# EQST insight

## A new paradigm in cloud security, CNAPP(Cloud Native Application Protection Platform)

You Jong-hoon, head of the cloud business group

### ■ Outline

The headline of last August described the background and necessity of the emergence of ASM (Attack Surface Management), which secures visibility for security in the On-Prem and Cloud environment and continuously manages the vulnerability of assets connected to the Internet.

In this headline, we would like to introduce CNAPP (Cloud Native Application Protection Platform), which is newly emerging amid the rapid transition of the existing IT environment to the cloud along with continuously increasing security threats.

The 'Establishment and building of consolidated security management in the multi-cloud environment', a project that SK Shieldus recently contracted for a customer in the financial sector, we were able to confirm, once again, the rapidly changing IT environment of customers and their security requirements that reflect it. The main requirements of customers used to be deployment of relatively light applications in the cloud first, and whether it is possible to implement the security measures that were effective in the on-prem. environment in the cloud.

From the viewpoint of solutions, WAF (Web Application Firewall) for web application protection, access control for databases and major servers (including management of account privileges), and agent-type security solutions for workload account for a large proportion. An important factor in evaluating a service vendor was whether it could provide a control service for management/operation of such solutions.

This evaluation method can be viewed as a rather traditional (legacy) solution and service in the Cloud era. However, it is a formidable task to verify, build, and operate the above solution in the various cloud environments used by customers. In fact, some customers are spending money on a complete review or establishment of a new architecture in terms of management, e.g., organization and policy as well as technical system from the viewpoint of cloud governance.

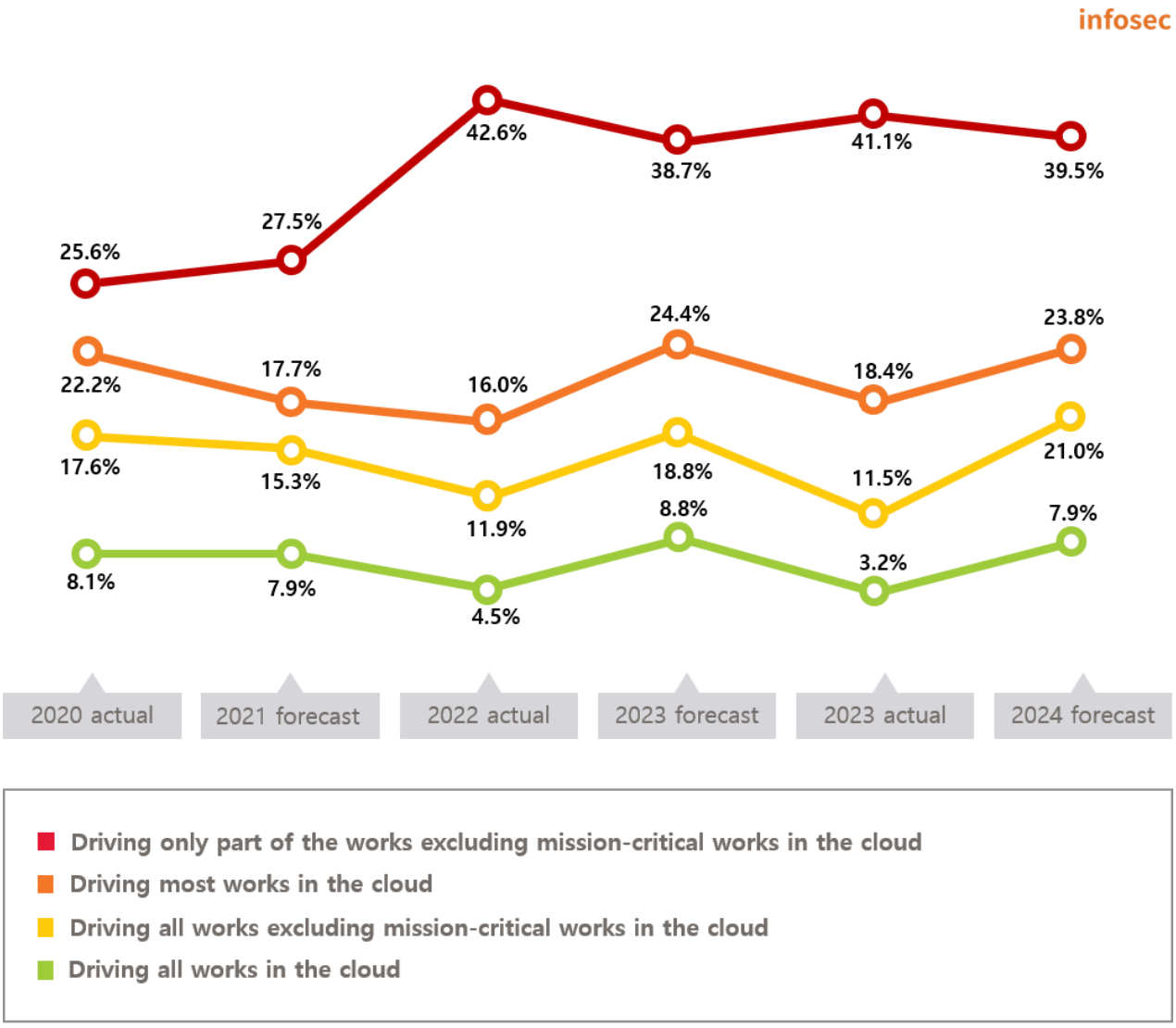
The following are the security functions required when major business systems are deployed in the cloud, and the requirements, apart from the existing perspectives, which I felt while in charge of this customer in the financial sector.

