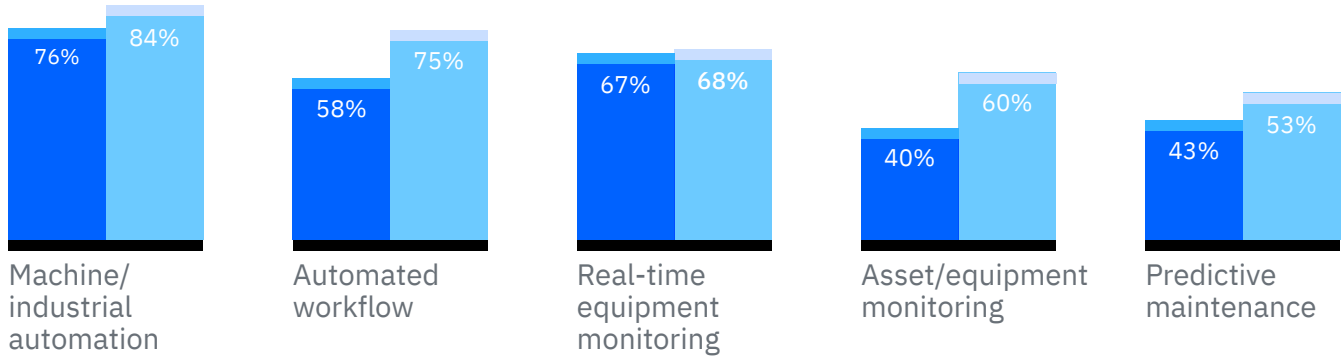


Automotive Industrial Internet of Things

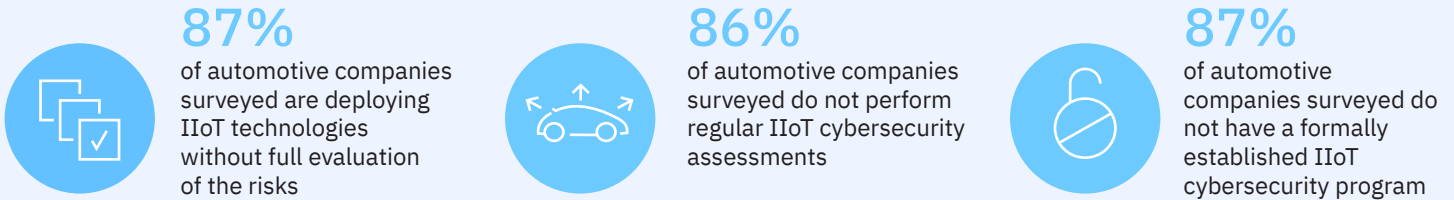
Quick to implement, slow to secure

IIoT technologies are widely adopted in automotive plants and assembly lines

OEMs Suppliers



Unprotected sensors and devices expose operational technology (OT)/ IIoT networks to significant risk



Top performers 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 system up to date

- 4 Inventory of authorized and unauthorized software
- 5 IIoT devices with built-in diagnostics
- 6 Automated scanning of connected devices
- 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/autoiiot