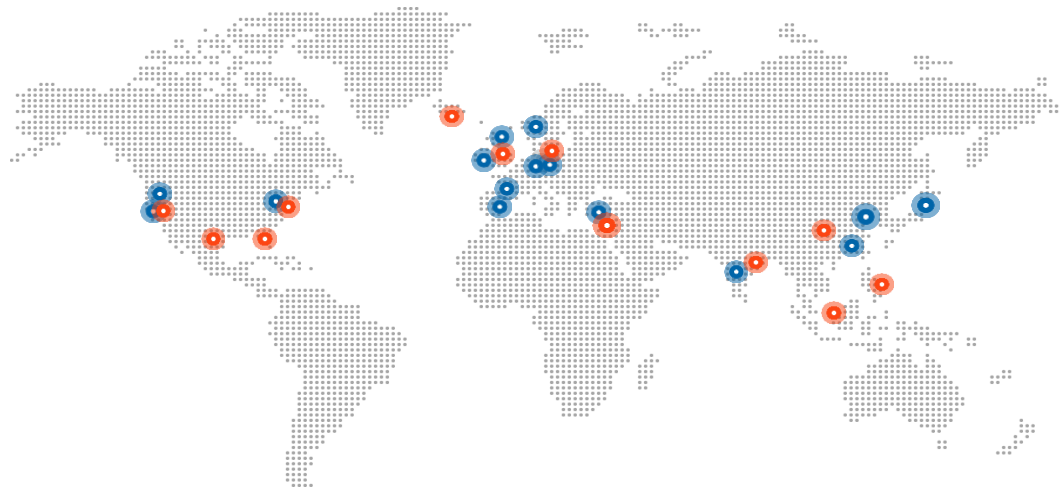# CYREN Web Security: Zero Hour Detection

Robert Bruce – Channel Sales Director

CYREN Powers the World's Security

200+
OEM customers

500K
Points of presence

600M
End users

17B
Daily Transactions

FireEye

intel Security

Check Point
SOFTWARE TECHNOLOGIES LTD.

Google

SOPHOS

Microsoft

zscaler

RSA
SECURITY

proofpoint

websense

DELL

YAHOO!

Symantec

IBM

CYREN

CYREN Platform Solutions

Our Cyber vision: To be the most accurate and actionable threat detection solution for unknown threats.

Global threat analysis, behavioral, and dynamic reputation scoring is only available via tools that use the Cloud.

