Securing the Internet of Things

Cisco ISE and Bayshore Networks

Beth Barach, Scott Pope and Francis Cianfrocca

May 2015

The Internet of Everything (IoE)

People
Connecting People in More Relevant, Valuable Ways

Process
Delivering the Right Information to the Right Person (or Machine) at the Right Time

Data
Leveraging Data into More Useful Information for Decision Making

Things
Physical Devices and Objects Connected to the Internet and Each Other for Intelligent Decision Making

Networked Connection of People, Process, Data, Things

“”The Internet of Things is the intelligent connectivity of physical devices driving massive gains in efficiency, business growth, and quality of life.”

The Trend of Network Threats

Data breaches and theft will continue to be a problem

- Cybercrime is lucrative
- Malware sophistication and ease of use has grown exponentially
- The barrier to entry is low

IoT devices are not designed for cybersecurity

- Some lack basic authentication functionality
- Designed under a model of implicit trust
- Use of unencrypted protocols

More devices mean more to protect

- Do you know the core systems and interconnections to keep your business running?
- How do you prioritize events?
- What's the best use of your resources?

Security is a Primary Inhibitor to IoT Adoption

- **73%** of business decision makers expect IoT to cause security threats to increase in severity over the next two years
- **49%** of business decision makers cite security threats among top application challenges
- **78%** of IT security professionals are either unsure about their capabilities, or believe they lack the visibility and management required to secure IoT devices
- **46%** of IT security professionals do not believe that they have policies in place that can drive the necessary level of visibility and management of IoT devices

IT and OT Are Inherently Different
Architecture

	IT	OT
Control	Centralized	Zone-based
Connectivity	“Any-to-Any”	Context-based (Hierarchical)
Focus	*Top-down:* Operations and systems required to run the business	*Bottom-up:* Plant, Processes and Equipment required to operate and support the business
Reach	Global (WAN)	Local (LAN)
Network Posture	Confidentiality, Integrity, Availability (CIA)	Availability, Integrity, Confidentiality (AIC)
Response to Attacks	Quarantine/Shutdown to Mitigate	Non-stop Operations/Mission Critical – Never Stop, even if breached

IT and OT Are Inherently Different

Attitudes and Behaviors

	IT	OT
Top Priority	Confidentiality • Secure Access • Data Protection • Risk Mitigation	Availability • Continuous Processes • 24/7 Operations
Biggest Fear	Network Intrusion • Loss of Integrity • Data Leakage	Loss of View/Control • Process Shutdown • Threats to Safety
Typical Security Solutions	Cybersecurity • Firewalls • IPS/IDS • Role-based Access Control	Physical Security • IP Cameras • Badge Readers
Weakness	Stringent Security Controls • Complex Passwords • Rigorous Policies	Insecure Behavior • Shortcuts • Improper Hygiene

Network Security with Differential Applications

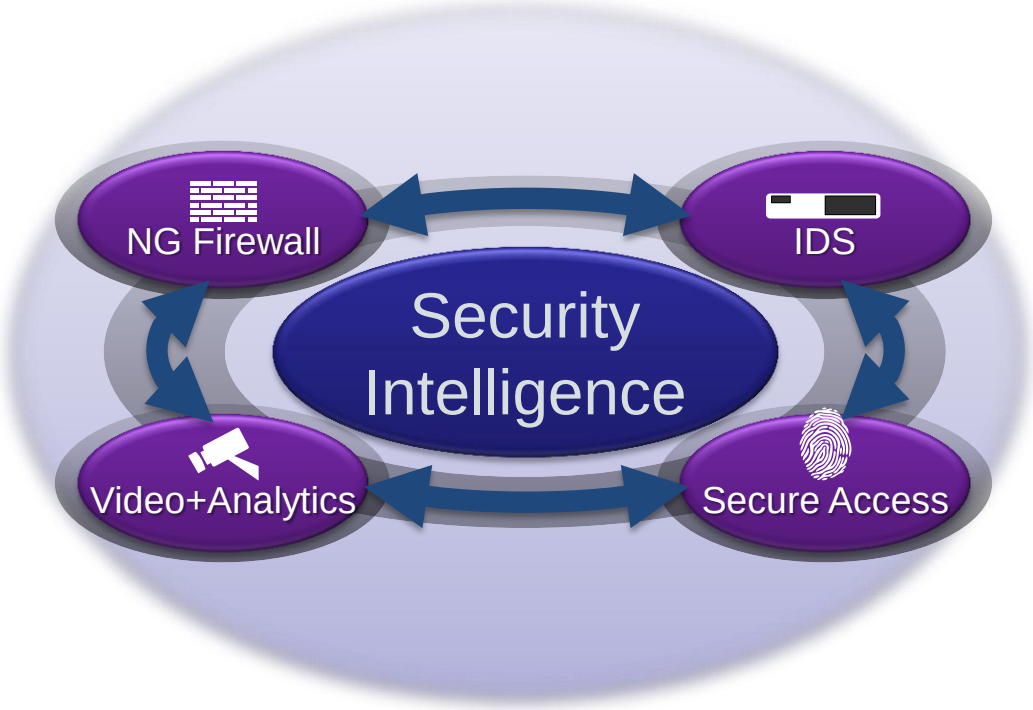
Security Activity	IT	OT
Secure Access	• Role-based access for individuals and groups • VPN/remote access for most systems throughout the network • Complex passwords with lockout policies • Application control	• Role-based access to few individuals • VPN to few systems and users • Badge readers/integrated sensors • IP cameras with video analytics • Simplified passwords (except for the most critical systems)
Intrusion Prevention/Detection	IPS – enforces policies	IDS – sends security alert only
Threat Mitigation	Quarantine affected system	Analysis of the threat to determine appropriate action
Data Integrity and Confidentiality	Data Loss Prevention (DLP)	Insecure Behavior • Shortcuts • Improper Hygiene

IoT Can Actually Increase Security Posture

Network of Security Devices
- Cyber Security
  - Firewall, IDS
- Physical Security
  - IP cameras, badge readers, analytics