First, as the cases of utilizing various cloud infrastructures provided by CSP (Cloud Service Provider) according to business characteristics increase, the complexity of security is greatly increasing, and first of all, securing the 'visibility' of the infrastructure is becoming more important. In addition, S/W supply chain security and compliance are emerging as important tasks for companies.

Second, while both workloads and environments are deployed in various ways, e.g., VM, Container (Kubernetes), and Serverless, the CWPP (Cloud Workload Protection Platform) solution mentioned in the market does not support all of the above environments.

Third, customers preparations and human capabilities to operate new security measures and solutions in the 'multi cloud environments' are insufficient, and the demand for 'security operation' to support them is newly emerging as well.

For this reason, when so-called mission-critical tasks are switched to cloud over the next few years, new security measures suitable for the true cloud environment have become necessary.




[[Figure 1] Current status of cloud computing utilization and forecast

* Source: Domestic cloud computing status and forecast for 2023 (April 2023, IT World/CIO) Report image reprocessing

## ■ Concept of CNAPP

Recently, solutions like Cloud Server Workload, CWPP (Cloud Workload Protection Platform), which is in charge of container security, CSPM (Cloud Security Posture Management), which can monitor compliance and configuration for overall infrastructure and individual resources, and CIEM (Cloud Infrastructure Entitlement Management), which manages various identities and privileges used in the cloud, CSNS (Cloud Service Network Security), and DSPM (Data Security Posture Management) are introduced one after another, and furthermore, CNAPP (Cloud Native Application Protection Platform), which consolidates all of them, is emerging.

First, let's look at the concept of CNAPP. According to Gartner, CNAPP is a "simplified security architecture that allows enterprises to fully leverage the benefits of the cloud native ecosystem." To expand a little further, it is 'consolidation of the tools that can continuously manage security and compliance from development to operations with regard to cloud native applications.'

## ■ Importance of introducing CNAPP

Before explaining the main components and functions of CNAPP, it is necessary to first think about the reason for the emphasis on consolidation, which has been repeatedly talked about.

First, it is consolidation from the technical viewpoint (functions). To manage a much more complex cloud infrastructure much more complex than existing On-Prem., companies need to efficiently respond to various security issues through an consolidated security tool and maintain an organic security system. For example, if security problems identified through CWPP are linked with CSPM, they can be resolved more quickly.

Second, it is consolidation of work processes. Looking at the reality where DevSecOps is applied beyond DevOps, various security policies and tools have been developed, and they are used to maintain consistent security in the application development, test, distribution, and operation processes. This is a very useful method not only in terms of cost, but also in quickly developing a business. Through this, it is possible to secure security level management and visibility across the business.

Finally, from a business perspective, the need for consolidation becomes clearer. Many companies purchase, build, operate and maintain about 40 to 70 solutions for security. Of course, there are customers who use some consolidated solutions, but the reality is that there are different vendors for different areas in most cases. This structure causes the complexity of security tasks, leading to a decrease in efficiency, and slowing down the response to increasing security threats.

It was confirmed at RSA Conference 2022 that in North America, this kind of consolidation movement was appearing in 'purchasing', and vendor consolidation is taking place through active M&A. (e.g., Microsoft, Palo Alto Networks, Orca Security, Aqua Security, Wiz, etc. …)

Other good examples of 'consolidation' include 'EDR (Endpoint Detection & Response), MDR (Managed Detection & Response), and XDR (eXtended Detection & Response)' that many vendors have recently emphasized. These solutions not only organically consolidate sensors (technologies) that detect the latest security threats, but also consolidate processes, i.e. 'threat detection → response → recurrence prevention and proactive response,' from the viewpoint of a platform.

## ■ Key functions of CNAPP

Looking closely at the main functions of CNAPP, CNAPP, like XDR, like XDR, it is approaching consolidation based on platforms rather than individual point solutions with the aim of providing complete end-to-end security in the 'Cloud Native' environment.

