The Network is the Cornerstone of Digital Success or Failure

integratedworks
WE CONNECT

CISCO

15 maart 2018 ••• Hart van Holland Nijkerk

Industrial Ethernet

integratedworks
WE CONNECT

Is Your IoT Strategy Ready for Digital Business?

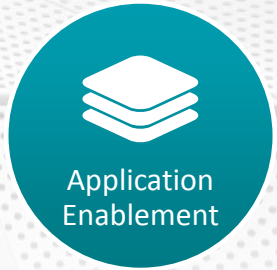
Can you support the growing number of devices in different environments?

Can you provide the secure connectivity for IT & OT convergence and support standard protocols for interoperability and scale?

Can you efficiently analyze and manage data from the edge to the cloud?

Can you provide the infrastructure and tools necessary to combine IoT analytics with business analytics?

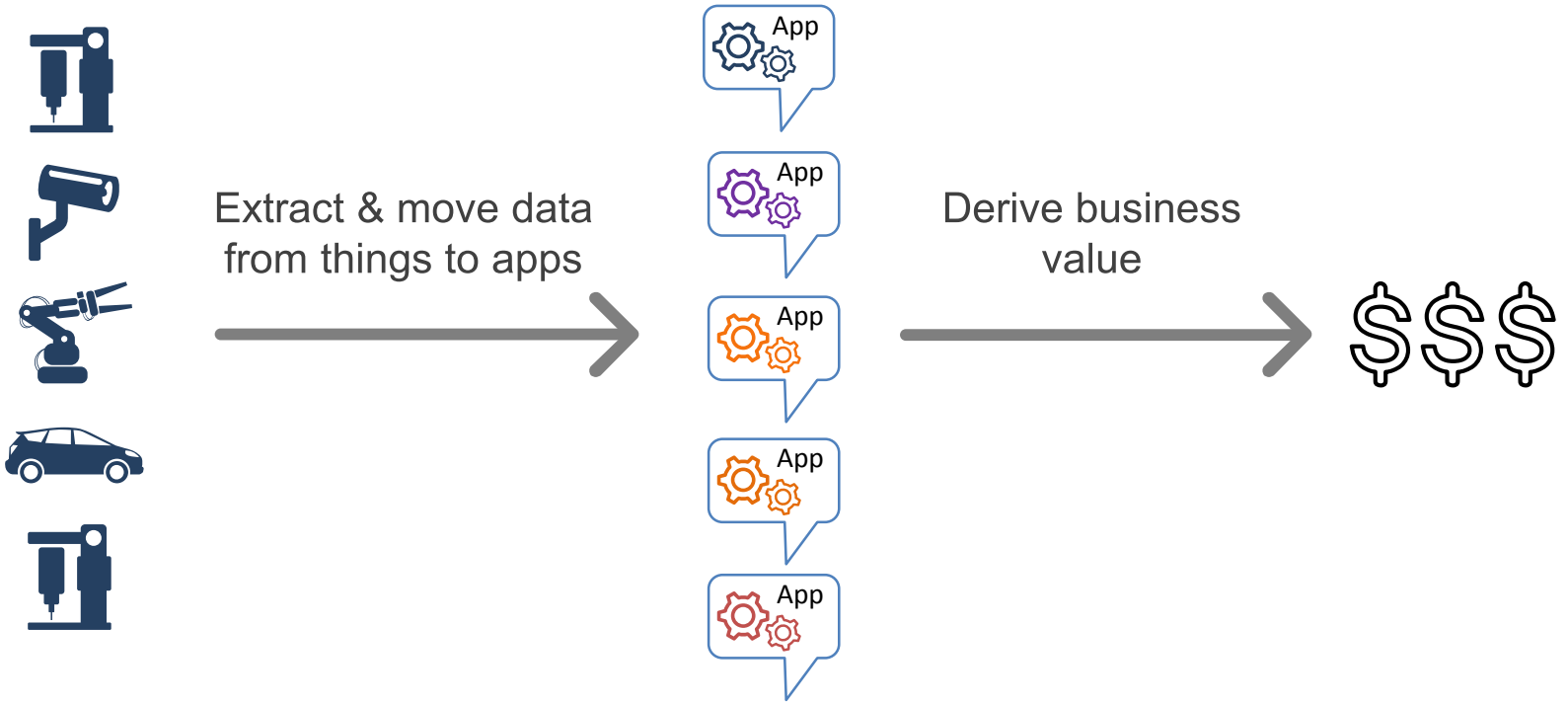
Can you enable convergence of OT and IT networks to create and enforce a consistent policy across the entire Enterprise?



