What is Cybersecurity Mesh Architecture?

What is it and what does it mean for business?

EXCLUSIVE NETWORKS

FORTINET

What is the **Cybersecurity Mesh?**

The cybersecurity mesh is a relatively new concept in the field of cybersecurity that refers to an approach to security that is more flexible, adaptable, and decentralized. It is based on the idea that the traditional perimeter-based security model, where an organization's security is focused on protecting its internal network and devices from external threats, is no longer sufficient in today's complex and dynamic digital environments.

In a cybersecurity mesh, security is distributed across various interconnected devices, applications and networks, creating a more resilient and adaptive security environment. The goal is to create a more dynamic security framework that can respond to threats quickly and effectively, rather than relying on a single point of protection.

Where did the term come from?

The phrase "cybersecurity mesh architecture" was coined by Gartner, a leading research and advisory company, in their report "The Future of Network Security Is in the Cloud" in December 2019. In this report, Gartner introduced the concept of a cybersecurity mesh architecture as a new approach to network security that is more flexible, scalable and resilient than traditional perimeter-based security models. Since then, the concept of cybersecurity mesh architecture has gained traction and has been adopted by many organizations as a key element of their cybersecurity strategy.

Gartner also identified cybersecurity mesh architecture as a **key technology trend** in their report **"Top Strategic Technology Trends for 2022".**

Download the report here

The cybersecurity mesh is based on several key principles, including:

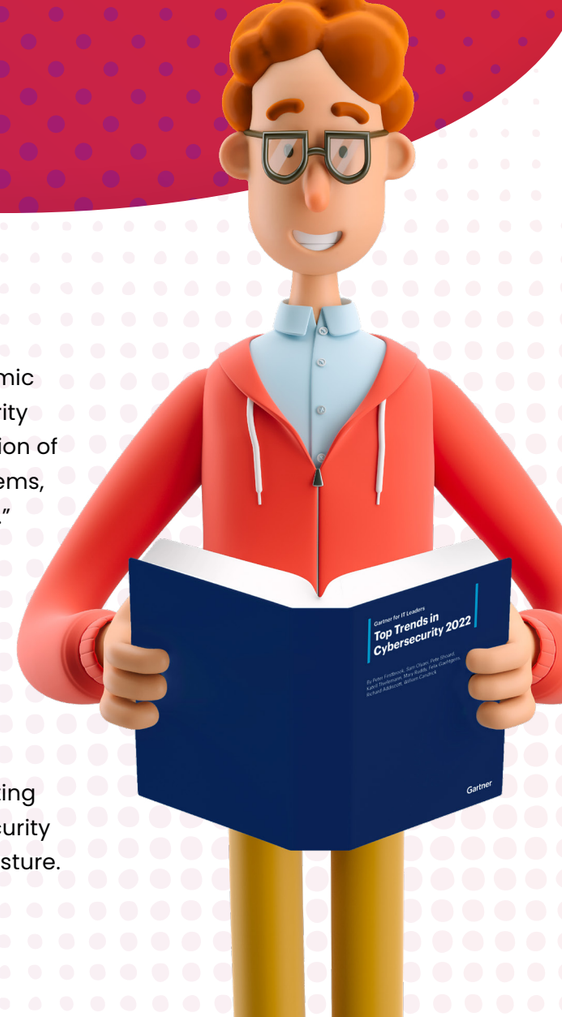
Identity-driven security:
Instead of focusing on securing devices or networks, security is focused on securing individual users and their access to resources.

Zero trust security:
The assumption is that all devices and users are potentially compromised, so access to resources is granted on a need-to-know basis and verified at every step.

Continuous adaptive risk and trust assessment (CARTA):
Security is continuously assessed and adapted based on changing risks and trust levels.

According to Gartner, cybersecurity mesh architecture is a response to the increasing complexity of modern IT environments and the need for a more flexible and dynamic approach to cybersecurity. Gartner describes cybersecurity mesh architecture as a model that "enables the distribution of security capabilities across a variety of devices and systems, allowing security to be delivered where it is needed most." They highlight the benefits of this approach, including enhanced resilience, improved visibility and simplified management.

