Why we need Intelligent Security?

Juha Launonen
Sourcefire, Inc.

11-2010

SOURCEfire®

About Sourcefire

Mission: To be the leading provider of intelligent cybersecurity solutions for the enterprise.

- Founded in 2001 by Snort Creator, Martin Roesch, CTO
- Headquarters: Columbia, MD
- Focus on enterprise and government customers
- Global Security Alliance ecosystem
- NASDAQ: FIRE

Agenda

- Gartner – Today's reality
- Our Challenges
- A New Approach
- Sourcefire NG Portfolio
- How it works
- Final thoughts
- Coming Up in 2011…
- Q/A

Today's Reality

"Begin the transformation to context-aware and adaptive security infrastructure now as you replace legacy static security infrastructure."

Gartner

Neil MacDonald
VP & Gartner Fellow

Source: Gartner, Inc., "The Future of Information Security is Context Aware and Adaptive," May 14, 2010

Dynamic Threats

- Organized attackers
- Sophisticated threats
- Multiple attack vectors

Static Defenses

- Ineffective defenses
- Black box limits flexibility
- Set-and-forget doesn't work

SOURCEfire®

Our Challenges

Modern Threat Landscape:

- APTs (Advanced Persistent Threats)
- Increasing number of 0-days
- Harder to discover
- Reaction time is in essence
- Hybrid forms - transformation
- Point targets – multiple vectors and sources
- Persistency
- *W32.Stuxnet...*

Our Challenges

Resource and Cost constrains:

- **Needed to deploy new systems to keep up…**
- How we can keep up with the needed expertise…
- Now we can keep up with the daily management resource needs…
- How we can keep up with the Incident Response time…
- TCO…

→ *How to justify this all emerging need and fit into our limited budgets?*

A New Approach

How about if you could have:

- Intelligent Integration and interoperability of your security systems
- Constantly and automatically updating view of your assets
- Automated correlation of the security events
- Appropriately automated counter measures
- Crucial detection of abnormal activity in your network…
- **I.e. Adaptive Security posture**

