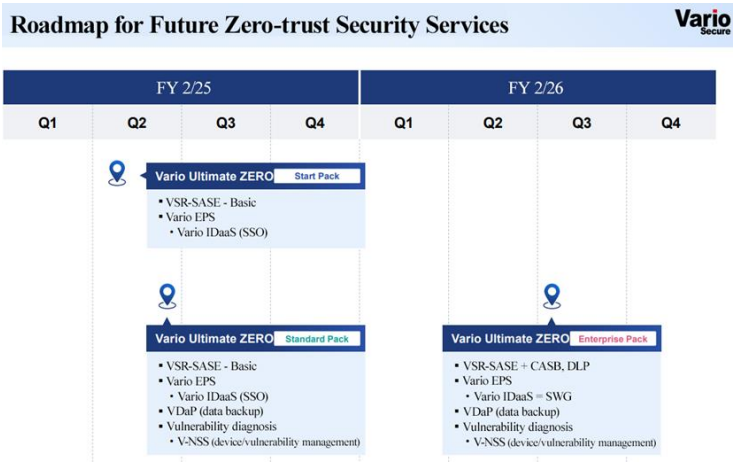
The clients of the company are mainly small and medium-sized enterprises, but due to the characteristics of the traditional security industry, it has been common for clients to choose and combine services to ensure the security of their systems by themselves.
The clients among large companies possess the knowledge of security, so that conventional style can work. The company aims to develop the style of providing clients with "comprehensive security" based on "Vario Ultimate ZERO" as a security BPO vendor, which ensures security in an integrated manner.




※ UTM(Unified Threat Management) : Management method for protecting computer networks from threats, including computer viruses and hacking, efficiently and comprehensively
※ SASE (Secure Access Service Edge) : Service, policy, or concept of offering network and security services in an integrated manner
※ SWG (Secure Web Gateway) : Proxy servers for allowing end users to safely access a network outside their company
※ DLP (Data Loss Prevention) : Functions to automatically identify confidential information and important data and keep monitoring and protecting data
※ EPS (End Point Security) : Security measures and solutions for protecting terminal devices connected to networks from cyberattacks

(Taken from the reference material of the company)

For completing their zero-trust service, they plan to release "Vario Ultimate ZERO－Start Pack," which is composed of VSR-SASE – Basic, Vario EPS, and Vario IDaaS (SSO), and "Vario Ultimate ZERO－Standard Pack," which is equipped with VDaP (data backup) and V-NSS (device/vulnerability management) for vulnerability diagnosis, in the second quarter of the fiscal year ending February 2025. In the third quarter of the fiscal year ending February 2026, they plan to release "Vario Ultimate ZERO－Enterprise Pack" with further enhanced functions for medium and large-sized enterprises.




(Taken from the reference material of the company)

**＊Policy 3: Strengthening the new sales system that differs from the existing sales network**

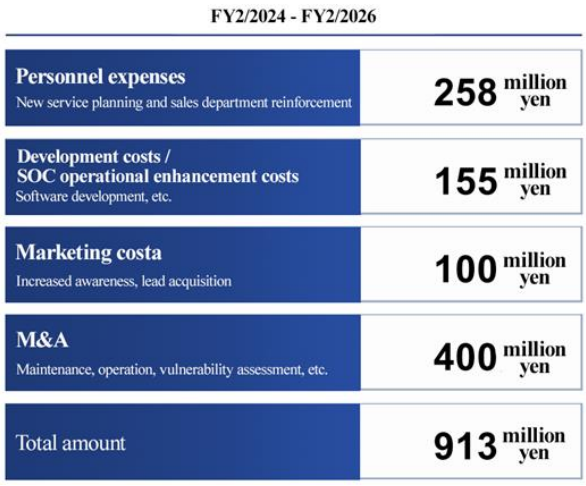
In addition to the conventional stable sales system centered on distributors, the company will build a solid direct sales system by actively investing in online marketing and inside sales. As the list of potential clients has been enriched to some degree, they will take measures for attracting new clients and finding new distributors with the system focused on profitability and efficiency without increasing employees so much.

| |
|---|
| Progress in the fiscal year ended February 2024<br><br>As they actively exhibited their products at events, etc., the number of prospective clients increased six times.<br>Through the enhancement of tele-marketing, the number of prospective clients that have made a deal with the company increased by 20%.<br>They opened a solution website and adopted marketing automation. |

### (4) Medium-term investment plan

Over the three years from fiscal year ended February 2024 to fiscal year ending February 2026, the company will invest in marketing for acquiring new sales channels and in personnel and development for strengthening sales capabilities. The company also plans to invest 400 million yen in M&A for a total of 900 million yen in growth investment.

