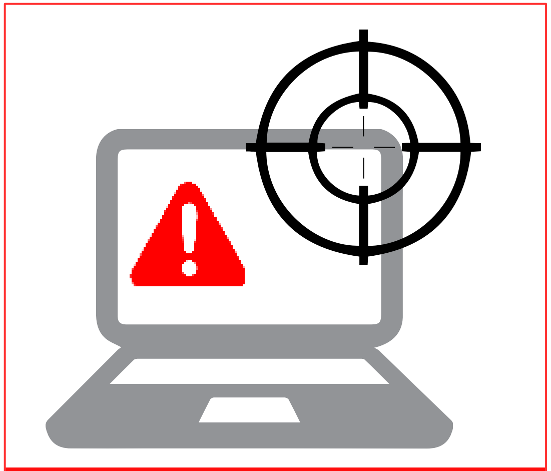
WatchGuard

# Threat Detection and Response

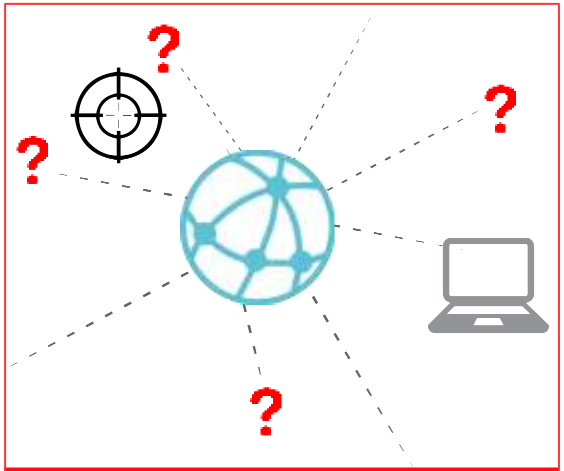
Christian L. Rochet, *CISM*
*Vice President*

ROCHET
Business Technologies

# The Market Problem



Endpoint and Network
prevention not
blocking all threats.



Difficult to connect the dots
between
Network and Endpoint

Not enough
staff, expertise, or time
to triage advanced threats

**SMBs are aware of the threat landscape.**
**It’s just not enterprises that are under attack.**
**SMBs, too, need the right tools to *reduce Time to Detection.***

# Defense in depth

# Threat Detection and Response

Threat Detection and Response correlates network and endpoint security events with threat intelligence to detect, prioritize and enable immediate action against threats.

# Intelligent Protection

CORRELATION
CORRELATION

**PREVENT**

Protect your network from threats before they ever execute on a host computer

**DETECT**

Observe hosts, files, applications and traffic for abnormal behavior

**RESPOND**

Set policies to automatically alert and/or respond to threats

Our unique threat correlation engine is constantly working to correlate network and endpoint security events with known threat intelligence data to identify and stop new threats and constantly improve preventative security measures.