Can you assist in the creation of highly sophisticated applications needed for your business?

integratedworks
WE CONNECT

To get value from data



integratedworks
WE CONNECT

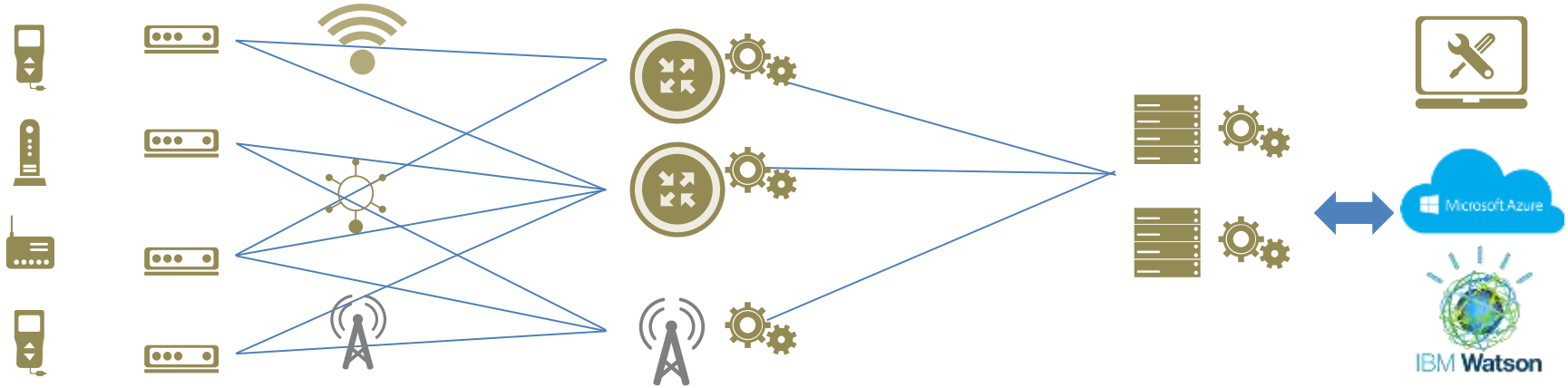
Sensors / Endpoint

Gateways

Routing & Switching

Enterprise Data Centers

Cloud / Applications



1. Fast and secure on-boarding of IoT devices to the network
2. Multiple access methods: Ethernet, WiFi, 3G/4G, LoRa, Mesh, NB-IoT...
3. Isolates network traffic of IoT devices with segmentation and prioritization
4. Meet environmental needs with portfolio of industrialized network products
5. Provides real-time visibility and control of connection to each IoT device