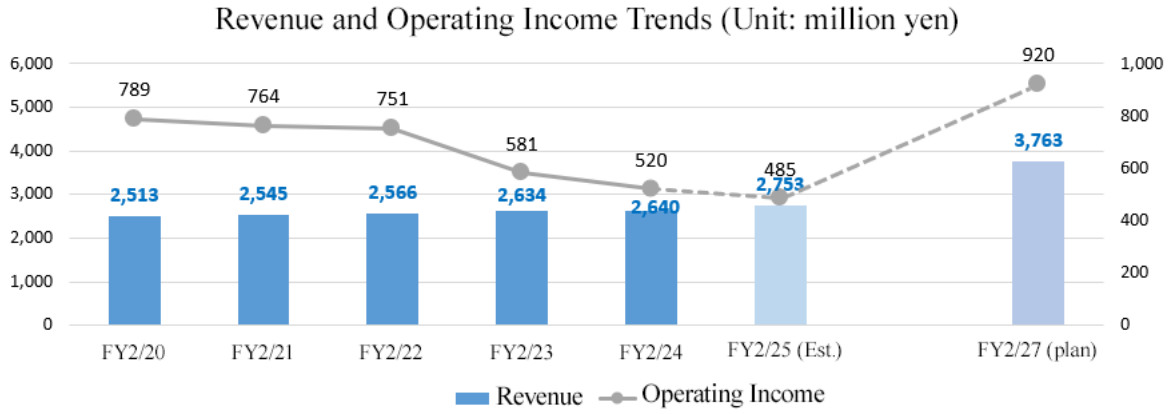
It assumes M&A with companies with expertise in vulnerability diagnosis and companies with strong sales capabilities targeting small and medium-sized enterprises.




(Taken from the reference material of the company)

### (5) Medium-term management targets

They aim to achieve a sales revenue of 3,763 million yen and an operating income of 920 million yen in the fiscal year ending February 2027, by increasing sales through the provision of value of the existing integrated Internet security and cross-selling for solving each client's issues and meeting new demand by releasing the zero-trust security product "Vario Ultimate Zero."
For the three years from fiscal year ended February 2024 to fiscal year ending February 2026, they aim to increase sales revenue by 42.8% (CAGR: up 9.3%) and operating income by 58.3% (CAGR: up 12.2%) from fiscal year ended February 2023.



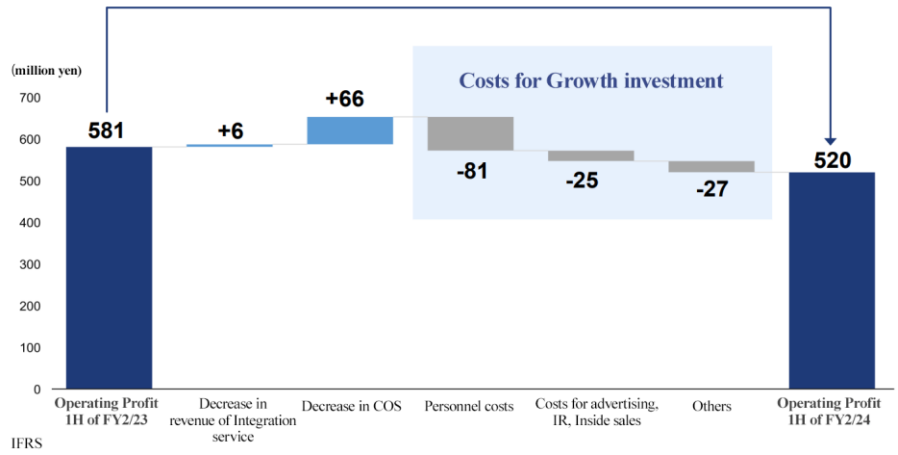

Through the expansion of security-related areas and sales channels, the sales composition ratio of Managed Security Services is expected to rise from 85.0% in fiscal year ended February 2023, 87% in fiscal year ended February 2024 to 89% (forecast) in fiscal year ending February 2025 and then to 94.3% in fiscal year ending February 2027.

