Fujitsu North America Technology Forum 2015

Securing the Industrial Internet

Panelists: Avradip Mandal, Jonathan Mayer, Masanobu Morinaga
Moderator: Jesus Molina

February 11, 2015

Jonathan Mayer
Stanford University

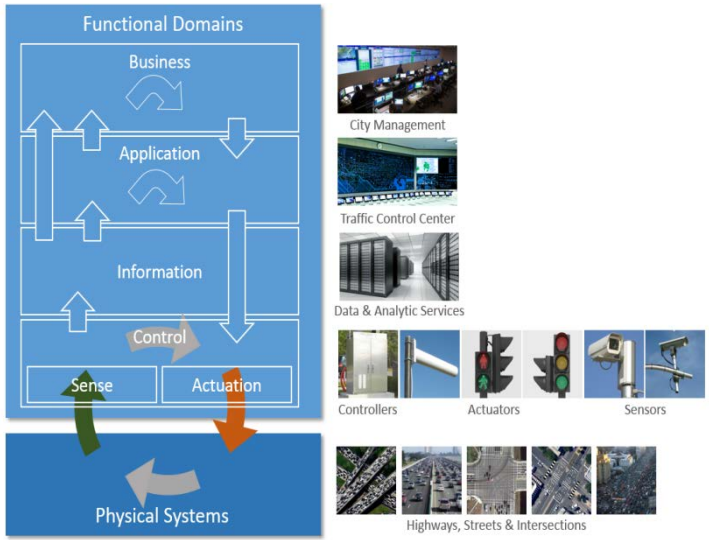
Avradip Mandal
Fujitsu Labs
Of America

Mosanobu Morinaga
Fujitsu Ltd.

Jesus Molina
Fujitsu Labs
Of America

Background

- The Industrial Internet is the second industrial revolution
- Loopback between data collected by sensors, algorithms and machines
- Unpreceded amount of data collected and high connectivity of cyber physical machines



FUJITSU

shaping tomorrow with you

Fujitsu North America Technology Forum

Privacy in the Industrial Internet

Jonathan Mayer, Stanford

February 11, 2015

FUJITSU

Boilerplate Disclaimer

This is not legal advice.

Privacy Restrictions on Consumer Data

FUJITSU

The United States does not have comprehensive electronic privacy laws.

Most privacy liability is for **deception**, either for **misrepresenting** practices, or for **failing to disclose** practices.

Takeaway: be **honest** and **transparent** with consumers about their data

Government Access to Stored Data

FUJITSU

Principle: if a business holds data, government **can** compel disclosure.

Question: in order to compel disclosure, how much **evidence** is required, and does a **judge** decide?

Answer: it's exceedingly complicated, involving the Fourth Amendment, ECPA, and FISA.

Government Access to Stored Data

FUJITSU

There is a **sliding scale** of procedures, differing in the evidence required and judicial oversight.

In many circumstances, Internet of Things data will be available with **less than a warrant**.

Government Access to Stored Data

FUJITSU

Example: electricity records are available with just an administrative **subpoena**

United States v. Golden Valley Electric Association (9th Cir. 2012)

Government Access to Stored Data

FUJITSU

coursera Courses Specializations New! Institutions About Log In Sign Up

Stanford

Surveillance Law

Learn how police and intelligence agencies can access your data, and how the law (might) protect you! Hackers, attorneys, and concerned citizens are all welcome.

Preview Lectures

About the Course

It's easy to be cynical about government surveillance. In recent years, a parade of Orwellian disclosures have been making headlines. The FBI, for example, is hacking into computers that run anonymizing software. The NSA is vacuuming up domestic phone records. Even local police departments are getting in on the act, tracking cellphone location history and intercepting signals in realtime.

Perhaps 2014 is not quite 1984, though. This course explores how American law facilitates electronic surveillance—but also substantially constrains it. You will learn the legal procedures that police and intelligence agencies have at their disposal, as well as the security and privacy safeguards built into those procedures. The material also provides brief, not-too-geeky technical explanations of some common surveillance methods.

Course Syllabus

Sessions

Jan 20, 2015 - Mar 9th 2015

Join for Free!

