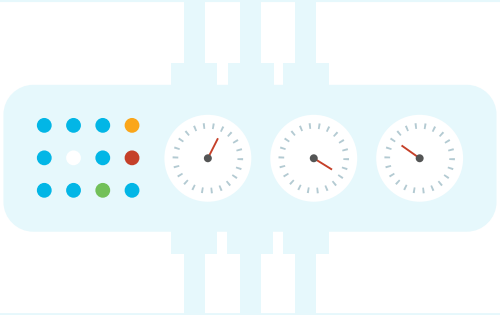
Do you have a defense-in-depth security strategy?

TAKE THE SELF-ASSESSMENT

1 Procedural security

- [ ] Are all of your policies and procedures documented?
- [ ] Has your staff been trained on policies and procedures?
- [ ] Are all policies uniformly enforced across sites and facilities?

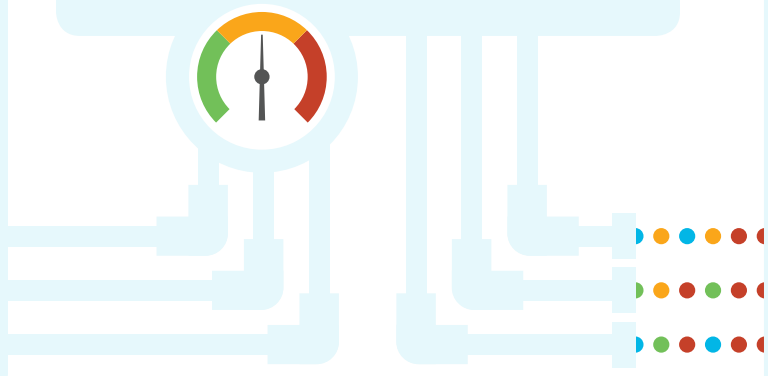


2 Physical security

- [ ] Do you use surveillance technology for live monitoring?
- [ ] Have you mapped out all of your machinery, equipment, business systems, people, and other assets?
- [ ] Have you assessed, ranked, and prioritized your most critical assets?
- [ ] Have you outlined who has access to which machines and devices?
- [ ] Do you limit physical access to security devices and critical infrastructure?

3 Electronic security

- [ ] Do you use only managed switches on your production floor?
- [ ] Is your network segmented into zones and conduits?
- [ ] Are you using industrial DMZs between industrial and external networks?
- [ ] Do you have centralized control of both OT and IT network security?
- [ ] Does your network support context-aware access management for staff, vendors, and partners?
- [ ] Is your network edge protected with:
  - Firewall and intrusion prevention?
  - Remote access VPN?
  - Deep packet inspection?
  - Current industry standard protocols?
- [ ] Do you have a patching plan in place that includes risk evaluation and reaction plans?
- [ ] Can your network quickly provision and securely adapt to new connections?



Not seeing as many check marks as you'd like?

LEARN MORE ABOUT CISCO CONNECTED FACTORY SOLUTIONS AT cisco.com/go/manufacturing