## 3. Fiscal Year Ended February 2024 Earnings Results

### (1) Overview of business results

| | FY 2/23 | Ratio to sales | FY 2/24 | Ratio to sales | YoY | Ratio to forecast |
|---|---|---|---|---|---|---|
| Revenue | 2,634 | 100.0% | 2,640 | 100.0% | +0.2% | -1.7% |
| Gross profit | 1,390 | 52.8% | 1,463 | 55.4% | +5.2% | - |
| SG&A and others | 810 | 30.8% | 943 | 35.7% | +16.3% | - |
| Operating profit | 581 | 22.1% | 520 | 19.7% | -10.4% | +14.0% |
| Profit before tax | 542 | 20.6% | 509 | 19.3% | -6.1% | - |
| Profit | 383 | 14.5% | 347 | 13.1% | -9.3% | +12.7% |

*Unit: million yen



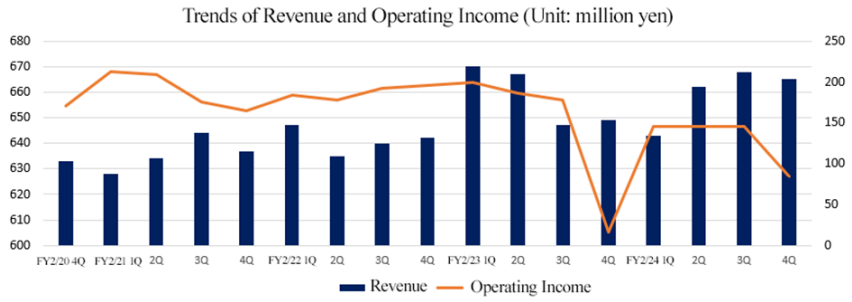

(Taken from the reference material of the company)

**Revenue increased and profit decreased**

Revenue increased 0.2% year on year to 2,640 million yen. While Managed Security Services, which are the mainstay, performed well, the Integration Services business was sluggish because competition got fiercer and fiercer.

Operating income dropped 10.4% year on year to 520 million yen. Gross profit rose thanks to the sales growth, but it was not enough to offset the augmentation of SG&A expenses due to the active business investment, such as service plans, the recruitment of engineers and operation support staff, and the enhancement of marketing based on the medium-term management policy.

Sales revenue was almost as forecast. Operating income exceeded the forecast, as they increased employees significantly through business investment, but personnel expenses fell below the forecast due to the decrease in recruitment costs and the postponement of start of working in the company.

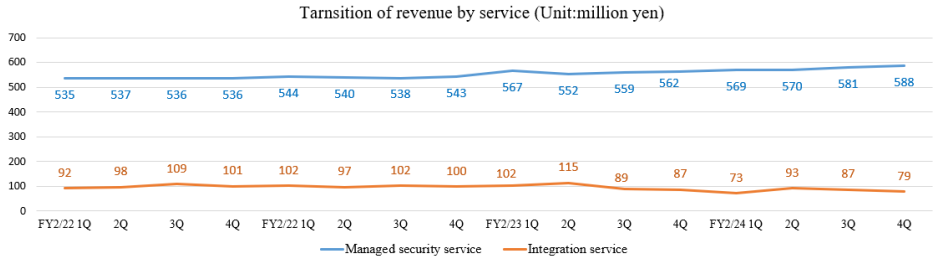



(Produced by Investment Bridge with reference to the material of the company)

## (2) Service trends

| Revenue | FY 2/23 | FY 2/24 | YoY |
|---|---|---|---|
| Managed Security Service | 2,240 | 2,308 | +3.0% |
| Integration Service | 393 | 332 | -15.6% |

