Stratejm

IGNITE YOUR

# CYBERSECURITY

## TRANSFORMATION

EMBRACING SECURITY-AS-A-SERVICE

# TABLE OF CONTENTS

# Chapter 1

## Unraveling the Digital Era: Why Cybersecurity Matters in Digital Transformation

In today's fast-paced, technology-driven world, digital transformation is not just a buzzword, it's a business necessity. It's a journey that organizations are undertaking to fully integrate and streamline their processes, workforce, and services using digital technologies. It's also about reimagining business models and processes to deliver more value to customers, and it often requires a significant cultural shift within the organization.

However, this transformative journey comes with its own unique set of challenges, particularly in the field of cybersecurity. As organizations embrace digital solutions, the volume and complexity of cyber threats they face also increase. From ransomware to phishing attacks, the diverse and evolving nature of these threats necessitate robust cybersecurity measures.

As we venture further into the age of interconnection, cybersecurity threats no longer solely target isolated parts of an organization's infrastructure. The risk has extended to every digital touchpoint, from the data centre to cloud services to individual employee devices. Thus, the role of cybersecurity has expanded far beyond perimeter defense-in-depth. It now includes protecting internal resources and securing private data across all platforms and devices.

Traditional approaches to cybersecurity are increasingly inadequate in this new landscape. The need for comprehensive, integrated, and scalable solutions is now evident. Today's models, which often involve significant capital investments in hardware and software combined with continuous updates and maintenance, are not sustainable for many organizations. Additionally, these models are often characterized by technology silos that hinder the swift detection of and response to threats.

This need for a change in the approach to cybersecurity ushers in the era of Security-as-a-Service (SECaaS). As a consumption-based model, SECaaS liberates enterprises from capital purchases and the ongoing challenges of managing multiple, disconnected products.

Another concept making strides in the cybersecurity realm is what is now being called the cybersecurity mesh architecture. The cybersecurity mesh approach seeks to break down the silos plaguing traditional cybersecurity solutions. By ensuring that all components can be interconnected, the cybersecurity mesh provides a seamless, integrated cybersecurity solution. This is particularly beneficial for early detection of malicious activity, for reducing the time to respond, and for enabling more efficient automation.

Combining SECaaS with a cybersecurity mesh architecture heralds a new age in enterprise cybersecurity and equips organizations with the tools they need to safeguard their digital transformation journey. This e-book will take you through the essentials of this revolutionary approach, providing insights into its significance and applications.

# Chapter 2

## Demystifying Security-as-a-Service (SECaaS)

Security-as-a-Service, by borrowing the '-as-a-service' concept from cloud computing, can offer organizations a flexible, scalable, and comprehensive solution for their cybersecurity needs. The essence of SECaaS is the delivery of cybersecurity services on a subscription basis via the cloud, usually provided and operated by third-party providers. This eliminates the need for organizations to make substantial upfront investments in security infrastructure, hardware, and software. Instead, they pay a regular fee for a portfolio of comprehensive, constantly updated security services.

SECaaS provides a host of benefits, making it an increasingly popular choice for organizations that are seeking efficient, cost-effective cybersecurity solutions:

1. Reduced Capital Expenditure: SECaaS reduces capital investment in security infrastructure. Organizations can invest more in their core operations, optimizing their budget for maximum efficiency.
2. Scalability and Flexibility: One of the most significant advantages of SECaaS is its scalability. SECaaS solutions can easily scale up or down based on evolving requirements, making it an excellent fit for both small businesses and large corporations.
3. Always Up-to-Date: Given the rapid evolution of cyber threats, having up-to-date security systems is crucial. Third-party SECaaS providers take responsibility for updating their services, and ensuring their clients have the latest protection capabilities.
4. Expertise and 24/7 Monitoring: Most SECaaS providers offer 24/7 monitoring, providing immediate alerts about potential security incidents. They also possess the technical expertise that many organizations lack, offering informed guidance for managing complex security landscapes.
5. Seamless Integration: Many SECaaS solutions are designed to integrate easily with existing systems and processes, allowing for a smooth transition with little disruption to the organization's operations.

