

# Smart Edge

|Secure| |Intelligent| |Automated|

**Abhishek Kumar**

Business Development Manager- India, Bangladesh, Bhutan & Nepal

# Allied Telesis Group

Established in 1987- Headquartered in Japan

37 group company in 24 countries around the world

Global R&D Facilities- USA, Japan, India, New Zealand,  
Taiwan, Israel, Singapore

Global Manufacturing Facilities- Singapore, Indonesia,  
China & Taiwan

Global Sales Location-65

**VISTA**  
MANAGER

**AMF**<sup>™</sup>

**AWC**



# Allied Telesis Portfolio “end-to-end” connection

Ethernet Switches



Industrial Ethernet Switch



Firewall Router



FTTx



Media Converters



Wireless



Network Adapters



Optical Modules



Management and automation

VISTA MANAGER EX **AMF™** **AMF-Sec™**  
VISTA MINI™ **AMF-WAN™**  
**AWC™** **AWC-CB™** **AWC-SC™**

Support and Service

**Net.AMF** **Net.Cover**  
**Net.Assist** **Net.Monitor**  
**Net.Pro** **Net.Campus**

# Smart City and Safe City

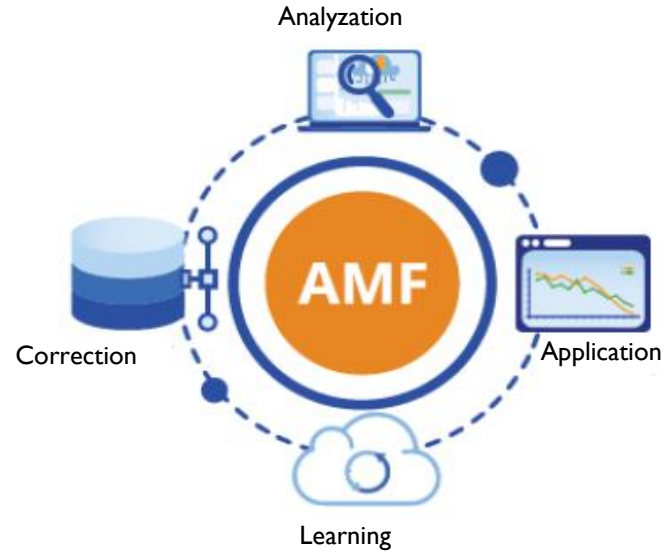
## Smart City

- Vadodara Smart City
- Raipur Smart City
- Agra Smart City
- Dehradun Smart City
- Varanasi Smart City