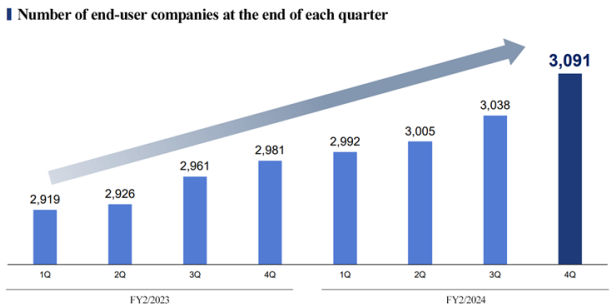
*Unit: million yen



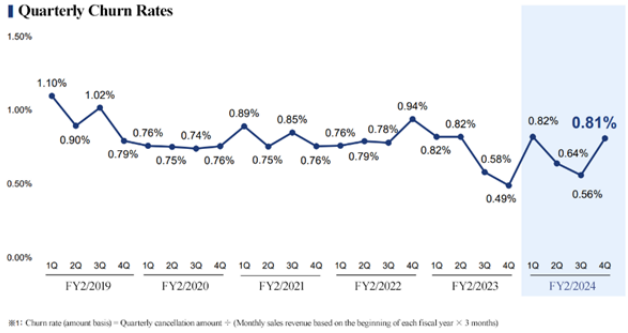

(Produced by Investment Bridge with reference to the material of the company)

### ① Managed security service

Sales grew stably. The number of enterprises as end users as of the end of February 2024 was 3,091, up 110 from the previous year, showing a steady growth. Cancellation rate remained low. It was 3% below the forecast.



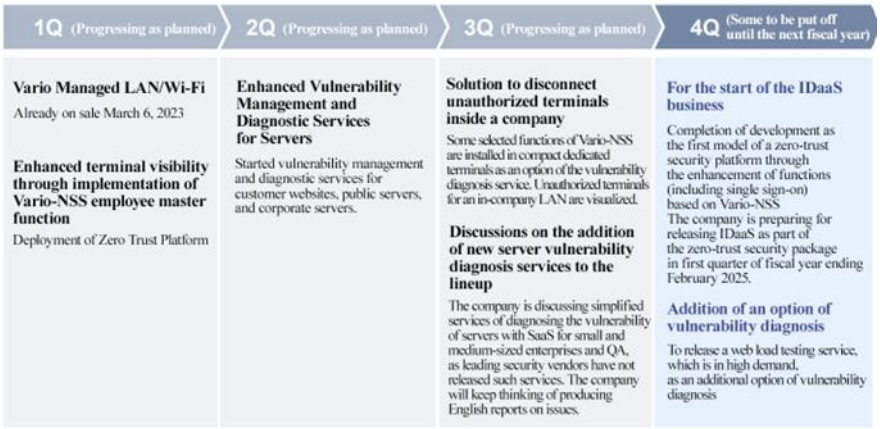

(Taken from the reference material of the company)




(Taken from the reference material of the company)

The performance of the services for coping with malware by detecting the intrusion into information devices, such as PCs and servers, and preventing the spread of viruses and the services for coping with ransomware by protecting data and helping restore data remained healthy.
The sales revenue of Vario Endpoint Security for detecting and blocking malware increased 85.4% year on year, while that of Vario Data Protect for backing up data to cope with ransomware rose significantly by 33.7% year on year.

In the first half of the fiscal year ended February 2024, they released managed LAN/Wi-Fi and services for managing and diagnosing the vulnerability of servers, and the development of the first zero-trust security platform was completed by enhancing the functions, such as single sign-on, based on Vario-NSS for launching the IDaaS business. Like this, they have been releasing new services almost as planned.
In the first quarter of the fiscal year ending February 2025, they are making preparations for releasing IDaaS as part of a zero-trust security package.




(Taken from the reference material of the company)

### ② Integration Services

As the sales of integrated security devices (VCR-Vario Communicate Router) for SMEs were sluggish and declined, but the overall sales of this service exceeded the full-year forecast by 10%, as the development of networks progressed steadily.

### (3) Business topics

* As they started offering vulnerability diagnosis and managed LAN/Wi-Fi services, a system for comprehensively supporting the security of SMEs has been established.

  The company began providing vulnerability diagnosis services. The company remotely conduct automated diagnosis with dedicated tools and diagnosis led by security engineers and check vulnerability, including "web application diagnosis," "penetration testing," "platform (network) diagnosis," and "smartphone application diagnosis."