The functions provided through CNAPP are as follows:

### CWPP (Cloud Workload Protection Platform)

- It provides security functions such as malware inspection, threat detection, intrusion prevention, application control, vulnerability diagnosis and management to various Workloads, VMs, Containers (Kubernetes), and Serverless on the Cloud infrastructure to help you run applications safely and quickly.

### CSPM (Cloud Security Posture Management)

- It records, detects, manages, and reports problems of cloud service configuration, security settings, compliance, and governance to provide monitoring, asset identification and classification, and resource configuration management functions for the entire cloud infrastructure.

### CSNS (Cloud Service Network Security)

- It is a comprehensive set of tools for IPs, data, applications and services. It protects the cloud infrastructure based on individual user network security policies and industry standards.

### CIEM (Cloud Infrastructure Entitlement Management)

- It provides identity and access governance control functions designed to reduce excessive cloud infrastructure privileges and enforce least privilege access.

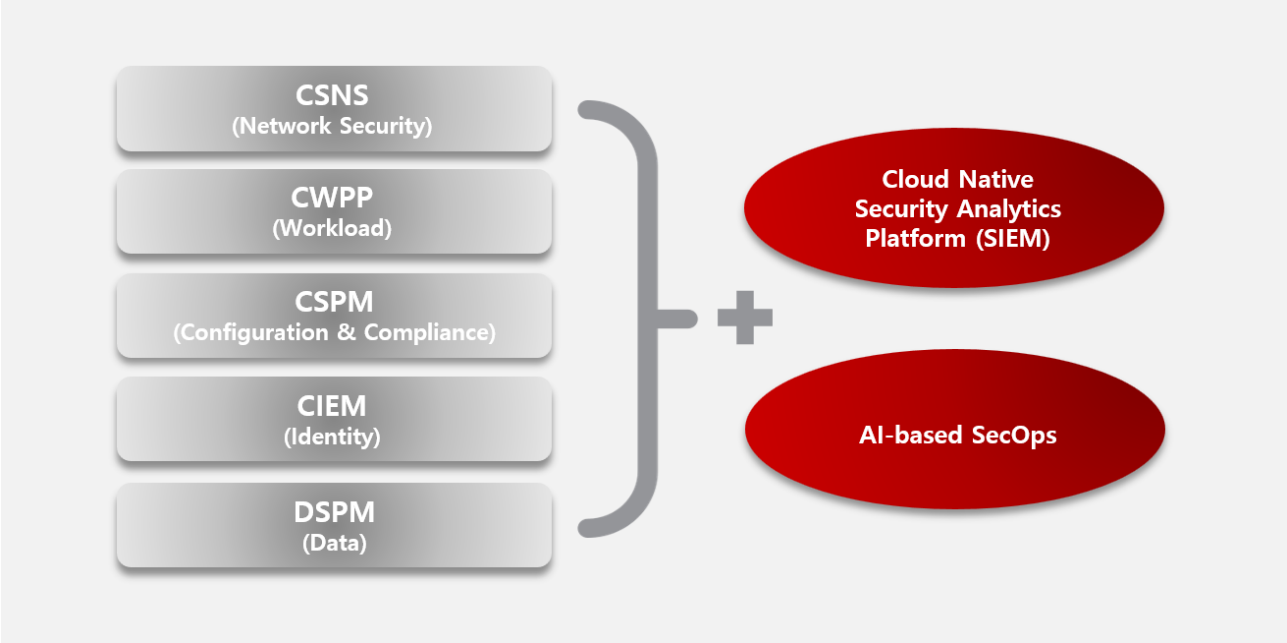
### DSPM (Data Security Posture Management)

- It provides functions that can discover/monitor sensitive data more effectively by automating key data detection and protection tasks within the cloud infrastructure. In addition, it corrects risks including improper privileges and incorrect qualifications for data access in a timely manner and prevents data loss.

If the above three functions are combined and consolidated into a single platform, companies can detect threats more quickly, ensure compliance according to consistent policies, and expect highly efficient security operations. This approach is a general trend for global security companies that provide cloud security.

The latest security operation techniques mentioned above are consolidated and schematized as follows:

infosec




## ■ Closing

Frameworks like this are quite common among global security companies and CNAPP vendors, but it is still too early to apply them to domestic customers and cloud environments. SK Shieldus ranks No. 1 in security service in the On-Premise and Cloud environment, has experience in carrying out projects in various industries, and maintains strong business competitiveness. In the future, we will continue to track the changing trends in cloud security, closely analyze the market and customers' needs, and work harder to become a more advanced security service specialist through close cooperation with vendors.