## Safe City

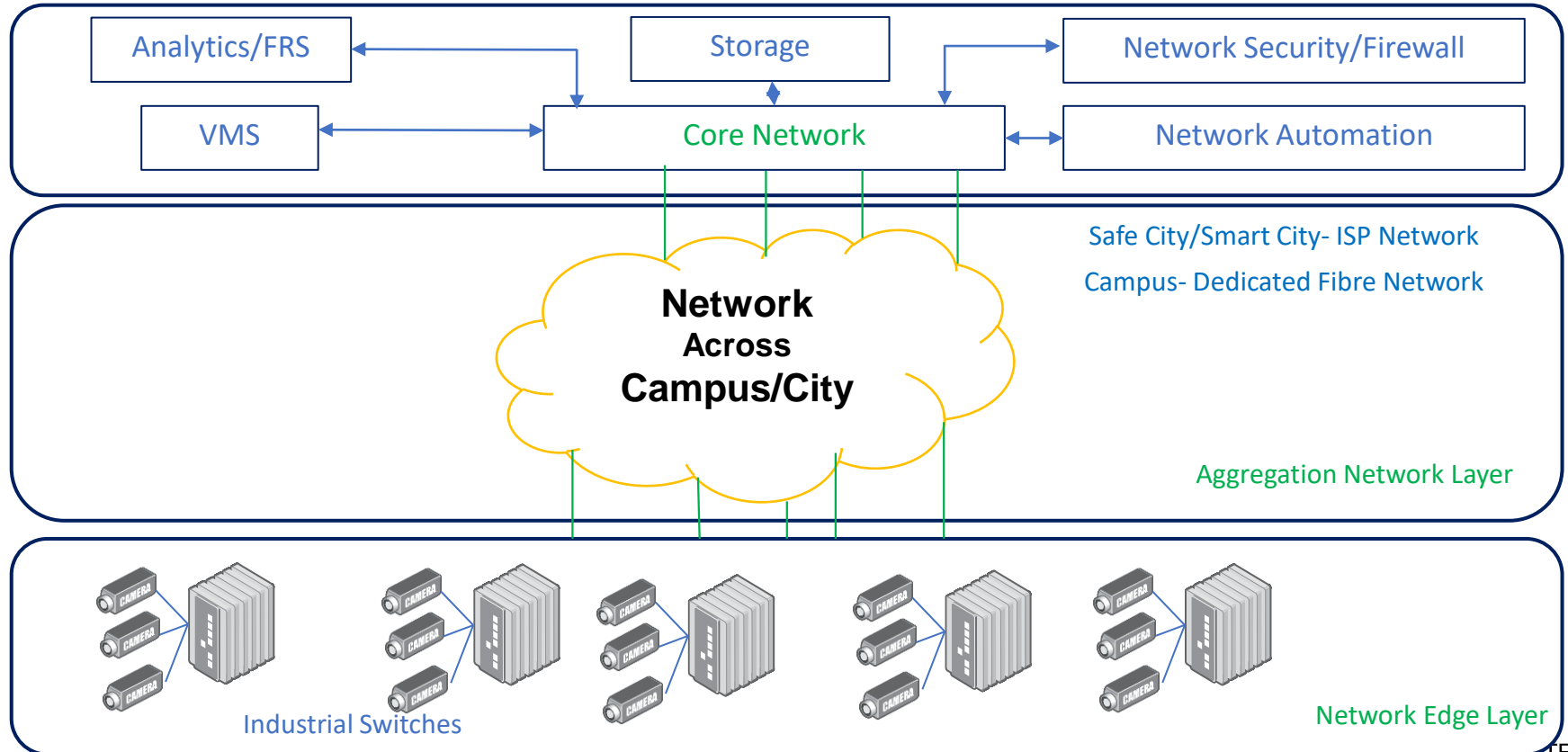
- Rajasthan State 23 Cities Surveillance (under deployment)
  - More than **10,000** switches for **55,000** Cameras
- Telangana and Cyberabad Safe City Project
  - More than **6500** switches for **15,000** Cameras
- Kolkata City Surveillance Phase-I & II
- Delhi City Surveillance – **1400** switches, **6000** cameras
- Dhanbad, Siliguri, Patna, Bhubneshwar, Orissa,
- 100 Police Stations of Tamil Naidu