After diagnosing vulnerabilities, the company flexibly provides security enhancements such as managed UTM operation services, next-generation endpoint measures, security-enhanced backup, and integrated management of switches and Wi-Fi APs within a LAN, depending on the customer's situation.

This service is positioned as a gateway to the realization of the Zero-Trust Security model, which is the company's goal.

* "AI SoC," a project for streamlining the processes for operating and managing network security by utilizing the AI technology of HEROZ, is progressing as planned.

The tasks at the technical support desk, which has been conducted by experienced operators, will be automatically dealt with by AI. The large language model (LLM) will be utilized on a full-scale basis for improving the quality and efficiency of support, conducting education on security, etc.
It is expected to reduce costs, improve quality, shorten working hours to increase the level of services, and expand the range of services by utilizing a great deal of data on teachers.

They have adopted AI for the task of changing settings in the VSR managed security service, so that the complexity of requirements for each client would be evaluated automatically and the following processes would be semi-automated. They inputted the data on teachers into the LLM, and started an experiment for checking whether the quality of veteran operators can be achieved.

They will apply AI to front desk support tasks, too, to reduce educational costs and improve the quality of answers.
They aim to offer necessary and sufficient operation services according to the characteristics of clients, by directly linking AI with the operational platform system, which manages clients and inquiries.

* They have strengthened the marketing measure based on the policy set in the medium-term plan. They aim to expand the demand through direct sale.

They established a solution website as a marketing measure. They will enhance cross-selling by putting together content about cyber security, including the descriptions of solutions, seminar information, archived videos of webinars, useful reference material, and cases of adoption of solutions.

They started streaming the archived videos of webinars in January 2024, and the number of such videos is now 9. The largest number of views exceeds 700.
As the cases of adoption of solutions, they outline client enterprises and describe how services were used, the effects of services, and interviews with staff in charge.

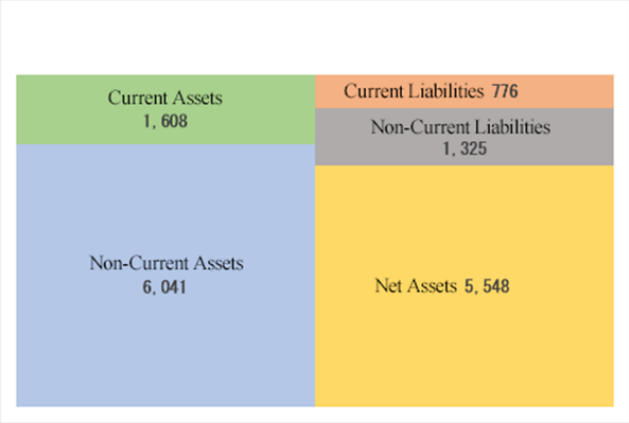
### (4) Financial position and cash flows

**◎ Main Balance Sheet**

| | End of February 2023 | End of February 2024 | Increase/ decrease | | End of February 2023 | End of February 2024 | Increase/ decrease |
|---|---|---|---|---|---|---|---|
| **Current Assets** | 1,925 | 1,608 | -316 | **Current Liabilities** | 832 | 776 | -56 |
| **Cash and Cash Equivalents** | 1,039 | 822 | -218 | **ST Interest Bearing Liabilities** | 200 | 200 | 0 |
| **Trade and Other Receivables** | 443 | 458 | +14 | **Trade and Other Payables** | 81 | 106 | +25 |
| **Non-current Assets** | 5,900 | 6,041 | +140 | **Non-current Liabilities** | 1,614 | 1,325 | -289 |
| **Tangible Assets** | 158 | 227 | +69 | **LT Interest Bearing** | 1,300 | 1,100 | -200 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | **Liabilities** | | | |
| **Goodwill** | 5,054 | 5,054 | 0 | **Total Liabilities** | 2,447 | 2,101 | -345 |
| **Intangible Assets** | 296 | 343 | +48 | **Net Assets** | 5,378 | 5,548 | +169 |
| **Total Assets** | 7,826 | 7,649 | -176 | **Retained Earnings** | 2,581 | 2,745 | +165 |
| | | | | **Total Liabilities and Net Assets** | 7,826 | 7,649 | -176 |
| | | | | **Total Borrowings** | 1,500 | 1,300 | -200 |

*Unit: million yen.