Gartner also notes that cybersecurity mesh architecture is not a replacement for traditional perimeter-based security models but rather a complementary approach. They recommend that organizations consider implementing cybersecurity mesh architecture as part of a broader security strategy, leveraging it to improve their overall security posture.



Why might you need a Cybersecurity Mesh Architecture?

As networks have become more complex and distributed, seeing and responding to threats has become increasingly difficult. This has led to security sprawl that complicates management, fragments visibility and limits the ability of organizations to respond effectively to threats. That's due, in part, to today's enterprises having deployed an average of 45 security solutions across their network, making any sort of centralized management nearly impossible. And worse, detecting and responding to a cyber incident requires coordination across 19 of those tools, leading to complex workarounds that need to be constantly managed and reconfigured every time a device is upgraded.

Despite these challenges, it is still all too common for organizations to move first and ask how best to secure and manage changes to their networks later — creating a perfect storm for attackers and threats looking to exploit silos, complexities, and visibility gaps that naturally arise from such complex and piecemeal environments.

What are the advantages of a Cybersecurity Mesh Architecture?

A cybersecurity mesh architecture offers several advantages over traditional perimeter-based security models. Some of the key advantages include:

Decentralised Security

In a cybersecurity mesh architecture, security is distributed across multiple nodes, rather than relying on a central perimeter. This makes it harder for attackers to breach the network and gain access to sensitive data.

Simplified Management

By distributing security across multiple nodes, cybersecurity mesh architectures can simplify security management. This is because there is no need to manage a complex perimeter-based security infrastructure. Instead, security policies can be managed on a per-node basis.

Resilience and Scalability

Cybersecurity mesh architectures are highly resilient and scalable. If one node is compromised, the rest of the network can continue to operate normally. Additionally, new nodes can be easily added to the network to expand its reach.

Enhanced Visibility

A cybersecurity mesh architecture provides enhanced visibility into network traffic and security events. This makes it easier to detect and respond to security incidents in real-time.

Zero Trust

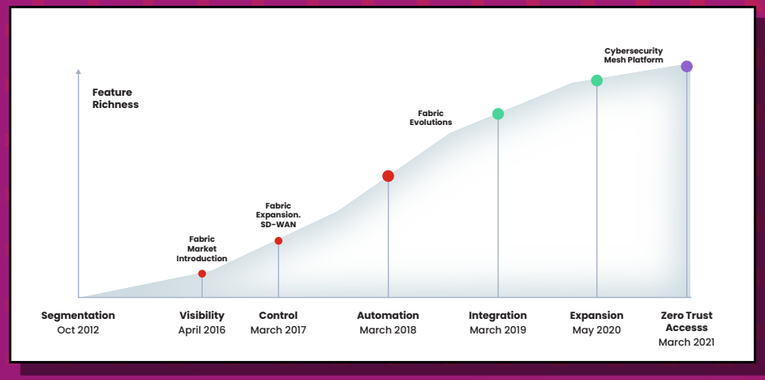
With a cybersecurity mesh architecture, there is a zero-trust approach to security. Each node is considered untrusted, and security policies are enforced on a per-node basis. This helps to prevent lateral movement by attackers who have gained access to the network.

