FIREEYE
CYBER DEFENSE
SUMMIT 2015

MIRcon.

FORESCOUT + FIREEYE JOINT SOLUTION

WALLACE SANN
FEDERAL CTO & REGIONAL VP OF SYSTEMS ENGINEERING, FORESCOUT

ForeScout

IT SECURITY CHALLENGES

The Home Depot

53 million email addresses and 56 million credit cards

Attackers used stolen vendor credential to access critical systems

SONY

Cyber attack cou… much as $1…

Disabled the ar… machines…

21m government employees identities stolen

OPM did not maintain a comprehensive inventory of servers, databases and network devices

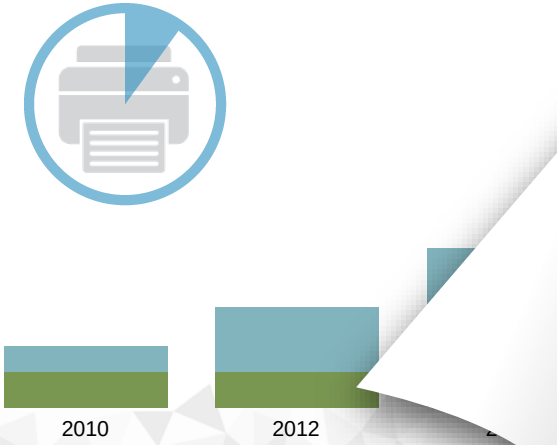
Attackers exploit vulnerable endpoints, easily move across big flat networks

“44 percent of known breaches came from vulnerabilities that are 2 to 4 years old”

HP Cyber Risk Report 2015

IT SECURITY CHALLENGES

Less than 10% of new devices connecting to the corporate environment will be manageable through traditional methods



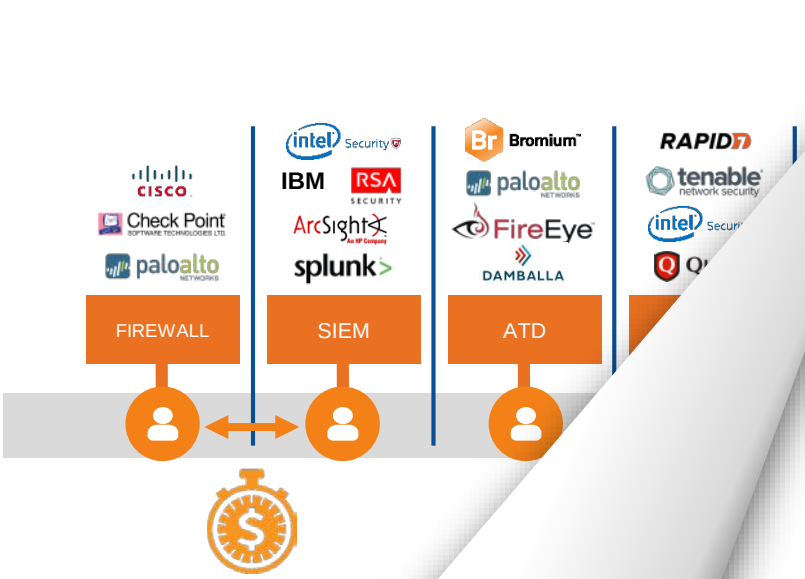
Source: Gartner, BI Intelligence, Verizon, ForeScout

Number of unmanaged devices is exploding

Dec 2014: “Within two years, 90% of all IT networks will have an IoT-based security breach”

IDC

IT SECURITY CHALLENGES



Fragmented security lets attackers in

"70 to 90 percent of all malicious incidents could have been prevented or found sooner if existing logs and alerts had been monitored"