Eligible for

Statement of Accomplishment

Course at a Glance

- 6 weeks of study
- 1-3 hours/week
- English

Instructors

(In)Secure Industrial IOT

Avradip Mandal

February 11, 2015

Industrial Internet of Things

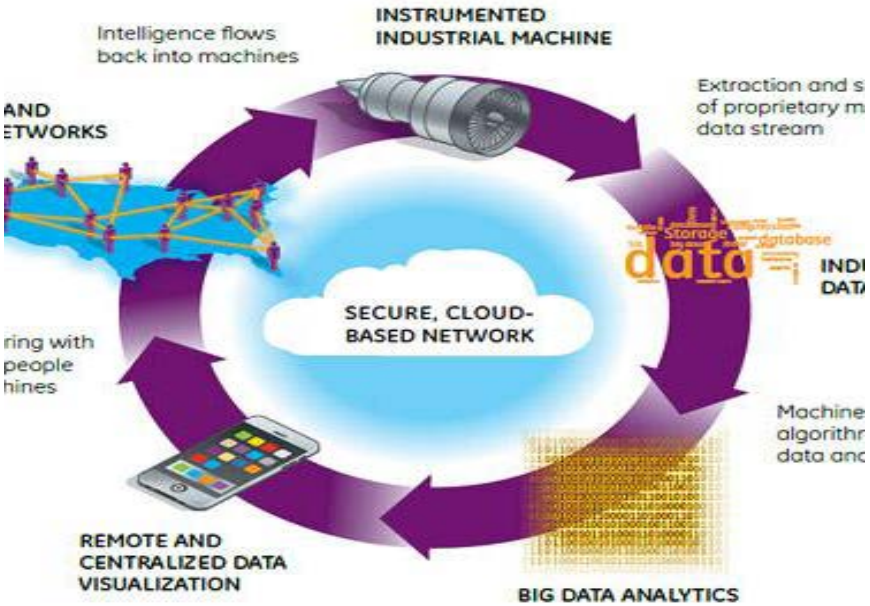


IMAGE SOURCE: DESIGNNEWS.COM

- It's everywhere, Today and tomorrow
- It's going to be a game changer. Better Service, Better Efficiency, Saving lives ...
  - Eliminate Preventable Hospital Errors
  - Improved efficiency in factory work floor
  - Driverless car
  - Smart city
  - ...

Security

IMAGE SOURCE: SECURITYLEDGER.COM

- There are bad guys
- Exponential increase of attack surface
  - Threats are not virtual, it's physical
  - Multiple security mishaps in 2014
    - Heartbleed bug – hitting hospital network
    - ATM Hacks
    - Point of Sale malware, stealing credit card info
    - Target data breach
    - Hacking oil rigs …

Heartbleed Explained

IMAGE SOURCE: INDIANIC.COM

- The bug allows attackers to grab 64K chunks of memory contents near the SSL heartbeat on a vulnerable host
- Random Chunks of data in memory space, it might contain private crypto keys, passwords and other sensitive information
- Affected the whole world, multiple online services (including amazon, github, reddit, etc) asked the users to change their password following the discovery of the bug
- 4.5 Million patient data were stolen from one of the largest hospital operator.
- 75 cisco systems were affected including ip phone systems, routers...

Solution ?

IMAGE SOURCE: SURFERQUEST.COM

- Trade off between Security and Utility ?
  - Security first
- Secure Architecture
- Defense in depth / Layered approach to security
- Security Testing, open source (?) for public scrutiny
- Security focused software development cycle
- Patchable system
- Data purging – Don't' gather/keep data that you don't need

FUJITSU

shaping tomorrow with you

Fujitsu North America Technology Forum

Malware Activity Quick Detection technology for Internal-Networks

Masanobu Morinaga, Fujitsu Laboratories LTD.