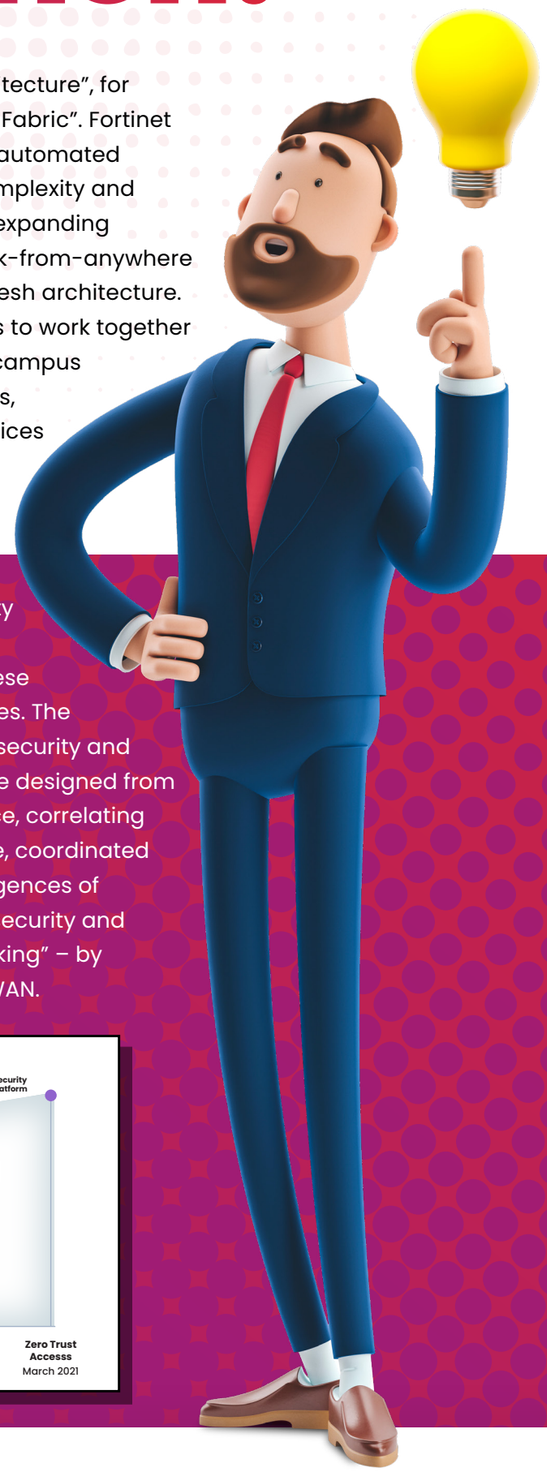
Is this a new phenomenon?

While Gartner calls this idea a “Cybersecurity Mesh Architecture”, for more than a decade Fortinet have called it the “Security Fabric”. Fortinet spearheaded the doctrine that a broad, integrated and automated cybersecurity mesh platform is essential to reducing complexity and increasing overall security effectiveness across today’s expanding networks. New and increasingly complex trends, like work-from-anywhere (WFA), are the perfect use cases for a unified security mesh architecture.

WFA requires multiple solutions to work together across a dynamic set of campus and data center assets, distributed home offices and cloud-based applications.

The Fortinet Security Fabric is ideally suited to address these new complex challenges. The portfolio of more than 50 security and networking technologies - the largest in the industry - are designed from the ground up to interoperate - sharing threat intelligence, correlating data and automatically responding to threats as a single, coordinated system. What’s more, Fortinet is delivering on the convergences of not just cybersecurity products, but the convergence of security and networking – what we like to call “security-driven networking” – by delivering industry-first innovations such as Secure SD-WAN.





Fortinet also believe that a true cybersecurity mesh platform should further break down technology and vendor silos by enabling and supporting a broad open ecosystem of technology partners.

To this point, Fortinet integrate and interoperate with over 450+ third-party technology partners as part of the Fortinet Security Fabric open ecosystem. Such an open ecosystem matters because it empowers organizations with flexibility across their deployments while benefitting from consolidated and converged operations, visibility, and security. It also preserves existing investments in technologies and solutions until they are ready to move towards an even more integrated and automated Security Fabric experience.

Watch the Security Fabric Video

A cybersecurity mesh platform, the Fortinet SecurityFabric integrates a range of security technologies to provide full protection across the digital attack surface, while addressing the long-standing security challenges that organizations struggle to deal with a lack of visibility, automation, and threat detection and response.

The Fortinet Security Fabric addresses these challenges head-on and through the principles of convergence and consolidation, while reducing complexity, enabling end-to-end visibility and automation and improving threat detection and response capabilities.