### SECaaS Models and Implementation Scenarios

There is no one-size-fits-all model for implementing SECaaS. The choice of services and the method of deployment depend on a variety of factors, including the company's size, the nature of its operations, and its specific security needs and risks. From identity and access management, network security, data loss prevention to intrusion management, and security assessment, the scope of SECaaS is extensive and caters to diverse industry needs.

SECaaS implementation scenarios range from fully managed services—with the provider taking full responsibility for security management—to hybrid models in which the in-house teams and external service providers collaborate.

As promising as SECaaS may sound, it isn't a silver bullet for all cybersecurity challenges. One potential issue is the lack of control some organizations may feel when relying on third-party providers for critical security operations. It can also be challenging to integrate SECaaS solutions with existing systems, particularly in more complex or larger organizations.

In the following chapters, we'll explore implementation scenarios in more detail, providing insights to guide your SECaaS deployment journey.



**From identity and access management, network security, data loss prevention to intrusion management, and security assessment, the scope of SECaaS is extensive and caters to diverse industry needs.**

# Chapter 3

## The Revolutionary Concept of Cybersecurity Mesh Architecture

With digitalization touching every facet of business operations, traditional cybersecurity approaches, often characterized by siloed tools, are becoming less effective. The concept of a Cybersecurity Mesh Architecture has come to the forefront to address the evolving security needs by breaking down the silos and integrating all security components into a seamless and robust security platform.

A Cybersecurity Mesh Architecture is not a distinct product or service – instead, it is a design pattern that represents a shift in the traditional approach to cybersecurity. It recognizes the evolving nature of digital environments and aims to provide security that is adaptable, scalable, and distributed across various endpoints and services. The cybersecurity mesh architecture is designed to address the challenges posed by the increasing complexity and interconnectivity of modern digital ecosystems.

In a cybersecurity mesh architecture, security is no longer concentrated solely at the network perimeter or on specific devices. Instead, it is extended and woven into every aspect of the digital environment, forming a protective layer that encompasses people, devices, applications, and data.

### There are several key characteristics and components of a cybersecurity mesh architecture:

Distributed Trust: Trust is established between various entities within the mesh, allowing for secure interactions and communication. Trust can be based on identity verification, device integrity checks, or other factors.

Scalability and Flexibility: The cybersecurity mesh architecture can adapt to dynamic environments, scaling up or down as needed. It accommodates the diverse set of endpoints and services present in digital ecosystems, including cloud resources, IoT devices, and remote workers.

Decentralized Enforcement: Security controls are distributed throughout the mesh, reducing reliance on centralized security mechanisms. This ensures that security is applied as close to the assets and users as possible, minimizing potential vulnerabilities and reducing the impact of a single point of failure.

Continuous Adaptive Risk and Trust Assessment (CARTA): The cybersecurity mesh incorporates real-time risk and trust assessment mechanisms. It leverages contextual information, such as user behavior, device posture, and threat intelligence, to dynamically adjust security measures and respond to emerging threats.

Zero Trust Model: The cybersecurity mesh architecture embraces a zero trust approach, assuming that no entity should be inherently trusted. Instead, it employs strict access controls, authentication mechanisms, and encryption protocols to verify and secure each interaction.

Improved Detection and Response Times: With all security components working together, the time taken to detect and respond to threats can be significantly reduced. Rapid detection and response are crucial in mitigating the impact of a cybersecurity breach.

Facilitates Automation: The integration offered by a cybersecurity mesh opens the door to powerful automation opportunities. Automated responses to certain types of threats can be enabled, reducing the burden on human security teams, and increasing the speed of threat response.

