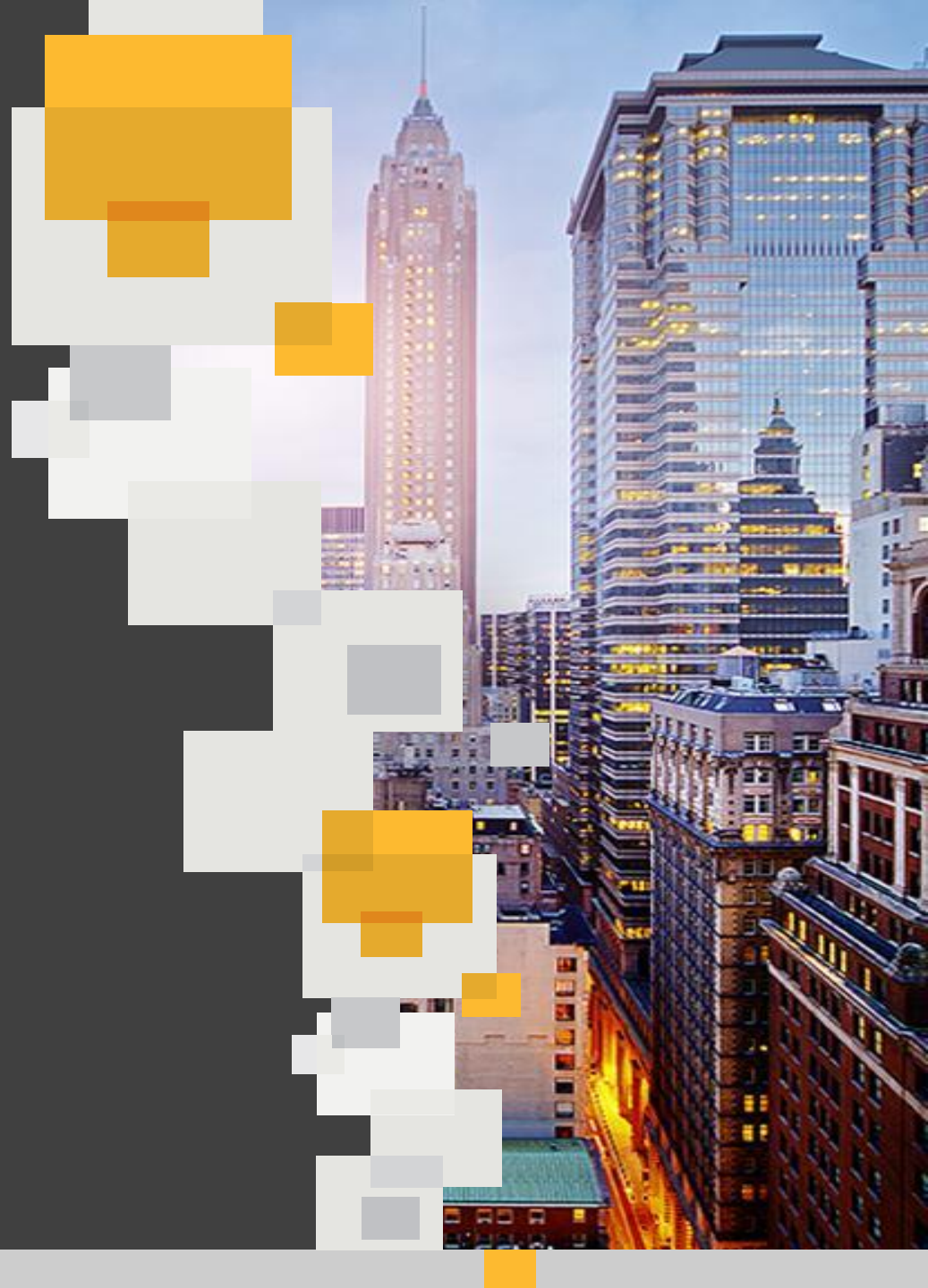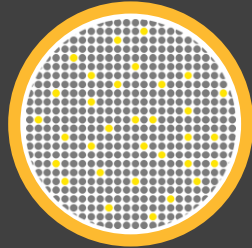# Internet of Things real life cases

Alex Ahlberg

Sales Manager, Symantec Finland & Baltics

Symantec | At a Glance

175M endpoints under protection

$4.6B annual revenue

2123 patents

385,000 customers worldwide
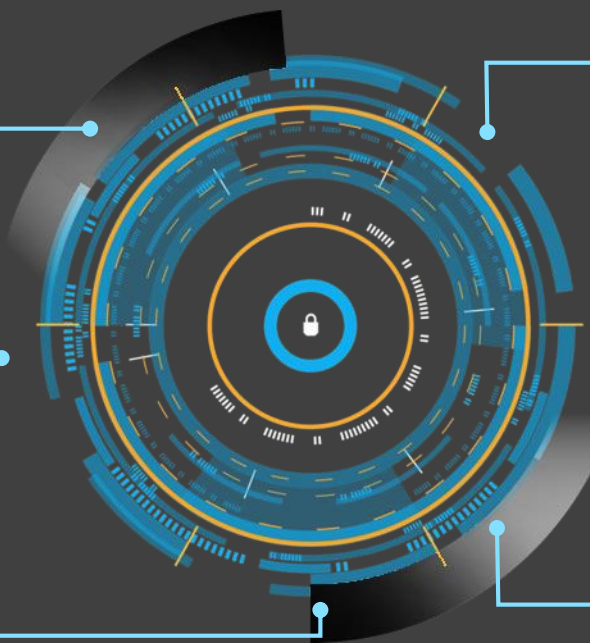

3000+ R&D engineers

6 SOCs threat response centers

Discovered **430 million** new unique pieces of malware last year

20,000+ Cloud applications discovered and protected

1B malicious emails stopped last year

182M web attacks blocked last year

100M social engineering scams blocked last year

CLOUD GLOBAL INTELLIGENCE SOURCED FROM:

