NIGHTWING

# ZERO TRUST FRAMEWORK

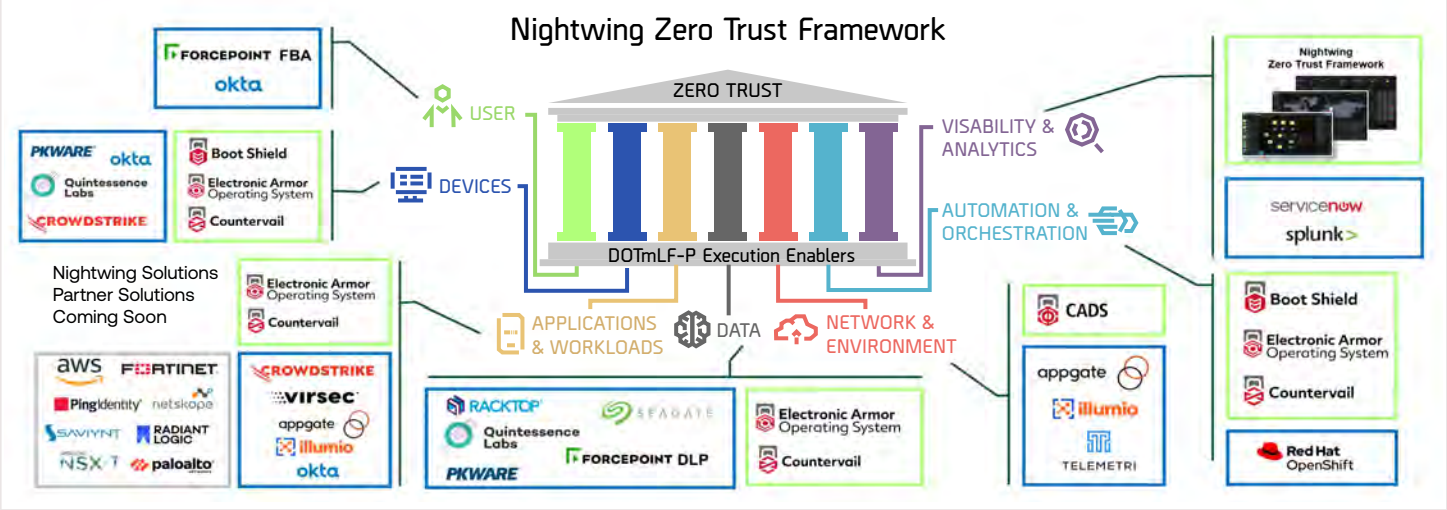
## WE DON'T JUST WORK ON THE CUTTING EDGE. WE CREATE IT.

The Nightwing Zero Trust Framework provides a non-disruptive path for organizations to achieve enterprise-level Zero Trust across all pillars of the DOD Zero Trust Reference Architecture, the CISA Zero Trust Maturity Model, the NIST SP 800-207 Zero Trust Architecture, and Forrester Research's commercially adopted Zero Trust Extended model. As an open integration framework, it facilitates the interoperability needed to design architectures that achieve capabilities and activities identified in the DoD Zero Trust Strategy.

Available as pre-built containerized or virtualized solutions, the Nightwing Zero Trust Framework is ready for implementation into vSphere, Red Hat OpenShift, Rackspace, AWS, or bare-metal infrastructures. Its use of common containerization technologies allows speed and ease of deployment at the tactical edge, on-premises, and across hybrid and multi-cloud environments, including Azure, Google Cloud, Oracle Cloud, or IBM Cloud. The framework is deployable to any environment: standalone, on-premises, hybrid, cloud, multi-cloud, or DDIL.

### Harness Your Zero Trust Architecture

- ***Open API.*** *Avoid proprietary integrations and leverage the technologies that are right for your environment.*
- ***Enterprise-wide Policy Enforcement.*** *Correlate cyberthreat detection and response across all pillars of Zero Trust.*
- ***Federation.*** *Embrace distributed enterprises, including Disconnected, Intermittent, and Low bandwidth (DDIL) environments.*
- ***Cyber Resiliency.*** *Leverage Zero Trust to anticipate, withstand, recover from, and adapt to enterprise threats.*
- ***Extensibility.*** *Enhance situational awareness by establishing Zero Trust workflows for your security and network operations centers.*




*The Nightwing Zero Trust integrated ecosystem provides best-of-breed technologies to accelerate your Zero Trust journey.*

## Streamline Zero Trust Adoption

### Ready, Out-of-the-Box.

Provides access to best-in-class Zero Trust solutions with mix and match options combined with Nightwing's best-in-class cyber resiliency tools.