Actionable Security Intelligence
- Automated / M2M
- Human Response

Remote Capabilities
- Configuration and Management
- Collaboration Between Groups



Securely Embrace IoT

New challenges require new thinking

- Avoid operational siloes
- Networking and convergence are key
- Sound security solution is integrated throughout
- Build for the future

Security must be pervasive

- Inside and outside the network
- Device- and data-agnostic
- Proactive and intelligent

Intelligence, not data

- Convergence, plus analytics
- Content-aware filtration is essential for secure, scalable IoT

Bayshore Networks

Bayshore Networks

Gartner 2015 Cool Vendor

IT/OT Gateway

- Inspects, dissects and filters industrial application data
  - Leverages Cisco ISE pxGrid and TrustSec technologies
- OT and IIoT cybersecurity policy and enforcement
  - Secure M2M communications
  - Network, protocol and application segmentation/isolation
  - Industrial operations and safety
  - Now available on the Cisco price list

IT Security Practices and Industrial IoT

Standard IT security practices fail in IoT environment

- More machines than computers
- OT machines/robots are static and rarely change
- Many devices on the factory floor share IP addresses

Bayshore and Cisco Content Aware Cybersecurity

- Content based network segmentation and isolation
- Automatic device discovery and mapping by behavior

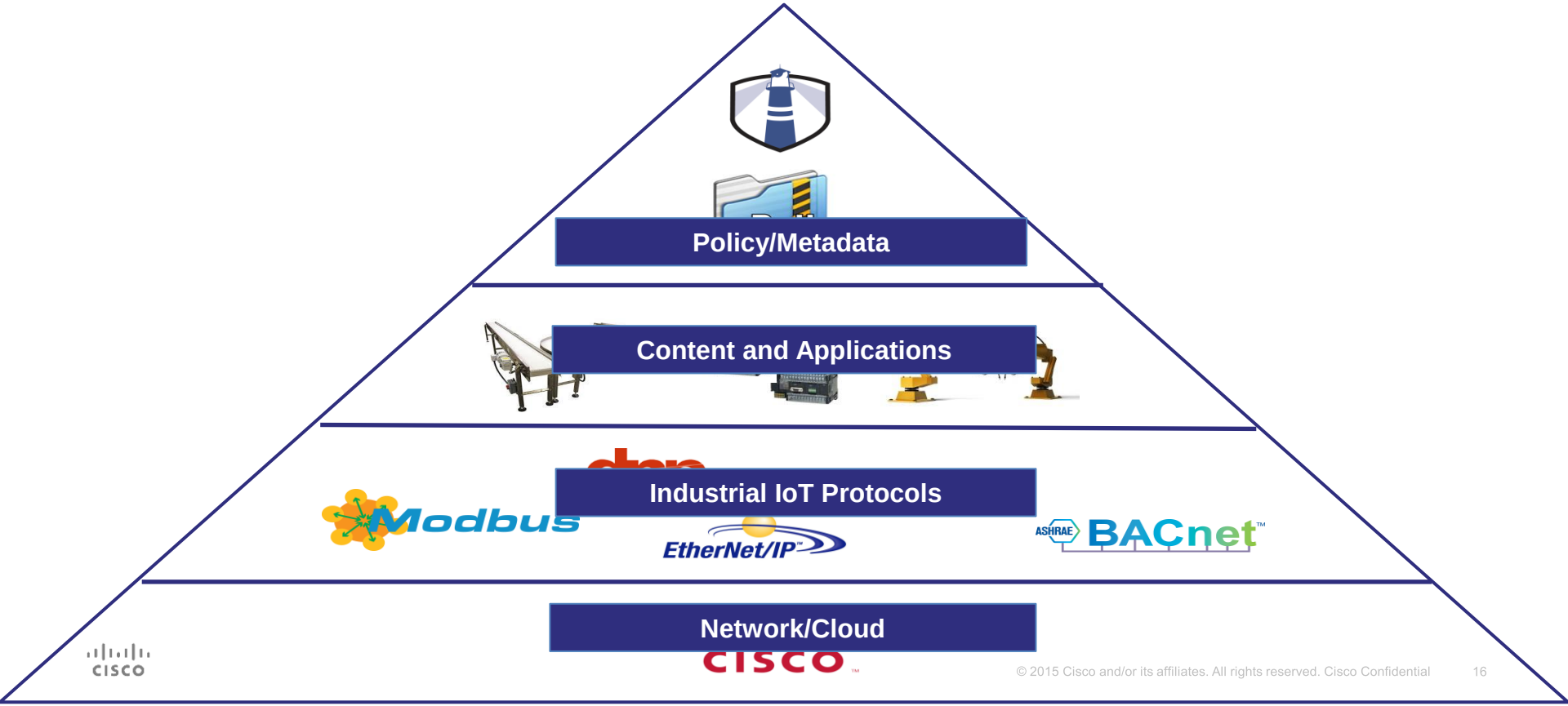
IT and OT Cybersecurity Threats/Questions

Threats to IT	Threats to OT
Malware, Viruses Worms	Life Safety
Information Theft	Operational Disruption
Data Loss, Data Leakage	Production Downtime
Employee Downtime	Physical Damage

OT Requires Machine Specific Protection

Traditional Firewall	Bayshore
Views packets	Looks at transational behaviors, protocols and the entire network flow
Rules based P/F decisions	Content and protocol aware policies
Need to add support for industrial protocals	Rapidly expanding library of industrial protocols . Supports any industrial protocols and transactions at the content layer
Signatures and Application IDs	Machine specific protection down to the data transaction and content layer