Sourcefire Next-Gen Portfolio

SOURCEfire®

Next-Generation IPS

NSS Labs TESTED

ICSA labs CERTIFIED NETWORK IPS

Defense Center Management Console

Intrusion Prevention

SNORT®

Awareness Technologies

CITRIX · Gmail · skype · AIM · ORACLE

Networks *Apps* *Behavior* *Users*

SSL Inspection

Virtualization

vmware®

Xen™

Sourcefire Ingredients

Defense Center

3D Sensors

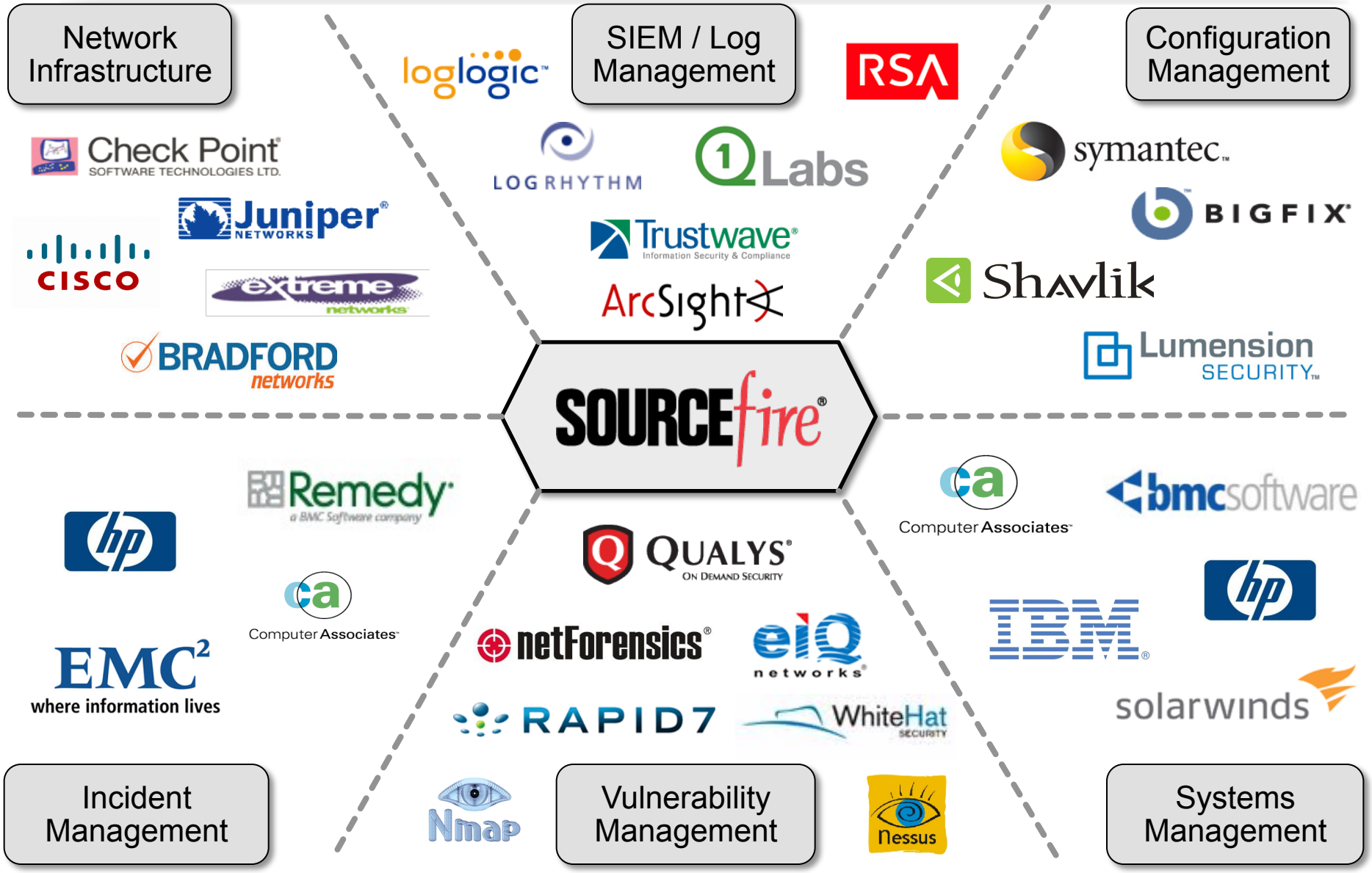
Sourcefire IPS Solution

Defense Center Awareness Bundle

3D Sensors

Sourcefire Next-Gen IPS Solution

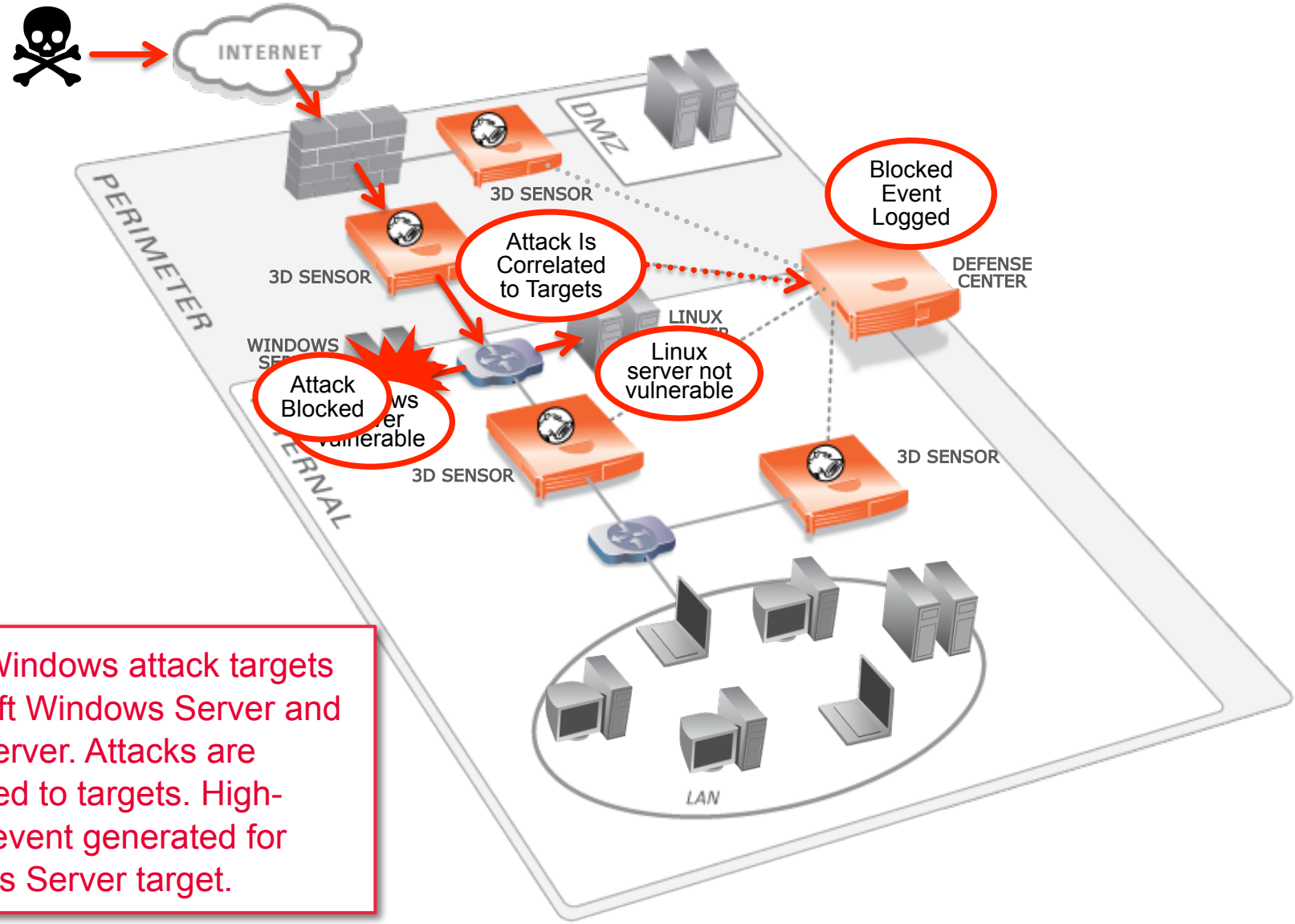
