WHITE PAPER

# COMPREHENDING DRIVERS TO ADOPT CENTRALIZED CLOUD SECURITY PLATFORMS


## Abstract

Today's enterprises are going through digital transformation for improving operational efficiency and cost optimization. One of the main levers for digital transformation is to adopt public cloud and cloud delivered services. As part of this transformation, enterprises are exposed to higher level of cyber risks due to increased digital attack surface and heightened cyber threat landscape. Organizations are looking at cloud delivered platform-based security solutions to mitigate the cyber risks and to optimize the cost of cybersecurity.
This whitepaper explores the drivers for this adoption.


Infosys®
Navigate your next

## Introduction

Enterprises today are remodeling traditional business models by adopting new technologies to improve operational efficiency, enhance customer experience, improve product quality, and optimize cost. While digital transformation helps to improve operational efficiency and innovation it also increases the cyber exposure of an organization. Unless cybersecurity is embedded right from the initial stages of digital transformation, the security posture of an organization will be impacted. Rapidly evolving threat landscape and lack of cybersecurity expertise make it difficult for enterprises to address the cybersecurity challenges.

## Technology trends

Some technology trends adopted by enterprises for digital transformation are listed below:

### Cloud adoption

Organizations are adopting public cloud and cloud delivered services as a means for rapid innovation and operational efficiency. Cloud computing has gained popularity across all industry verticals, including financial services. It also helps organizations to move to an API based integration model, which helps in data sharing and improving customer experience.

### Artificial Intelligence & Machine Learning

AI & ML based solutions help in analyzing various type of data sources to get accurate analytics in areas such as risk management, pattern detection, fraud detection as well as for automation and customer service (chatbots).

### Internet of Things

Widespread adoption of IOT started with manufacturing and automotive industry and later spread to other industries like retail and logistics. Now intelligent devices are prevalent in all segments with sensors and cameras.

### 5G & Edge computing

5G mobile networks will increase the bandwidth by an order of magnitude from 4G and reduce network latency. It will enable intelligent devices to connect with edge networks which will bring compute capabilities and decision making closer to the end user. Together these technologies will help in collecting and processing massive volumes of real-time data to optimize various operations resulting in improved productivity and customer experience.

## Cybersecurity challenges faced by enterprises

Digital transformation using these technologies poses new cybersecurity challenges to enterprises. Key challenges faced by enterprises are listed below:

### Securing hybrid workforce

Post pandemic, hybrid workforce has become the new normal. Due to a rising demand in work from home arrangements, organizations observed that the traditional network security solutions have become ineffective and fragmented. Organizations are facing challenges to provide the same level of security to an employee working from home, on-the-move and in office.

### Securing hybrid workplace

As part of the digital transformation, organizations across the world have adopted SaaS services and public cloud. While this helped the IT teams to provide seamless services for a hybrid workforce, it introduced challenges of shadow IT and security loop holes due to disparate security solutions for the hybrid IT landscape (spread across on-prem and cloud).

### Poly-cloud security

As more organizations adopt cloud-based services across multiple public cloud providers, CxOs are facing challenges in securing cloud infrastructure as most of the traditional solutions are not capable of extending on cloud. Challenges become worse on a multi-cloud environment as there is no single pane of glass view of the security posture due to lack of centralized reporting, visibility, and governance.

### Cost takeout due to economic situation

The present economic environment has forced organizations to look at cost takeout measures in all areas of the enterprise including cybersecurity. Traditional network security models are mostly CAPEX based which require upfront investment, rack-space, electricity, and other resources. Hence traditional security models are expensive to implement and maintain.

### Multiple point products & interoperability

Traditional point solutions which were designed to address specific problems often run-on proprietary protocols and platforms. These point products do not integrate and interoperate with each other unless there is a strategic partnership between product vendors. The life cycle management of these tools makes the life of a CISO difficult due to the time spent on vendor management and negotiations with multiple stakeholders. Security teams have challenge in ensuring each product is up to date and having the latest threat information and security policies. As threat vectors and attacks are evolving rapidly, lack of an integrated suite of security solutions with the latest security policy severely impacts the security posture of the organization. As applications and services migrate to cloud these challenges are worsened as all these point solutions are duplicated for the cloud landscape as well.

## Centralized platforms delivered from cloud will solve those challenges

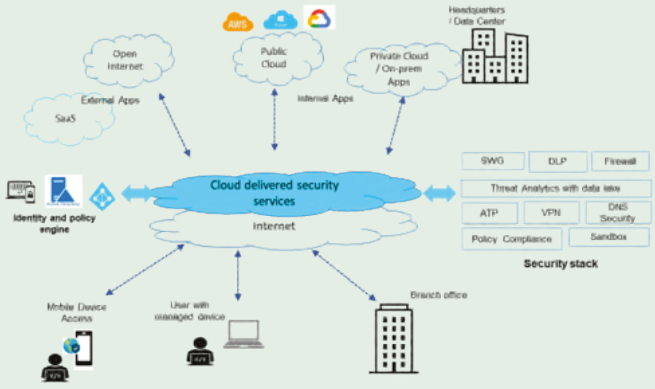
To address these challenges, enterprises are looking at two-pronged strategy of platform-based consolidation of security solutions and cloud delivered security solutions.

