Zero Trust Network Architecture Strategy and Roadmap Consulting

Streamline your journey to a Zero Trust Network Architecture

The traditional network architecture approach leverages a hardened external perimeter to protect initial entry. However, limited security measures to protect internal resources can be easily defeated by attackers and criminals. The results of these attacks include rampant proliferation of ransomware incidents costing organizations millions of dollars while putting the information of customers, patients, residents, and others at risk.

Zero Trust is a transformative strategy enabling the workforce to work seamlessly and securely from anywhere. Zero Trust assumes that the environment itself is potentially hostile and verifies every digital transaction to ensure that it is legitimate and authorized. It increases the resiliency of systems to thwart attackers through improved protections and visibility.

The journey to Zero Trust may be complicated, but GDT can provide you with the strategy and roadmap to get you there.

GDT Zero Trust Network Architecture Strategy

Evolving to a Zero Trust Network Architecture helps your organization to meet compliance regulations and provides assurance that systems and data can be protected. GDT's comprehensive Zero Trust Network Architecture Strategy engagement helps you start on the path by creating a roadmap to success. We dive deep into your entire organization, including infrastructure, applications, data, users, and identity functions to maximize the potential of a Zero Trust Network Architecture and minimize disruption, with a timeline that factors in organization dynamics and risk.

GDT's Zero Trust Network Architecture Strategy engagements provide:

- **Expertise:** Analysis conducted by cybersecurity experts knowledgeable in all industry and business types, bringing deep expertise across the full range of technologies
- **Partnership:** A trusted partner to accompany you from the outset of the journey through all phases of the planning, procurement, implementation, execution, and ongoing operation of Zero Trust capabilities
- **Comprehensive recommendations:** Detailed recommendations aligned to your organization's needs along with a roadmap of phased priorities to advance maturity in the areas needed to evolve to Zero Trust Architecture

Zero Trust Network Architecture Strategy Methodology:

Our methodology analyzes technologies to gain the utmost efficiencies.

- Comprehensive Zero Trust security model across five key pillars that include: identity, devices, network/environment, applications, and data
- GDT-tailored approach based on the Department of Defense (DoD) Zero Trust Strategy and CISA Zero Trust Maturity Model

Security is part of our DNA

As a full-service IT provider, GDT takes a 360-degree, risk-based approach to cybersecurity, offering comprehensive lifecycle security and compliance services. GDT has a proven track record of helping clients fortify their digital defenses against security threats and vulnerabilities. Our highly skilled and experienced team of experts is committed to delivering the highest level of service and protection.

GDT takes a modern cybersecurity mesh approach designed for the distributed enterprise – allowing security to be extended confidently where it is most needed. We recognize our client's need to adapt security measures to their evolving needs, whether they are expanding their infrastructure, adopting new technologies, or accommodating a distributed workforce. Our goal is to ensure that security remains an enabler rather than an obstacle to progress, allowing you to pursue new business opportunities and technologies while effectively managing cybersecurity risks.

Contact us

www.GDT.com/solutions/security
www.gdt.com/contact-us