



Satoshi Yamamori
CEO

Vario Secure Inc. (4494)

Vario
Secure

Company Information

Exchange	TSE Standard
Industry	Information and Communications
CEO	Satoshi Yamamori
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

Share Price	Number of shares issued (Term-end)	Total market cap	ROE (Act.)	Trading Unit	
¥584	4,522,961 shares	¥2,641 million	6.4%	100 shares	
DPS (Est.)	Dividend yield (Est.)	EPS (Est.)	PER (Est.)	BPS (Act.)	PBR (Act.)
¥0.00	-	¥74.47	7.8x	¥1,227.87	0.5x

*The share price is the closing price on October 17. The number of shares issued, DPS, and EPS were taken from the brief report on financial results in the second quarter of the fiscal year ending February 2025. ROE and BPS are the results in the previous fiscal year.

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 the second quarter of the Fiscal Year Ending February 2025, etc.

Table of Contents

[Key Points](#)

[1. Company Overview](#)

[2. Medium/long-term growth strategy](#)

[3. The Second Quarter of the Fiscal Year Ending February 2025 Earnings Results](#)

[4. Fiscal Year Ending February 2025 Earnings Forecasts](#)

[5. The Comments by CEO Yamamori](#)

[6. Conclusions](#)

[<Reference: Regarding Corporate Governance>](#)

Key Points

- In the second quarter of the fiscal year ending February 2025, sales revenue rose 3.7% year on year to 1,354 million yen. The Managed Security Services, which is the mainstay, performed well, and the Integration Services business, too, showed healthy performance in the development of networks. Operating income declined 6.0% year on year to 273 million yen. Gross profit declined, as sales grew, but the Integration Services business, which has a low gross profit margin, grew and they invested in development and human capital. SG&A expenses, too, decreased, but profit dropped.
- The earnings forecast was left unchanged. 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 “24/7 operation and management, and strengthening of the nationwide system for dispatching engineers,” “entering the growing security market,” and “establishment of a new sales system focused on customer needs” 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.
- We interviewed President Satoshi Yamamori about his missions, initiatives for growth, message toward shareholders and investors, etc. He said “Historically, in the world of security it has been difficult to create world-changing inventions and innovations. So, while advertising our strengths of 24-hour, 365-day operation system, we want to actively approach customers through new sales methods and produce good numerical results. We sincerely hope you look forward to our company's future.”
- President Yamamori has the experience of working as an engineer in the network security field and engaged in the business of monthly charging subscription services for a long period of time before joining Vario Secure, so he is expected to lead the company by utilizing his abundant knowledge and experience accumulated in his career. Vario Secure has explained and provided products and services using jargon, such as UTM, IDS, and ADS, to clients. However, clients just hope that “in-company LAN will be protected,” “in-company PCs will be protected,” and “their accounts will be safeguarded.” He hopes to change the current marketing method significantly and establish a marketing method that gives top priority to the provision of easy-to-understand services.

- **There is no revision to the target figures in the medium-term management plan, but we would like to expect that new paths to them will be indicated and growth will become more feasible.**

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. They announced rankings for “individuals” and “organizations.”

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

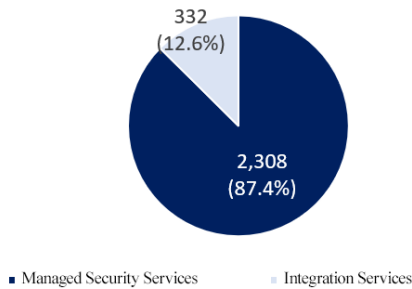
*Created by Investment Bridge based on the Ministry of Economy, Trade and Industry’s “Survey on Supply and Demand of IT Human Resource (Summary)” (April 2019).

[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).

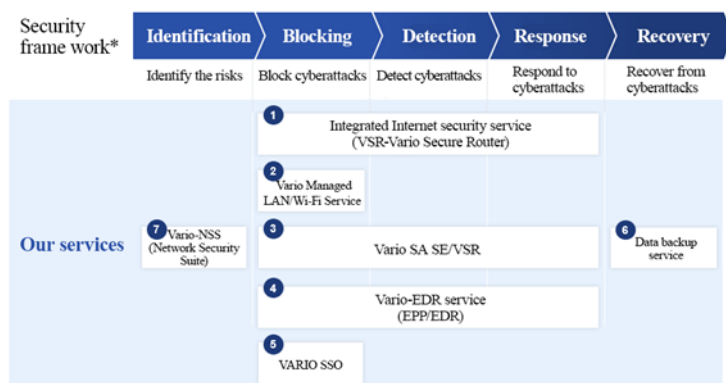
Service components (FY Feb. 2024 unit: million yen)



(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.