Bayshore – Cisco Stack



OT visibility enables business value

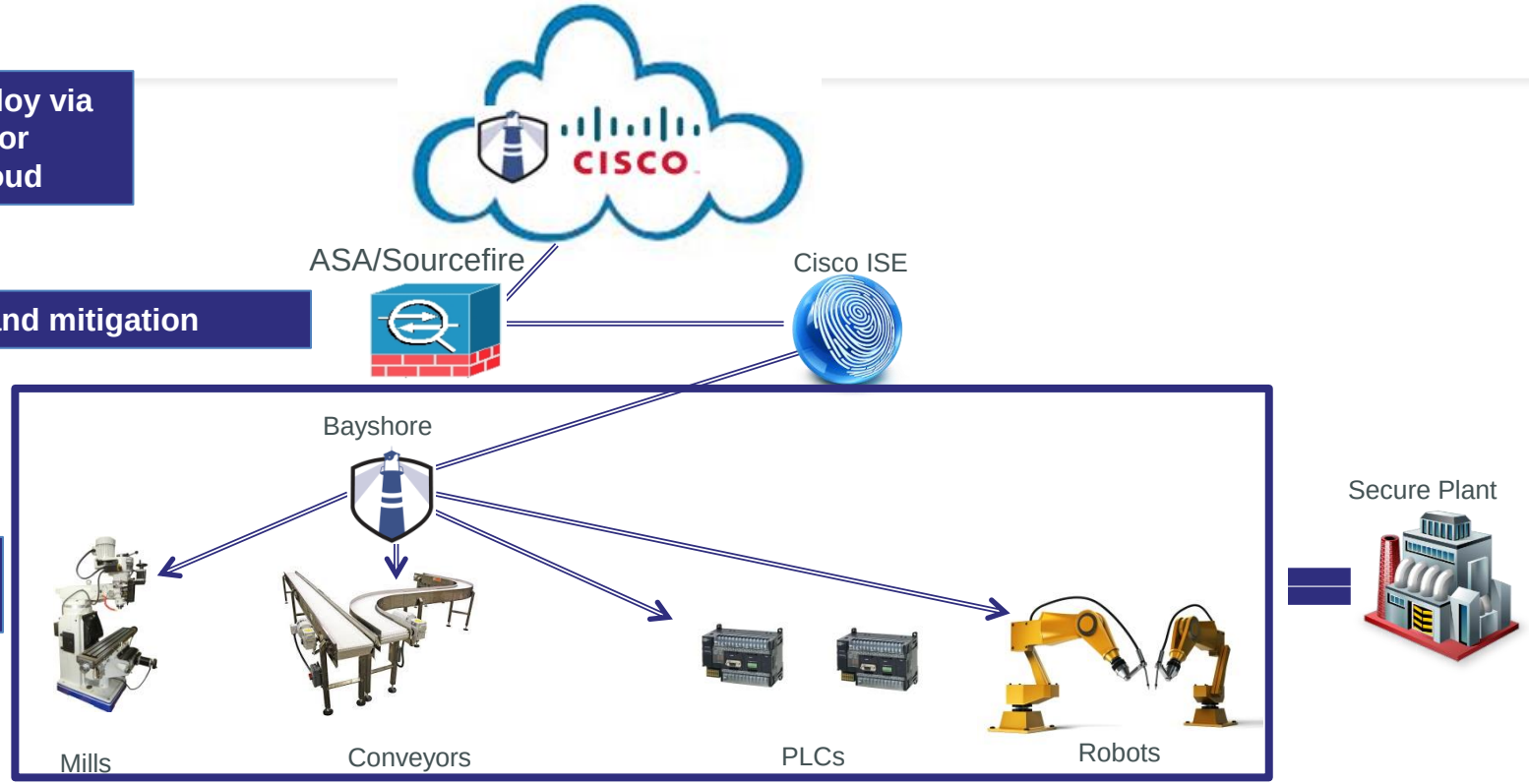
- Prevents disruptions in operational process continuity
- Machine specific attacks are blocked in the cloud
- Efficient centralized management of industrial security signatures and policy changes
- Easily enforces process specific policies such as line-of-sight rules at scale

