FORCEPOINT

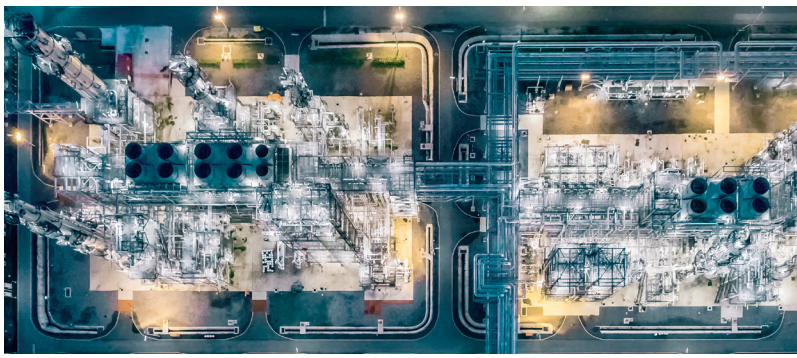
CRITICAL INFRASTRUCTURE SECURITY

Security and visibility across the OT/IT boundary

Our nations, economies, and lives rely on a backbone of critical infrastructure industries. Today, more than ever, these industries are at increasing risk of a malicious cyberattack. Effective protection against these attacks requires flexible solutions that can adapt to their unique industrial contexts and challenges while being strong enough to keep out even the most persistent or advanced adversary.

We cannot afford a siloed approach to critical infrastructure protection, where information technology (IT) or operational technology (OT) systems are managed separately. Forcepoint has a true end-to-end approach to cybersecurity—from mission-critical, end-user devices to the most sensitive, strategic, and operational cloud defense environments—delivering the security and visibility required through all levels of an industrial control environment.

- Protecting operational systems while permitting secure connections and communications with external systems—other OT systems, IT systems, or the internet—for integrated enterprise visibility and operational efficiencies
- Enabling the secure movement of data between physically segregated OT and IT systems, greatly reducing the risk of compromise on either side
- Securing business systems with a risk-adaptive, human-centric approach to protect people and data from end-user devices to the cloud