February 11, 2015

Background

FUJITSU

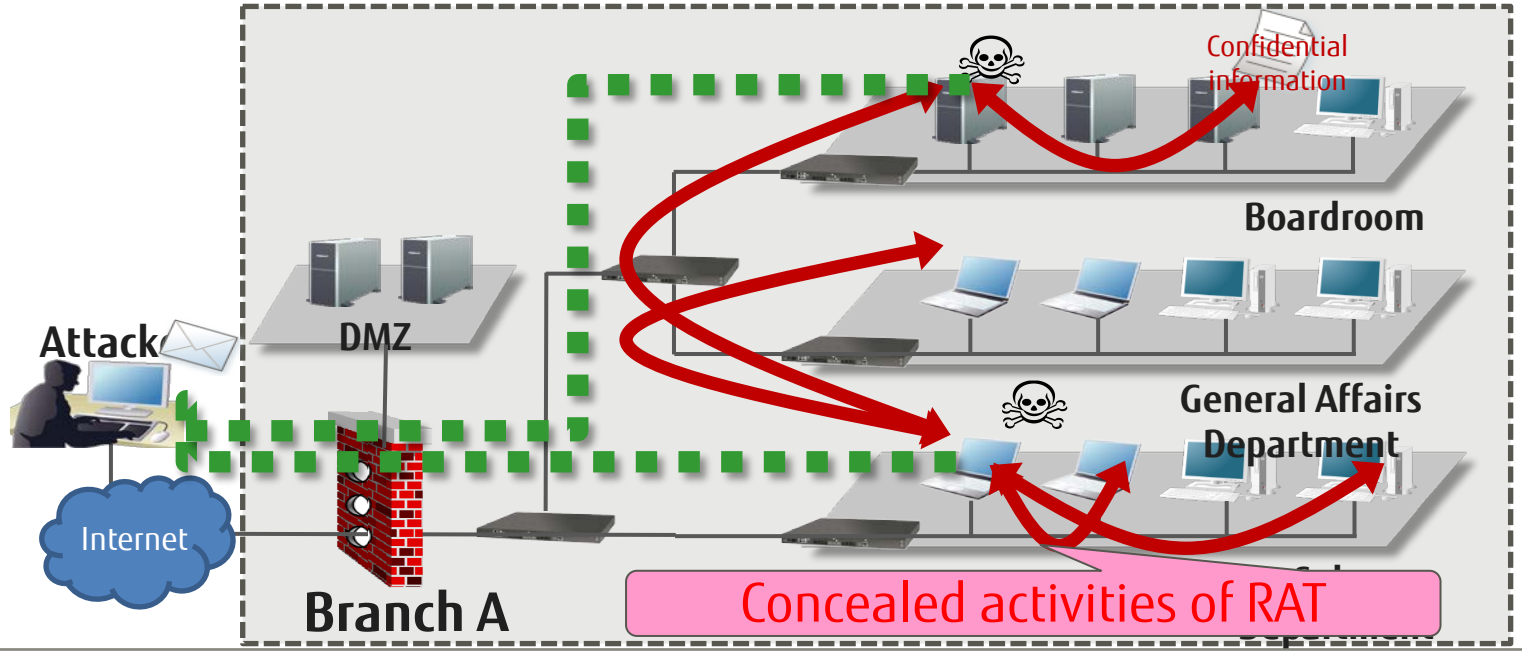
- Threats of cyber attack are widening
  - Intrusion, web defacing, information leakage
- APT (Advanced Persistent Threat) has become a serious issue
  - Highly sophisticated and persistent cyber attack
  - Targets specific companies or organizations
- The attack methods are getting shrewder
  - Remote Access Trojan (RAT): Remote-controlled malware
  - Existing countermeasures cannot cope with them

Typical Steps Taken by APT(Advanced Persistent Threat)