Cloud-driven cybersecurity solution enabling full content inspection, including SSL traffic to better protect users from rapidly evolving cyber threats
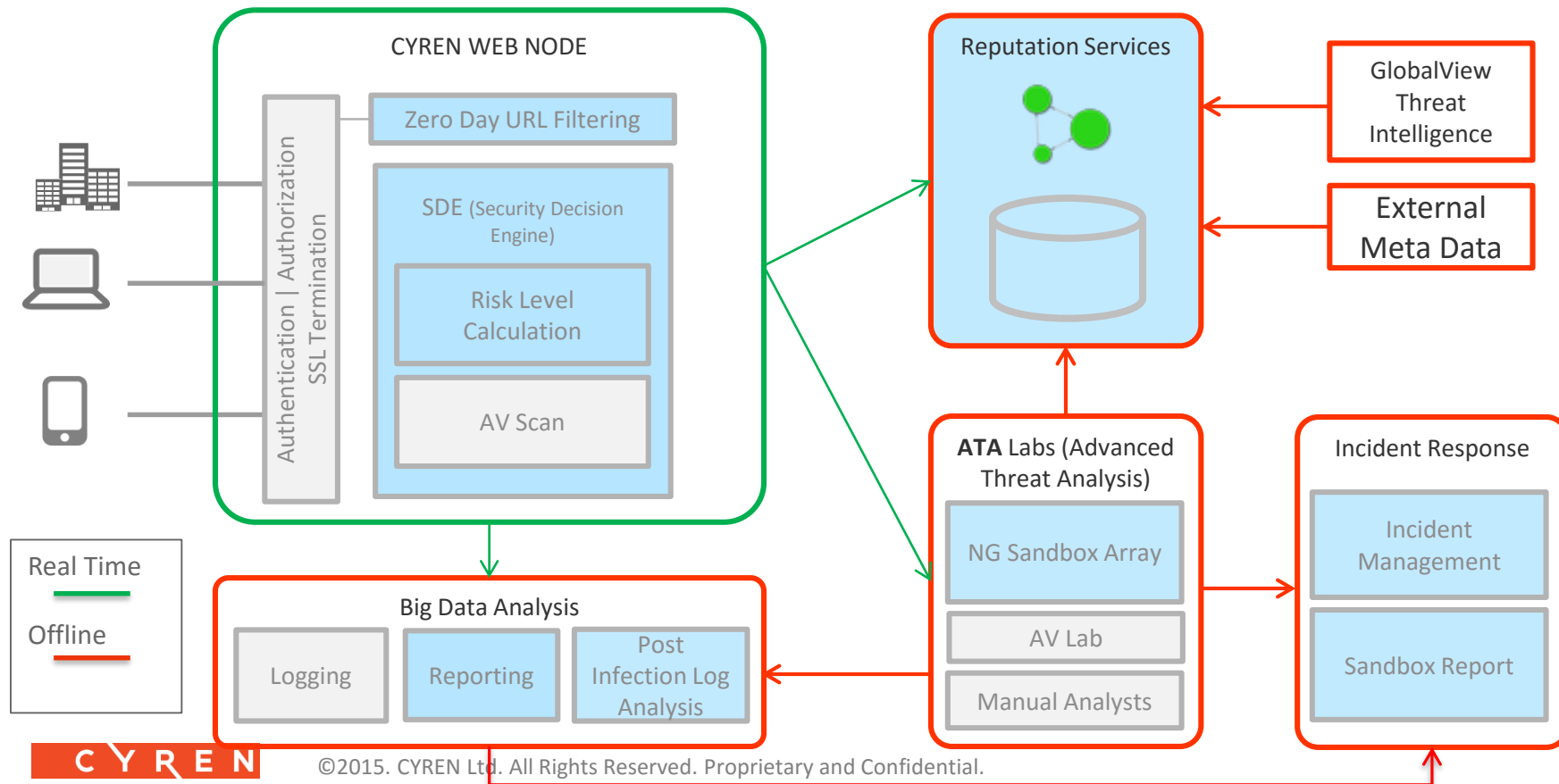
CYREN
WebSecurity

Cybersecurity products and solutions responsive to advanced malware and other cyber attacks, which target data centers and routinely bypass conventional signature-based defenses

CYREN
Cyber Threat Protection

Use cloud-based solutions to arm your organization with the intelligence needed to prevent and handle breaches.

CWS 3.0 Threat Architecture

CYREN WEB NODE

Zero Day URL Filtering

SDE (Security Decision Engine)

Risk Level Calculation

AV Scan

Authentication | Authorization SSL Termination

Reputation Services

GlobalView Threat Intelligence

External Meta Data

ATA Labs (Advanced Threat Analysis)

NG Sandbox Array

AV Lab

Manual Analysts

Incident Response

Incident Management

Sandbox Report

Real Time

Offline

Big Data Analysis

Logging

Reporting

Post Infection Log Analysis

CYREN

The Security Decision Engine

- Goal: Activate security measures based on a transaction's risk level

- How:
    - Checks the URL / Host / Domain / IP reputation

    - Maps the reputation score to a risk level
        - Clean, Probably Clean, Unknown, Suspicious, Probably Malicious, Malicious