Within the context of digital transformation, the cybersecurity mesh architecture becomes important for several reasons:

Increased Attack Surface: As organizations adopt new technologies and expand their digital footprint, the attack surface for potential cyber threats also grows. The mesh architecture provides a more comprehensive and adaptable security framework to protect against evolving threats across a wider range of endpoints and services.

Dynamic Workforce and Connectivity: Digital transformation often involves a mobile workforce, remote work arrangements, and reliance on cloud services. The cybersecurity mesh architecture accommodates these dynamic environments by extending security controls to different locations, devices, and networks, ensuring consistent protection regardless of the user's location.

Interconnected Components: Digital transformation often involves integrating various systems, applications, and third-party services. The cybersecurity mesh facilitates secure interactions and data exchange between these interconnected components, reducing the risk of unauthorized access or data breaches.

Agility and Scalability: Traditional security approaches can struggle to keep pace with the rapid changes associated with digital transformation. A cybersecurity mesh architecture offers greater agility and scalability, allowing security controls to be dynamically adjusted and scaled based on evolving requirements and emerging threats.

The Cybersecurity Mesh Architecture is indeed a revolutionary approach to enterprise security. However, its maximum potential is unlocked when it works in synergy with Security-as-a-Service (SECaaS).

**As an organization grows and changes, so too can its security mesh. It's a solution that can adapt and evolve with a businesses needs.**

# Chapter 4

## The Power Duo: The Symbiosis of SECaaS and Cybersecurity Mesh

The combination of Security-as-a-Service (SECaaS) and the cybersecurity mesh architecture brings about a novel and powerful approach to enterprise cybersecurity. While each concept brings its unique set of advantages, their symbiosis catalyzes a transformative shift in how businesses address security in the era of digital transformation.

Let's delve deeper into how SECaaS and the cybersecurity mesh architecture work together and why the combination is so pivotal:

1. Enhanced Security Integration and Collaboration: The cornerstone of the cybersecurity mesh architecture is its emphasis on integrating all security components into a cohesive, communicative mesh. When combined with the comprehensive security services offered by SECaaS, the result is a fully integrated, efficient security system that significantly improves threat detection and response times. This combination ensures that every part of an organization's security toolset is working together towards a common goal.

2. Scalable and Flexible Cybersecurity: Both SECaaS and the cybersecurity mesh architecture promote scalability and flexibility, which become even more pronounced when combined. As an organization grows and its security needs evolve, both its SECaaS subscriptions and its cybersecurity mesh can be adjusted to match. This flexibility allows organizations to maintain an optimal level of security at all times without incurring unnecessary costs.

3. Comprehensive Automation: Automation is one of the greatest boons of combining SECaaS with a cybersecurity mesh architecture. By integrating all security components and utilizing the services offered by SECaaS providers, organizations can automate many aspects of their cybersecurity operations. This not only increases efficiency and decreases response times but also reduces the burden on in-house security teams.

4. Reduced Complexity and Management Overhead: By outsourcing security functions to SECaaS providers, organizations can reduce the complexity and management overhead associated with maintaining and updating security infrastructure. SECaaS providers handle tasks such as system updates, threat intelligence gathering, and security incident response, allowing organizations to focus on their core digital transformation objectives.

5. User-Centric Approach: One of the unique strengths of the cybersecurity mesh architecture is its focus on the individual user's identity. By combining this user-centric approach with SECaaS's comprehensive security solutions, organizations can better protect their users, regardless of the device or platform they're using.

6. Agility and Rapid Deployment: SECaaS solutions are typically cloud-based and can be rapidly deployed and updated. This agility aligns well with the dynamic nature of digital transformation initiatives. As the cybersecurity mesh architecture evolves, organizations can easily integrate new SECaaS offerings or update existing ones to address emerging security challenges and requirements.

7. Cost-Effective and Resource-Saving: By eliminating the need for substantial upfront investments in security infrastructure and reducing the demands on internal IT teams, SECaaS can significantly lower costs. When combined with a cybersecurity mesh architecture, which can further improve efficiency and threat response times, organizations can achieve top-tier cybersecurity without breaking the bank.

