Infosys cobalt

VIEW POINT

DECHIPHERING CYBERSECURITY MESH ARCHITECTURE

Abstract

This Point of View discusses the Cybersecurity Mesh Architecture (CSMA) in a simplified manner so that it can be consumed by various stakeholders in an organization - right from a security analyst to a CXO. The architecture has been elaborated starting with the challenges faced by organizations in a distributed cyber defense system, need for a CSMA in which distinct security services work in collaboration to create a dynamic security environment, and eventually the future roadmap for enterprises to adopt CSMA which can protect businesses from complex and NextGen cyber threats.

Infosys®
Navigate your next

Introduction

The rapid evolution of cyberattacks and high velocity of digital transformation, where enterprises are migrating their digital assets to the hybrid multi-cloud, is creating deep cybersecurity challenges. Enterprise IT leadership must contemplate to integrate cybersecurity tools into a cooperative ecosystem using a composable or interoperable and scalable CSMA. "Cybersecurity mesh" is a new term coined by Gartner in 2021 to describe a security approach that could lessen the financial impact of cyber breaches by 90% in the next two years.

CSMA offers a foundational layer that enables multiple security services to work together which eventually creates a dynamic security environment resulting in consistent security posture & increased agility against breaches and attacks. Enterprises are investing in new technology to enable accelerated digitalization wherein CSMA provides a flexible and scalable security foundation with better defensive posture through a collaborative approach between integrated security tools, detective and predictive analytics.

Cybersecurity technology delivered through CSMA model takes less time to deploy and maintain, while minimizing the potential for security blind spots, therefore improves the productivity and innovation for the security teams.

Need for Cyber Mesh

Gartner defines CSMA as a security approach for the modern businesses opting for digital as a business theme. These enterprises have complex network infrastructures and face constant cyber threats. The value CSMA brings against traditional security approach are:

Responsive & standardized security

Well-designed CSMA increases the agility and resilience of an enterprise's cybersecurity setup. Security controls working collaboratively on the same standards of zero trust, CSMA ensures the best real-time defense against known & evolving threats. Data gathered from each enterprise security controls & broader ecosystem can be leveraged to quickly address complex cyber threats. Therefore, it improves the velocity & efficacy of threat detection, and consequently the response.

Emergence of decentralized identity standards

Most enterprises utilize a centralized approach of managing user/ identity data which eventually creates critical vulnerabilities. Security analysts predict that most enterprises shall migrate to a portable, decentralized identity standard which will be globally acceptable.

A cybersecurity mesh is going to handle more IAM (Identity Access Management) requests, providing more mobile, adaptive, and unified access management. An enterprise shall have a more reliable approach to manage access and control its digital assets which are spread out ever before.

Improved collaboration and reduced security gaps

With single set of interoperating controls, CSMA extends security across the entire enterprise network. With rapid digitalization & cloud adoption, enterprises are putting greater efforts to not only integrate 3rd party applications but also ensure these technologies are appropriately secure. With CSMA, enterprises can understand the latest & upcoming security trends & implement them easily. With much updated security, there are high possibilities of no or minor security gaps such as early detection of weaknesses and vulnerabilities.

Scalability & flexibility of security solutions

One of the fundamental building blocks of CSMA is its distributed nature & ability to create individual security perimeters around each access point within enterprise IT ecosystem. This further offer a deep visibility of the enterprise network edges and ensures that all areas are well against next generation threats in equal measure.

The flexibility this offers gives organizations agility to build new IT infrastructure & introduce new solutions as needed without compromising on cyber protection. With CSMA, enterprise IT department is better able to keep up with the evolution distributed & extended IT infrastructure.

Easier deployment & management

The agility of a CSMA also benefits organizations by making it easier and quicker for security teams to deploy and configure new solutions. Gartner's proposed consolidated dashboard, which makes up one of the layers of CSMA, would enable organizations to better adapt their security structure to meet evolving business and security needs.

An integrated security architecture would remove the need for security teams to switch between and operate various tools, which takes up precious time. Instead, it frees them up to focus on deploying, configuring solutions and for other critical security tasks, thereby improving efficiency overall.