integratedworks
WE CONNECT

Key Challenges for Traditional Networks

Difficult to Segment

Ever increasing number of users and endpoint types

Ever increasing number of VLANs and IP Subnets

Complex to Manage

Multiple steps, user credentials, complex interactions

Multiple touch-points

Slower Issue Resolution

Separate user policies for wired and wireless networks

Unable to find users when troubleshooting

integratedworks
WE CONNECT

IT and operations

Digital business strategy

People and culture

Analytics

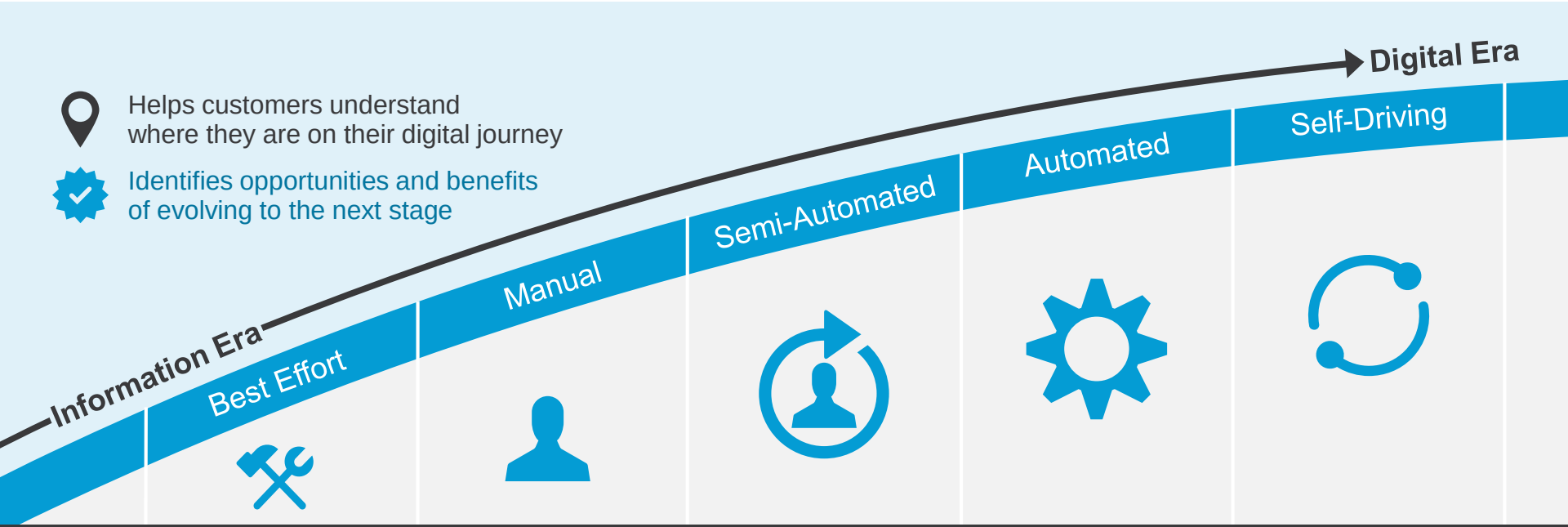
Security

Technology and orchestration

Must come together!

integratedworks
WE CONNECT

Digital Network Readiness Model



The Digital Network Readiness Model follows the standard five stages of maturity adopted broadly in business and consulting communities

Details of the Five Categories

Stage / Domain	Best Effort	Manual	Semi-Automated	Automated	Self-Driving
Architecture	Siloed, hardware/ device-centric	End to end, hardware/ device-centric	Hybrid hardware/ device-centric and software centric	End to end, software-centric	Fully integrated, software-centric, policy-driven
Automation	Manual device configuration	Basic configuration automation	Controller-based per-domain automated provisioning	Controller-based, network-wide automated provisioning	Automated provisioning of devices in self-organized, self-diagnosing and dynamically updated network
Security	Fragmented policy and limited device detection	Centralized policy and basic access controls	Unified policy management and dynamic enforcement	Rapid threat containment	Continuous self-learning threat control
Service assurance	Manual quality of service (QoS) policy definition	Orchestrated manual application optimization	Controller-based quality of experience (QoE)	Controller-based QoE and validation of experience (VoE)	Automated business service/application-aware policy-driven networks
Analytics	Individual device visibility	Alarm-triggered device-level insights	Global centralized insights	Adaptive and preventive insights	Automated and predictive insight

integratedworks
WE CONNECT

Some examples…

integratedworks
WE CONNECT

Context is everything

Poor context awareness

IP Address: 192.168.2.101

Unknown

Unknown

Unknown

Unknown

Unknown

Unknown

Rich context awareness

Operator device

Vendor

Factory-A Floor-1 Zone-B

10:30 AM EST on April 27

Wireless / Ethernet / Zigbee

No Threats / Vulnerabilities

Known

Result

Access to IP (Any Device/User)

Result

Role Based Access

integratedworks
WE CONNECT

Introducing Identity Services

A centralized security solution that automates context-aware access to network resources and shares contextual data