Cybersecurity for Industrial IoT

Bayshore can deploy via VM on Cisco UCS or from the Cisco Cloud

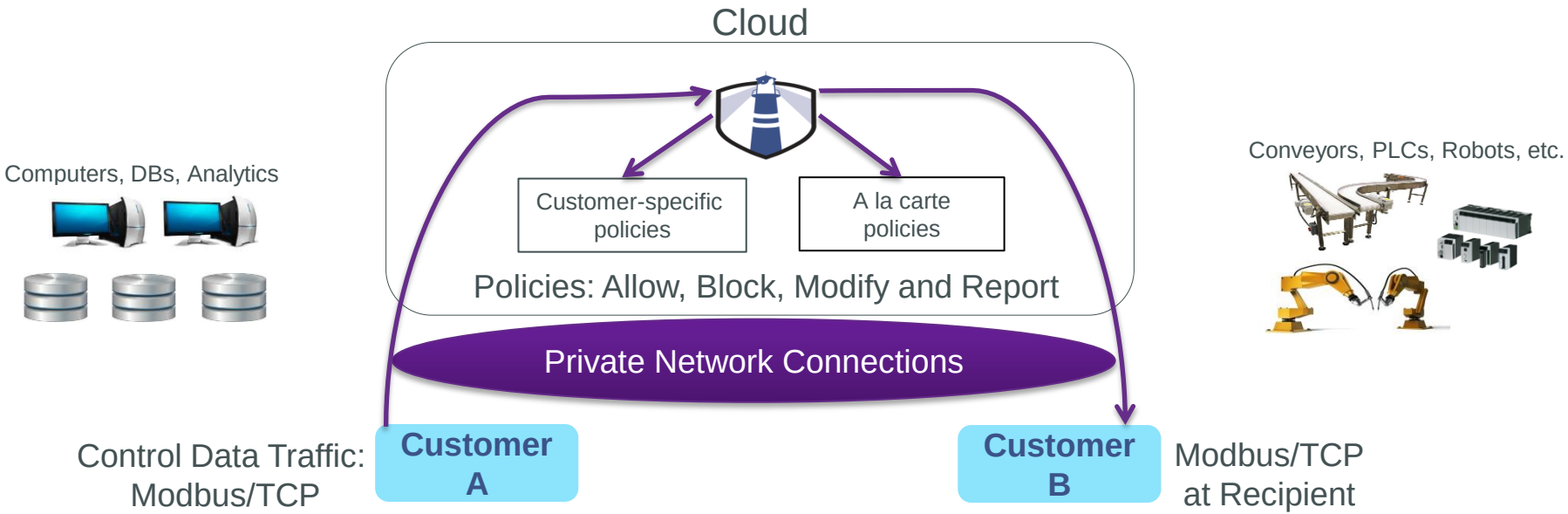
Inspection and mitigation

Plant systems current and secure



Bayshore Manufacturing Demo

Protocol Verification - Manufacturing

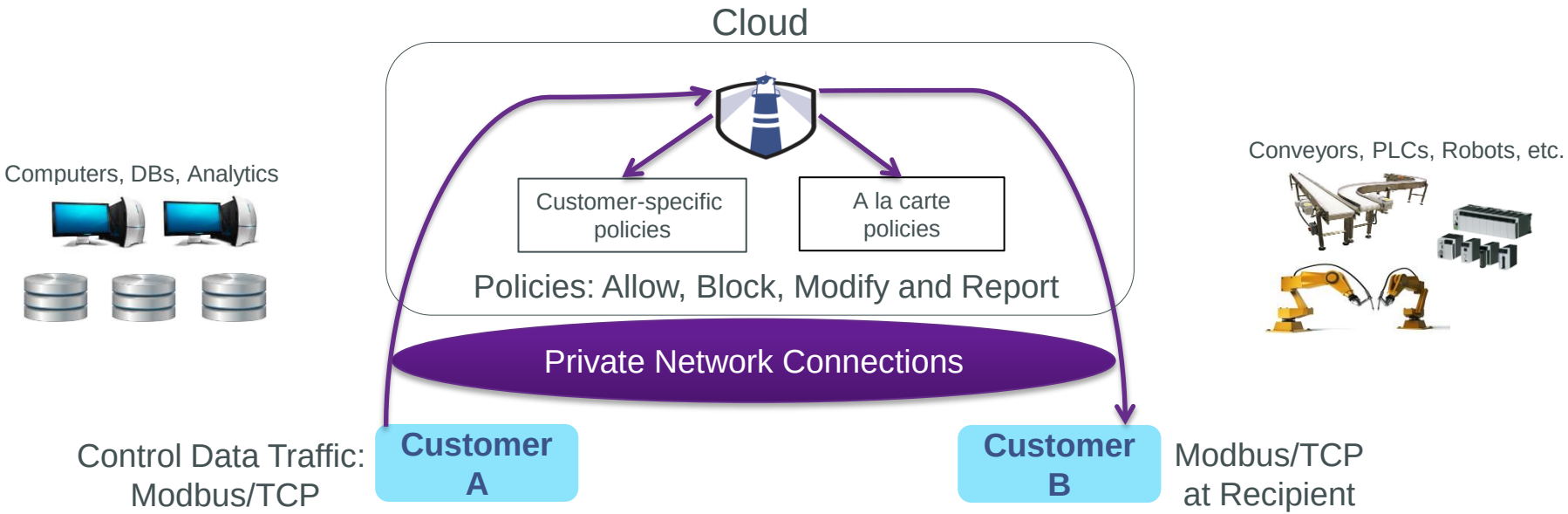


ATTACK

```
root@sushi:/opt/BayshoreNetworks/
modbustcp_client1#

./bufferoverflow_unfiltered.sh
```

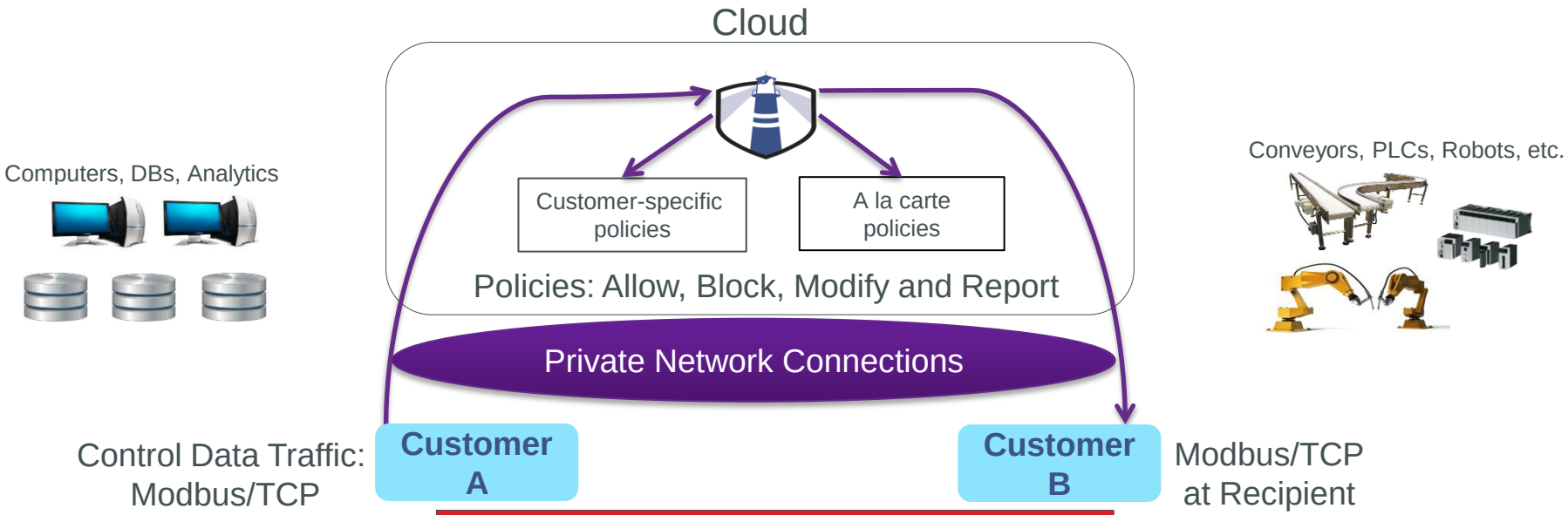
Protocol Verification - Manufacturing



RECEIVING MACHINE

```
Raw Request Payload: 414141414141
4141414141414141414141414141414141
4141414141414141414141414141414141
4 is disconnected
[]
```