Tenets Of CSMA

While adoption of CSMA shall ensure each enterprise asset is cyber secured, however understanding of CSMA in details will help the enterprises to make full use of the architecture. CSMA has four major tenets and each has specific tasks to do. Following is the summary of all four layers:

Security analytics and intelligence

This is very critical layer of CSMA in terms of centralized administration across enterprise cybersecurity ecosystem. All the data that is used for IT systems will be collected, sorted & analyzed on real-time basis. Therefore, allowing enterprises to enhance the cyber risk assessment, mitigation & threat response abilities. This layer is responsible for collecting data from key threat resources and analyzing them accurately. Based on the analyzed data, CSMA propels rapid threat response strategy.

Distributed identity fabric

With this layer of CSMA, adaptive or context aware access, identify proofing, decentralized identity management & directory services can be achieved by an enterprise.

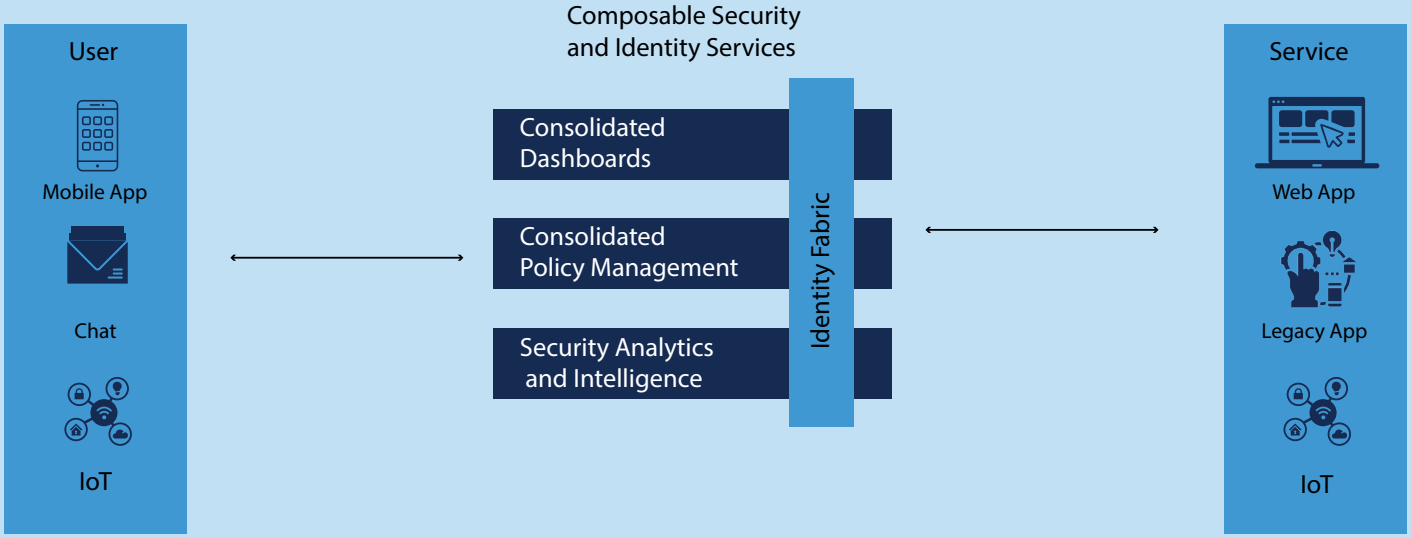
Consolidated policy & posture management

This layer of CSMA is mainly responsible for effective cybersecurity posture management. CSMA essentially translates the enterprise cybersecurity policy into the foundational baseline/outline of every security tool. With that effective compliance risk assessment can be easily executed for an enterprise.

Consolidated dashboards

With single dashboard, CSMA provides full visibility of the implemented security approach. Dashboard data providing end to end visibility can be sorted out to gather the insights on security-related tasks or risks.

Cybersecurity Mesh Architecture



Challenges in building CSMA

CSMA has multiple benefits and shall become one of the leading approaches to defend enterprises from cyber threats in near future however there are challenges as well with total overhauling of the existing approach to CSMA approach. A few challenges are listed below:

Complex and expensive overhaul an existing cyber ecosystem

CSMA is one of the core elements of zero trust. Adopting CSMA will be easier in a greenfield environment or incorporating it during the design & plan phase of an enterprise security ecosystem. Enterprises which are opting CSMA in already existing cyber ecosystem shall find it more challenging. This shift in stakeholder's mindset requires significant change therefore could pose a bigger hurdle, apart from the cost that it shall need to implement CSMA.