*Cyber Security Framework, CSF published by government agency (National Institute of Standards and Technology, NIST) in 2014

<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

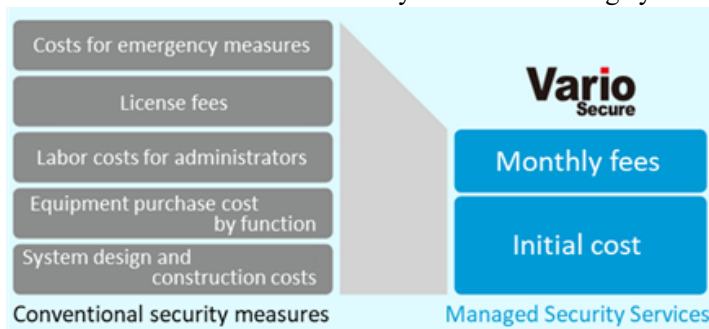
Previously, to introduce the security system such as above, it was necessary to install various security devices in-house and maintain them, making it more difficult for many companies to introduce sufficient network security measures because they required highly skilled engineers and high investments.

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 August 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 2024, 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 3,074 as of the end of August 2024, increased 69 from the previous fiscal year.

[1-5 Characteristics and Strengths]

(1) Unique business model

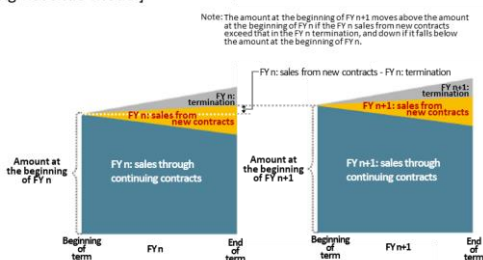
The company provides one-stop service for (1) procurement of equipment used in security services, (2) development of core software to be installed on equipment, (3) installation/setting of equipment, and (4) monitoring and operation after installation of equipment. There is no need for end-users to individually 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, a stable earnings model has been built, and it is possible to forecast revenues at a relatively early stage in the fiscal year.

[Recurring Revenue Model]



(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%

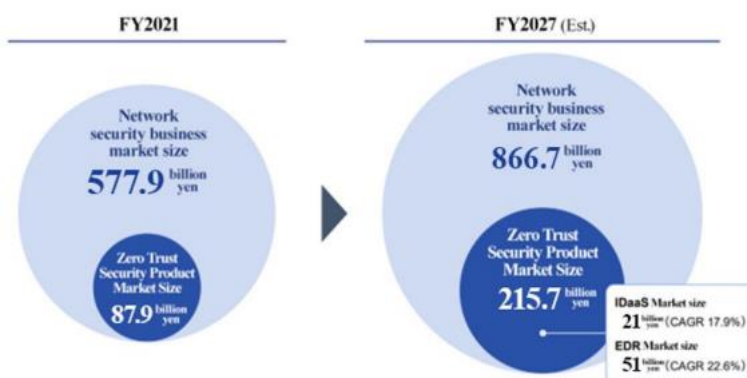
*Source: ITR “ITR Market View: Gateway Security-Based SOC Service Market 2023” Market of Firewall/UTM operation monitoring services (FY 2022), produced by Investment Bridge with reference to the material of the company.

* 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
<ul style="list-style-type: none"> ■ The conventional perimeter defense market is expected to grow at an annual rate of around 1.3% ■ There is a need for multi-layered zero-trust security measures that "do not allow intrusion" and "allow intrusion" ■ Demand for zero trust security is expected to grow further in the future 	<ul style="list-style-type: none"> ■ 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. ■ Our main service is a perimeter defense type for the purpose of "not allowing newcomers" ■ Malware detection and prevention (Vario Endpoint Security) and ransomware-resistant backup (Vario Data Protect) show double digit growth

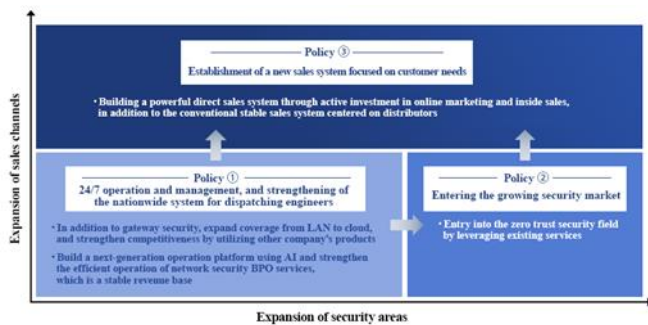
(Taken from the reference material of the company)

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)

“Expanding managed service areas and strengthening competitiveness,” “Entering the growing security market,” and “Establishment of a new sales system focused on customer needs”

*** Policy 1: 24/7 operation and management, and strengthening of the nationwide system for dispatching engineers**

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.