### Seamless Integration.

Ensures rapid integration with your existing security infrastructure, including custom and legacy IT security systems, preserving current investments.

### Flexible Customization and Adaptability.

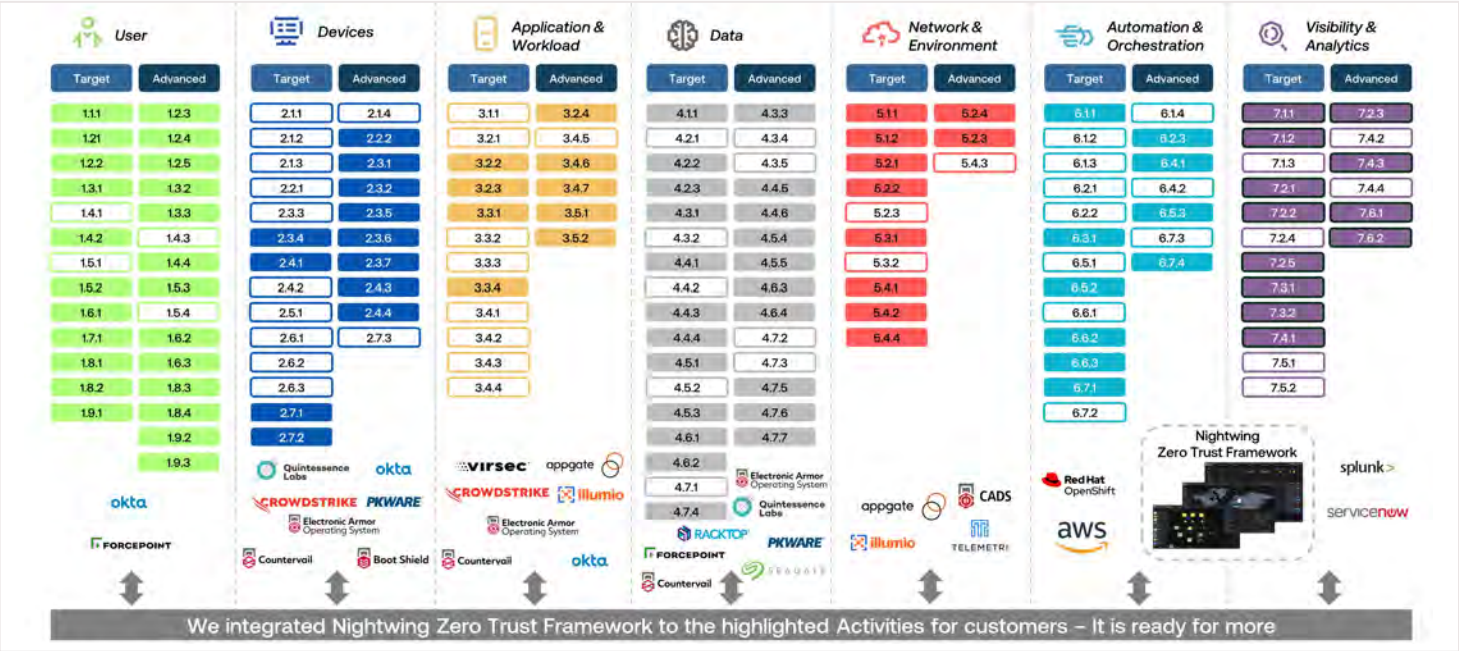
Tailored to suit any environment, the Nightwing Zero Trust Framework supports on-premises, cloud, multi-cloud, and hybrid deployments.

### Deliver Zero Trust to the Tactical Edge.

Harnesses the power of both Zero Trust and Nightwing's Cyber Resiliency technologies, ensuring robust and adaptable protection.

We implement our highly scalable framework alongside existing Zero Trust-capable infrastructure or in conjunction with initiatives to deploy new Zero Trust technologies within an organization's Information Technology, Operations Technology, or mission systems environments. This allows the Nightwing Zero Trust Framework to serve as an open integration harness that extends Zero Trust interoperability and policy enforcement from a single Zero Trust pillar to all other pillars.

***Nightwing is ready with the people, processes, and technologies needed to help you succeed on your journey to Zero Trust.***




*Example coverage of DoD Zero Trust Strategy 55 target & 44 advanced activities using the Nightwing ZeroTrust Framework & Zero Trust integrated ecosystem*

**Contact**
Nightwing
22270 Pacific Blvd.
Sterling, VA 20166
cyber-Resiliency@nightwing.com

nightwing.com

NIGHTWING