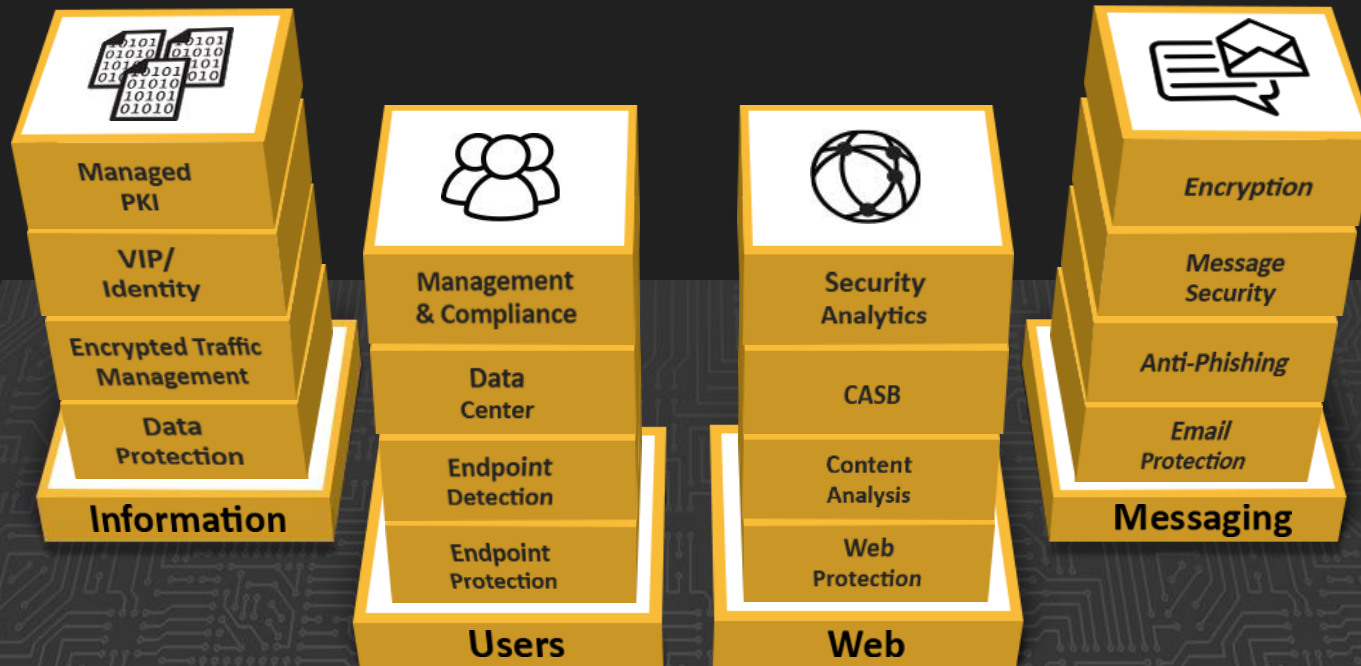**1 Billion** previously unseen web requests scanned daily