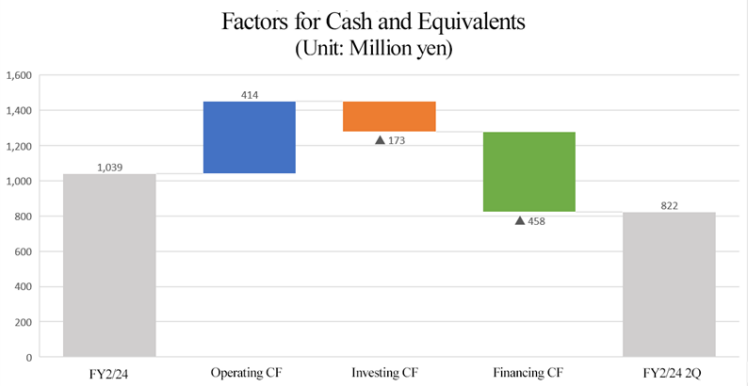

* Prepared by Investment Bridge Co., Ltd. based on the disclosed material.

Total borrowings decreased 200 million yen from the end of the previous fiscal year. Net D/E ratio was 8.6%, unchanged from the end of the previous fiscal year.
Capital-to-asset ratio rose 3.8 points from the end of the previous fiscal year to 72.5%.
Repayment of interest-bearing liabilities and financial soundness improvement are progressing as planned.

**◎ Cash Flows**

| | FY 2/23 | FY 2/24 | Increase/decrease |
|---|---|---|---|
| **Operating Cash Flow** | 522 | 414 | -107 |
| **Investing Cash Flow** | -138 | -173 | -35 |
| **Free Cash Flow** | 383 | 240 | -143 |
| **Financing Cash Flow** | 266 | -458 | -725 |
| **Balance of Cash and Equivalents** | 1,039 | 822 | -218 |

*Unit: million yen




* Prepared by Investment Bridge Co., Ltd. based on the disclosed material.

The surpluses of operating CF and free CF decreased between fiscal year ended February 2023 and fiscal year ended February 2024. The cash position declined.

## 4. Fiscal Year Ending February 2025 Earnings Forecasts

### (1) Earnings forecasts

| | FY 2/24 | Ratio to sales | FY 2/25 Est. | Ratio to sales | YoY |
|---|---|---|---|---|---|
| Revenue | 2,640 | 100.0% | 2,753 | 100.0% | +4.3% |
| Operating profit | 520 | 19.7% | 485 | 17.6% | -6.9% |
| Profit before tax | 509 | 19.3% | 474 | 17.2% | -6.7% |
| Profit | 347 | 13.2% | 336 | 12.2% | -3.2% |

*Unit: million yen

**Increase in revenue and decrease in profit estimated.**

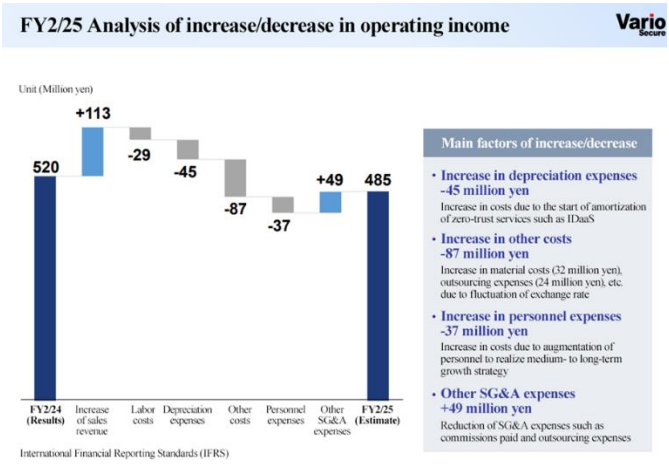
Revenue is expected to increase 4.3% year on year to 2,757 million yen, and operating income is expected to decrease 6.9% year on year to 485 million yen.

Managed Security Services are forecast to perform well, while the sales of the Integration Services are forecast to drop.

Under the steady sales growth, continuing from the previous fiscal year, the company will actively implement business investments such as hiring staff to expand its network and the security operation center (SOC), newly recruiting employees for planning new services and strengthening the sales department, marketing activities to develop new sales channels, and investment in the zero-trust security model.

