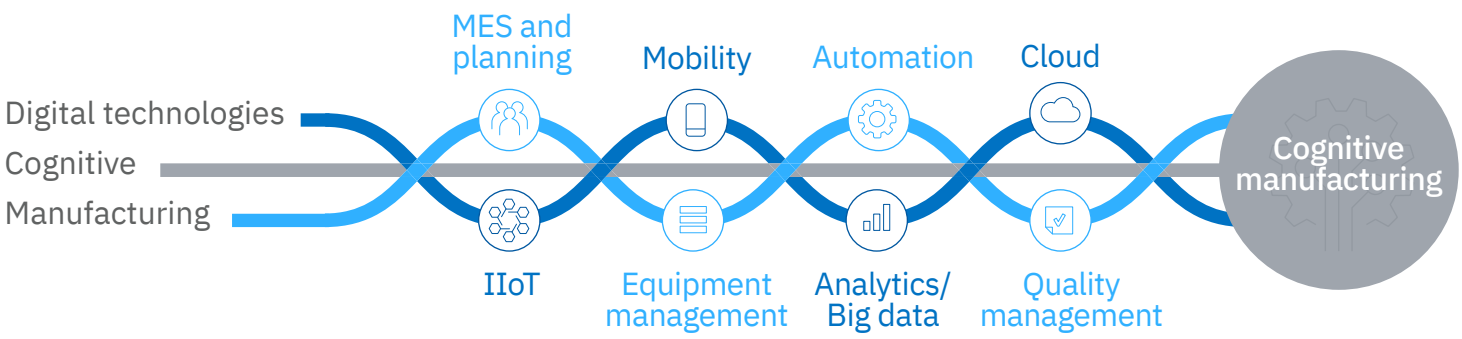
Electronics Industrial Internet of Things cybersecurity

As strong as its weakest link

The IIoT is a core component of cognitive manufacturing



IIoT technologies are applied widely in electronics plants and assembly lines, with the potential for vastly improved operational efficiencies

65% Real-time equipment monitoring

58% Predictive maintenance

52% Asset/equipment monitoring

45% Machine/ industrial automation

43% Automated workflow

However, unprotected sensors and devices expose IT-OT (operational technology)-IIoT networks to significant risk

82% of electronics companies surveyed are deploying IIoT technologies without fully evaluating the risks

91% of electronics companies surveyed do not perform regular IIoT cybersecurity assessments

82% of electronics companies surveyed do not have a formally established IIoT cybersecurity program

Early leaders differentiate in three areas by applying a risk- and compliance-based approach to security while focusing on nine practices

Protecting data throughout the IIoT ecosystem

1. IIoT device user privacy controls
2. IIoT authentication for user verification
3. Clear service-level agreements for security and privacy

Protecting IIoT devices throughout their lifecycles, keeping security systems up to date

4. Inventory of authorized and unauthorized software
5. Automated scanning of connected devices
6. IIoT devices with built-in diagnostics
7. Secure and hardened device hardware and firmware

Augmenting detection and response with automation and cognitive intelligence

8. Advanced behavioral analytics for breach detection and response
9. AI technology to enable real-time security monitoring and response

Are your IIoT-enabled plants and assembly lines secure? To learn more, visit: ibm.biz/electronicsiiot

ibm.com/iibv

41020141USEN-01