Comprehensive Ecosystem



How It Works

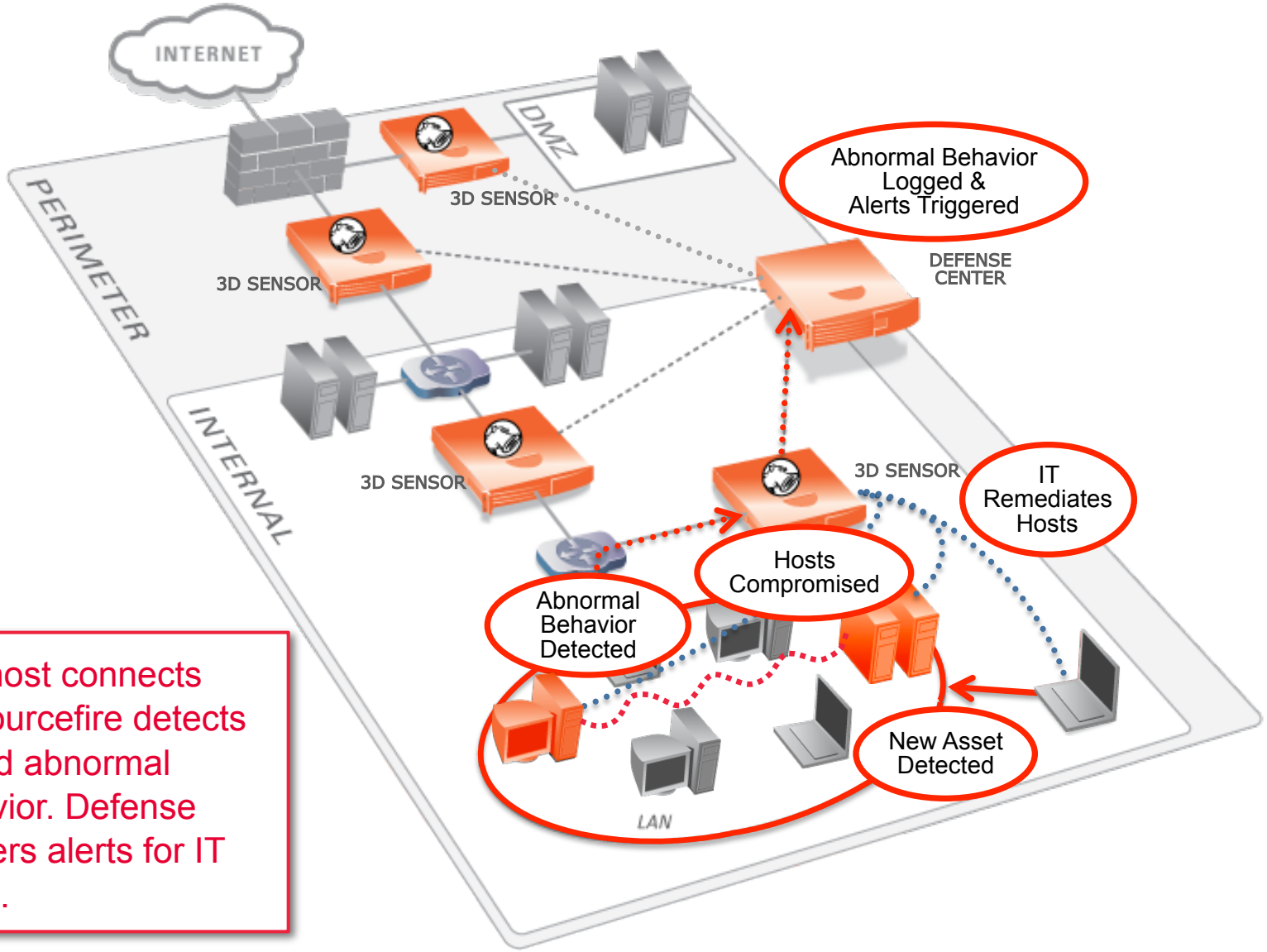
SOURCEfire®

Intelligent Correlation to the Target



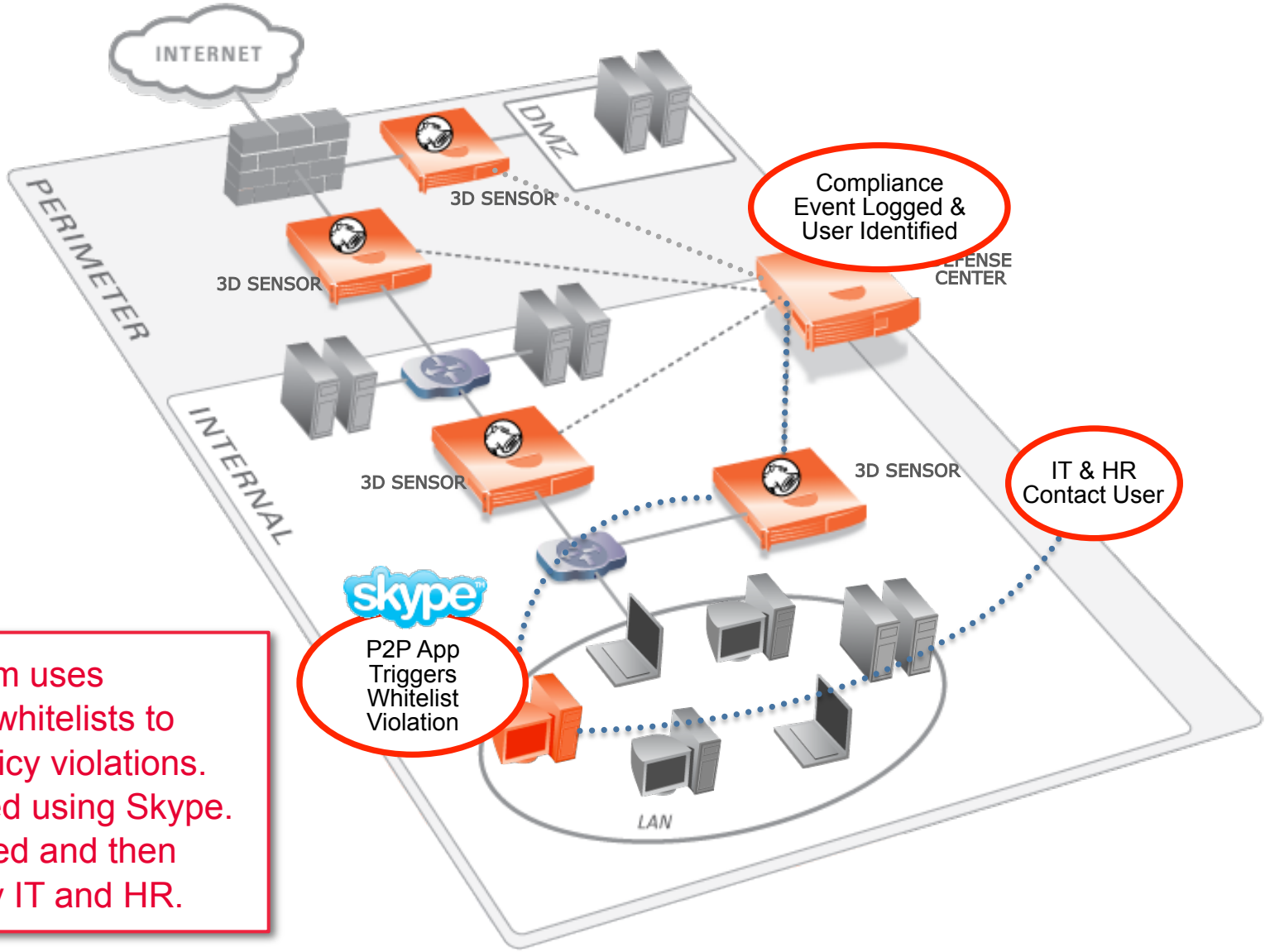
Latest Windows attack targets Microsoft Windows Server and Linux Server. Attacks are correlated to targets. High-priority event generated for Windows Server target.

Intelligent Anomaly Detection



New rogue host connects internally. Sourcefire detects new host and abnormal server behavior. Defense Center triggers alerts for IT to remediate.

Intelligent Application Violation



Security team uses compliance whitelists to detect IT policy violations. Host detected using Skype. User identified and then contacted by IT and HR.

Final thoughts

- Network security is tough and will remain so while hackers are intelligent and motivated
- Intrusion prevention can be easy, through the power of *accurate detection* coupled with *intelligent automation*
- Take the first step. Evaluate Sourcefire!

FAIL is never more than a second away…

Questions?

Juha Launonen
jlaunonen@sourcefire.com

SOURCEfire®