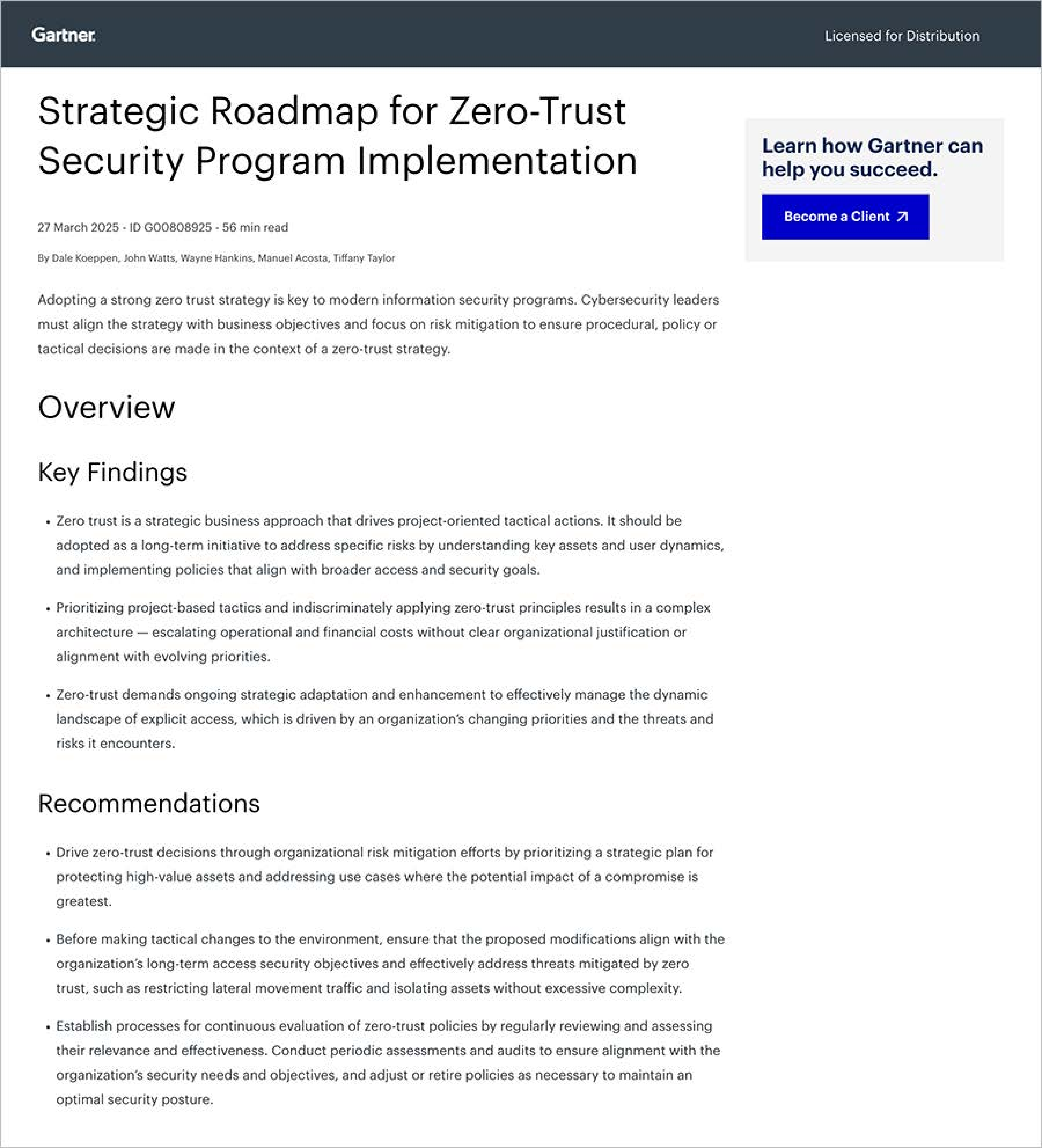

Strategic Roadmap for Zero-Trust Security Program Implementation

27 March 2025 - ID G00808925 - 56 min read

By Dale Koeppen, John Watts, Wayne Hankins, Manuel Acosta, Tiffany Taylor

Adopting a strong zero trust strategy is key to modern information security programs. Cybersecurity leaders must align the strategy with business objectives and focus on risk mitigation to ensure procedural, policy or tactical decisions are made in the context of a zero-trust strategy.

Overview

Key Findings

- Zero trust is a strategic business approach that drives project-oriented tactical actions. It should be adopted as a long-term initiative to address specific risks by understanding key assets and user dynamics, and implementing policies that align with broader access and security goals.
- Prioritizing project-based tactics and indiscriminately applying zero-trust principles results in a complex architecture — escalating operational and financial costs without clear organizational justification or alignment with evolving priorities.
- Zero-trust demands ongoing strategic adaptation and enhancement to effectively manage the dynamic landscape of explicit access, which is driven by an organization's changing priorities and the threats and risks it encounters.

Recommendations

- Drive zero-trust decisions through organizational risk mitigation efforts by prioritizing a strategic plan for protecting high-value assets and addressing use cases where the potential impact of a compromise is greatest.
- Before making tactical changes to the environment, ensure that the proposed modifications align with the organization's long-term access security objectives and effectively address threats mitigated by zero trust, such as restricting lateral movement traffic and isolating assets without excessive complexity.
- Establish processes for continuous evaluation of zero-trust policies by regularly reviewing and assessing their relevance and effectiveness. Conduct periodic assessments and audits to ensure alignment with the organization's security needs and objectives, and adjust or retire policies as necessary to maintain an optimal security posture.