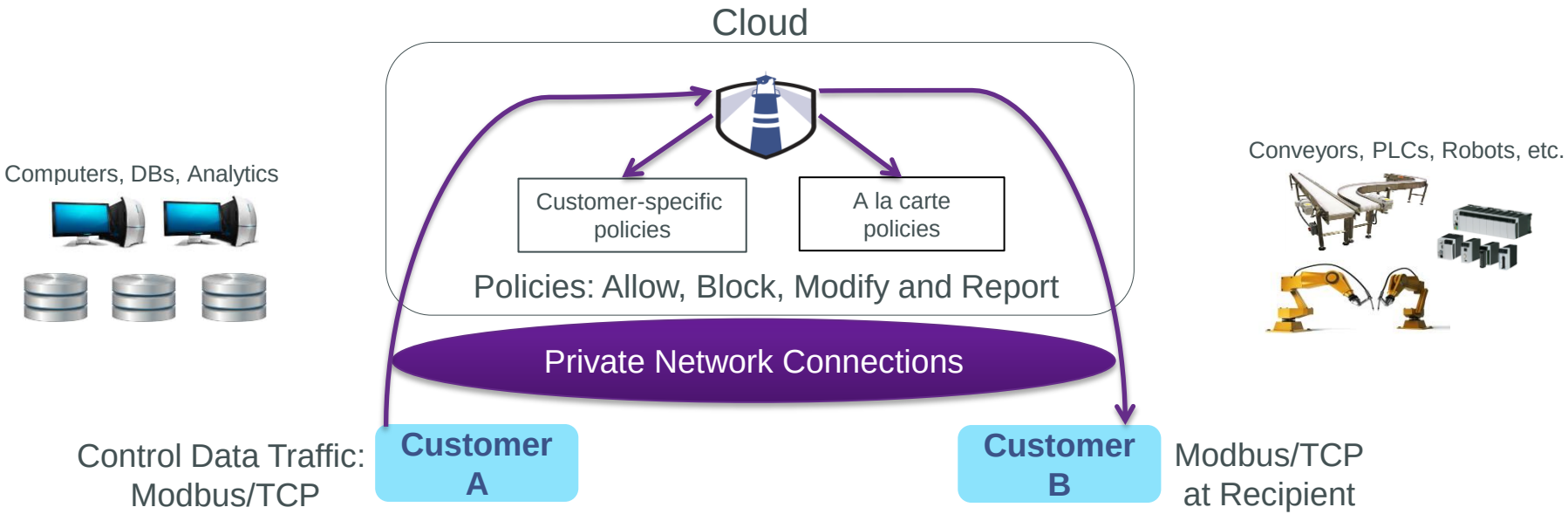
Protocol Verification - Manufacturing



ATTACK WITH FILTER

```
[-] This anomaly is of interest:
    [-] Host: 192.168.1.4
    [-] Port: 502
    [-] Slave ID: 5
    [-] Target Type: Holding Register
    [-] Function Code: 16
    [-] Reason: No response received
```

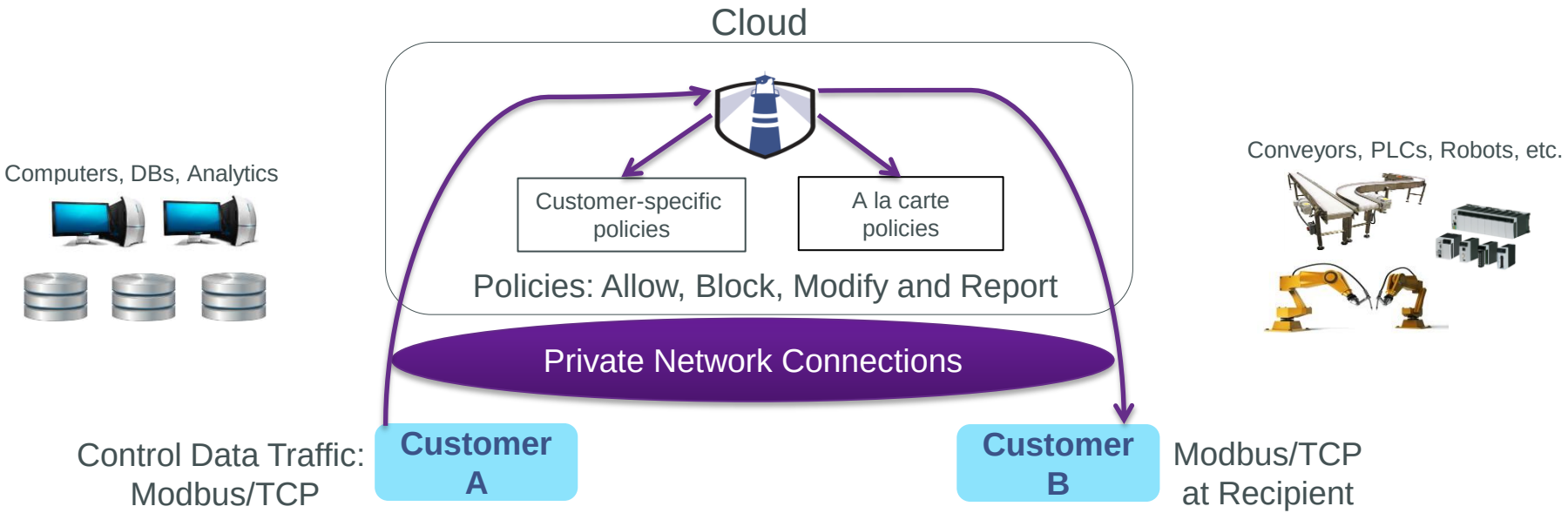
Protocol Verification - Manufacturing



RECEIVING MACHINE

```
('192.168.0.149', 49133) is
connected with socket 4…
4 is disconnected
[]
```

