PUTTING EXPANSIVE INTELLIGENCE TO WORK:

Cybersecurity Mesh Architecture

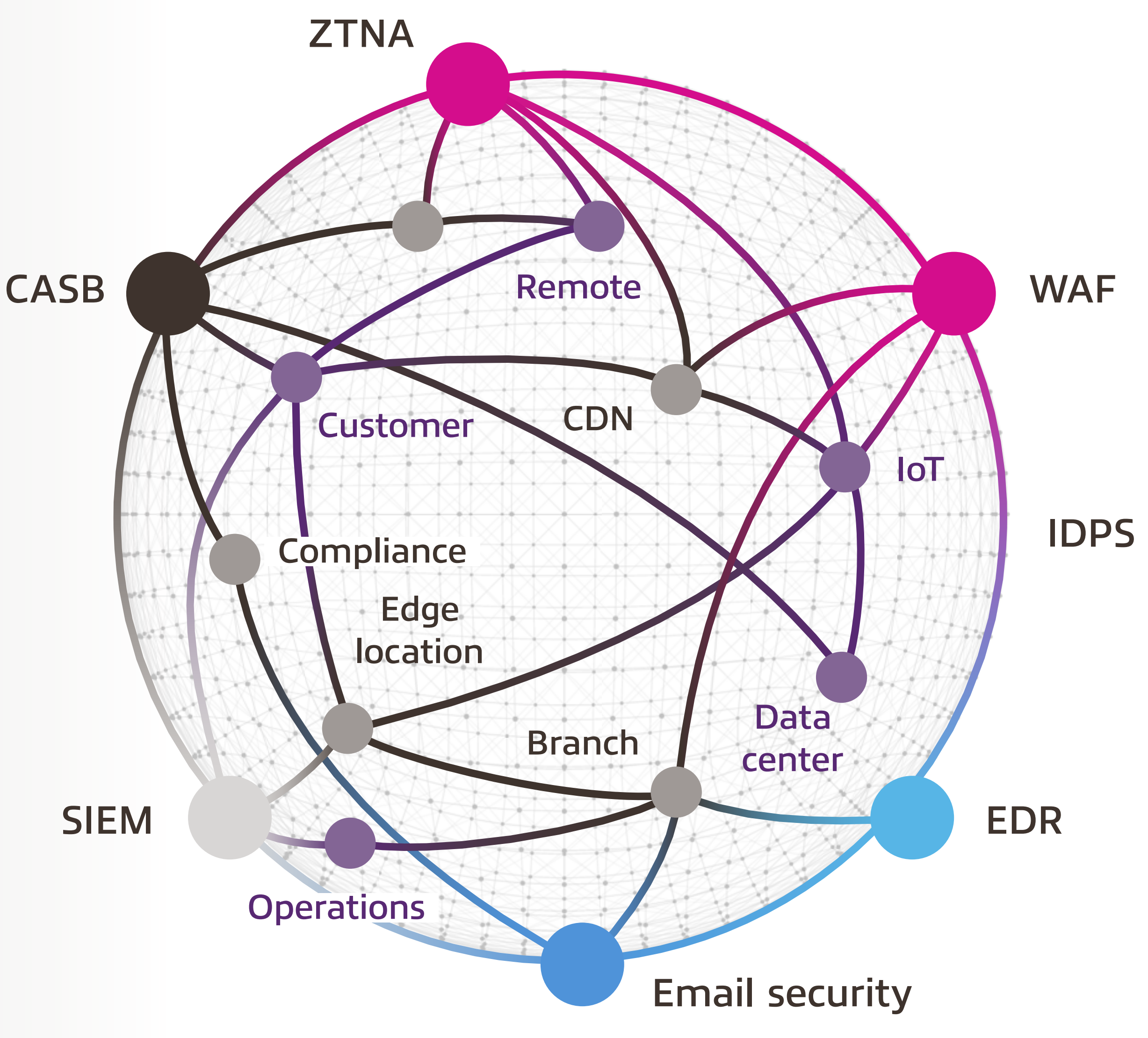
Insight

According to Gartner®,

"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."[1]

WITH CYBERSECURITY MESH ARCHITECTURE,

you can confidently navigate the growing complexity of modern cyberthreats. Widely distributed assets and numerous cybersecurity tools are no match for this holistic and layered approach — CSMA closes the gaps between different security platforms and establishes unity among them without sacrificing strength, scale or flexibility in your cybersecurity ecosystem.



According to a 2020 Ponemon Institute report:

ORGANIZATIONS DEPLOY MORE THAN

45 SECURITY SOLUTIONS AND TECHNOLOGIES

ON AVERAGE.[2]

ADDRESSING THE CHALLENGES OF MODERN CYBERSECURITY

Attack sophistication
Tactics are increasingly complex, with new methods constantly being developed. Organizations need predictive and dynamic responses to these threats.

Siloed security approaches
Multiple security platforms means the tools and data are siloed. Cross-monitoring and managing these tools is time consuming and leaves potential security gaps.