Profit is projected to decline, due to the augmentation of depreciation for zero-trust services, such as IDaaS.

Until the fiscal year ending February 2027, we will allocate funds to the investment in human resources, the development of services, M&A, etc. on a priority basis, in order to realize the medium-term business plan for further growth, and refrain from paying dividends this fiscal year, too.




(Taken from the reference material of the company)

### (2) Service trends

| Revenue | FY 2/24 | FY 2/25 Est. | YoY |
|---|---|---|---|
| Managed Security Service | 2,308 | 2,452 | +6.3% |
| Integration Service | 332 | 300 | -9.5% |

*Unit: million yen

◎ Managed Security Services

Sales are expected to grow.

They will establish a new business by enhancing cross-selling through the enrichment of their service lineup, including managed LAN/Wi-Fi, and releasing IDaaS as part of zero-trust security.

◎ Integration Services
They will operate mainly the business of network development, for which demand is steady, but the sales of integrated security equipment (Vario Communicate Router [VCR]) for SMEs are projected to decline.

## 5. The Comments by President Kajiura

**＊Regarding Employee Development**
With competition becoming increasingly intense, unless employees acquire the ability to survive on their own, neither employees nor the company will be able to grow in order to achieve the medium-term management plan and attain sustainable growth.
For this reason, since assuming the position of president, I have been working to develop young employees and raise the overall company's standards.
Up until this point, I believe that our employees have developed beyond our expectations.

**＊Changes in Sales Organization**
In March of this year, we made significant changes to our sales structure.
Until now, we have had a sales force for each product, but when we think about focusing more on customers, including distributors, there is no need to have different sales forces for each product, as Vario Secure is one company from the customers' point of view.
Another reason for the reorganization is that we are now able to sell not only VSR, but also VDP and Vario-EDR.
We considered that such a sales structure would be necessary for the provision of "Vario Ultimate Zero," a zero-trust security product that puts together various commercial products.

**＊Role as a Security BPO Vendor**
Our customers are mainly small and medium-sized enterprises, but due to the traditional nature of the security industry, customers mainly chose several services, and were responsible for ensuring their own security.
Large companies have their own security-related expertise, so the above-mentioned conventional style is fine, but for our customers, such a style is extremely difficult due to the shortage of manpower and costs.
Therefore, our company, as a security BPO vendor that provides integrated security assurance to our customers, will aim to provide comprehensive security with "Vario Ultimate ZERO."

**＊Message to Shareholders and Investors**
In the fiscal year ended February 2024, we were able to release vulnerability assessment services and other products as planned in preparation for our entry into the "Zero-Trust Security Field."
We have plans to release "Vario Ultimate ZERO Start Pack" and "Vario Ultimate ZERO Standard Pack" for small and medium-sized enterprises in the fiscal year ending February 2025, and "Vario Ultimate ZERO Enterprise Pack" with even more enhanced functions for medium and large-sized enterprises in the fiscal year ending February 2026, and we will proceed with full-fledged entry into the "Zero-Trust Security Field."

Based on the stability that has characterized our company to date, we will continue to take on new challenges and meet the expectations of our shareholders and investors, and we hope that you will continue to support us in the future.

## 6. Conclusions

The growth of the top line is slow, but they are developing products for entering the “zero-trust security field” steadily. In addition, “AI SoC,” a project for rationalizing the operation and management of network security by utilizing the AI technology of HEROZ, is progressing as planned.
For this fiscal year, profit is projected to decline due to the augmentation of costs through investments, but they said that they have been offsetting the augmentation of VSR procurement costs due to the global inflation and the yen depreciation so far.
We would like to keep an eye on the progress of sale of “Vario Ultimate ZERO－Start Pack” and “Vario Ultimate ZERO－Standard Pack,” which are scheduled to be released this fiscal year.

# <Reference: Regarding Corporate Governance>

**◎ Organization type and the composition of directors and auditors**

| | |
|---|---|
| Organization type | Company with Audit Committee |
| Directors | 10 directors, including 4 outside ones (4 independent executives) |

**◎ Corporate Governance Report**

Last update date: September 5, 2023

<Basic Policy>

Our company's mission is "to ensure that all enterprises using the Internet can easily and securely carry out their business, we will offer the very best services to Japan and to the world," and have conducted our business to meet the expectations of our various stakeholders. Business management based on corporate governance, which forms the core of our business, is the most important administrative category and through a highly transparent, optimized management with a strengthened monitoring system, we are aggressively taking initiatives to improve our corporate value.