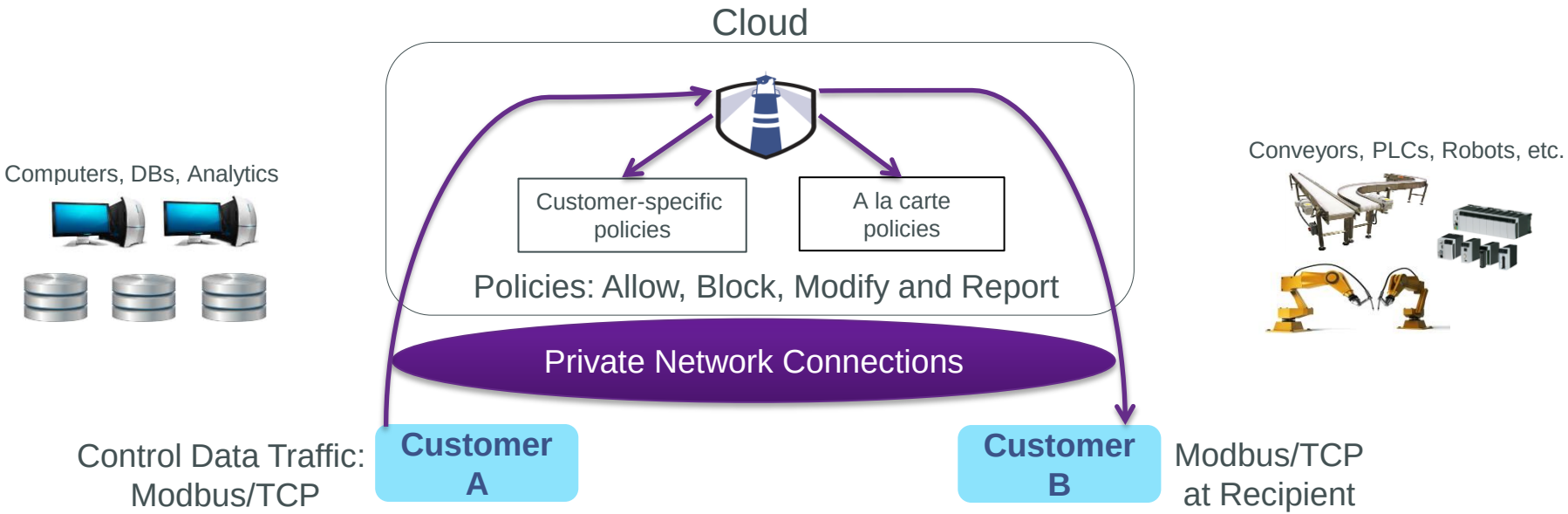
Protocol Verification - Manufacturing



SYSLOG TRAIL

```
May 28 18:06:33 mockingbird AAP/
fproxd[6606]: ruleset=modbuscisco"
(ModbusTCP))
attacksignature="Report Modbus
function" value="16"
```