Poor visibility
Without a composite view of security tools, organizations don't have the visibility they need to stop or predict cyberattacks.

Lack of security tool integration
Current tools are unable to make informed security decisions fast enough to meet business needs.

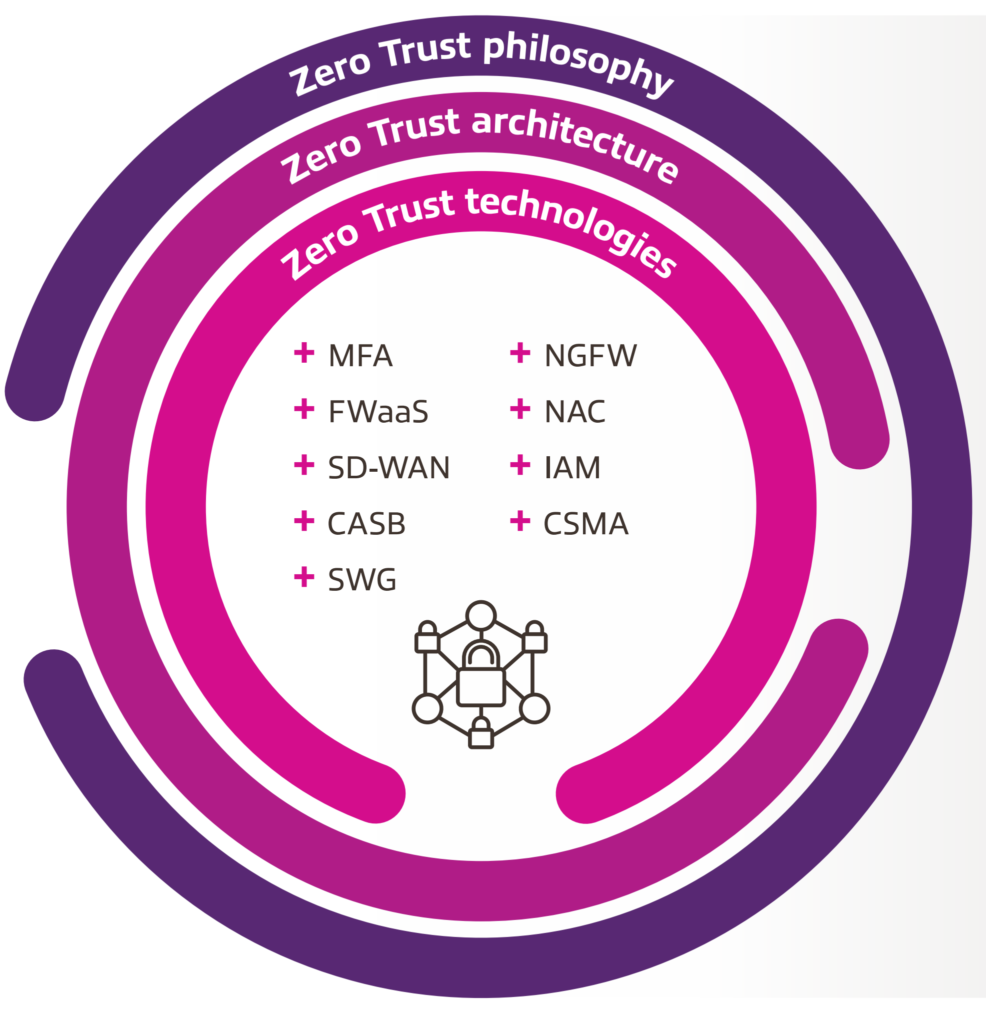
WHY CYBERSECURITY MESH ARCHITECTURE?

Security analysis
Combined data and lessons learned across all tools provide a thorough analysis of threats — and help craft responses in real time.

Identity management
User and endpoint validation, stronger identity authentication and reinforced Zero Trust practices are central to CSMA.

Consolidated policy
Central security policy is translated within cybersecurity tools, closing validation and authentication gaps across the board.

Centralized dashboards
A composite view of your cybersecurity ecosystem allows for faster and more efficient responses to threats, with less cross-monitoring.



CYBERSECURITY MESH ARCHITECTURE & ZERO TRUST

Zero Trust is all about ensuring we provide as little access as possible across users to valuable assets. CSMA is an extension of the Zero Trust framework. The layered approach of CSMA ensures there are no gaps in identity validation across a multitude of platforms and tools used by an organization.

TAKE THE FIRST STEP.

Working with an experienced partner can help you properly implement an integrated, flexible and scalable security solution with cybersecurity mesh architecture. **Explore Insight's strategic approach to learn more.**

See how we can help →

Sources:

[1] Gartner IT Glossary, "Cybersecurity Mesh" as of 24 November 2022. www.gartner.com/en/information-technology/glossary/cybersecurity-mesh.
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

[2] Ponemon Institute. (July 2020). Cyber Resilient Organization Report 2020. Sponsored by IBM Security.