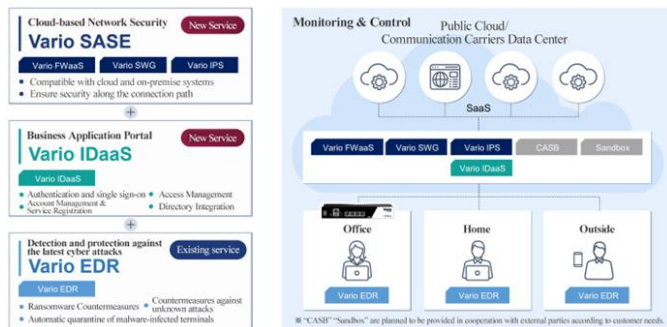
Moreover, the company will build a next-generation operation platform using AI through an alliance with HEROZ and strengthen the efficient operation of managed services, which is a stable revenue base.

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

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

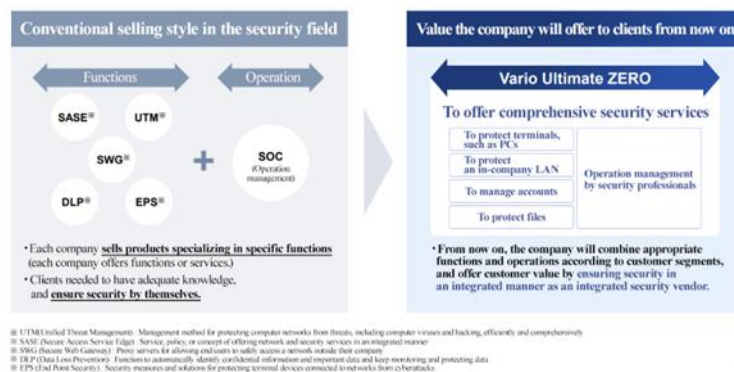
They offer security services suited for the scale of small and medium-sized enterprises, which are targeted by the company, for protecting the cloud and office environments, and started providing “Vario Ultimate ZERO” for ensuring security and saving labor for operation and management in August 2024.

Managed services for zero-trust security with minimal configuration = Vario Ultimate ZERO



(Taken from the reference material of the company)

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 Data security” based on “Vario Ultimate ZERO” as a security BPO vendor, which ensures security in an integrated manner.



(Taken from the reference material of the company)

*** Policy 3: Establishment of a new sales system focused on customer needs**

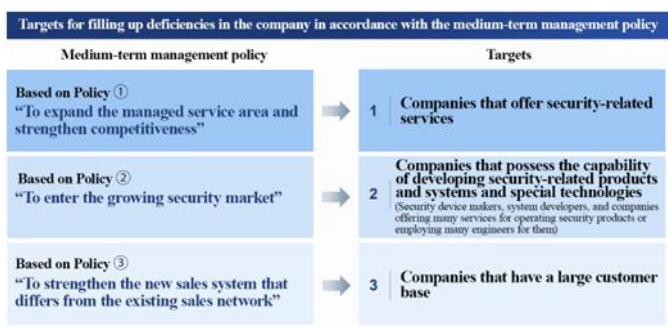
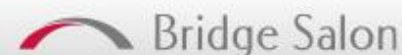
In addition to the conventional stable sales system centered on distributors, the company will build a solid direct sales system by actively investing in online marketing and inside sales. As the list of potential clients has been enriched to some degree, they will take measures for attracting new clients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

(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.

As part of business investment, they will concentrate on M&A. They will target mainly “security-related IT companies,” while narrowing down targets and setting priorities, with the aim of cooperating with companies with which synergy can be expected.