2 Billion emails scanned per day

175M Consumer and Enterprise endpoints protected

9 global threat response centers with
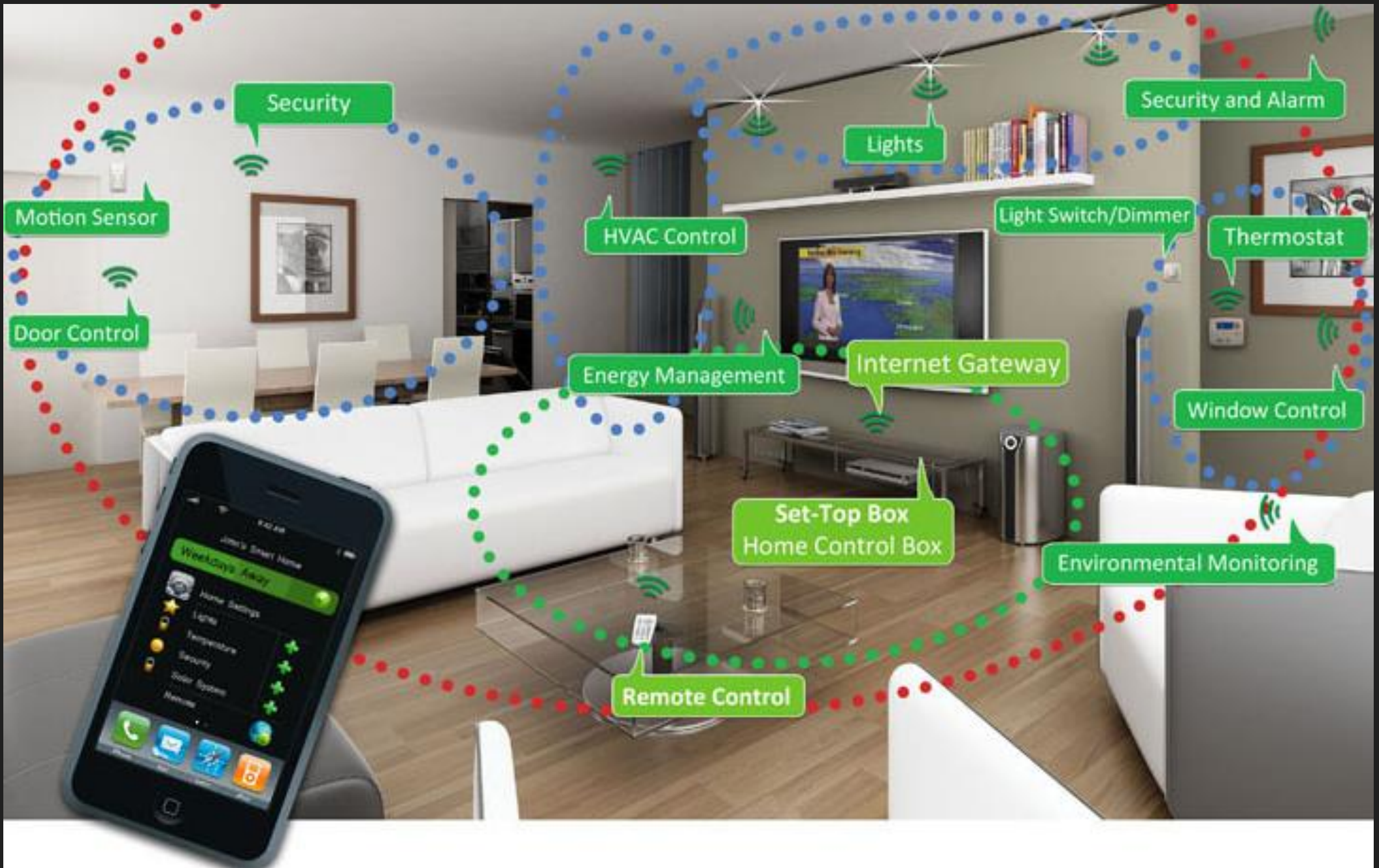
3,000 Researchers and Engineers

