An Executive Guide to Zero Trust

October 11, 2022

Lead Research Analyst, Cybersecurity

Michael is a world-leading IT industry analyst. He has led North American and global initiatives focused on developing insights and strategies that connect technology solutions with business needs, combining data, knowledge, analysis and advanced content delivery to define options for IT and buy-side businesses.

Submitted by Michael O'Neil on 11, Oct 2022

An Executive Guide to Zero Trust

Zero trust thought leadership group members: Geeta Kapoor (MSC Direct), Noah Davis (Trane Technologies), Leon Ravenna (KAR Global), Barney Baldwin (ex-MUFG,

Columbia), Chase Cunningham (Ericom), Eve Maler (ForgeRock), Sean Frazier (Okta).

Drivers, Objectives, and Strategic Considerations

Zero Trust (ZT) defines security principles for the digital world. An approach predicated on hardening the corporate network—the concept driving cybersecurity investment for the past 50 years—doesn't work in an environment where mobility, cloud, and extensive connections between suppliers and customers render the concept of "perimeter" obsolete. CISOs are, or soon will be, organizing strategy around key intellectual property (IP) assets such as data and the identity processes that grant access to and across core IT/ZT pillars, including devices, network, infrastructure, and applications.

Click to read An Executive Guide to Zero Trust: Drivers, Objectives, and Strategic Considerations