BRIDGE REPORT



FY2/2024 - FY2/2026

Personnel expenses New service planning and sales department reinforcement	258 million yen
Development costs / SOC operational enhancement costs Software development, etc.	155 million yen
Marketing costs Increased awareness, lead acquisition	100 million yen
M&A Maintenance, operation, vulnerability assessment, etc.	400 million yen
Total amount	913 million yen

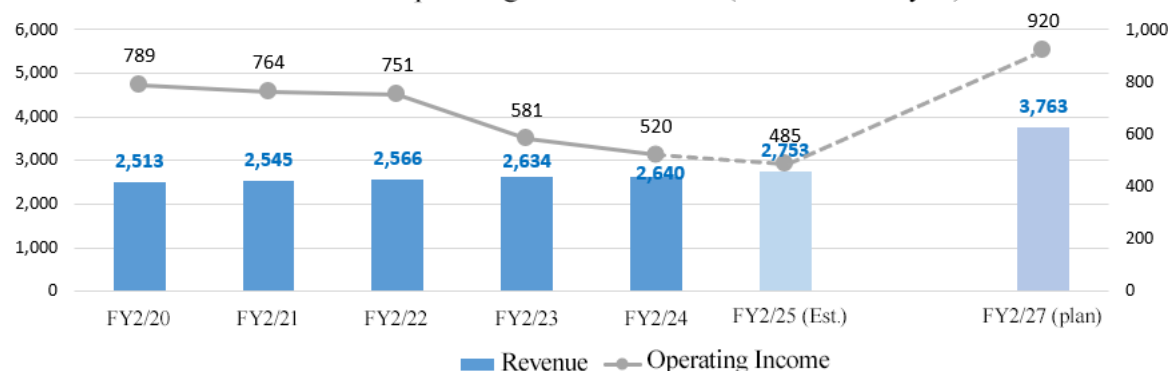
(Taken from the reference material of the company)

(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.

Revenue and Operating Income Trends (Unit: million yen)



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. The Second Quarter of the Fiscal Year Ending February 2025 Earnings Results

(1) Overview of business results

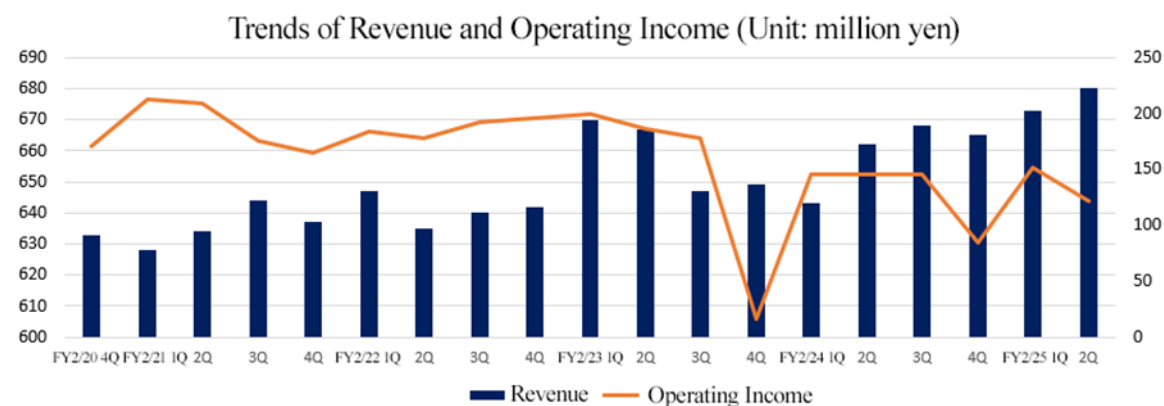
	FY 2/24 2Q	Ratio to sales	FY 2/25 2Q	Ratio to sales	YoY
Revenue	1,306	100.0%	1,354	100.0%	+3.7%
Gross profit	773	59.2%	714	52.7%	-7.6%
SG&A and others	482	36.9%	442	32.6%	-8.3%
Operating profit	290	22.3%	273	20.2%	-6.0%
Profit before tax	285	21.8%	265	19.6%	-6.9%
Quarterly profit	190	14.6%	182	13.5%	-4.1%

*Unit: million yen

Revenue increased and profit decreased

Sales revenue rose 3.7% year on year to 1,354 million yen. The Managed Security Services, which is the mainstay, performed well, and the Integration Services business, too, showed healthy performance in the development of networks.

Operating income declined 6.0% year on year to 273 million yen. Gross profit declined, as sales grew, but the Integration Services business, which has a low gross profit margin, grew and they invested in development and human capital. SG&A expenses, too, decreased, but profit dropped.