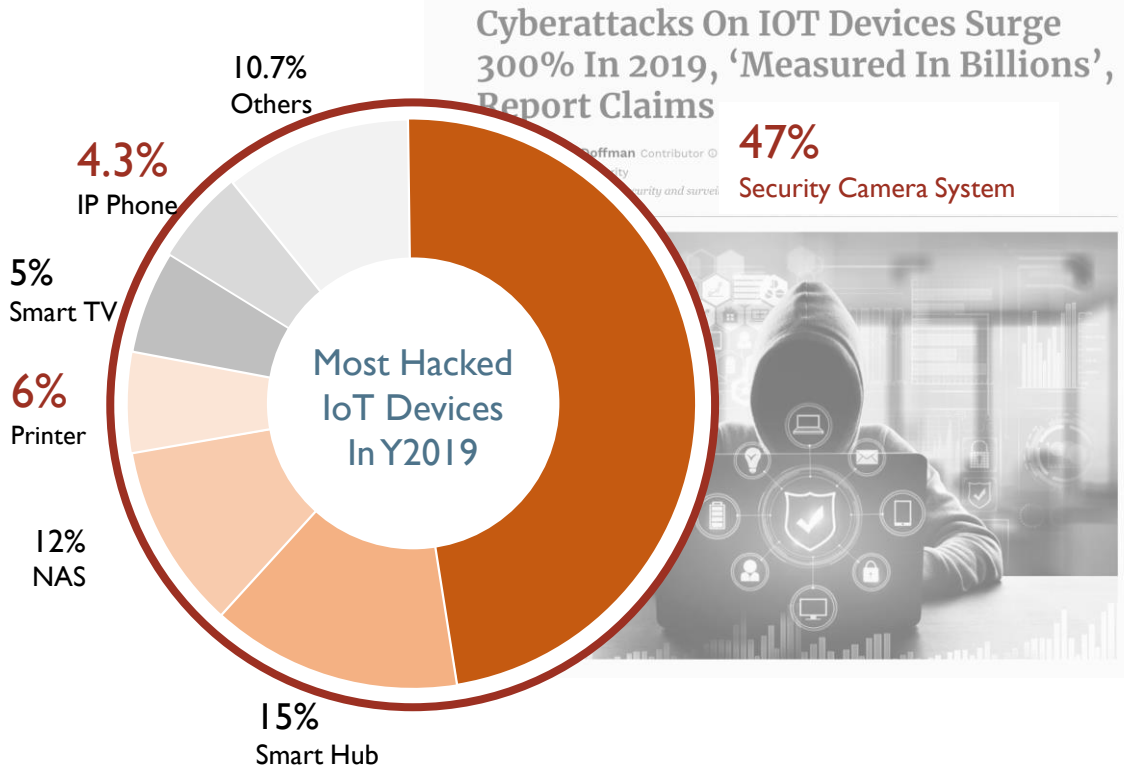
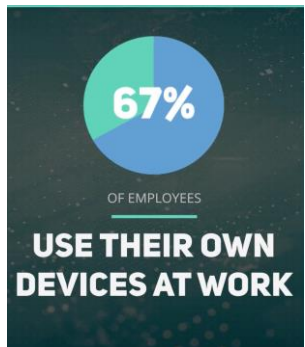
# Smart Edge

|Secure| |Intelligent| |Automated|

# Smart City Design Architecture



# Cyber Attack Trends



# Recent Cyber Attacks!!

## The White House Security

2019- According to The Wall Street Journal, Eight days before Donald Trump's presidential inauguration, the Secret Service received an urgent call saying hackers had seized control of most of the video surveillance cameras that keep watch over the U.S. capital. The Secret Service had been alerted that hackers had seized control of a majority of the cameras that watch over the U.S. capital—eight days before the inauguration. The computer



screens in the command centre where police monitor the camera feeds read,

*“YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!” instead of displaying the regular streaming videos. The hackers demanded \$68,000 in Bitcoin in change for surveillance system control.*



A posted sign on the door of the DPW's water department office. Baltimore City residents were not able to conduct business with the city or pay bills by cash or credit cash at the Abel Wolman Municipal Building because of a ransomware attack on the city's computer system. (Kenneth K. Lam / Baltimore Sun)

EDITORS' PICK | 711,991 views | Dec 14, 2019, 06:51am EST

## New Orleans Declares State Of Emergency Following Cyber Attack



**Davey Winder** Senior Contributor @  
Cybersecurity

*I report and analyse breaking cybersecurity and privacy stories*

## State of emergency declared by City of New Orleans

During a press conference, Mayor Cantrell confirmed that this was a ransomware attack. A declaration of a state of emergency was filed with the Civil District Court in connection with the incident.

www.alliedtelesis.com

Baltimore officials on Wednesday voted to transfer \$6 million from a fund for parks and public facilities to help pay for the devastating impact of the May ransomware attack on the city.

The funds will help pay for “cyber-attack remediation and hardening of the environment,” according to the city’s spending panel, the Board of Estimates, which is controlled by Mayor Bernard C. “Jack” Young.