Verizon Data Breach Investigations Report

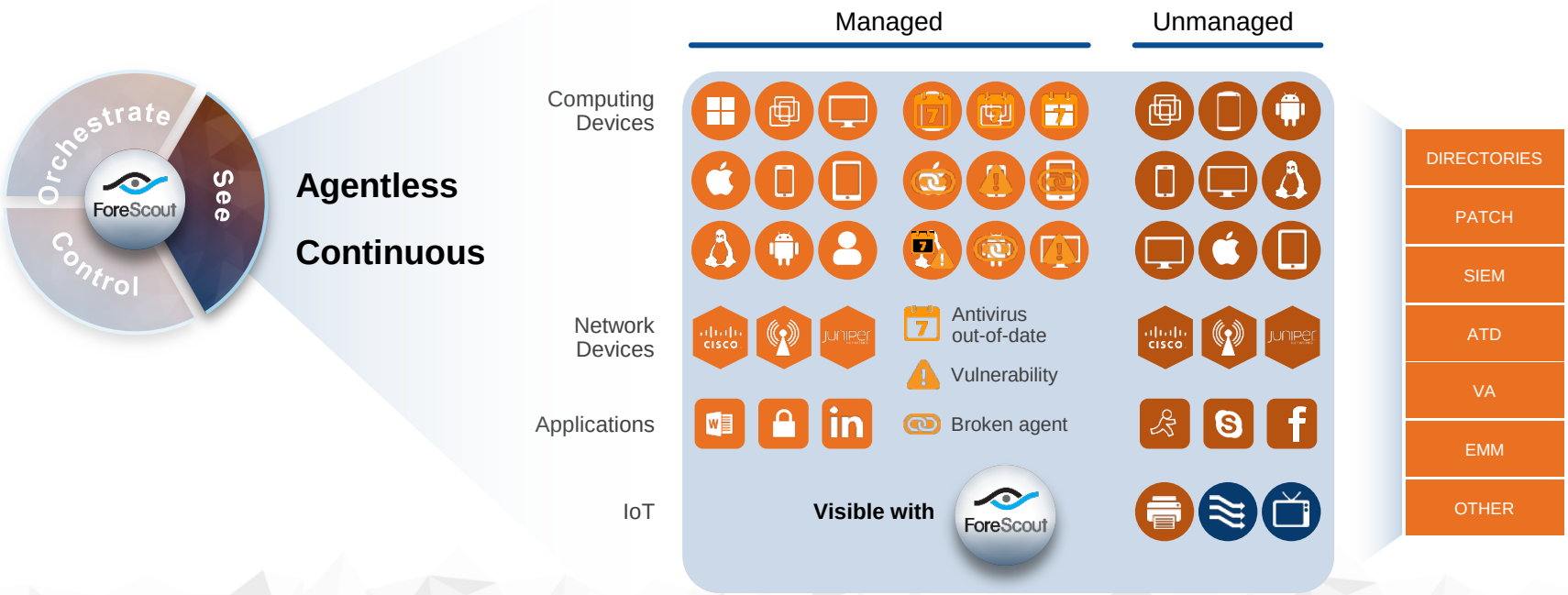
"Average time to contain a cyber attack is 31 days"

Ponemon Institute "2014 Global Report on the Cost of Cyber Crime"

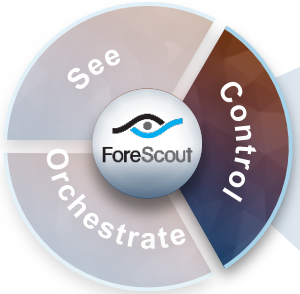
JOINT SOLUTION

1. Reveal unknown risks on your network
2. Enforce policy to reduce risks and shrink attack surface
3. Detect and block advanced threats
4. Rapidly respond to security breaches