Integrated Cyber Defense

Internet of Things

View from Symantec and customer use cases

LIVING_ROOM   2014-11-09 12:46:16

REC   08/07/2016 SUN 10:57:1?   11 DAYS

2013/01/06 10:10:20

Attacks against Symantec IoT honeypots doubled from January to December **2016**

DEC | 2016

JAN | 2016

9/hour

5/hour
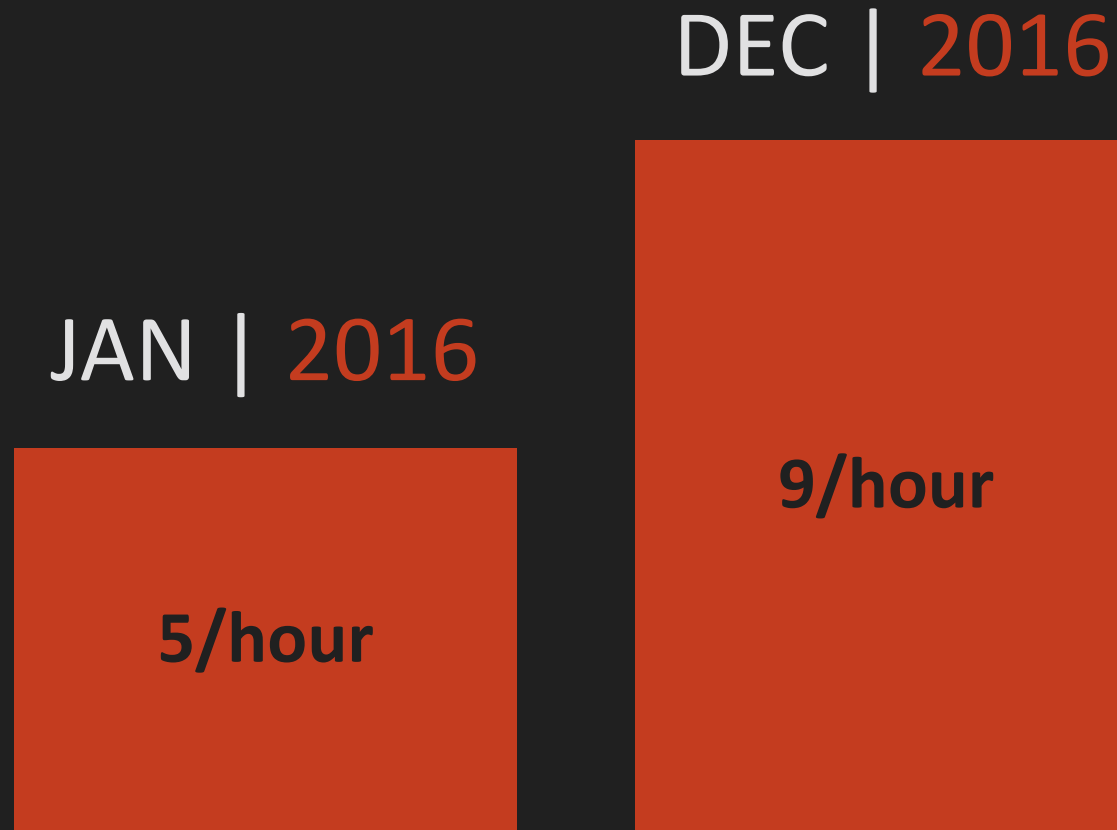
In 2016 Symantec researchers put an IoT device on the internet
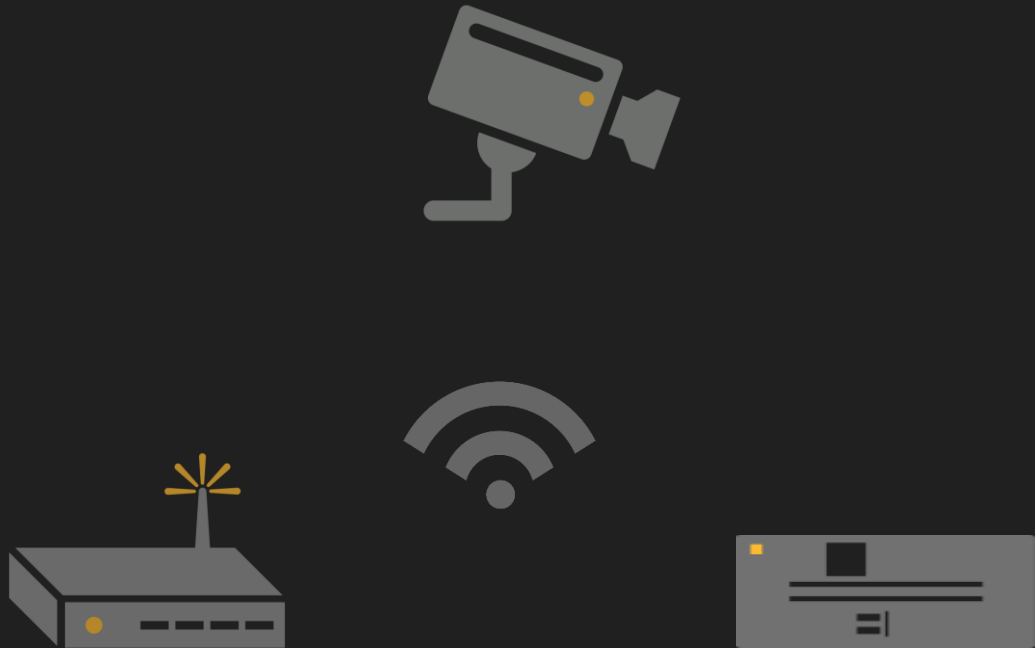
It was attacked within

2 minutes

Use Case 1:

Remote Monitoring
& Inventory Control

Use Case 2:

Securing CCTV
Systems

Use Case 3:

Smart TV

Use Case 4:

Connected Car

Use Case 5:

Securing POS/ATM
Devices

Use Case 6:

Country-Wide Smart
Meter Deployment

Use case 1: Remote monitoring and inventory control

Large Beverage Company Revolutionizing How Beverages Get Dispensed in Restaurants

Computer Chip	Inventory	Cost
New beverage dispensers have computer chips built into them	Identified need to access inventory and usage data remotely	Lower dispensing cost per beverage and reduce cost of inventory replacement
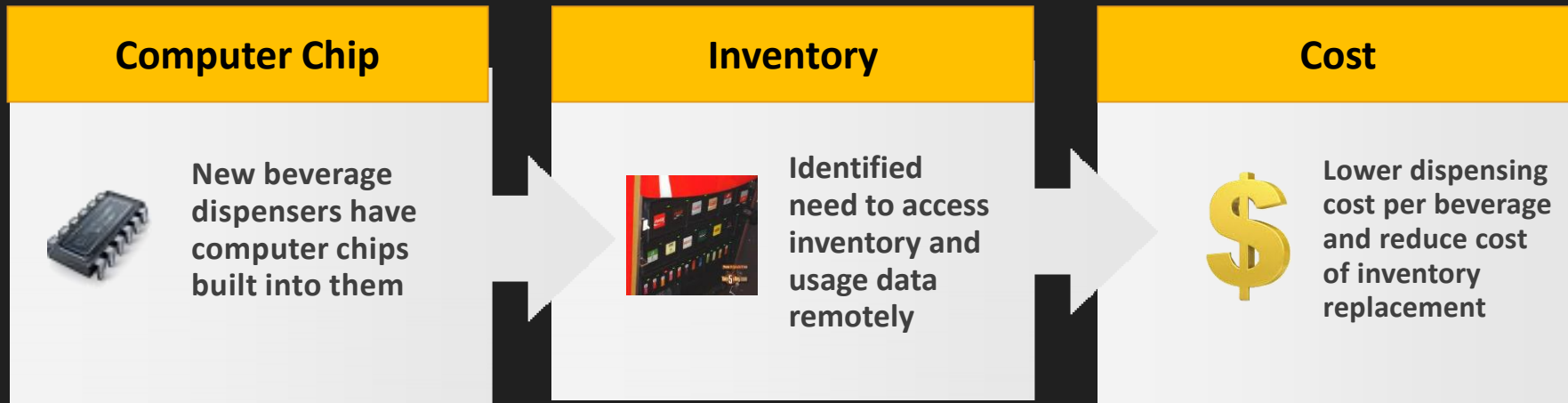
Use Case 1: Remote Monitoring & Inventory Control