Cybersecurity

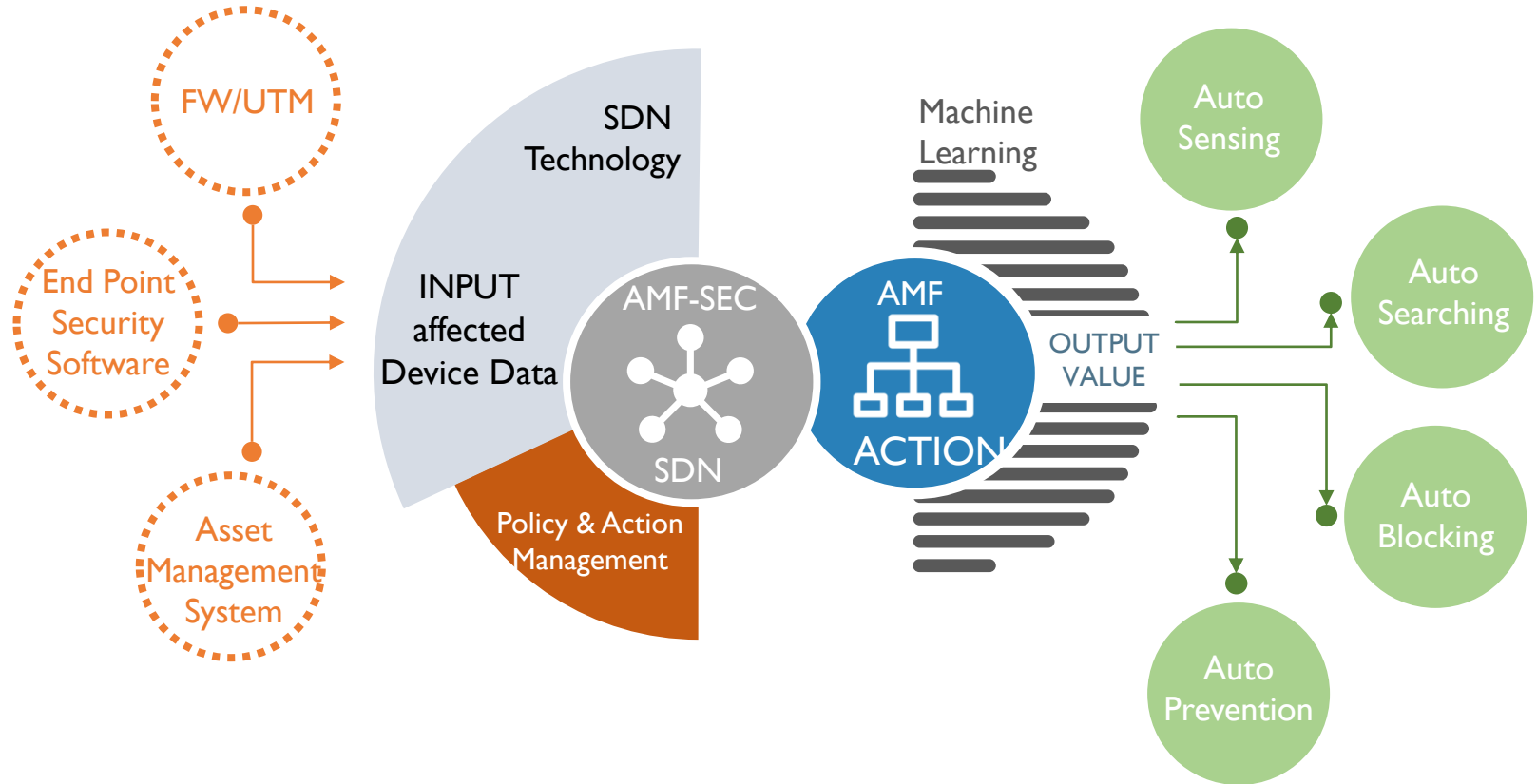
## Louisiana Target of Attempted Ransomware Hack, Governor Says