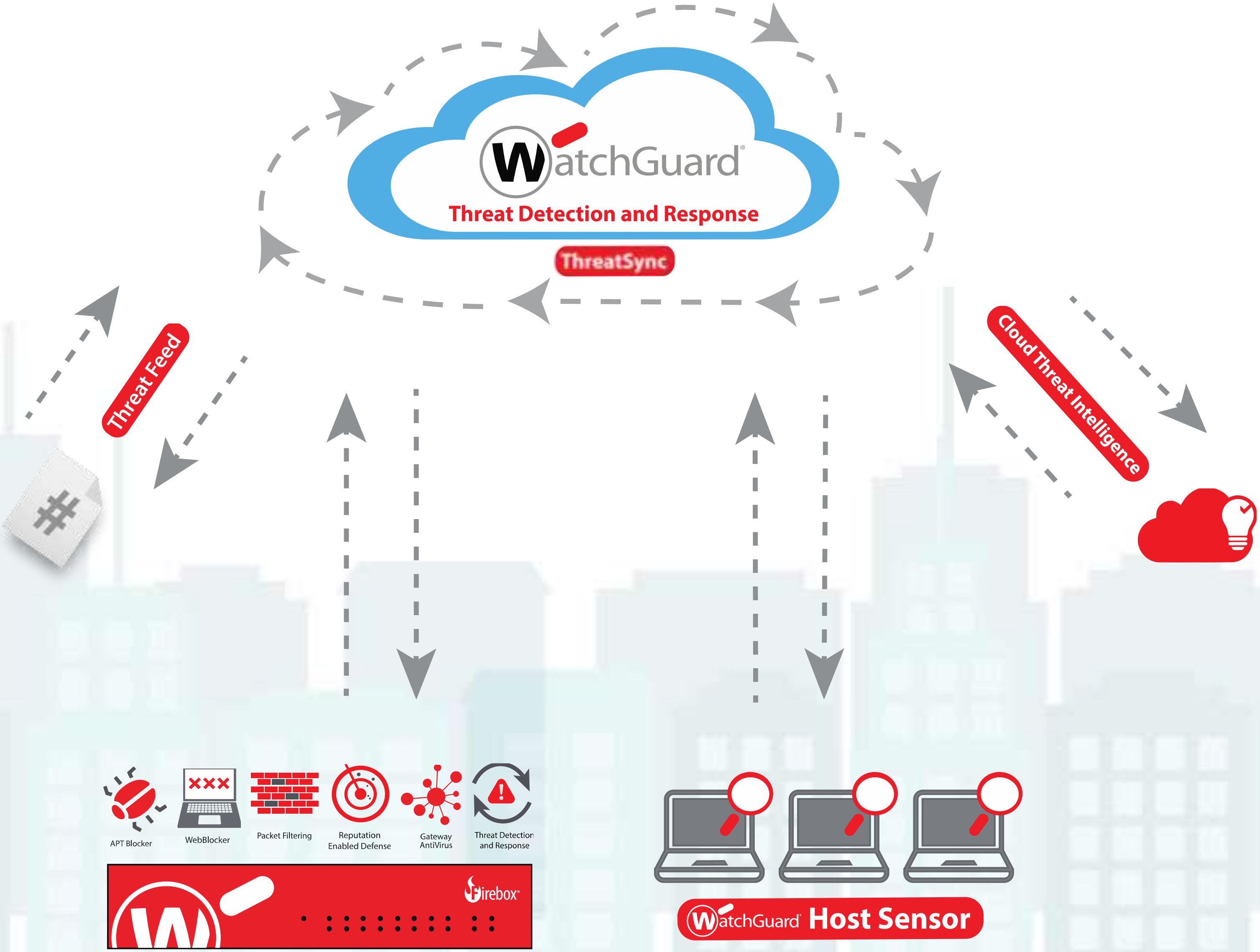
# TDR Components

**Host Sensor**
Provides *visibility* into the endpoint and also facilitates *response* on the endpoint when a threat is detected.

**ThreatSync**
A one-of-a-kind *threat correlation engine* that collects security events from the endpoint, the network, and 3rd party threat feeds, correlates and then scores those threats for automated or manual response.