OUR APPROACH

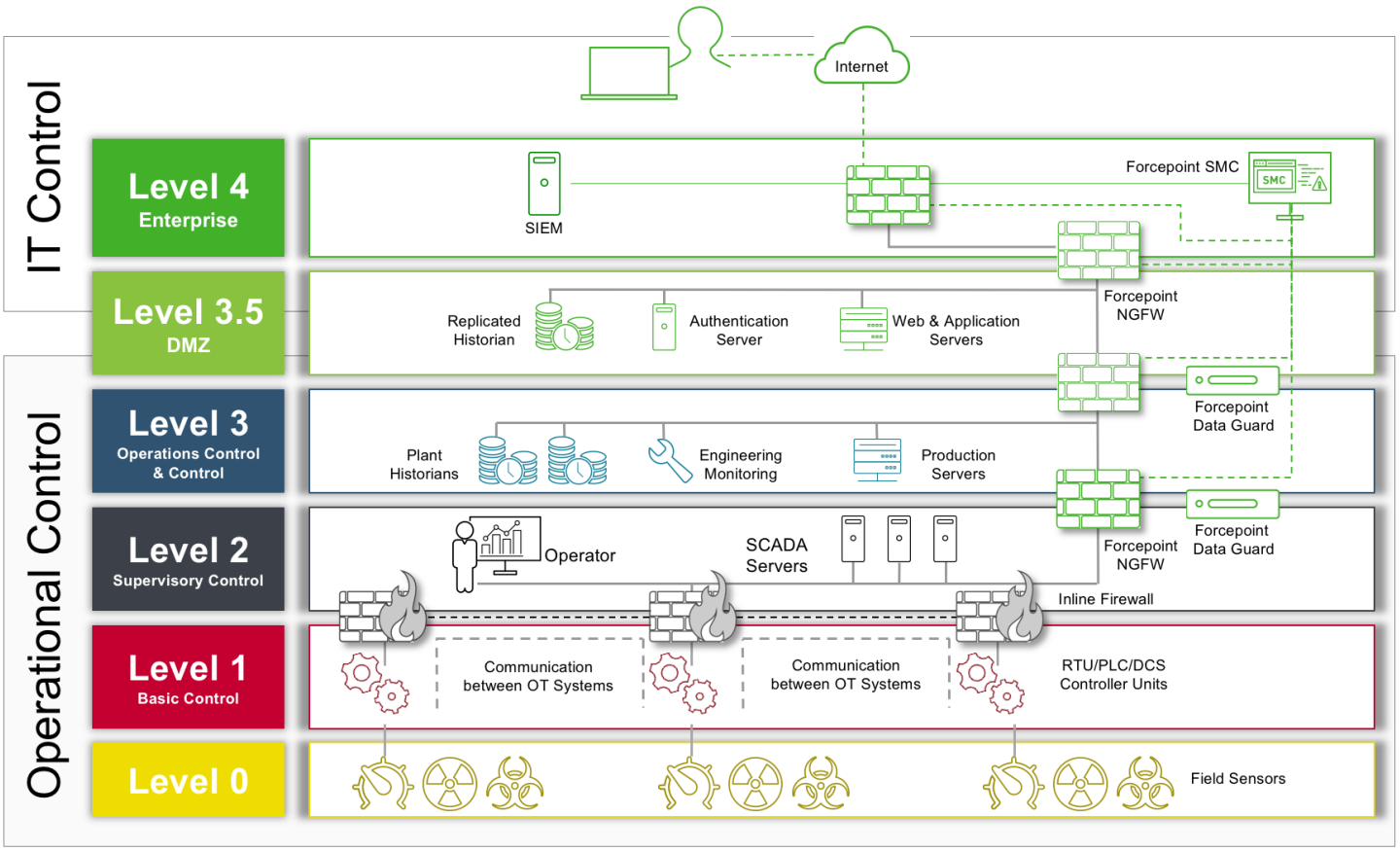
Forcepoint brings unique, proven experience to help our customers address their IT and OT enterprise cybersecurity needs.

- More than 20 years enabling the secure connection between physically separated and sensitive networks in the most challenging environments
- Leaders in enabling secure data sharing between entities (e.g., threat intelligence between public and private sector)
- 1000s of customers protecting the world's most sensitive data and networks
- 100% focused on our customers' missions around the globe. High-consequence missions are in the Forcepoint Global Governments & Critical Infrastructure DNA
- Firewall and Guard solutions, such as Forcepoint NGFW and Forcepoint Data Guard, secure traffic flow above and below the DMZ (Level 3.5), allowing for visibility through the full IT/OT stack

One of the primary challenges faced by critical infrastructure sectors, whether in critical manufacturing, energy, defense industrial base, government facilities or any other sector, is that of unified visibility throughout the IT and OT stack. Forcepoint solutions specialize in providing secure means to remotely manage communications and move data between and across all levels of IT and OT control without risk to availability.

The diagram below highlights where Forcepoint NGFW or Forcepoint Data Guard can be used to provide this visibility both above and below the DMZ (Level 3.5). Forcepoint Data Guard is unique in that it enables visibility with strict traffic segmentation in highly regulated environments where a firewall is not permitted and where a hardware diode may not be well suited.

Conceptual placement of Forcepoint solutions in "always on" environments



CONTACT
www.forcepoint.com/contact

PLEASE VISIT:
www.forcepoint.com/solutions/critical-infrastructure

ABOUT FORCEPOINT
Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. Based in Austin, TX, Forcepoint supports more than 20,000 organizations worldwide. For more about Forcepoint, visit www.forcepoint.com and follow us on Twitter @ForcepointSec

[FP_CIP-FLYER_G2CI] 082418