Training & support

Since CSMA is a new framework therefore implementing it would need a significant change in the mindset, technologies, and integrations. Those enterprises which want to build a CSMA shall have to make enough investments on their Cybersecurity & IT professionals to support such transition.

Creating Identity Based Systems without productivity loss

CSMA is related to having newly defined security perimeter. Enterprises shall have to ensure that various stakeholders are able to access the enterprise network in a secured manner without it creating distraction which eventually lead to reduced productivity.

How should an enterprise approach to CSMA adoption

Currently CSMA is in its initial phase of standardization and specifics of it shall mature in coming times. But as the first steps enterprises can conduct asset protection inventory which shall help in assessing maturity of the existing enterprise cyber controls against their capabilities of integration, analytics, and risk scoring. The subsequent step is to evaluate the enterprise appetite the invest. Once these initial steps are completed following are the advance steps to achieve CSMA.

Exploit existing integration options

Designing or setting up CSMA is about designing and integration (building connections) between security controls and tools. Foundational step to create a CSMA starts with assessing current security tools thatenterprises have already installed, and the compatibility between various tools to integrate. To have effective integration among existing enterprise security tools, shall involve using a mix of OEM's' proprietary integrations as well as open specifications & standards for addressing any vendor interoperability gaps.

Implement consolidated security platforms

Vendor consolidation is another theme every cybersecurity OEM focuses on. These OEMs are continuously trying their best efforts to offer consolidated security platforms which are essentially made up of tightly coupled security tools and utilize common data & control planes. Enterprises which adopt these kinds of platforms can get much closer to achieve CSMA & its benefits.

Build new security layers

Enterprise security teams can opt an approach of "do it yourself", proposing and ensuring targeted investments in each of the four CSMA layers. These investments can offer enterprises, security capabilities in the short term aligned with CSMA & carry forward the long-term goal of a CSMA. Products that are interoperable, easy to integrate over open APIs and can follow the cybersecurity analytics approach will be able to offer greatest value while creating CSMA.

Evaluate emerging technologies

Cybersecurity OEM's do recognize the value of the CSMA and are launching new products to market and capitalize the strength of this new phenomenon of CSMA. Enterprises will have to explore, evaluate & judicially invest in emerging technology solutions, with a sharp focus on those solutions that apply data & analytics principles to secure the enterprise information, applications, infrastructure, and users.

Conclusion

Enterprises face the challenge of protecting their digital assets i.e., data, networks, applications, infrastructure etc. in a rapidly increasing dispersed technology environment and CSMA is becoming an emerging option to protect against next generations cyber threats. Cybersecurity mesh helps enterprises to make effective cyber defenses using full capacity of the interoperable security controls and tools. Cyber vendor consolidation approach and CSMA can work hand in hand for creating the next generation cyber defense systems. CSMA has the potential to make security operations easier and more effective with the right framework.

References

- https://www.mimecast.com/blog/cybersecurity-mesh-architecture-what-it-is-and-how-to-build-it/
- https://10xds.com/blog/what-is-cybersecurity-mesh/
- https://www.ciso-portal.com/cybersecurity-mesh-and-its-advantages/
- https://www.makeuseof.com/what-is-cybersecurity-mesh/
- https://www.linkedin.com/pulse/what-cybersecurity-mesh-its-benefits-applications-businesses-/?trk=pulse-article_more-articles_related-content-card
- https://www.fortinet.com/resources-campaign/fabric-mesh/fortinet-cybersecurity-mesh-for-dummies

Author

Darshan Singh is Industry Principal having rich experience in Cybersecurity domain of more than 17 years. He is currently a part of the Infosys Cyber Innovation, Strategy & Excellence Team which dwells into next generation cybersecurity solutions and strategies. He is also heading the Cloud & Microsoft Security Practice. Darshan has versatile experience in multiple subdomains of Cybersecurity i.e. in the field of Cloud Security, Infrastructure security, data security, OT Security, vulnerability management, security monitoring & analytics etc. Darshan is an engineering graduate from the college of engineering Roorkee (COER).

For more information, contact askus@infosys.com

Infosys®
Navigate your next