By [Kartikay Mehrotra](#)

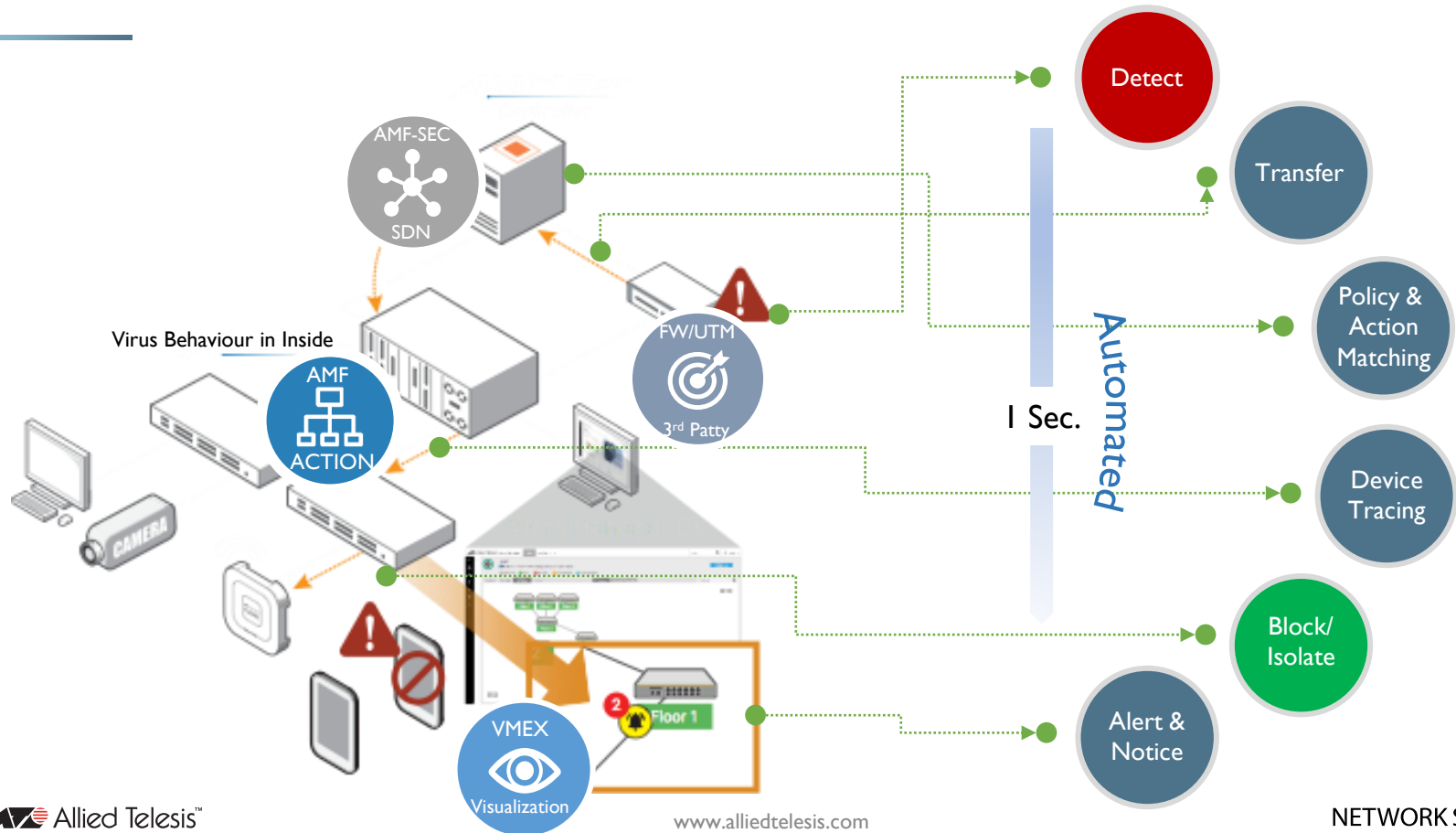
November 19, 2019, 4:51 AM GMT+5:30 Updated on November 19, 2019, 6:36 AM GMT+5:30



