Cybersecurity in Manufacturing:

Cyberthreats targeting the Factory
Protecting the path to digital manufacturing

1. 20%
   By 2021, 20% of the largest manufacturers will depend on secure backbone intelligence to automate processes

2. 1/3
   By 2020, one-third of all manufacturing supply chains will be using analytics-driven cognitive capabilities

3. 15%
   By 2019, 15% of data-intensive and supply chain processes manufacturers will be using cloud-based execution models

IDC FutureScape: Worldwide Manufacturing 2018 Predictions

The very nature of manufacturing creates cybersecurity challenges that other industries do not face

Manufacturing is the 2nd most attacked industry behind Financial Services

Evolution of malware/botnets

Sabotage of Operations

Logical attacks against physical infrastructure

Operational Downtime

Compliance

Stealth of Intellectual Property & Sensitive Data

This sector is more susceptible to cybercrimes because companies in manufacturing have not fully realized the importance of cybersecurity yet. They are not fully ready and equipped to cope with an attack. And now cyber criminals know this. – 2017 Infoguard security
Safeguard your organization with a multi-layer approach powered by Threat Intellect®, advanced data analytics, to help protect against security breaches.

To learn more about AT&T Cybersecurity Consulting, visit www.att.com/security-consulting.

© 2018 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo and other marks are trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.