Remote device management

Custom designed dispsener using inkjet technology for flavoring

Replace existing fountain dispensers when they get low

Solution Benefits

Gain business intelligence from data analysis

Remotely update beverage recipe updates

Monitor device health through periodic device state

Ability to scale to millions of dispensers

Use case 2: Close Circuit Television Camera (CCTV) solution

Log collection Server

Correlation Analysis

IPS/IDS

Surveillance system

Send log information

Collector Agent

Use case 2: CCTV solution

① Penetration

Digital Certification (PKI)

SSL Module Technology

Key Generation Technology

Symantec SES:CSP

② Aware and Send log

Symantec Security Monitor (MSS)

Security aware function

③ Notice something strange.
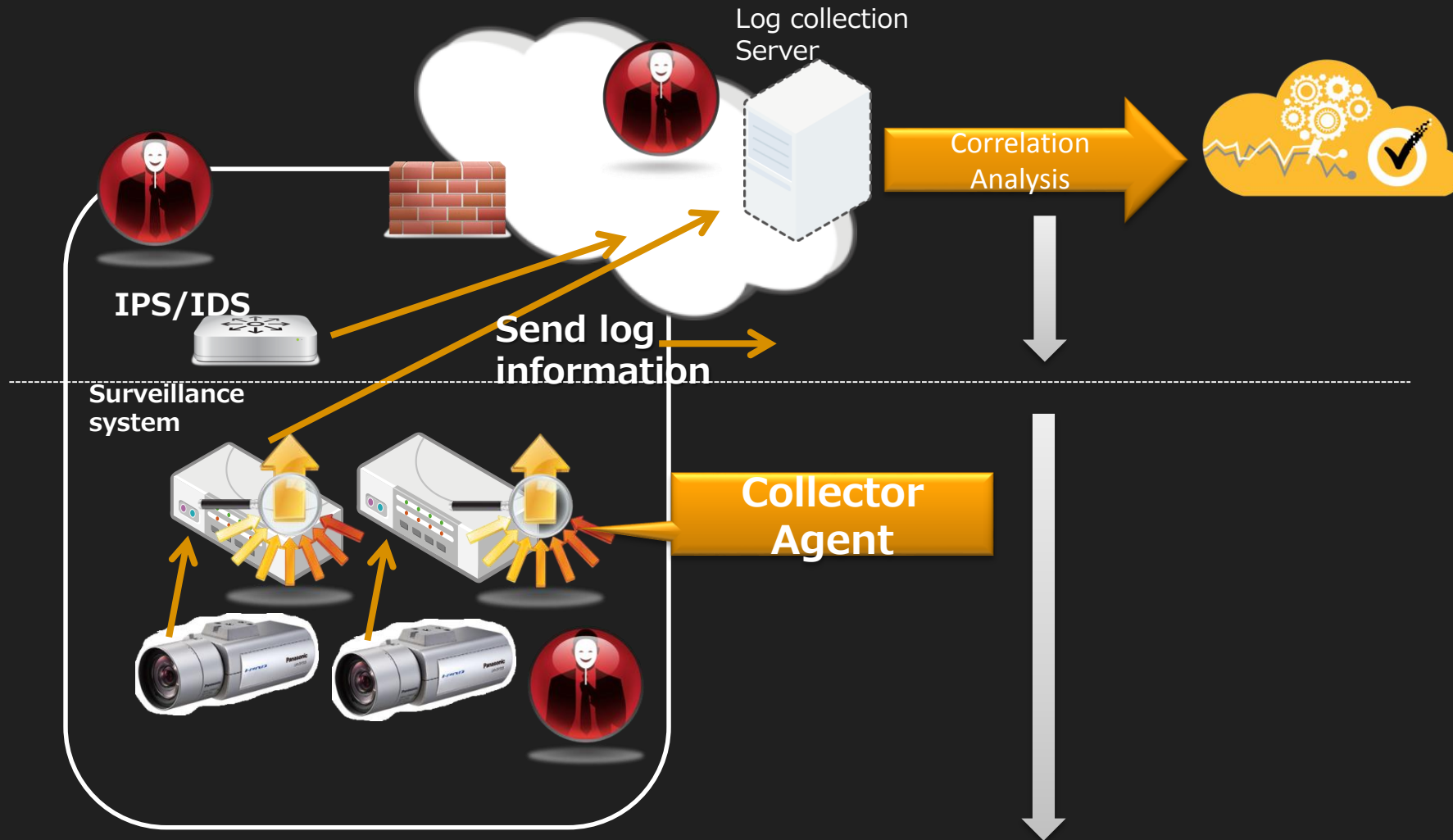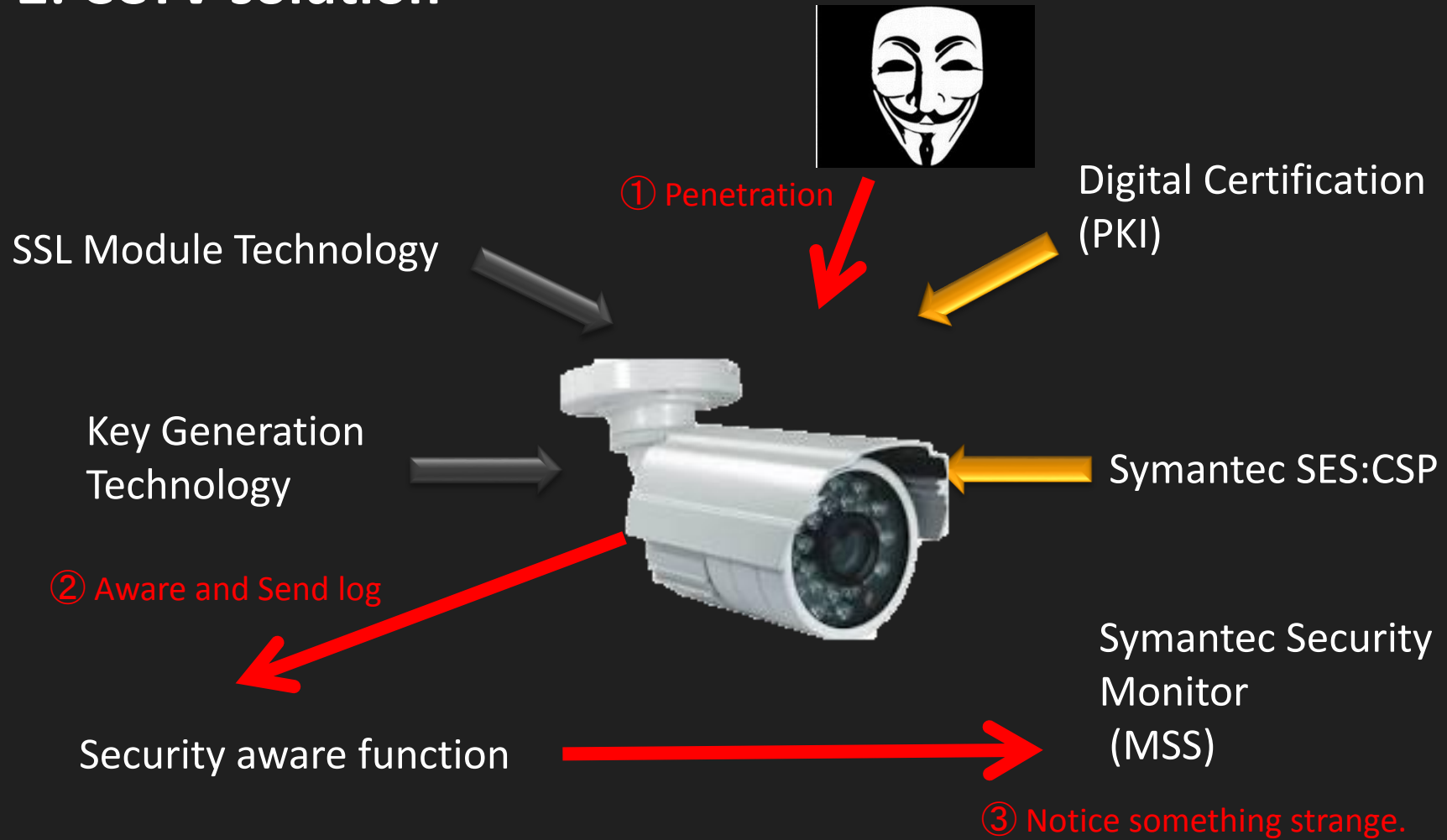
Use case 3: Smart TV protection