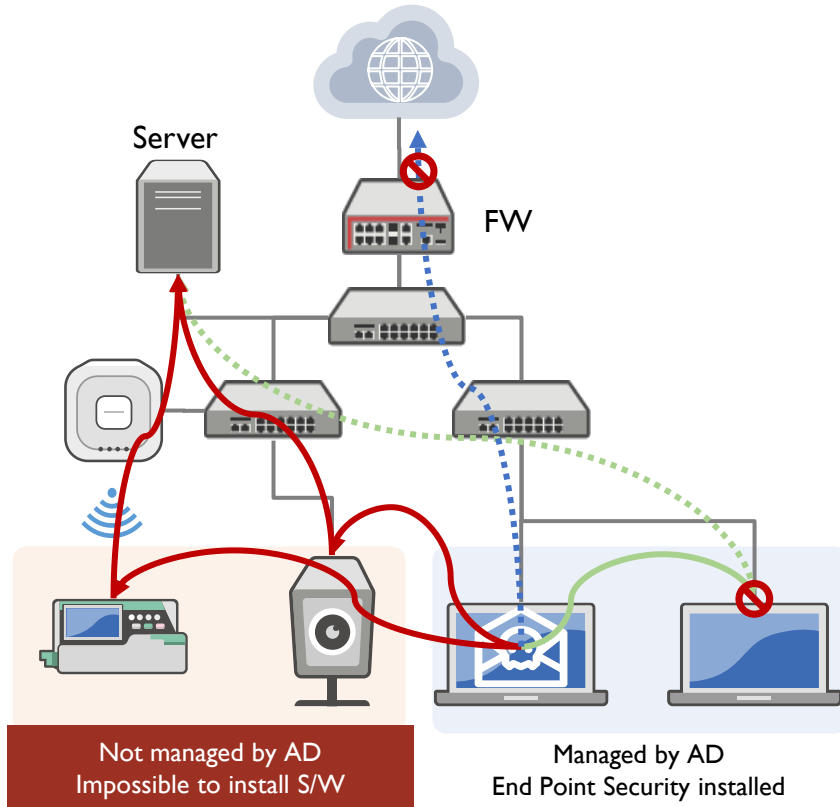
# Software Defined Network to block Cyber Attacks



# SDN Cyber Security- How it Works?



# Blocks Any Infected Device



## UTM/IPS

- ✓ Block virus on the boundary
- ✓ Not block internal & horizontal behavior

**Server Highjacked!**

## End Point Security

- ✓ Block virus on devices
- ✓ No block for machines which can't install S/W

**Server Highjacked!**

## Competitors

- ✓ Block virus behavior on network edge
- ✓ Can't block devices out of AD/Radius Server