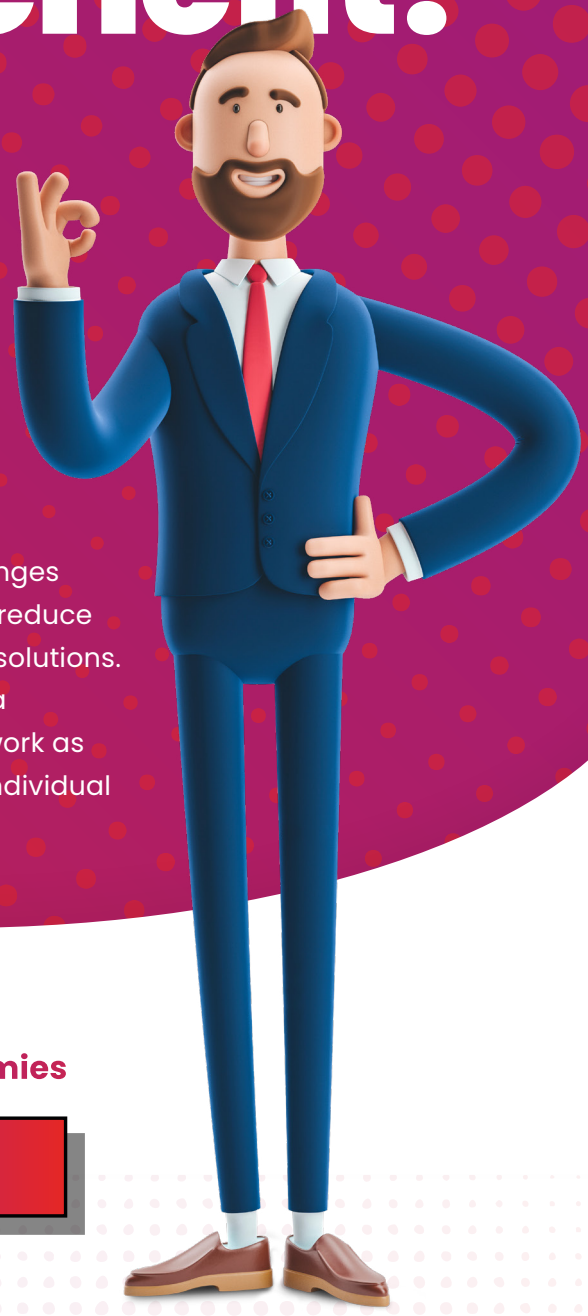
The great news for Fortinet customers is that they don’t have to wait until 2024 for the industry to deliver a new cybersecurity mesh architecture – they can reap those benefits today with the **Fortinet Security Fabric.**

Those benefits include:

- Deep visibility across all edges
- Centrally managing distributed solutions
- Consistent enforcement of policies
- Leveraging anonymized threat intelligence provided by Fortinet Security Fabric customers around the world
- Third-party integrations for improved protection against known and unknown attacks
- Automating actionable responses across hybrid environments.

Whether one wants to call it a “cybersecurity mesh architecture,” a “cybersecurity platform,” or “Fortinet Security Fabric,” the results are the same. The important thing is that organizations embrace and adopt an integrated approach to security as part of their digital acceleration initiatives. This will provide them with reduced complexity, simplified operations and greater security effectiveness regardless of where their journey takes them.

How can partners benefit?



Such an approach is not just suitable for enterprises. Channel partners can provide their customers with a more robust solution - and make more money - with a mesh platform strategy than simply selling point products. A broad portfolio of genuinely integrated solutions allows them to add real value by applying their expertise and architectural capabilities to solve the more considerable challenges today's organizations face.

The trend towards a more unified approach to security is inevitable, whether to secure emerging network security challenges like WFA, to combat the increasing threat of ransomware, or to reduce the overhead of managing a sprawling set of isolated security solutions. In fact, Gartner believes that "by 2024, organizations adopting a cybersecurity mesh architecture to integrate security tools to work as a collaborative ecosystem will reduce the financial impact of individual security incidents by an average of 90%."

Get help to start building a cybersecurity mesh architecture

Watch the video

Download the Guide for Dummies

Downlaod

Learn more

Fortinet Security Fabric with Cybersecurity Mesh Architecture | Security Fabric

To break the attack sequence, you need to be able to rapidly adjust the security posture to defend cohesively against newly discovered attacks across ever-expanding attack surfaces. Learn how our broad, integrated and automated approach delivers on this critical initiative with...

WATCH THE VIDEO

EXCLUSIVE NETWORKS

FORTINET