This synergy of SECaaS and cybersecurity mesh architecture forms the crux of a modern, effective cyber-security ecosystem.



**The symbiosis of SECaaS and Cybersecurity Mesh catalyzes a transformative shift in how businesses address security in the era of digital transformation.**

# Chapter 5

## Harnessing Innovation: Why SECaaS & Cybersecurity Mesh are Integral to Digital Transformation

The shift to a digital-first transformation mindset isn't without its challenges, especially when it comes to maintaining robust cybersecurity. This chapter explores why Security-as-a-Service (SECaaS), built on a cybersecurity mesh architecture, is indispensable for organizations that are on their digital transformation journey.

Some aspects to be considered include:

1. Addressing Increased Security Complexity: Digital transformation often involves leveraging multiple technologies, platforms, and devices, which adds to the complexity of securing business operations. An integrated approach using SECaaS built on a cybersecurity mesh architecture simplifies managing this complexity by bringing all security elements into one cohesive system.

2. Enhancing Speed and Agility: The rapid pace of digital transformation necessitates a cybersecurity approach that is both quick to deploy and flexible enough to adapt to ever-changing scenarios. SECaaS offers scalability and agility, while the cybersecurity mesh architecture facilitates quick detection of and response to threats.

3. Facilitating Compliance: As businesses go digital, they often need to comply with a host of regulatory standards related to data security and privacy. A centralized management approach, inherent in the cybersecurity mesh architecture, makes it easier to enforce consistent policies across the organization and maintain compliance.

4. Securing Remote Work and BYOD Policies: The rise of remote work and BYOD (Bring Your Own Device) policies has been accelerated by digital transformation. This expands the potential attack surface for cyber threats, making a user-centric approach like the cybersecurity mesh architecture more critical. Coupled with the comprehensive protection offered by SECaaS, businesses can secure their operations regardless of where their employees are working from or what devices they're using.

5. Achieving Cost-efficiency: Digital transformation is an investment, and cost-efficiency is critical. SECaaS, with its subscription-based model, reduces the need for significant upfront capital investments in security infrastructure. Additionally, the cybersecurity mesh architecture improves efficiency, contributing to overall cost savings.

6. Enabling Innovation: To stay competitive, businesses must continuously innovate, which often involves adopting new technologies. A flexible and scalable security approach like SECaaS with cybersecurity mesh architecture ensures that organizations can secure these new technologies without hindrance, promoting a culture of innovation.

7. Empowering Smaller Organizations: Smaller businesses and startups, which often lack the resources for a comprehensive in-house cybersecurity team, can particularly benefit from SECaaS and cybersecurity mesh. This combination offers top-tier, scalable security without the need for extensive resources.

Digital transformation is changing the face of business. But with new opportunities come new threats. That's why the combination of SECaaS with a cybersecurity mesh architecture is so important—it provides a robust, scalable, and efficient approach to cybersecurity that can help businesses of all sizes navigate their digital transformation journey safely and successfully.



**With new opportunities come new threats. That's why the combination of SECaaS and cybersecurity mesh architecture is so important—it provides a robust, scalable, and efficient approach to cybersecurity.**

# Chapter 6

## Success in Action: Stratejm's Revolutionary Approach to SECaaS and Cybersecurity Mesh Architecture


Stratejm, a leading Next Generation Managed Security Service Provider (NG-MSSP), serves as an exemplary case study of a forward-thinking company effectively leveraging Security-as-a-Service (SECaaS) built on the cybersecurity mesh architecture to address contemporary cybersecurity challenges.

1. The Vision: Stratejm recognized early on the limitations of traditional, siloed security products. They envisioned an integrated, consumption-based cybersecurity service that would eliminate the need for hefty capital investments and the complications of managing disjointed security products.