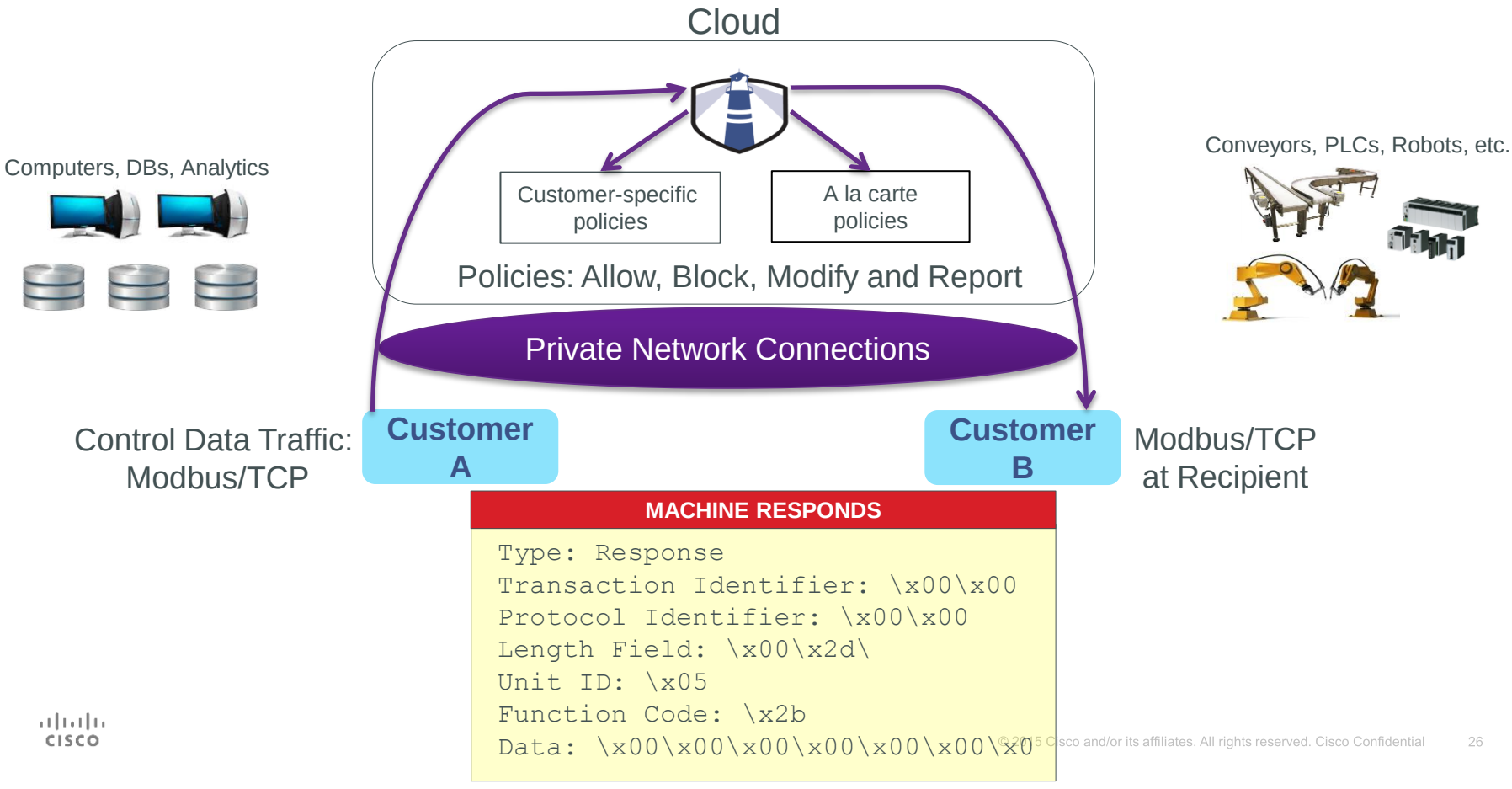
Device Fingerprinting - Manufacturing



PROBING

```
[!] Attempting to fingerprint
    '192.168.0.15' on port 502,
    Slave ID: 5
[+] Device ID value returned: Bay
    shore Networks Modbus Slave v1.0
```

Device Fingerprinting - Manufacturing



MACHINE RESPONDS

```
Type: Response
Transaction Identifier: \x00\x00
Protocol Identifier: \x00\x00
Length Field: \x00\x2d\
Unit ID: \x05
Function Code: \x2b
Data: \x00\x00\x00\x00\x00\x00\x0
```

Device Fingerprinting - Manufacturing

Cloud

Computers, DBs, Analytics

Customer-specific policies

A la carte policies

Policies: Allow, Block, Modify and Report

Private Network Connections

Conveyors, PLCs, Robots, etc.

Control Data Traffic: Modbus/TCP

Customer A

Customer B

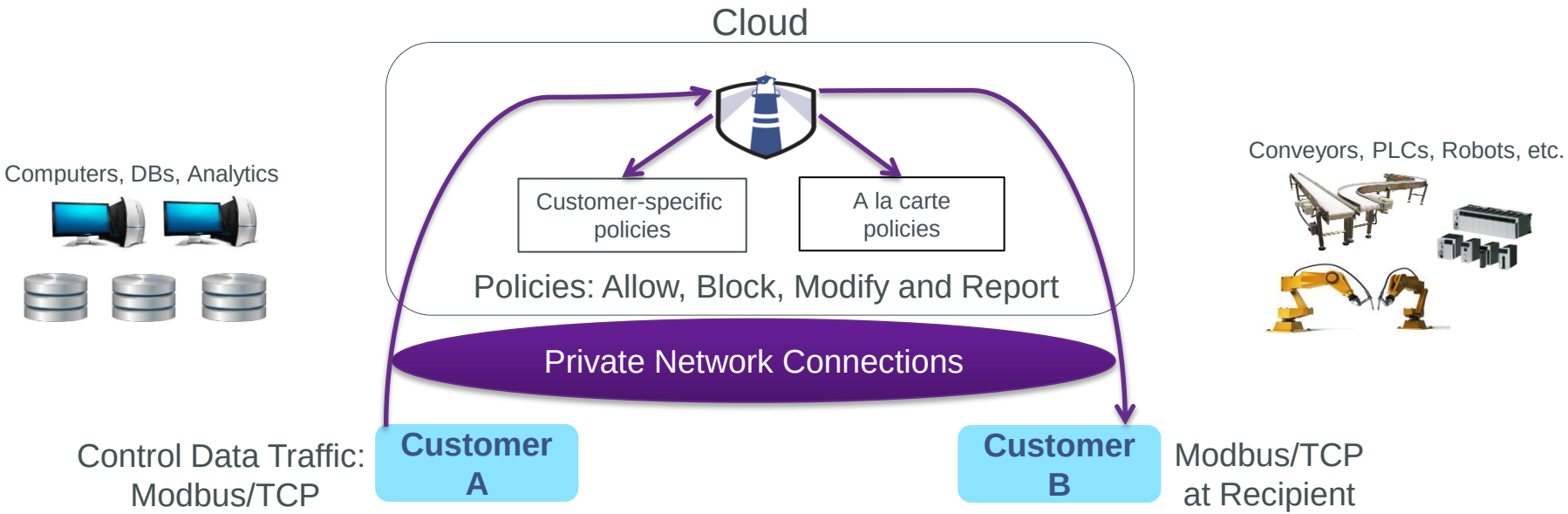
Modbus/TCP at Recipient

PROBE WITH FILTER

```
Socket Timeout

[!} Attempting to fingerprint
    '192.168.1.4' on port 502,
    Slave ID 5
[-] No device ID value returned
```