Symantec SES:CSP
- Application sandboxing, Device + Configuration control, Host firewall
- Restriction of application, operating system behavior

Symantec Digital Certs
- Certificate management system
  - Prevent unauthorized access with enhanced authentication

Symantec MSS
- Monitoring of individual + aggregate TV sets
- Unfiltered log analysis
- Identification of security events

Symantec Code Signing
- Verification of application integrity
- Grant access to download or run an application
- Vet and approve developers and organizations

Use case 4: Future of the connected car
Connectivity and Diagnostics Interfaces Lead to Vulnerabilities

TCU / ECU

TMPS

Anti-Theft

Telematics

Keyless Entry

OBD-II
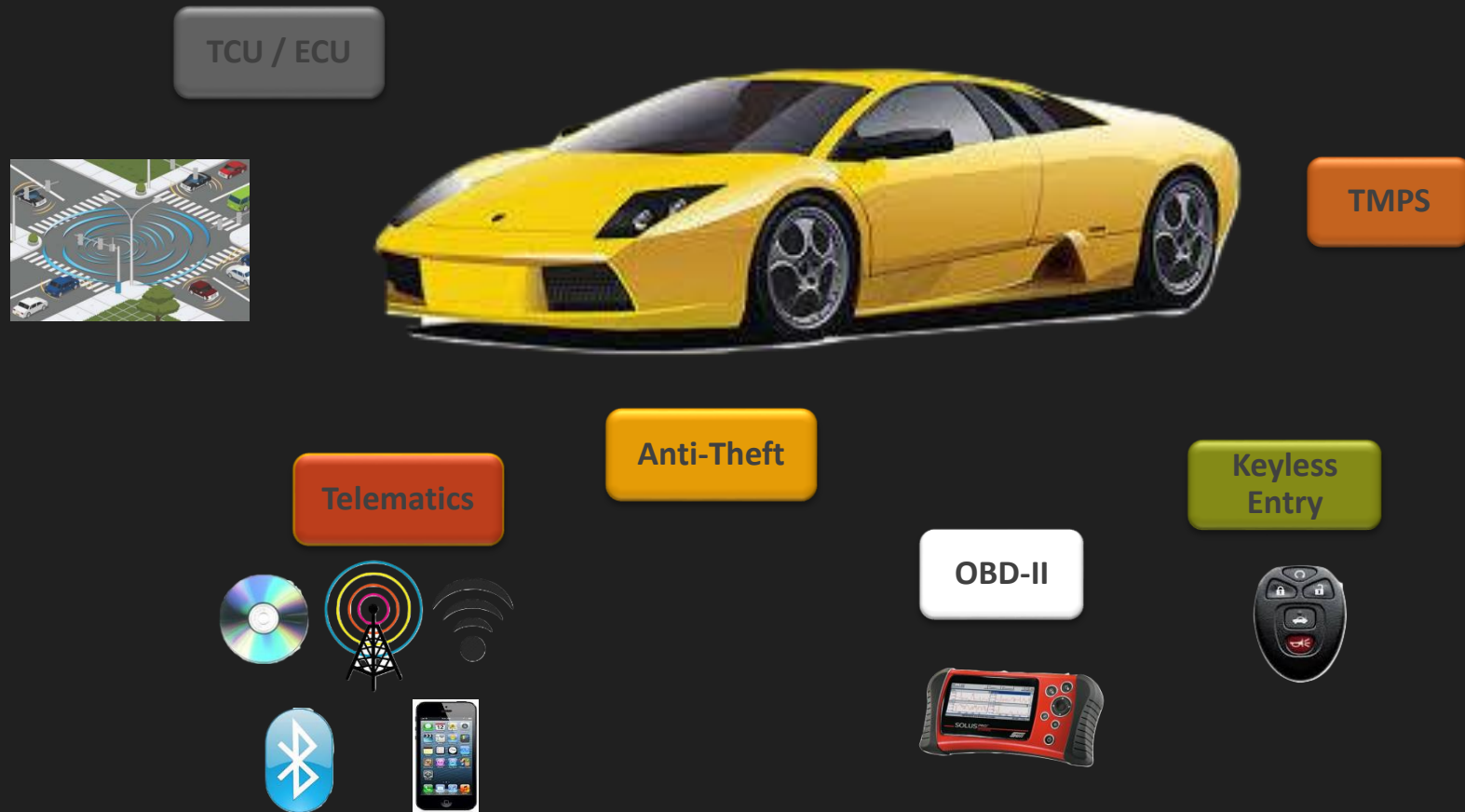
Use case 4: Protecting cars with Web Security Service

- Devices run Android. Applications such as Spotify, navigation, web browser.

- Headache was Android security. Required an external anti-malware service.

3G/4G
using
paired
cellphone
or dongle

X Cloud
Datacenter

Symantec Web
Security Service

Scan and block malware
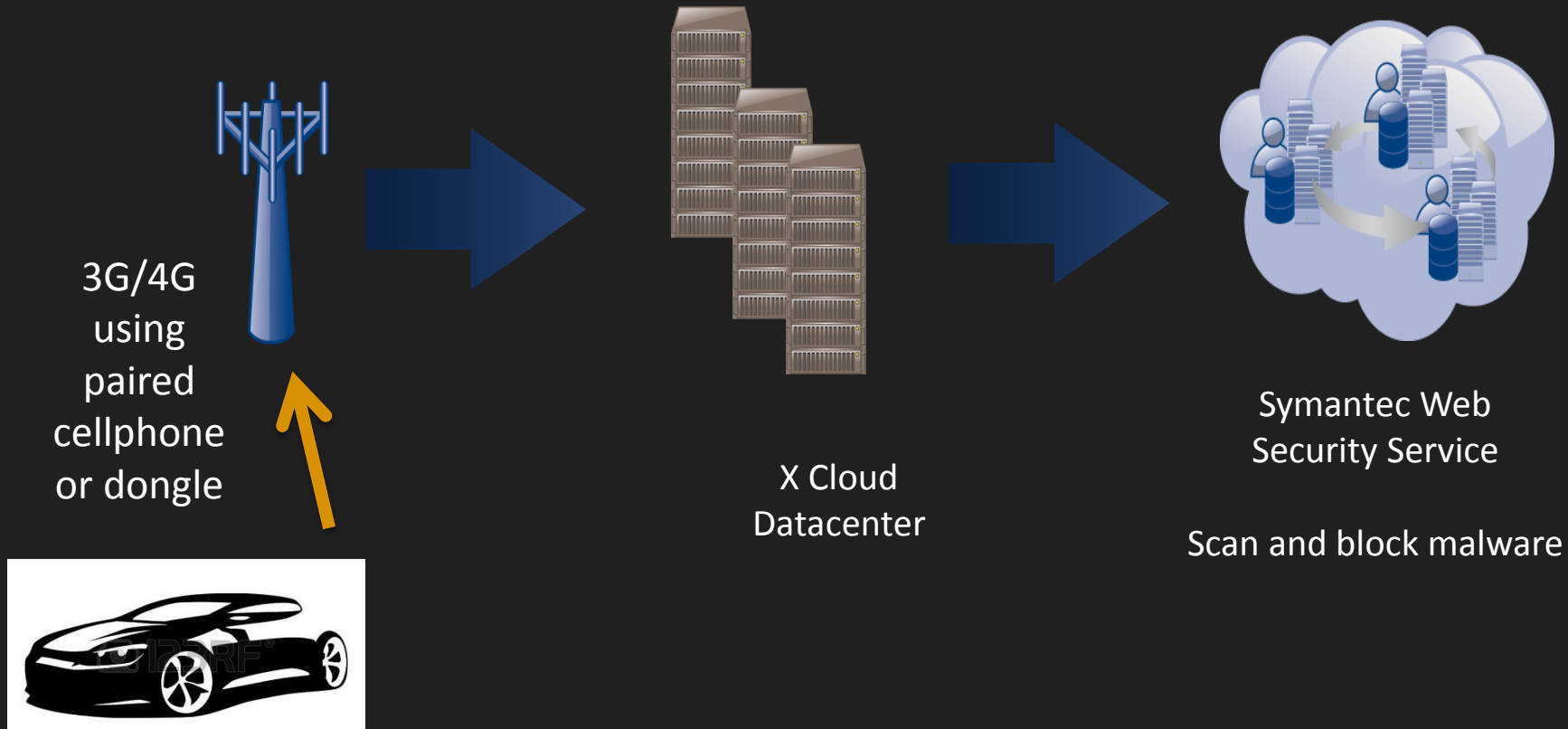
Use case 5: System hardening on POS / ATM systems