2. The Implementation: Stratejm implemented a cybersecurity mesh architecture that successfully integrated all security components, breaking the silos that characterized traditional security approaches. This integration allows for faster detection of malicious activities and reduces the time between detection and response. It also opens the door for efficient and effective automation. By combining this mesh architecture with SECaaS, they created a unified, flexible, and robust security solution that could adapt to the evolving needs of businesses in the digital age
.

3. The Benefits: Stratejm's security solution offers a host of advantages to its clients. Here are a few key points:

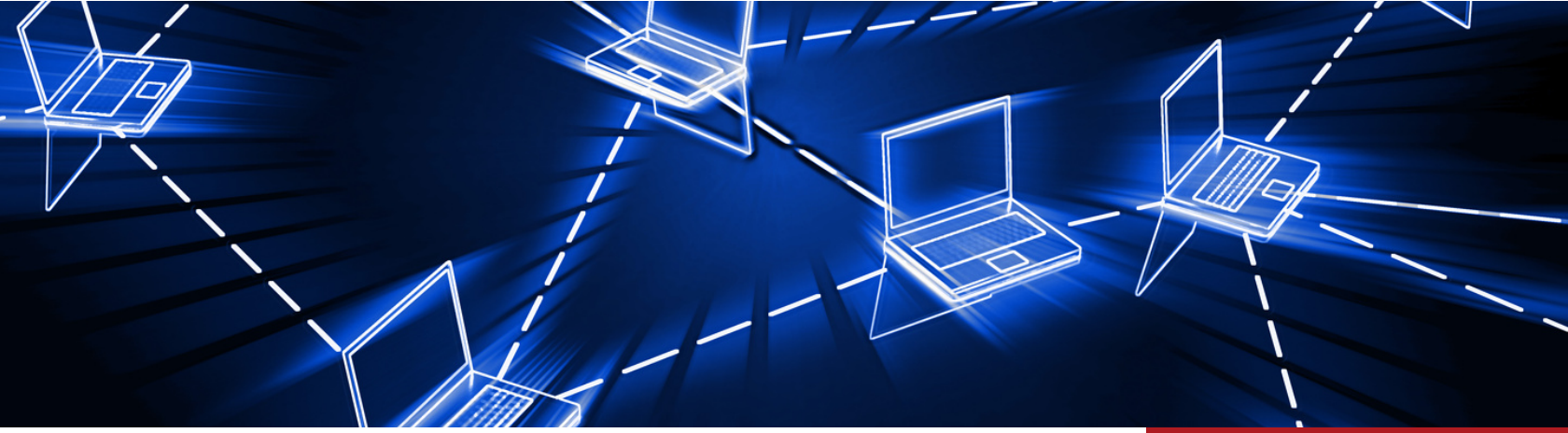
    - Cost Efficiency: By using a consumption-based SECaaS model, Stratejm's customers can avoid the high upfront costs typically associated with cybersecurity. This model offers the flexibility to scale services according to needs and budget, making it an affordable option for businesses of all sizes.

    - Enhanced Threat Detection and Response: The mesh architecture allows for swift detection of potential threats and rapid response, reducing potential damage and downtime.

    - Automation: The integrated nature of the cybersecurity mesh architecture enables efficient automation, reducing manual effort and improving speed and accuracy in threat respo

    - User-Centric Security: The mesh architecture allows for a user-centric approach, making it suitable for organizations with remote workforces and those implementing BYOD (Bring Your Own Device) policies.

4. The Outcome: Stratejm's integrated approach to cybersecurity has enabled them to provide superior security solutions for their clients. Their innovative use of SECaaS combined with the cybersecurity mesh architecture not only offers robust security but also aids businesses in their digital transformation journey.



5. The Future: With the continually evolving threat landscape and the increasing pace of digital transformation, the demand for integrated, flexible, and robust security solutions like the one offered by Stratejm will only increase. Their approach is a testament to the potential of SECaaS and cybersecurity mesh architecture in shaping the future of cybersecurity.