    - Decides if to calculate the actual file type

    - Decides if to send the file for AV scanning

    - Decides if to send the file for Sandbox analysis

    - Enforces the customer's policy

Sandboxin

AV Scanning

URL Reputation

URL Filtering
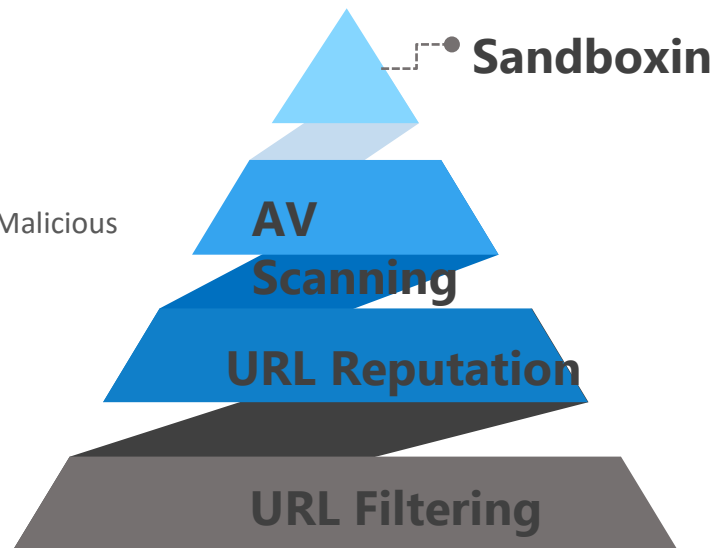
The Zero Day Categories

- Goal: Blocking zero day malware, phishing and C&C

- Feed URLF with suspicious URLs from sandbox analysis

- Introducing 3 new categories in CWS
  - Zero Day Malware
  - Zero Day Phishing
  - Command and Control (C&C)

Security Decision Engine

👤 Users | 🌐 Locations   📄 **Policy Sets**   🛡 Protection

Recent Policy Sets:

Security   Compliance   Productivity

▾ Security

ⓘ It is storngly recommended to use the default settings

Anti Malware [OFF]

When Anti-Malware Scanning is on, web resources are scanned for malware.
Note: We strongly recommend you use the default settings.

SafeSearch [ON]

When SafeSearch is on, adult content is excluded from search results generated by the leading search engines (Google, YouTube, Yahoo, and Bing). When DNS-based filtering is used, adult content is excluded from Google and YouTube results.
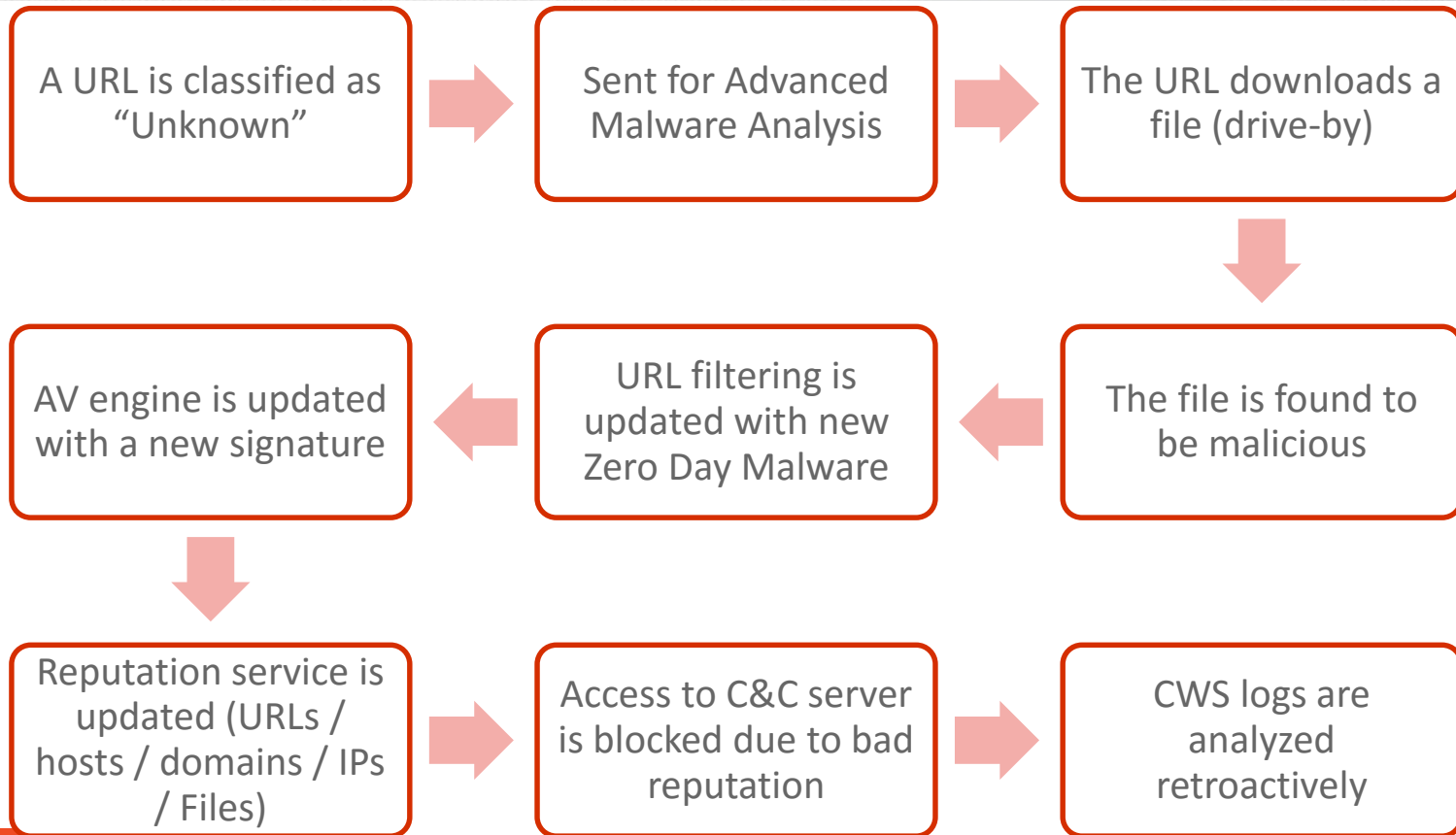
**ATP Threshold** [ON]