<Reasons for Non-compliance with the Principles of the Corporate Governance Code (Excerpts)>

| Principle | Disclosed Content |
|---|---|
| <Supplementary Principle 2-4 ① Ensuring Diversity of Human Resources> | The company believes that it is important for each and every employee to embody the company's mission to enhance corporate value, and is working to ensure diversity by actively appointing excellent human resources without regard to gender, nationality, disability, or other factors. We will continue to consider the medium- to long-term human resource development policy and internal environment improvement policy. |
| <Supplementary Principle 3-1 ③ Sustainability Initiatives, etc.> | We provide comprehensive network security services so that all companies engaged in business can use the Internet safely and comfortably, and we believe that by promoting our business, we are responding to the resolution of issues concerning the sustainability of society. We are considering disclosing our investment in human capital and intellectual property in the future. |
| <Supplementary Principle 5-2 Formulate and Publish Management Strategies and Plans > | The Company has developed a management strategy and earnings plan, which is shared among the directors. We do not disclose our profitability and capital efficiency so that we can change our strategy flexibly as we are still a small company. In the future, when the company reaches a certain level of scale, we will consider the information for disclosure. |

<Reasons for Non-compliance with the Principles of the Corporate Governance Code (Excerpts)>

| Principle | Disclosed Content |
|---|---|
| <Principle 1-4. Strategically Held Shares> | The company does not possess any strategically held shares. Further, the company will not hold any such shares, unless the alliance with invested companies would contribute to the improvement of the medium or long-term corporate value and is considered to contribute to the benefits of shareholders based on objective discussions, such as the comparison between the benefits and risk of ownership and the company's capital cost. |
| <Principle 3-1. Information Disclosure Enhancement> | In addition to the timely and appropriate legal disclosure of information, the company also publishes the following policies: |

| | |
|---|---|
| | (i) Management Philosophy, Strategy, and Plan<br>The company's corporate ethos is described on its website:<br>https://www.variosecure.net/company/mission/<br>(ii) Basic Policies and Way of Thinking Regarding Corporate Governance<br>Kindly refer to "I.1. Basic Way of Thinking" of this report for details on the company's basic policies and way of thinking regarding corporate governance.<br>(iii) The Board of Directors' Policies and Procedures for Determining the Compensation for Management Staff and Directors<br>The Board of Directors consults a discretionary compensation committee regarding the compensation system and policies for Directors, the calculation method for determining the exact compensation amount, and individual compensation amounts. The Board of Directors has decided that the Representative Director will make the final decision on the individual compensation amounts reported by the discretionary compensation committee, within the compensation amount limit approved in the Stockholders' General Meeting through a resolution.<br>(iv) Policies and Procedures for the Selection and Removal of a Management Staff Member by the Board of Directors and the Nomination of a Candidate for a Director<br>Regarding the selection and removal of a Director, the Board of Directors will hold a final resolution based on the comprehensive decision on each employee's character as a manager as well as their experience, results, and expertise as a manager.<br>(v) Explanation Regarding the Individual Nomination and Appointment During the Appointment or Removal of a Management Staff or the Nomination of a Candidate for the Board of Directors<br>The reasoning behind each individual nomination is recorded in the regular General Meeting of Stockholders held every term, or in an extraordinary General Meeting of Stockholders. |
| Supplementary Principle 4-1 (2) Disclosure of information on the medium-term management plan | Our company has announced our medium-term management plan and is striving to achieve it. Regarding the progress of the medium-term management plan, our company's policy entails working toward achieving the plan while making revisions to it as needed, taking into account environmental and strategy changes. |
| <Principle 5-1. Policies Regarding Constructive Dialogue with Stockholders> | The company uses its IR Department as a medium to promote dialogue with stockholders every day instead of only during Stockholders' General Meetings and offers information through its website and through phone calls. Further, the company has a system where the opinions of investors and stockholders obtained through these dialogues are reported to the Management Staff every time. |