Through this case study, we can clearly see how the combination of SECaaS, and cybersecurity mesh architecture has the potential to revolutionize cybersecurity.

**Stratejm's innovative use of SECaaS combined with the cybersecurity mesh architecture not only offers robust security but also aids businesses in their digital transformation journey.**

# Chapter 7

## Anticipating Challenges and Opportunities in Next-Gen Cybersecurity

As the digital landscape continues to evolve, so does the realm of cybersecurity. The revolution brought by integrating Security-as-a-Service (SECaaS) with the cybersecurity mesh architecture is just the beginning. This chapter will explore what to expect as we move forward:

1. Growing Cyber Threat Landscape: As digital transformation accelerates, so does the sophistication of cyber threats. Businesses need to be prepared to face a wide range of evolving threats, from ransomware to sophisticated phishing attacks.

2. Cybersecurity Skills Gap: There is a large shortage of cybersecurity professionals worldwide. This resource gap can leave businesses vulnerable to attacks. Leveraging SECaaS can alleviate some of the strain, as the responsibility for maintaining the security infrastructure lies with the provider.

3. Regulation and Compliance: As more data is digitized, maintaining data privacy and meeting compliance regulations becomes increasingly complex. Centralized policy management, an inherent part of the cybersecurity mesh, can simplify compliance management.

4. Increased Adoption of AI and Machine Learning: Artificial Intelligence (AI) and Machine Learning (ML) are already playing a significant role in cybersecurity, and their influence is only expected to increase. These technologies can automate threat detection and response and predict potential threats, enhancing the benefits of a SECaaS and cybersecurity mesh approach.

5. IoT and Edge Security: The Internet of Things (IoT) and edge computing are expanding the boundaries of the enterprise, necessitating a decentralized approach to security. The flexibility and user-centric approach of the cybersecurity mesh architecture make it an excellent fit for securing these evolving networks and systems.

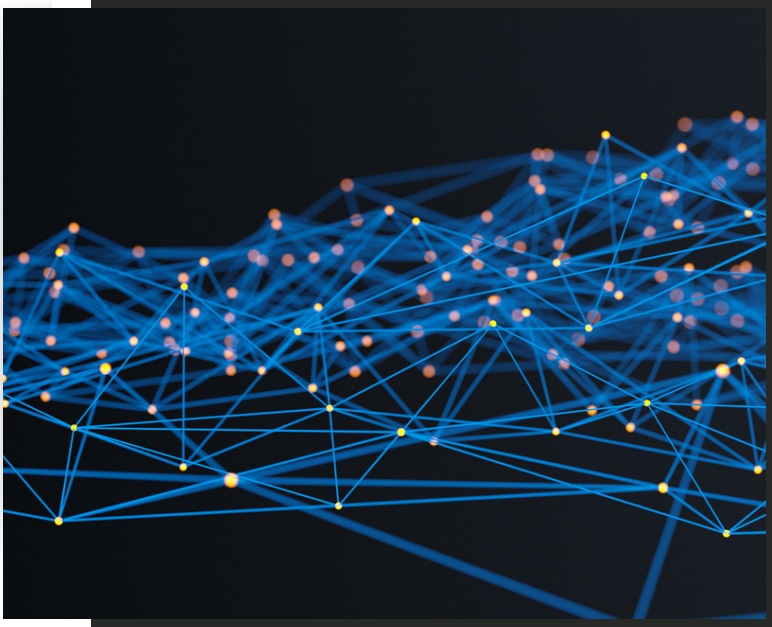
6. Privacy Enhancing Technologies: As privacy concerns grow, technologies like zero-knowledge proofs and homomorphic encryption, which allow data to be analyzed without revealing sensitive information, will become more prevalent. Integrating these technologies into SECaaS offerings will further enhance security and privacy.

7. Quantum Computing: While still emerging, quantum computing poses both a challenge and an opportunity for cybersecurity. It has the potential to break many current encryption algorithms, but it can also usher in a new era of ultra-secure quantum encryption.

