INC. MASTERS

Cybersecurity Mesh and Zero Trust: The Future of Data Privacy and Protection

Making the move from centralized to decentralized cloud security

BY KELLY DYER, FOUNDER & EXECUTIVE CHAIRMAN, INVENTORY SOURCE, AND CO-FOUNDER & CO-CEO, SOURCEFUSE

APR 27, 2022

Getty Images

Cybersecurity Mesh and Zero Trust: The Future of Data Privacy and Protection

Making the move from centralized to decentralized cloud security

According to Gartner, 'Cybersecurity Mesh' is one of the top tech trends for 2022, and it predicts that "by 2024, organizations adopting a cybersecurity mesh approach will reduce the financial impact of individual security incidents by an average of 90 percent."

It's well known that cyberthreats are on the increase and the real challenge is staying ahead of increasingly creative malicious cyberattacks. All enterprises will have information security policies in place, but what exactly is cybersecurity mesh? And how can it provide even better safeguards against data breaches, in particular health care cybersecurity for protecting the most sensitive data of all? Here we uncover what is meant by cybersecurity mesh and the security advantages it can offer. Understanding cybersecurity mesh

With so many organizations moving from an office-based work to a flexible 'work anywhere' approach, cloud security of IT infrastructures has never been more important. Many IT environments use 'single perimeter' security to encompass the entire network of services and portals, regardless of where they are being accessed from.

In contrast, cybersecurity mesh is a distributed-;or modular-;architectural approach, focused on reinforcing protection by bringing security tools into closer proximity with potentially vulnerable assets. It enables organizations to manage their networks by providing different levels of identity and access management (IAM), which reduces the risk of an entire network being hacked.

Cybersecurity mesh is at the core of a 'zero-trust' strategy, i.e., any device or connection being used to access the organization's network is deemed untrustworthy unless verified by the security protocol. Therefore, by using a distributed mesh approach, security perimeters can be defined around the identity of a person or asset.The benefits of cybersecurity mesh

Improved IAM support: Gartner predicts that by 2025, the cybersecurity mesh approach will support more than 50% of digital access requests, as compared to 'single perimeter' security.

Increase in MSSPs: the skills and expertise that Managed Security Service Providers provide is resulting in more enterprises outsourcing IAM services to service partners. In fact, Gartner predicts that by 2023, 40% of IAM application unification will be driven by MSSPs.

Identity-proofing tools: distinguishing between authorized and unauthorized remote access is a huge security weakness. Cybersecurity mesh can leverage additional identity-proofing, supporting the management of workforce identity life cycles.

Reduced demographic bias: the increase in remote work drew attention to the ways in which prejudice can occur, regarding protected characteristics identification. By the end of this year, it's predicted that 95% of organizations will require that identity-proofing tools minimize any demographic bias.

Decentralized identity standards: with the decentralized mesh approach, block technology ensures identity privacy and anonymity. In addition, validated information requests only require the minimum amount of personal information.

The bottom line

There may be no one perfect solution for cybersecurity, but just as working environments have adapted to the 'new normal,' so too we must the focus on IAM and digital asset security. Highly sensitive personal health care information (PHI) and personally identifiable information (PII) in the health care industry still remains one of the most attractive sources of data for cybercriminals. As such, external access to PHI and PII must be protected by the most rigorous data security services.

The flexible and reliable approach of a cybersecurity mesh maximizes protection through robust IAM, which can scale with company growth and adapt to changing demands, enabling a systemic ethos of continuous improvement in cybersecurity.