Individual point solutions are combined into a suite of solutions which are well integrated with a single management console constituting a "platform". This approach provides a more cost-effective approach to security that eliminates the need for multiple point solutions (optimized effort of upgrading, maintaining, and managing individual point solutions), resulting in reduced cost and improved operational efficiency.

Cloud delivered security solutions provide security-as-a-service from cloud on subscription-based model allowing organizations to opt for "pay per use", which allows flexibility to eliminate feature which is not relevant at this point of time and "pay as you grow", which allows organizations to have flexibility for capacity planning. It helps to convert the expense from a Capex to Opex model.

### SASE (Secure Access Services Edge)

SASE is a prime example of cloud-delivered security service. SASE provides a comprehensive approach to network security that combines various security functions such as firewall, secure web gateway, and Cloud Access Security Broker (CASB) into a unified platform. SASE is a cloud-based solution enabling organizations to provide secure access to corporate resources from anywhere in the world. It eliminates the challenges with respect to user experience (ex. VPN) and have uniform security policies enforced irrespective of remote or onsite worker. This reduces complexity and improves the security posture.




### Cloud Native Application Protection Platform (CNAPP)

CNAPP is the term coined by Gartner to denote the combination of multiple point solutions required to address complex security challenges faced by an organization's cloud-based operations. Cloud security Posture Management (CSPM) provides complete visibility in a multi cloud environment to help identify and highlight vulnerabilities caused due to misconfigurations and regulatory compliance. Cloud Workload Protection (CWP) provides real time protection for workloads and sensitive data on cloud environment from threats. Cloud Infrastructure Entitlement Management (CIEM) helps to mitigate the risks arising from excessive permissions and manage cloud identities, entitlements, and enforce the principle of least-privileged access. Code security requires static and dynamic application security tools to be embedded into the dev-sec-ops pipeline and helps "shift-left" of cybersecurity in the code-build-deploy-run pipeline.

Platform based solutions (such as SASE, CNAPP and next-gen SOC) provide a stack of multiple solutions which are integrated and managed uniformly. These platforms offer a common set of interfaces, protocols and standards that enable different systems to connect and share valuable information which can be acted upon automatically. This also enables enterprises to have visibility of all network and security relevant information about traffic flow, incidents etc. available on a single pane of glass.

Platform based solutions that are delivered from cloud as a service, enable enterprises to have a centralized policy management for cybersecurity. Centralized security policy management allows organizations to enforce consistent policies across entire IT infrastructure (on-prem vs cloud vs SaaS) and workforce (onsite vs remote). Centralized policy management ensures organizations can more easily standardize policies across all of their systems, applications and devices and enforce policies based on regional / business regulatory requirements to maintain organization's security policies in line with Zero Trust principles.

Cloud delivered security solutions have the added advantage of leveraging latest threat intelligence from across the industries to update security policies centrally. In a rapidly changing threat landscape, the ability to react to zero- day vulnerabilities within minutes is a critical requirement for maintaining a healthy security posture.

## Summary

Gartner has identified platform-based consolidation of cybersecurity solutions as a technology trend in 2023. Security leaders are increasingly focusing on operational inefficiencies and lack of integration of a heterogenous security stack. As organizations look to simplify operations, vendors are consolidating platforms around one or more major cybersecurity domains. For example, identity security services may be offered through a common platform that combines governance, privileged access, and access management features. SASE, CNAPP and XDR are other examples.

The current economic situation will further constrain the Capex budgets which will in turn fuel the demand for cloud delivered security services. Together with the cost take-out opportunity the advantages of an integrated security stack and centralized security policy management will drive platform- based consolidation of security solutions which are delivered from cloud.

## About the Author

### Anil J Rajan

**Senior Industry Principal**

Anil possesses over 25 years of experience in the industry with specialization in cybersecurity and networking domains. He is the offering leader for joint go to market offerings in cybersecurity domain as part of the strategic partnership between Infosys and Palo Alto Networks. Anil has managed the Europe portfolio of cybersecurity practice in Infosys for Fortune 2000 clients across industry segments. Anil has program managed cloud security implementation for green field cloud platform implementation for a financial services giant in APAC. He has also been involved in transformation programs, end-to-end outsourcing programs and service delivery within cybersecurity.

For more information, contact askus@infosys.com

Infosys®
Navigate your next