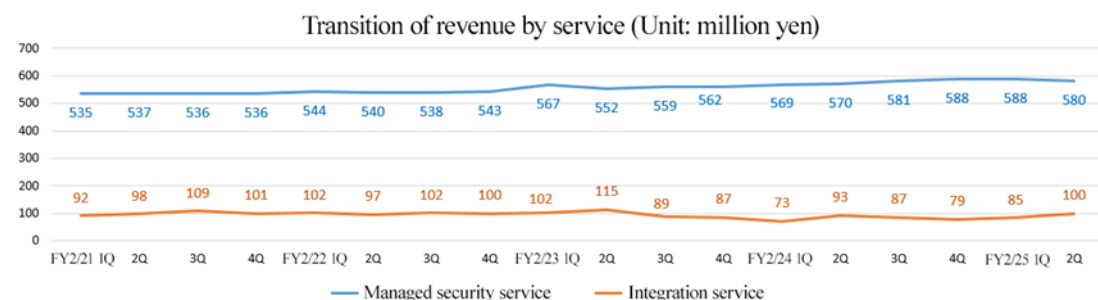


(Produced by Investment Bridge with reference to the material of the company)

(2) Service trends

	FY 2/24 2Q	FY 2/25 2Q	YoY
Revenue			
Managed Security Service	1,139	1,168	+2.6%
Integration Service	166	185	+11.4%

*Unit: million yen



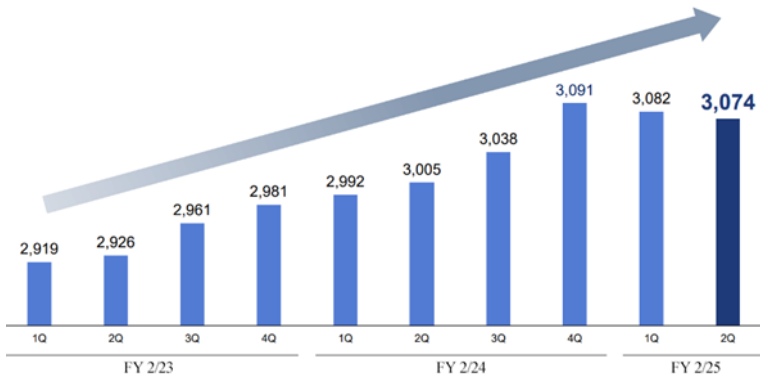
(Produced by Investment Bridge with reference to the material of the company)

BRIDGE REPORT



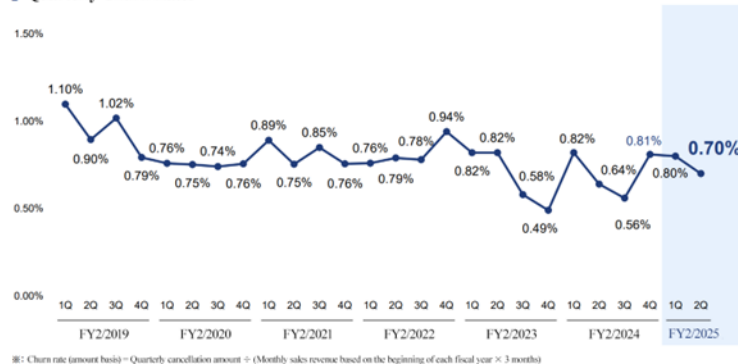
① Managed security service

Sales grew through enhanced cross-selling with the enriched service lineup, including Vario-EDR and Vario Managed LAN/Wi-Fi. The number of end-user companies as of the end of August 2024 was 3,074. It decreased quarter on quarter for the second consecutive quarter, but the number of user companies varies according to whether agencies concentrate on increasing new subscribers to lines or up-selling. In the long term, it has been increasing steadily, and churn rate has been as low as 1% or lower, so they consider that a stable revenue base has been established.



(Taken from the reference material of the company)

Quarterly Churn Rates



※: Churn rate (amount basis) = Quarterly cancellation amount ÷ (Monthly sales revenue based on the beginning of each fiscal year × 3 months)

(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 33.9% 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 second quarter of the fiscal year ending February 2025, they released “Vario Ultimate ZERO” based on a zero trust architecture, which secures security and saves labor for operation and maintenance.