To navigate this future landscape, businesses will need flexible, integrated, and forward-thinking security solutions. By leveraging Security-as-a-Service built on the cybersecurity mesh architecture, businesses can not only protect themselves from contemporary threats but also prepare for the future. By remaining adaptable and vigilant, we can turn the challenges of the digital future into opportunities for growth and innovation.

# Chapter 8

## Embracing the Future: Implementing SECaaS with a Cybersecurity Mesh Architecture



As we embark on a future characterized by pervasive connectivity and sophisticated cyber threats, it's clear that traditional, siloed approaches to cybersecurity will not suffice. The shift towards Security-as-a-Service (SECaaS) built on cybersecurity mesh architecture is not just preferable—it's essential. But understanding the theory isn't enough. It's time to delve into the practicalities of how businesses can embrace this innovative approach to cybersecurity:

1. Recognizing the Need for Change: The first step towards implementation is acknowledging the limitations of current cybersecurity practices and the need for a more integrated, scalable, and flexible approach. This requires a comprehensive evaluation of existing security infrastructure and potential vulnerabilities.

2. Partnering with the Right Provider: Choosing a Managed Security Service Provider (MSSP) that can offer SECaaS built on cybersecurity mesh architecture is a crucial step. It's essential to select a provider like Stratejm that has proven expertise and a strong track record in this field.

3. Tailoring the Solution: While the principles of SECaaS and the cybersecurity mesh architecture are universally applicable, the specific implementation will vary based on an organization's unique needs. Factors such as the size of the business, the nature of its operations, its regulatory environment, and the specific threats it faces will all influence the final solution.

4. Prioritizing User Education: Even the most robust cybersecurity solution can be undermined by user error. Regular training sessions and ongoing education are critical to ensuring that all users understand the importance of cybersecurity and how to behave safely online.

5. Continual Evaluation and Adaptation: Cybersecurity is not a one-time project but an ongoing process. Regular evaluations are essential to assess the effectiveness of the security measures in place and to make any necessary adjustments. As new threats emerge and the organization evolves, the cybersecurity program must adapt accordingly.

6. Future Proofing: With rapid advancements in technologies such as AI, Machine Learning, and quantum computing, it's essential to choose a solution that can evolve with the times. When selecting an MSSP, consider their commitment to staying at the forefront of cybersecurity developments.

The journey towards robust, integrated cybersecurity may seem complex, but the rewards are well worth the effort. By embracing Security-as-a-Service built on cybersecurity mesh architecture, businesses can secure the present and pave the way for a safe and secure digital future.

As we conclude this book, remember that cybersecurity is an ongoing journey, one that requires constant vigilance, continuous learning, and a willingness to adapt and evolve.

# REFERENCES


1 Cisco Systems Inc. – Cisco Annual Internet Report (2018–2023) White Paper

2 Gartner, Inc. – The Future of Network Security Is in the Cloud (available from Amazon AWS)

3 (ISC)2 – Strategies for Building and Growing Strong Cybersecurity Teams

4 Stratejm – Stratejm Security as a Service Overview

5 Symantec – Internet Security Threat Report

6 Verizon – Data Breach Investigations Report

7 Fortinet – What is Cybersecurity Mesh?

8 CrowdStrike – Security as a Service

9 Motley Fool – Security as a Service (SECaaS): A Beginner's Guide for Small Businesses

10 InfoSec Report – Security-as-a-Service (SECaaS): A Cost-Effective Way of Cybersecurity

# DECIPHERING THE JARGON: A GLOSSARY OF KEY TERMS

Note: Terms are taken from the Gartner Glossary except where noted.

AI (Artificial Intelligence): Artificial intelligence (AI) applies advanced analysis and logic-based techniques, including machine learning, to interpret events, support and automate decisions, and take actions.