- Point-of-sales (POS) systems, kiosks and ATMs are mission-critical equipment for many organizations

- These systems often have little protection against targeted attacks, running unauthorized applications and credit card theft

- Traditional antivirus software can be employed by organizations, but they can negatively impact system performance through continuous signature updates

Use Case 5: System Hardening of POS/ATM Machines

Characteristics of POS Systems

CSP System Lockdown Features

Purpose built, embedded systems that run a pre-determined set of applications (e.g., ring up sales, accept credit cards)

System lockdown ensures that only approved applications can run on the device; all other applications are blocked from running

Limited processing and storage capability

Does not require significant processing power or storage

Devices not always connected to the Internet

Complete protection even if devices are not connected to the Internet

Use Case 6: Country-Wide Smart Meter Project

- UK Government visioin every home to have smart energy meters. Significant Security Concerns

- Can the manufacturer be trusted?

- Could any firmware upgrades introduce bad code?

- How can the usage (KWh) information being transmitted from the meter be protected?

- How are users who want access to their usage data authenticated?
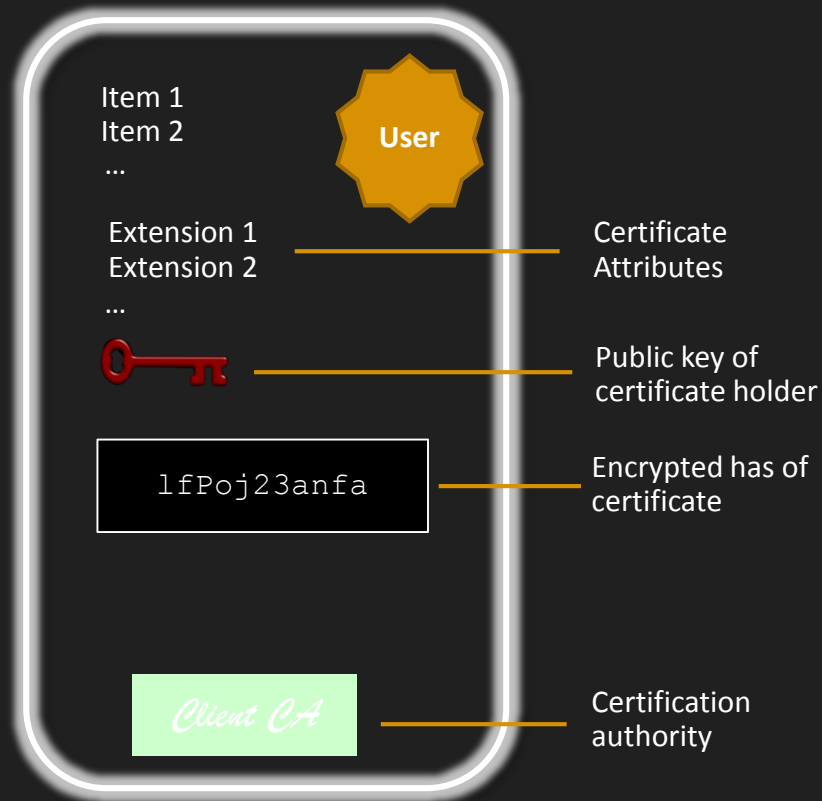
Replace with fake

Load bad software

Recalibrate meters

Monitor communications; change code to retrieve usage

Monitor communications; change code to retrieve usage

Use Case 6: Country-Wide Smart Meter Project

- Smart Meter Certificates

Item 1
Item 2
…

User

Extension 1
Extension 2
…

Certificate Attributes

Public key of certificate holder

`lfPoj23anfa`

Encrypted has of certificate

Client CA

Certification authority

- By implementing Symantec PKI into the meters themselves, the government has ensured that the there is security at the communication layer
  - Identifies connected meters as being authentic
  - Verifies that meters are configured correctly
  - Ensures meters haven't been altered
  - Validates the meters for network access

Thank you for listening!

alex_ahlberg@symantec.com