Choose on what level the user will be blocked:

SUSPICIOUS

Low   High

The Story of a New Threat

A URL is classified as "Unknown" → Sent for Advanced Malware Analysis → The URL downloads a file (drive-by)

AV engine is updated with a new signature ← URL filtering is updated with new Zero Day Malware ← The file is found to be malicious

Reputation service is updated (URLs / hosts / domains / IPs / Files) → Access to C&C server is blocked due to bad reputation → CWS logs are analyzed retroactively

Setting a New Standard for Regional Privacy

Comply with privacy laws prohibiting transfer of users' personal data outside the region

- Application layer is served within the region

- Personal private (PII) data (user name, email, site name, customer name) <u>never leaves the home region</u>

- Public data (policy, configuration, hashed values) replicated across regions enables seamless roaming

- Logs do not include any PII

- Hashed values map to private data for reporting purposes <u>only in the relevant home region</u>
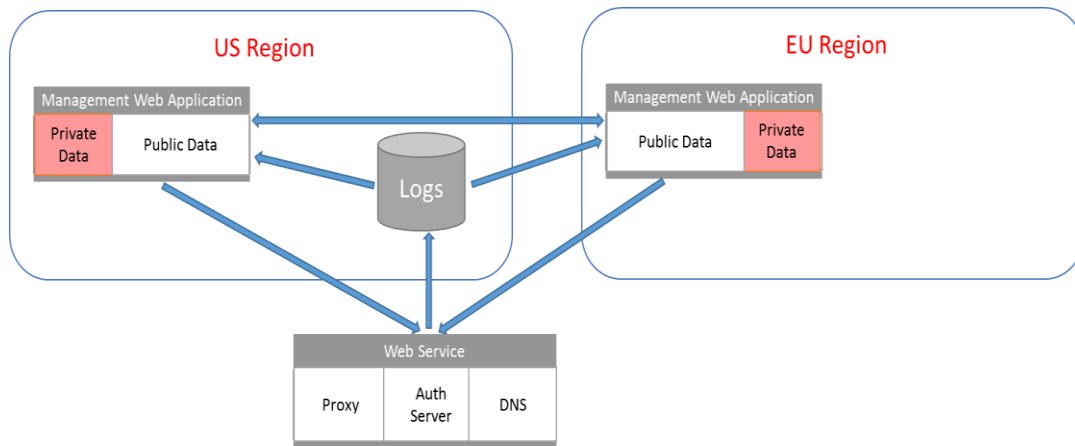
CYREN

Any Questions?

Thank You. Any Questions or Thoughts?

Pete Starr

Principle Sales Engineer

+44 7595 397777

pete.starr@CYREN.com

Rob Bruce

Channel Sales Director

+44 7966 405361

pete.starr@CYREN.com

You can also find us here:

www.CYREN.com

twitter.com/cyreninc

linkedin.com/company/cyren