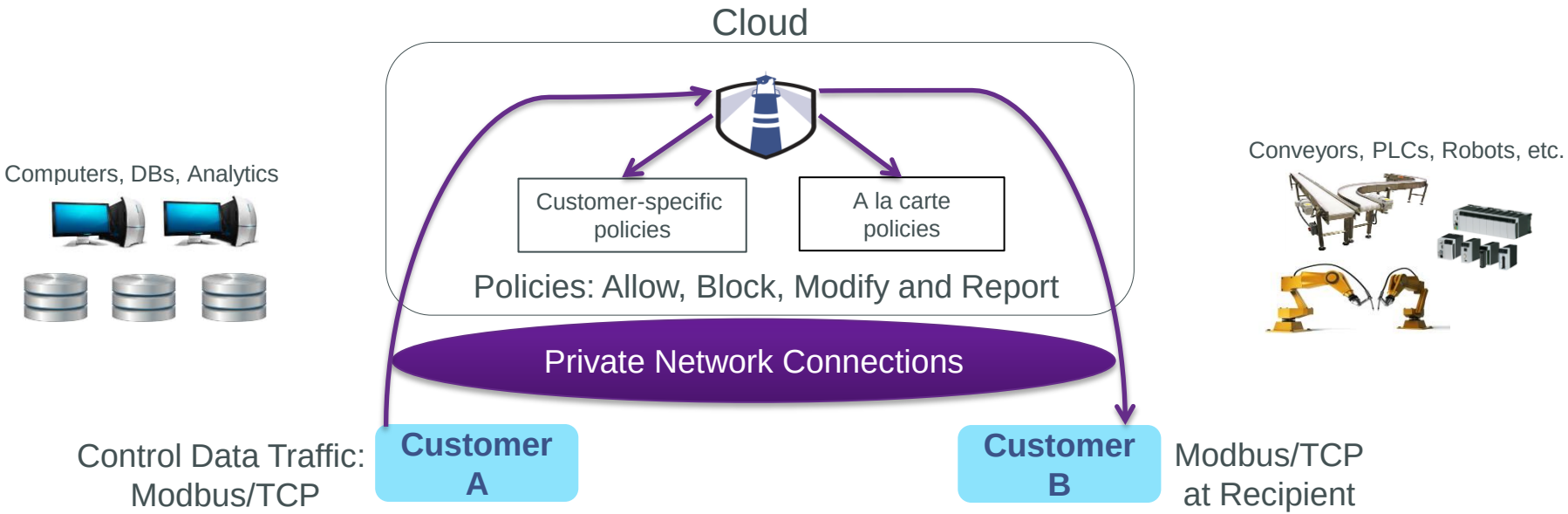
Device Fingerprinting - Manufacturing



RECEIVING MACHINE

```
('192.168.0.149', 49133) is
connected with socket 4…
4 is disconnected
[]
```

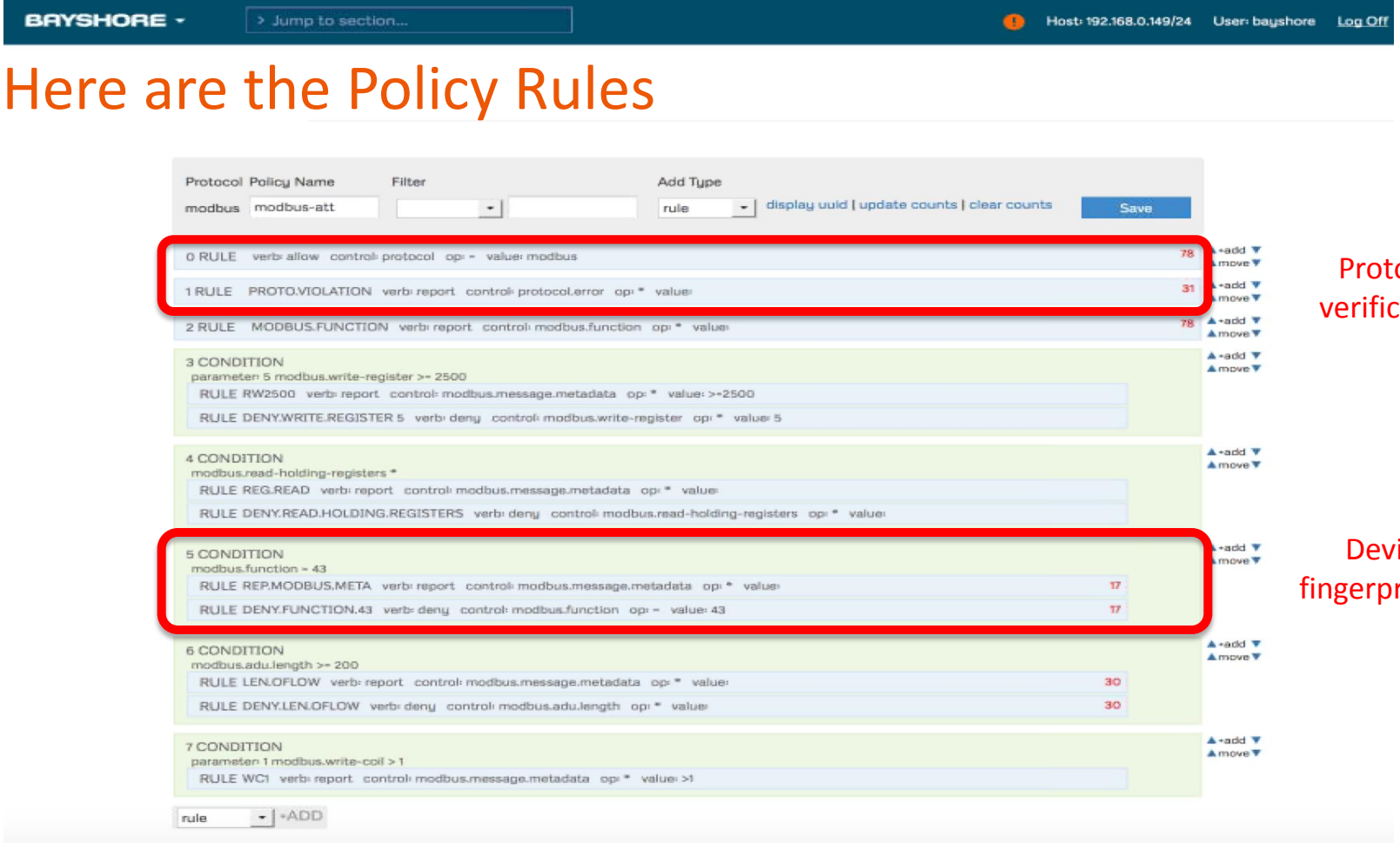
Device Fingerprinting - Manufacturing



SYSLOG TRAIL

```
May 28 18:07:33 mockingbird AAP/
fproxd[6606]: ruleset=modbuscisco"
"(Modbus TCP)" attacksignature=
"Modbus/TCP Device Fingerprint
Attack Blocked" value="43"
```

Here are the Policy Rules



Protocol verification

Device fingerprinting

Thank you.