BRIDGE REPORT



1Q (Progressing as planned)	2Q (Progressing as planned)	3Q (Progressing as planned)	4Q (Some to be put off until the next fiscal year)
<p>Vario Managed LAN/Wi-Fi Already on sale March 6, 2023</p> <p>Enhanced terminal visibility through implementation of Vario-NSS employee master function Deployment of Zero Trust Platform</p>	<p>Enhanced Vulnerability Management and Diagnostic Services for Servers</p> <p>Started vulnerability management and diagnostic services for customer websites, public servers, and corporate servers.</p>	<p>Solution to disconnect unauthorized terminals inside a company</p> <p>Some selected functions of Vario-NSS are installed in compact dedicated terminals as an option of the vulnerability diagnosis service. Unauthorized terminals for an in-company LAN are visualized.</p> <p>Discussions on the addition of new server vulnerability diagnosis services to the lineup</p> <p>The company is discussing simplified services of diagnosing the vulnerability of servers with SaaS for small and medium-sized enterprises and QA, as leading security vendors have not released such services. The company will keep thinking of producing English reports on issues.</p>	<p>For the start of the IDaaS business</p> <p>Completion of development as the first model of a zero-trust security platform through the enhancement of functions (including single sign-on) based on Vario-NSS. The company is preparing for releasing IDaaS as part of the zero-trust security package in first quarter of fiscal year ending February 2025.</p> <p>Addition of an option of vulnerability diagnosis</p> <p>To release a web load testing service, which is in high demand, as an additional option of vulnerability diagnosis</p>

(Taken from the reference material of the company)

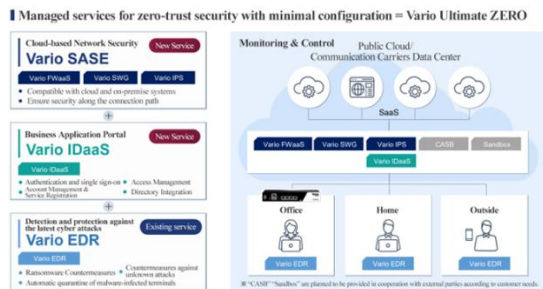
② Integration Services

The sales revenue of the network Integration Services for procuring and configuring devices increased considerably by 48.9% year on year.

(3) Business topics

In August 2024, they released “Vario Ultimate ZERO” based on a zero trust architecture, which secures security and saves labor for operation and maintenance.

They offer security services suited for small and medium-sized enterprises with the minimum configuration for various environments, including cloud and offices, based on “Vario Ultimate ZERO,” which is composed of “Vario EDR,” which is an existing service for detecting and blocking the latest cyber attacks, “Vario SASE,” a new service for cloud-based network security, and “Vario IDaaS,” which is a portal for applications for business operations.



(Taken from the reference material of the company)

Based on the medium-term management policy, they are strengthening marketing measures. They aim to expand demand through direct sale.

In May 2024, they started monthly webinars for specific industries and corporate scales. In addition, they started regularly distributing column-like e-mail newsletters regarding security, added white paper focused on the cases of utilization of their services, exhibited their products and services at the artificial intelligence (AI) expo (HEROZ booth), implemented measures for attracting prospective customers in the manufacturing and construction fields, and started accepting online applications for charge-free trial of EDR/EPP.

BRIDGE REPORT



(4) Financial position and cash flows

◎ Main Balance Sheet

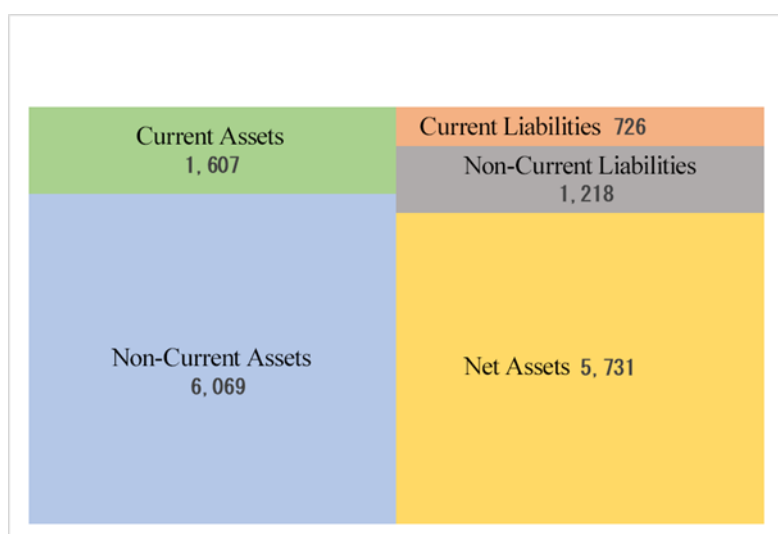
	End of February 2024	End of August 2024	Increase/ decrease		End of February 2024	End of August 2024	Increase/ decrease
Current Assets	1,608	1,607	-1	Current Liabilities	776	726	-49
Cash and Cash Equivalents	822	794	-27	ST Interest Bearing Liabilities	200	200	0
Trade and Other Receivables	458	482	+24	Trade and Other Payables	106	117	10
Non-current Assets	6,041	6,069	+28	Non-current Liabilities	1,325	1,218	-106
Tangible Assets	227	300	+72	LT Interest Bearing Liabilities	1,100	1,000	-100
Goodwill	5,054	5,054	0	Total Liabilities	2,101	1,945	-156
Intangible Assets	343	343	0	Net Assets	5,548	5,731	+183
Total Assets	7,649	7,676	+26	Retained Earnings	2,745	2,928	+182
				Total Liabilities and Net Assets	7,649	7,676	+26
				Total Borrowings	1,300	1,200	-100