RAT* is often used in APT

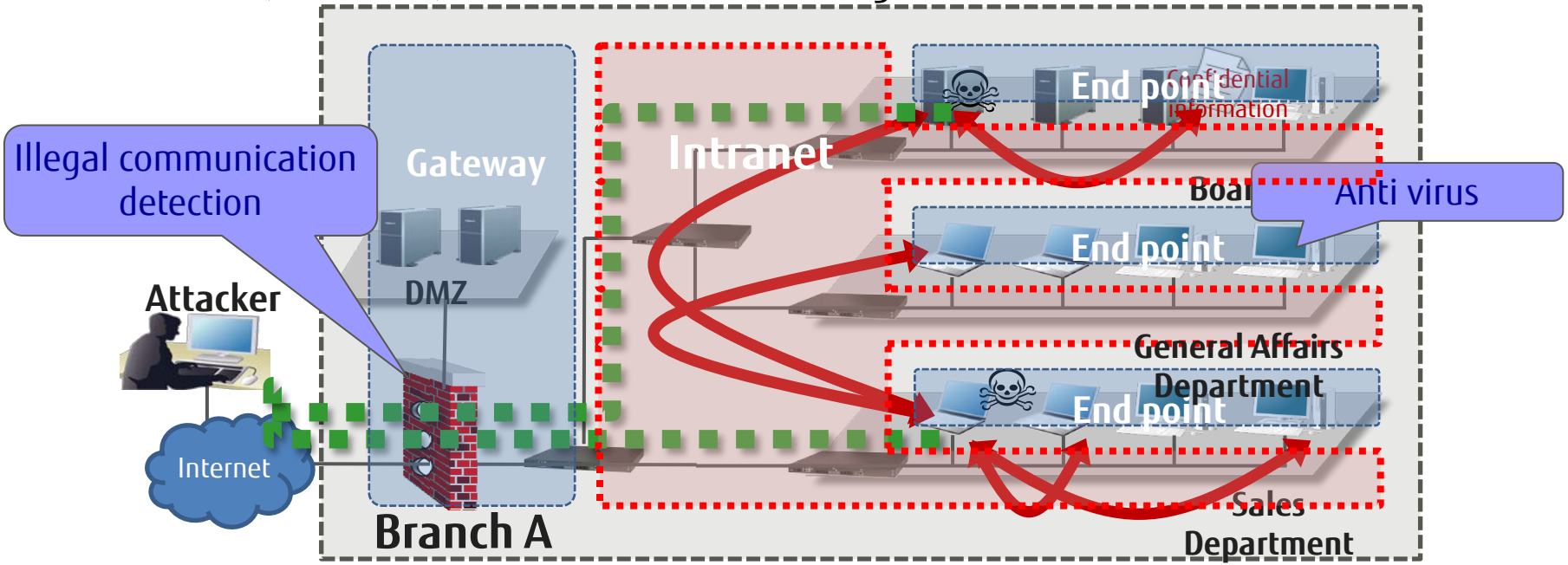
*RAT: Remote Access Trojan – Malware that acts stealthily and controlled remotely

- Intrudes the intranet by avoiding cyber-attack countermeasures.
- Repeats illegal accesses to eventually reach and steal confidential information.
  - RAT communication mixed in normal communications are difficult to detect.



Existing Measures Are Not Enough

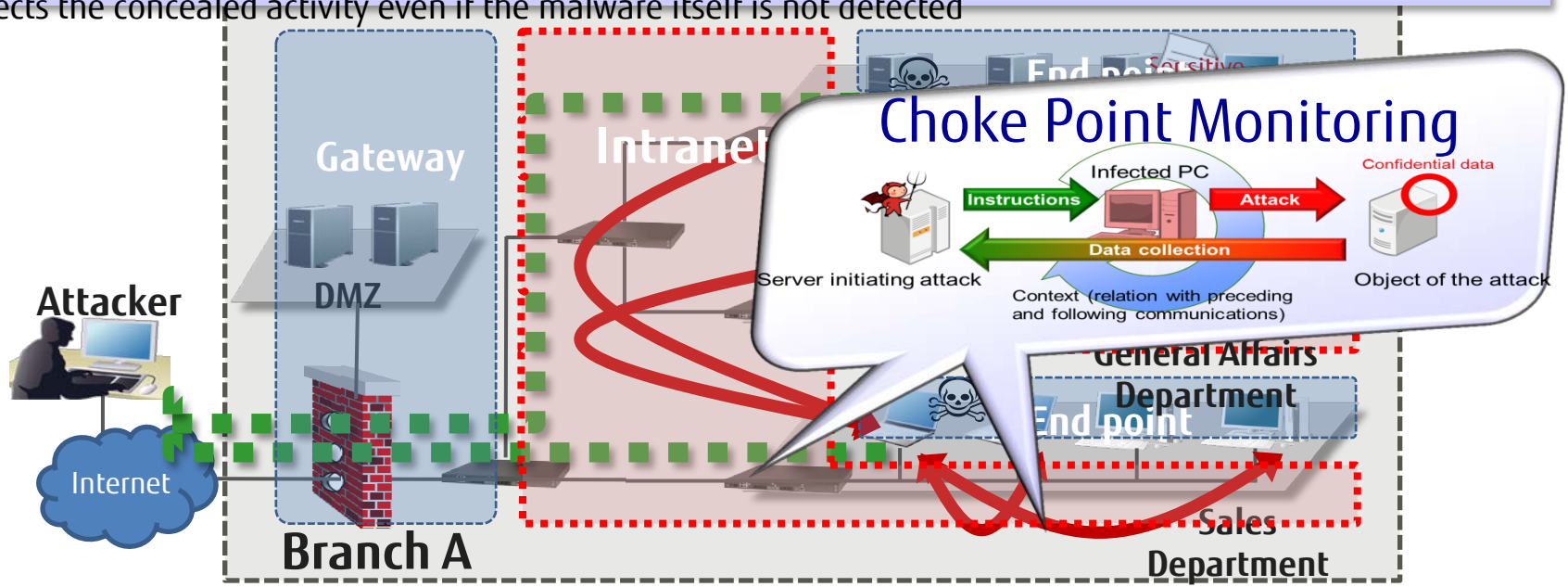
- At gateways
  - RAT (malware) communication is often encrypted, so detection is difficult.
- At endpoints
  - Each RAT (malware) is customized to its target, so detection is difficult.