1. SEE UNKNOWN RISKS ON YOUR NETWORK

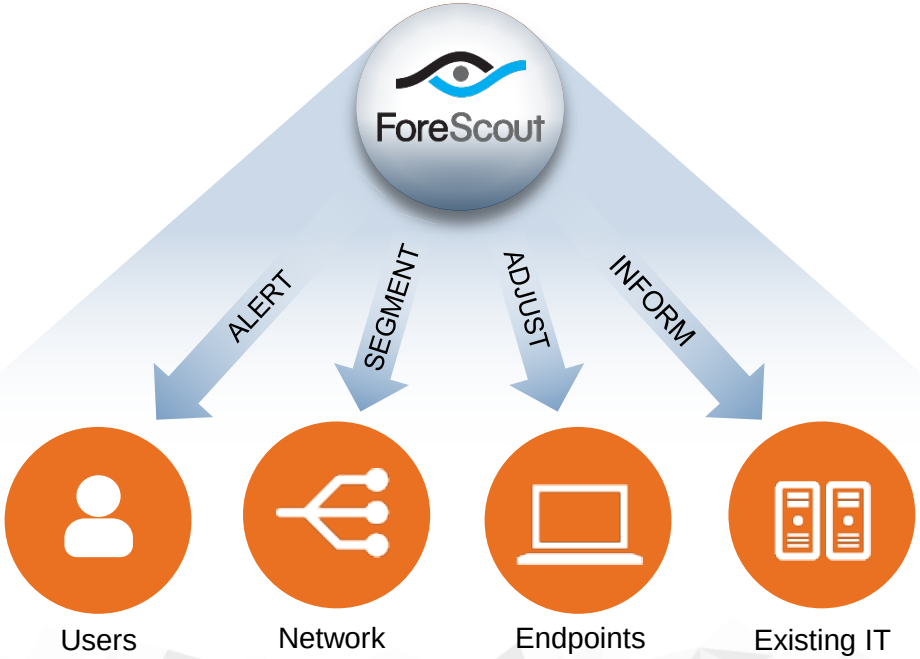


2. CONTROL ENVIRONMENT TO REDUCE RISKS



Policy-driven

Automated



3. DETECT AND BLOCK ADVANCED THREATS

4. RAPIDLY RESPOND TO SECURITY BREACH

When FireEye detects advanced threats

- First infection may have already occurred (patient zero)

Pre-infected endpoints could connect to the network

- Infected on public networks, infection pathways such as USB drives etc.

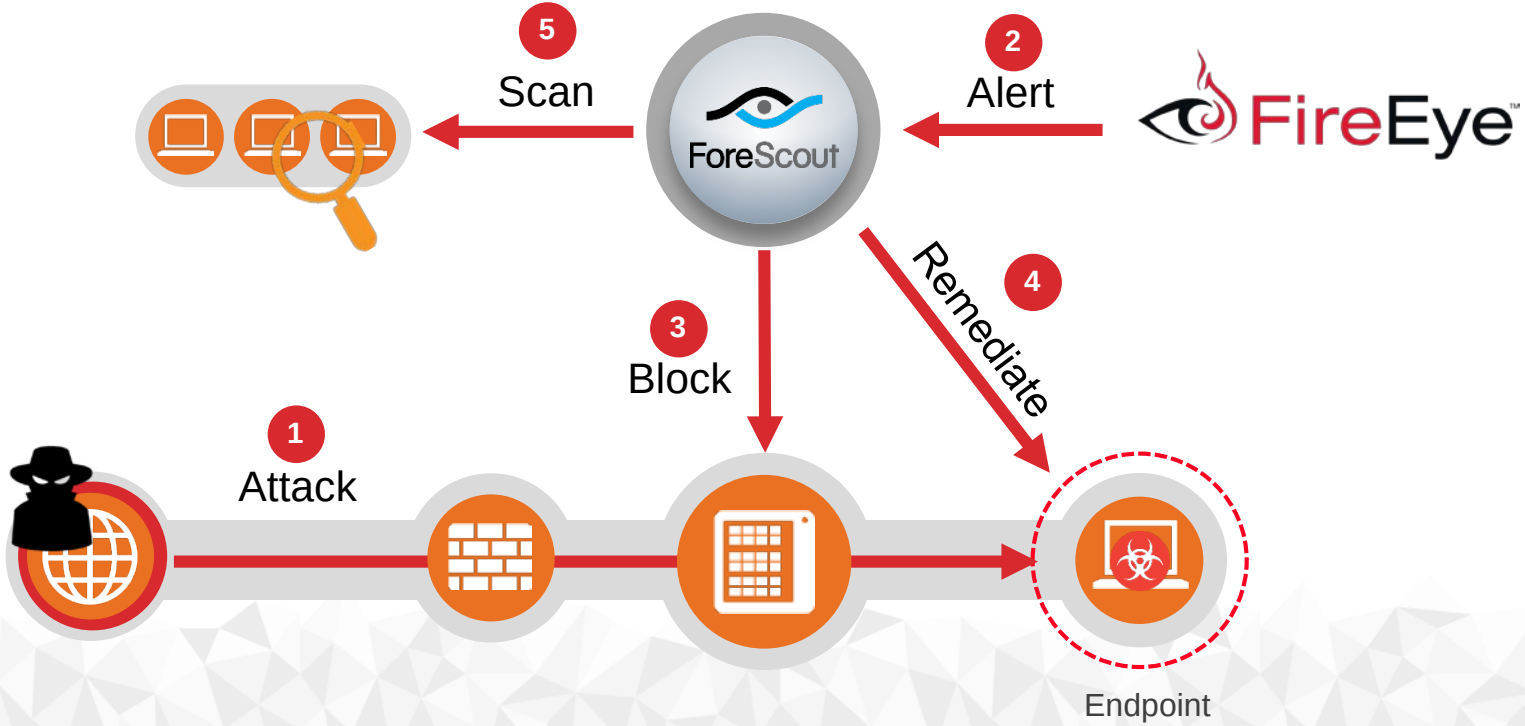
Internal propagation can start from infected endpoints