*Unit: million yen.

Total debts decreased 100 million yen from the end of the previous fiscal year. Net D/E ratio dropped 1.5 points from the end of the previous fiscal year to 7.1%.

Capital-to-asset ratio rose 2.2 points from the end of the previous fiscal year to 74.7%.

Repayment of interest-bearing liabilities and financial soundness improvement are progressing as planned.



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

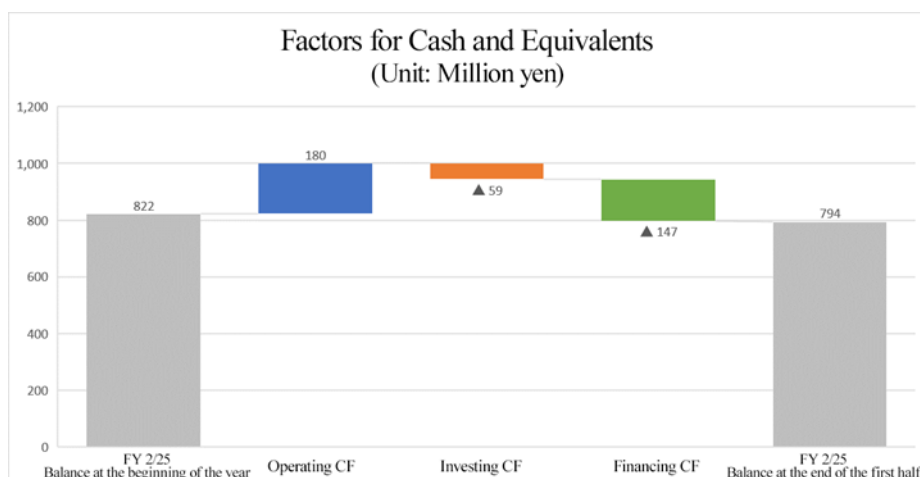
BRIDGE REPORT



◎ Cash Flows

	FY 2/24 1H	FY 2/25 1H	Increase/decrease
Operating Cash Flow	176	180	+3
Investing Cash Flow	-90	-59	+30
Free Cash Flow	85	120	+34
Financing Cash Flow	-331	-147	+183
Balance of Cash and Equivalents	793	794	+0

*Unit: million yen



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

In the first half of the fiscal year ending February 2025, the cash inflow from operating activities and the surplus of free cash flow increased year on year. The cash position is unchanged.

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	Progress rate
Revenue	2,640	100.0%	2,753	100.0%	+4.3%	49.2%
Operating profit	520	19.7%	485	17.6%	-6.9%	56.4%
Profit before tax	509	19.3%	474	17.2%	-6.7%	56.0%
Profit	347	13.2%	336	12.2%	-3.2%	54.4%

*Unit: million yen

No revision to the earnings forecast. Increase in revenue and decrease in profit estimated.

The earnings forecast was left unchanged. 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 for med-term growth 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.

Until the fiscal year ending February 2027, they 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.

(2) Service trends

Revenue	FY 2/24	FY 2/25 Est.	YoY	Progress rate
Managed Security Service	2,308	2,452	+6.3%	47.6%
Integration Service	332	300	-9.5%	61.7%

*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 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. Interview with President Yamamori

We asked President Satoshi Yamamori about his mission, initiatives for growth and message to shareholders and investors.

After gaining experience as a network engineer at several IT companies, as well as building a career in management, President Yamamori was invited to join the company in 2018 as Director and Head of the Technology Department, and in September 2024 he was appointed as President and Head of the Technology Department.

In addition to his experience in the network security field as an engineer, he had been involved in the monthly subscription-based service business for a long time before joining the company, and is expected to lead the company with his wealth of knowledge and experience in both areas.

Q: What do you consider to be your mission as President?