Our Technology: Choke Point Monitoring

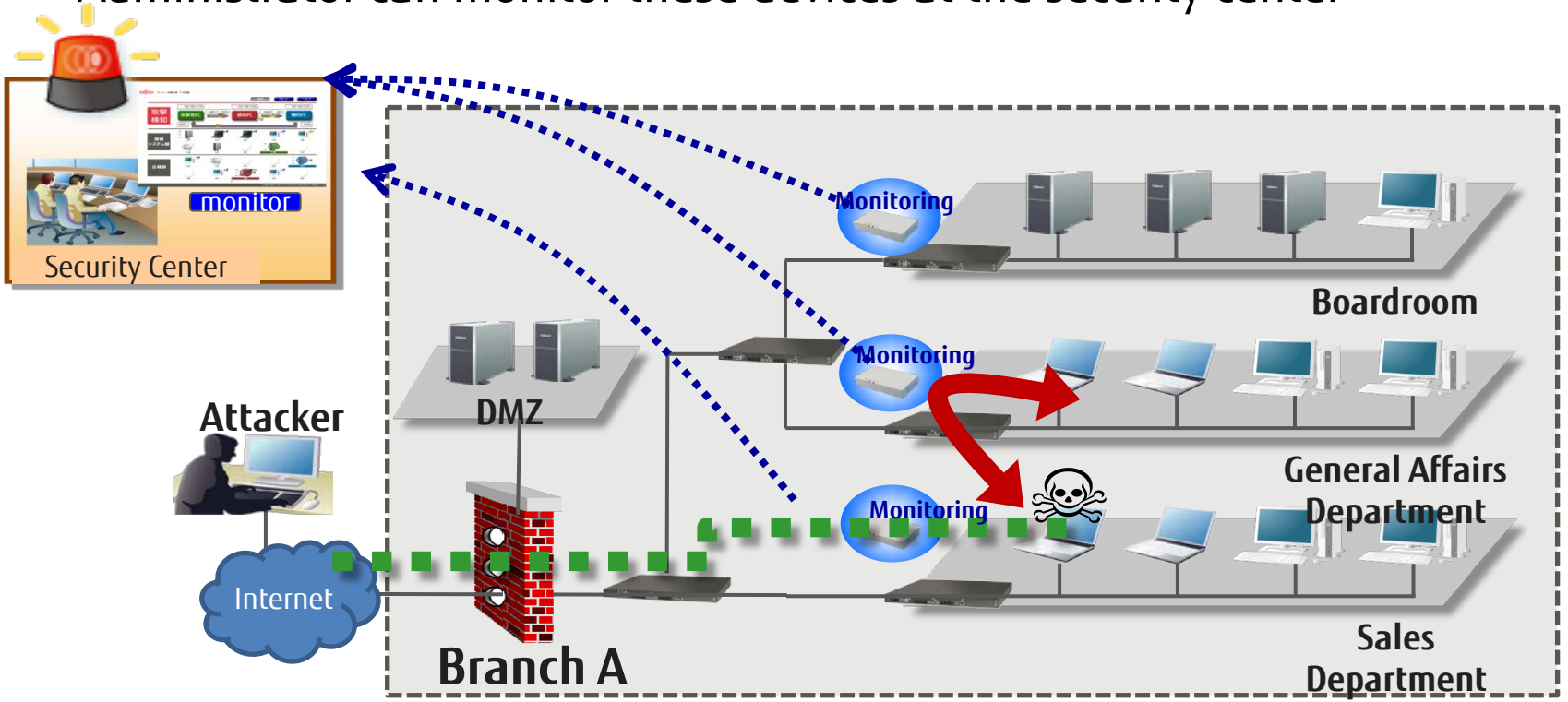
New technology which overcomes difficulty of malware detection.