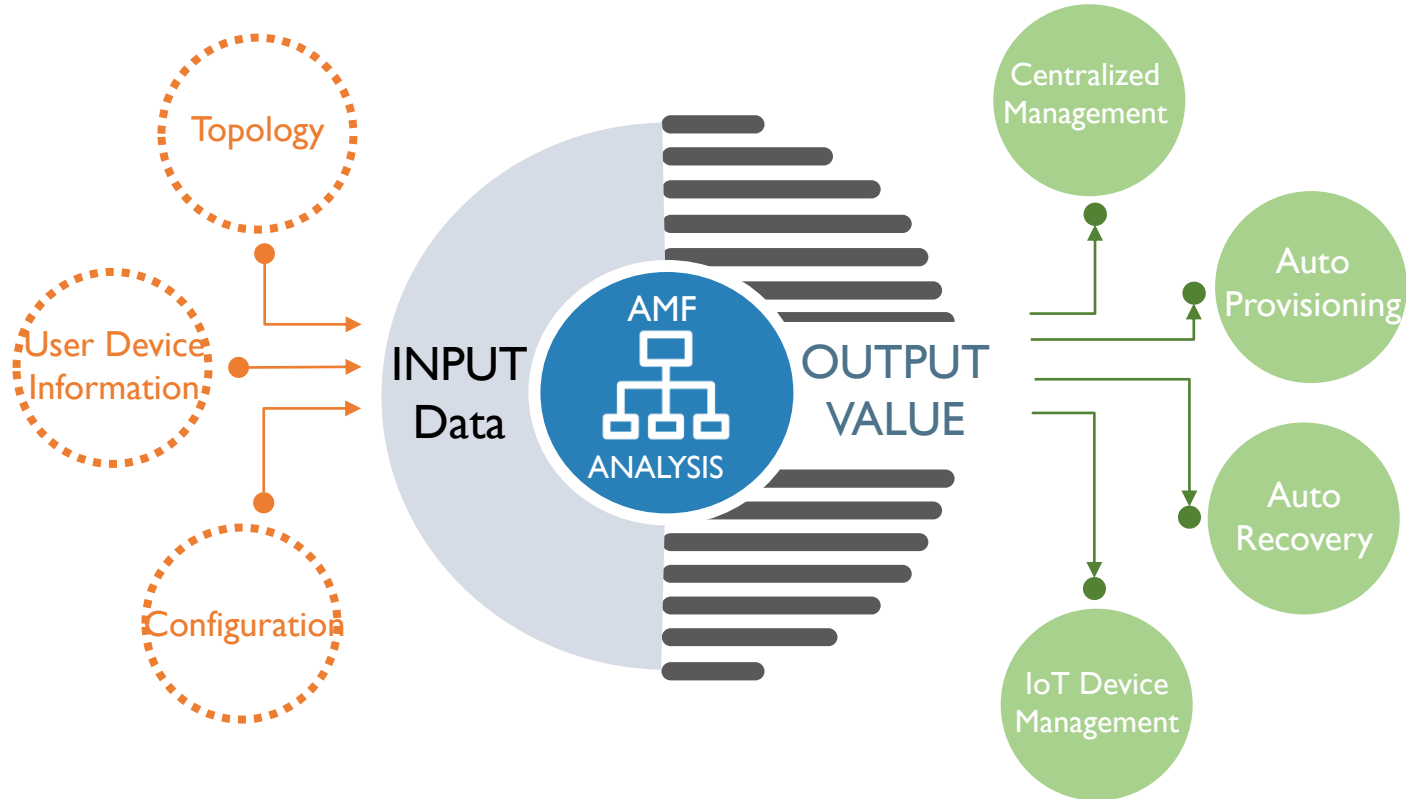
**Server Highjacked!**

## AMF-SEC

- ✓ Block virus behavior on network edge
- ✓ Can block any devices because AMF build own device DB

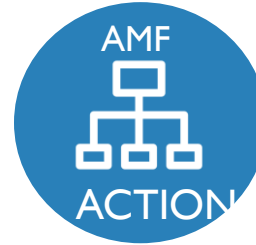
**Server Protected!**

# Automate Network Operations with AI “AMF”



# The IE340 Series – Best Product for Smart City Edge

- Layer 3 Switch 8 and 16x I G Base-T PoE+ and 4x I G SFP slots
- Layer 2/Layer3- RIP, OSPF, BGP, **PIM** for IPv4 and IPv6
- Software Defined Networking- **OpenFlow v1.3**
- Industrial grade **operate reliably and consistently under extreme conditions:**
  - High ambient temperature
  - Electromagnetic disturbance
  - Power/voltage fluctuations
  - Machine vibration and mechanical hazards
- Fanless with wide operating temperature range
  - from **-40°C** to **75°C** (tested at **85°C** for days)
- Certification
  - **NEMA-TS2, EMI EMC IP30**



# Thank you!



Open Up your AI experiences

[abhishek\\_kumar@alliedtelesis.com](mailto:abhishek_kumar@alliedtelesis.com)

Americas Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895  
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830  
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