Prior to being appointed as President, I established Strategic Management Office earlier this year and held the position of Chief Strategy Officer as head of the office, and from that position I have believed that our business approach needs to be changed.

Our security business has become an abstruse business for the small and medium-sized enterprises (SMEs) who are major clients.

Customers are very clear of what they want: "Protect our internal LAN," "Protect our company's PCs," and "Protect our accounts."

In contrast, we have used difficult terms such as UTM, IDS, and ADS to explain and provide our products and services to our customers. I aim to make a significant change to this current situation and establish a sales approach that prioritises the provision of easy-to-understand services to customers.

We have advertised that we developed various products, including VSR, in house, but our real strength and competitive advantage is our "24-hour, 365-day operation system." Through a collaborative structure with business partners across Japan, we can rush to anywhere in Japan within four hours and take over the complete operation of the customer's security system on their behalf.

Although the products and services we offer will not suddenly change, but we aim to change our sales approach to highlight these strengths and promote sales to customers we have not been able to reach, who are unaware of their security situation. with a clear approach: "We protect your PCs, we protect your internal LAN, and we protect your accounts."

Q: As an investor, how should I view the medium-term management plan?

Although the targets of the medium-term growth strategy itself remain unchanged, I believe that, in addition to organic growth, the changes in sales methods that I have just mentioned will create changes in the path to achieving the targets, and we will make such appeals clear at the time of announcement of the full-year financial results next year.

For M&A, our main targets are "security-related IT companies," with the aim of narrowing down and prioritising targets and working with companies with which we can expect synergy.

I had experienced several M&A deals before joining the company, and I believe I can facilitate PMI (Post merger integration or the

integration process after a merger or acquisition) smoothly.

Q: Lastly, what is your message to shareholders and investors?

Since assuming the position of President, I have had more opportunities to speak to people involved in the stock market, and I have been told that the management is solid and profit margin is at a high level. And despite the company's extremely high potential, including its 24-hour, 365-day operation system, its low valuation on the stock market may still be due to a lack of investor relations.

I would like to promise that we will take such external feedback seriously and make it a mission of mine and the rest of the management team to promote our business model and advantages more firmly.

Historically, in the world of security it has been difficult to create world-changing inventions and innovations. So, while advertising our strengths of 24-hour, 365-day operation system, we want to actively approach customers through new sales methods and produce good numerical results. We sincerely hope you look forward to our company's future.

6. Conclusions

President Yamamori has the experience of working as an engineer in the network security field and engaged in the business of monthly charging subscription services for a long period of time before joining Vario Secure, so he is expected to lead the company by utilizing his abundant knowledge and experience accumulated in his career. Vario Secure has explained and provided products and services using jargon, such as UTM, IDS, and ADS, to clients. However, clients just hope that "in-company LAN will be protected," "in-company PCs will be protected," and "their accounts will be safeguarded." He hopes to change the current marketing method significantly and establish a marketing method that gives top priority to the provision of easy-to-understand services.

There is no revision to the target figures in the medium-term management plan, but we would like to expect that new paths to them will be indicated and growth will become more feasible.

<Reference: Regarding Corporate Governance>

◎ Organization type and the composition of directors and auditors

Organization type	Company with Audit Committee
Directors	8 directors, including 3 outside ones (3 independent executives)

◎ Corporate Governance Report

Last update date: October 10, 2024

<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.

<Disclosure Based on 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

	<p>The company’s corporate ethos is described on its website: https://www.variosecure.net/company/mission/</p> <p>(ii) Basic Policies and Way of Thinking Regarding Corporate Governance 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.</p> <p>(iii) The Board of Directors’ Policies and Procedures for Determining the Compensation for Management Staff and Directors 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.</p> <p>(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 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.</p> <p>(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 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.</p>
<p>Supplementary Principle 4-1 (2) Disclosure of information on the medium-term management plan</p>	<p>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.</p>
<p><Principle 5-1. Policies Regarding Constructive Dialogue with Stockholders></p>	<p>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.</p>

BRIDGE REPORT



This report is not intended for soliciting or promoting investment activities or offering any advice on investment or the like, but for providing information only. The information included in this report was taken from sources considered reliable by our company. Our company will not guarantee the accuracy, integrity, or appropriateness of information or opinions in this report. Our company will not assume any responsibility for expenses, damages or the like arising out of the use of this report or information obtained from this report. All kinds of rights related to this report belong to Investment Bridge Co., Ltd. The contents, etc. of this report may be revised without notice. Please make an investment decision on your own judgment.

Copyright(C) Investment Bridge Co., Ltd. All Rights Reserved.