Cybersecurity Mesh: Cybersecurity mesh, or cybersecurity mesh architecture (CSMA), is a collaborative ecosystem of tools and controls to secure a modern, distributed enterprise. It builds on a strategy of integrating composable, distributed security tools by centralizing the data and control plane to achieve more effective collaboration between tools. Outcomes include enhanced capabilities for detection, more efficient responses, consistent policy, posture and playbook management, and more adaptive and granular access control — all of which lead to better security.

Endpoint*: Endpoints are physical devices that connect to and exchange information with a computer network. Some examples of endpoints are mobile devices, desktop computers, virtual machines, embedded devices, and servers. Internet-of-Things devices—like cameras, lighting, refrigerators, security systems, smart speakers, and thermostats—are also endpoints. When a device connects to a network, the flow of information between, for instance, a laptop and a network, is much like a conversation between two people over the phone. (*Source: Microsoft)

Edge Computing: Edge computing is part of a distributed computing topology where information processing is located close to the edge, where things and people produce or consume that information.

5G: 5G is the next-generation cellular standard after 4G. It has been defined across several global standards bodies, including the International Telecommunication Union (ITU), 3GPP and ETSI. The official ITU specification, International Mobile Telecommunications-2020, targets maximum downlink and uplink throughputs of 20 Gbps and 10 Gbps, respectively; latency below 5 ms endpoint to RAN; and massive scalability, although initial deployments may be less ambitious. New system architecture includes core network slicing and edge computing.

Internet of Things (IoT): The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.

Machine Learning: Advanced machine learning algorithms are composed of many technologies (such as deep learning, neural networks and natural language processing), used in unsupervised and supervised learning, that operate guided by lessons from existing information.

Managed Security Service Provider (MSSP): A company that provides outsourced monitoring and management of security devices and systems. Services often include managed firewall, intrusion detection, virtual private network, vulnerability scanning, and anti-viral services.

Security as a Service (SECaaS)*: SECaaS is a cloud-based method of outsourcing your cybersecurity. Outsourced security can cover data protection, VoIP security, database security, and general network security. All of these can help an organization combat SECaaS threats, such as malware and botnets. SECaaS is an increasingly popular data security solution for corporations because it is easier to scale as the business grows. It also makes it possible to circumvent the expense of establishing an elaborate on-premises security architecture. (*Source: Fortinet)

Threat Intelligence*: Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes. (*Source: NIST)

Virtual Private Network (VPN): A VPN is a system that delivers enterprise-focused communication services on a shared public network infrastructure and provides customized operating characteristics uniformly and universally across an enterprise. The term is used generically to refer to voice VPNs. To avoid confusion, IP-based data services are referred to as data VPNs. Service providers define a VPN as a WAN of permanent virtual circuits, generally using asynchronous transfer mode (ATM) or frame relay to transport IP. Technology providers define a VPN as the use of encryption software or hardware to bring privacy to communications over a public or untrusted data network.

Zero Trust Architecture (ZTA)* or Zero Trust Network Access (ZTNA): ZTNA is a product or service that creates an identity- and context-based, logical access boundary around an application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities. The broker verifies the identity, context and policy adherence of the specified participants before allowing access and prohibits lateral movement elsewhere in the network. This removes application assets from public visibility and significantly reduces the surface area for attack. (*ZTA not defined by Gartner).

## About

Stratejm is a next-generation managed security services provider, driving superior cybersecurity outcomes through our innovative "Security-as-a-Service" model. Leveraging the potential of the cybersecurity mesh architecture, we achieve unprecedented integration of diverse security tools. This approach, fosters exceptional defensive capabilities, enabling enterprises to effectively confront ever-evolving cyber threats and affirm their security posture in the digital landscape.

Stratejm's Security as a Service (SECaaS) represents a revolution in the way businesses handle cybersecurity. As a leading Managed Security Service Provider, Stratejm has developed a comprehensive, innovative solution designed to eliminate the complexity of siloed security products and provide a unified, robust defense against cyber threats.

---

## Follow Stratejm on LinkedIn