Unless deployed inline, endpoints can connect to C&C servers

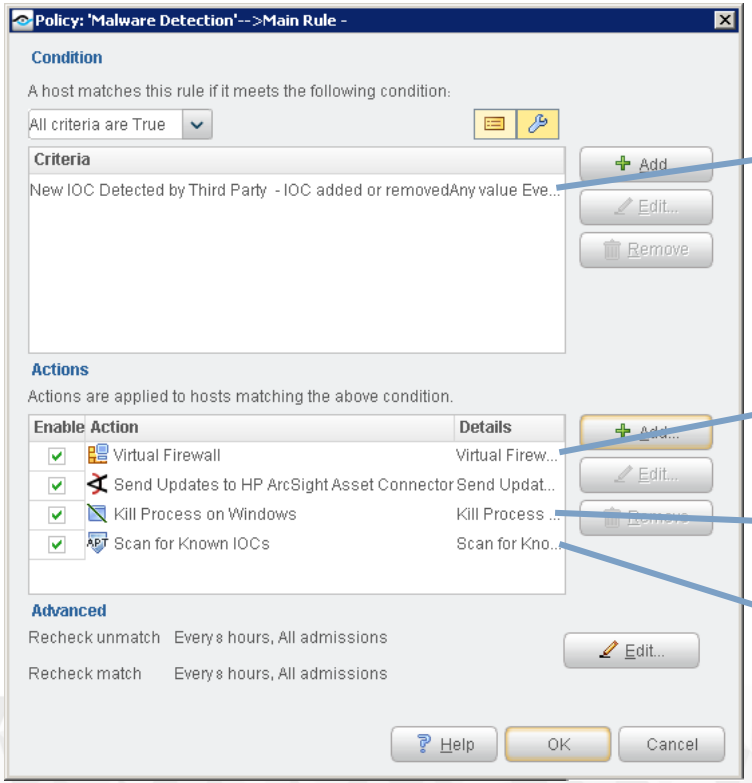
ForeScout works with FireEye to rapidly respond to prevent threat propagation and data exfiltration

- Network – quarantine infected systems
- Endpoint – confirm and kill malicious processes

4. RAPIDLY RESPOND TO SECURITY BREACH



4. RAPIDLY RESPOND TO SECURITY BREACH



IOC detected by FireEye

Quarantine System

Automate Mitigation Actions

Scan Other Systems

JOINT INTEGRATION BENEFITS

1. Gain real-time visibility
2. Expanded intelligence
3. Reduce endpoint risks and attack surface
4. Detect and block advanced threats
5. Expedite response to security breaches
   - ✓ Network – quarantine device
   - ✓ Endpoint – confirm and kill malicious processes

QUESTIONS

FIREEYE
CYBER DEFENSE
SUMMIT 2015

MIRcon.

THANK YOU