Physical or VM

Identity Profiling and Posture

- Threat
- Vulnerability
- Who
- What
- When
- Where
- How
- Compliant

Context

Access Policy

Traditional | TrustSec®

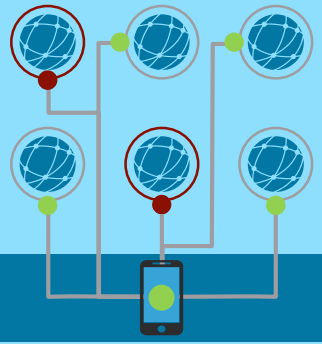
Guest

Enterprise Mobility

Role-Based Access

Threat Containment

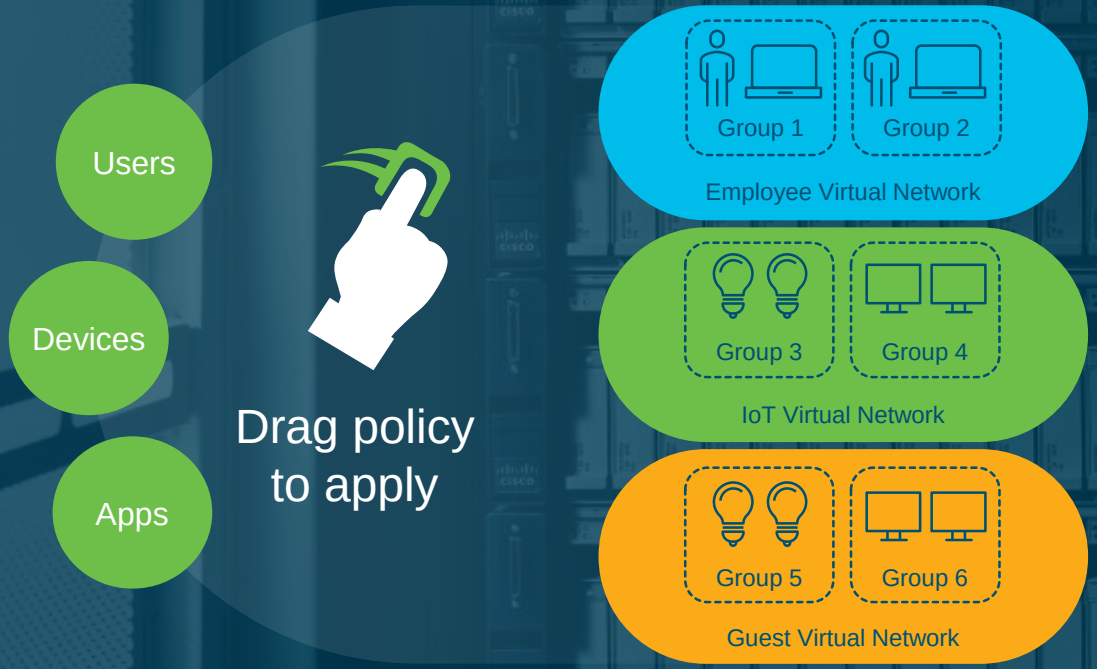
Network Resources



15 maart 2018 ••• Ha ijkerk

Industrial Ethernet

Secure Segmentation and Onboarding: Software Defined Access



IT Simplicity

- No VLAN, ACLs or IP Address management required
- Single network fabric
- Define one consistent policy

Security

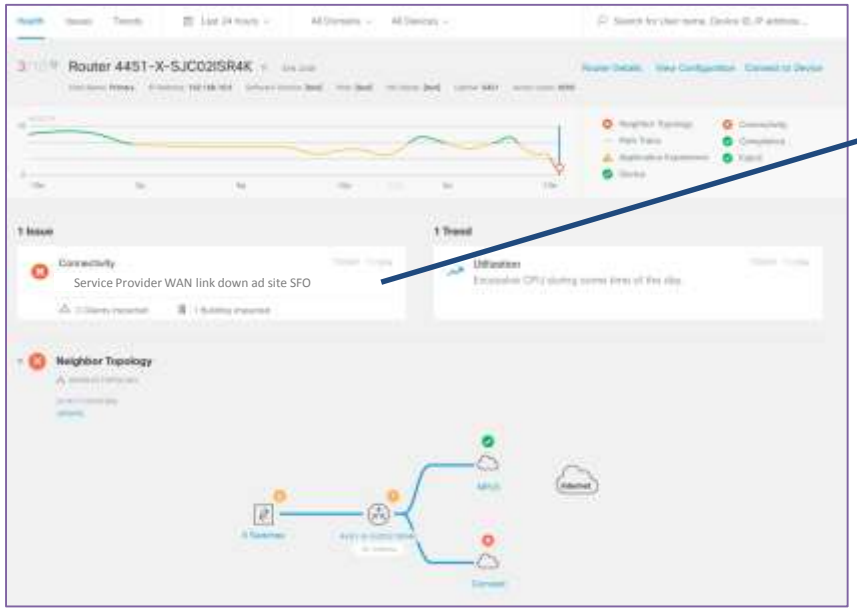
- Simplified Micro-Segmentation
- Policy enforcement

Completely Automated | Policy follows Identity | Minimize Lateral Threat Movement

integratedworks
WE CONNECT

Site connectivity issue

1 **Navigate to site from search of network health**
Check what issue is there



2 **See the details of the issue to get more insights about its effects and get suggestions on how to solve it**

Automate IoT Deployments at Scale

Software Defined Access

Box by Box

Manual | Error Prone

Automation

Scalable | Simple

Design	2 hours	→	15 minutes		
Policy	4 hours	→	5 minutes		
Provision	5 hours	→	5 minutes		

Mass Scalability | Users, Device & IoT Segmentation | Policy-based Automation

Is your Network Digital Ready?

Win a free scan at the booth!

integratedworks
WE CONNECT

Remco Apon
remco.apon@integratedworks.nl

CISCO

Peter Dijkstra
pdijkstr@cisco.com