- Monitoring choke points and analyzing the context of intranet communication
  - Choke points are steps common for most malware, which the attacker cannot do without
  - E.g., internal access (SMB) are generated, after receiving instruction (HTTP) from the outside.
- Detects the concealed activity even if the malware itself is not detected



Use Case: Remote Monitoring Service

- Monitoring devices are distributed and deployed to all departments
- Administrator can monitor these devices at the security center



Commercialization of Our Technology

- Our technology is implemented and used in iNetSec Smart Finder.
  - We are demonstrating it at our booth J04.

PFU a Fujitsu company

iNetSec Smart Finder

IPS Malware Detection & Threat Prevention

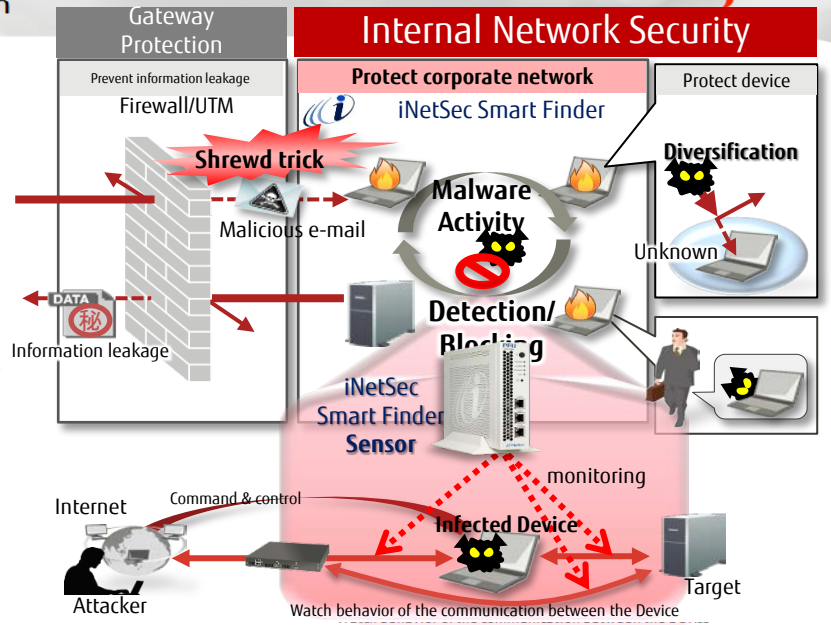
FUJITSU

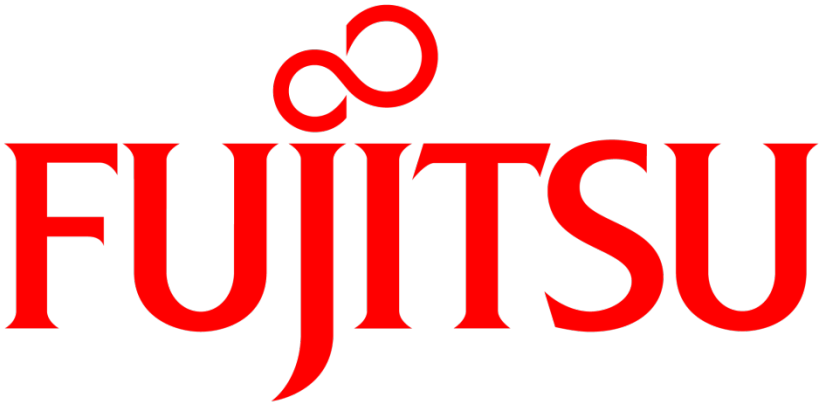
Advantage

- "Behavior Detection Engine":
  detects APT malware and blocks the infected device.
- "Application Visualization and Control":
  visualizes use and operating behaviors of risky network applications and enforces policies.

How it works

- Analyzes characteristics of the behaviors such as network communication to bypass security measures which may be caused by APT and/or RAT(Remote Access Trojan).





shaping tomorrow with you