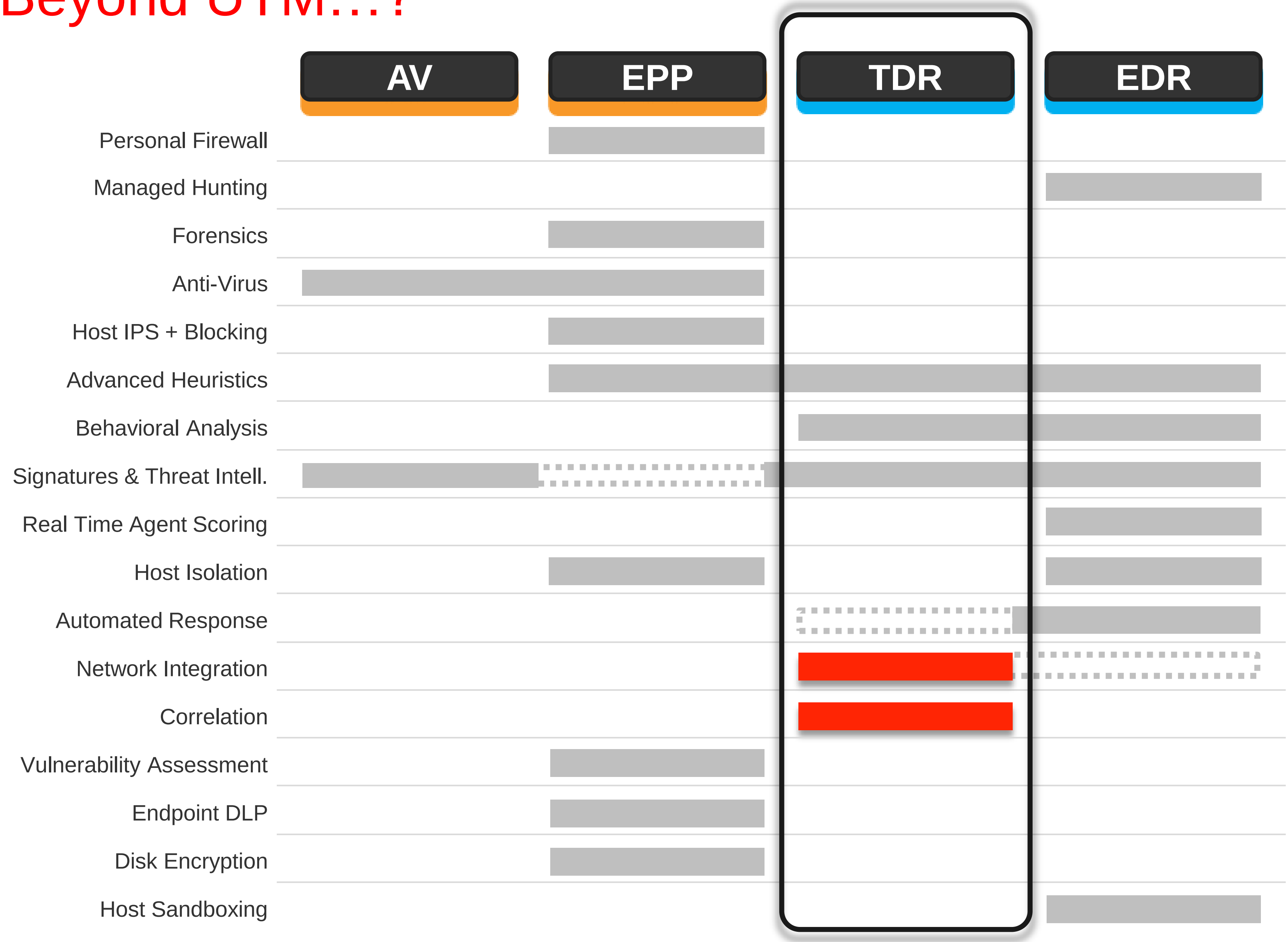
**Host Ransomware Prevention**
Host Ransomware Prevention prevents the execution of ransomware *before any encryption* takes place, mitigating the ransomware attack before any damage is done.

# ThreatSync



WatchGuard
Threat Detection and Response
ThreatSync
Threat Feed
Cloud Threat Intelligence
APT Blocker
WebBlocker
Packet Filtering
Reputation Enabled Defense
Gateway AntiVirus
Threat Detection and Response
Firebox
WatchGuard Host Sensor

# Beyond UTM…?



| | AV | EPP | TDR | EDR |
|---|---|---|---|---|
| Personal Firewall | | ■ | | |
| Managed Hunting | | | | ■ |
| Forensics | | ■ | | |
| Anti-Virus | ■ | ■ | | |
| Host IPS + Blocking | | ■ | | |
| Advanced Heuristics | | ■ | ■ | ■ |
| Behavioral Analysis | | | ■ | ■ |
| Signatures & Threat Intell. | ■ | ⬚ | ■ | ■ |
| Real Time Agent Scoring | | | | ■ |
| Host Isolation | | ■ | | ■ |
| Automated Response | | | ⬚ | ■ |
| Network Integration | | | 🟥 | ⬚ |
| Correlation | | | 🟥 | |
| Vulnerability Assessment | | ■ | | |
| Endpoint DLP | | ■ | | |
| Disk Encryption | | ■ | | |
| Host Sandboxing | | | | ■ |

# Huge Value for Customers

- Prevention of Advanced Threats
- Holistic Detection and Response across the Network and Endpoint
- Continuous Monitoring and Analytics
- Enterprise Grade Correlation to Remove Silos & Connect the Dots
- Automated Threat Response
- Enterprise-Grade Threat Intelligence
- Low TCO – Savings

# The WatchGuard Difference

## Enterprise-Grade

Best-in-class security services without the cost or complexity.

## Simplicity

Easy and straight-forward to configure, deploy, and centrally manage.

## Top UTM Performance

Fastest UTM performance at all price points.

## Threat Visibility

Full network visibility with the power to take action immediately.

## Future-Proof

The quickest access to new and improved security services.

# NOTHING GETS PAST RED.