Deep Discovery

Technical details

Deep Discovery Technologies

Entry point

Lateral Movement

Exfiltration

360°Approach

- Network Monitoring
- Content Inspection
- Document Emulation
- Payload Download
- Behavior Tracing
- Exploit Detection

More than 80 protocols analyzed

HTTP | SMTP | DNS | FTP

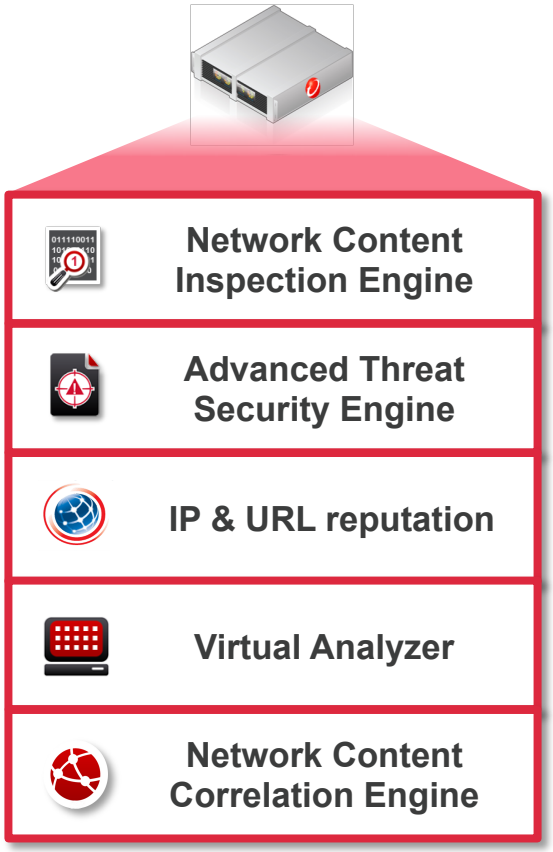
CIFS | SQL | P2P | -----

Embedded doc exploits
Drive-by downloads
Dropper
Unknown Malware
C&C access
Data stealing
Worms/Propagation
Backdoor activities
Data exfiltration…

Single Appliance for Advanced Protection

Deep Discovery Inspector

- Appliance **All-in-One**
  Up to 4 Gbps model
- Bare Metal & VA available
- **Custom sandboxes** embedded
- Can be linked to external SB



All protocols analyzed on a **single box**

- Detect known, **unknown** and **custom** threats
- Leverage Trend Micro **Threat Intelligence** technologies
- **Adapts** and **responds** to threats in your unique environment

Deeper Look into Deep Discovery
Virtual Analyzer

Your Custom Sandbox

- Custom OS image
- Execution acceleration
- Anti-Analysis detection
- 32 & 64 bits
- Execute binaries, documents, URL...

LoadLibraryA ARGs: (NETAPI32.dll) Return value: 73e50000
LoadLibraryA ARGs: (OLEAUT32.dll) Return value: 75de0000
LoadLibraryA ARGs: (WININET.dll) Return value: 777a0000

Modifies file with infectible type : **eqawoc.exe**
Inject processus : **2604 taskhost.exe**
Access suspicious host : **mmlzntponzkfuik.biz**

internet_helper API Name: InternetConnectA ARGs: (cc0004,
mmlzntponzkfuik.biz, 10050, , , 3, 0, 0) Return value: cc0008
.....

Live monitoring

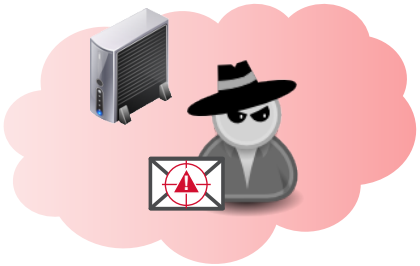
- Kernel integration (hook, dll injection..)
- Network flow analysis
- Event correlation

Deep Discovery
Simple & Efficient

Infection & payload

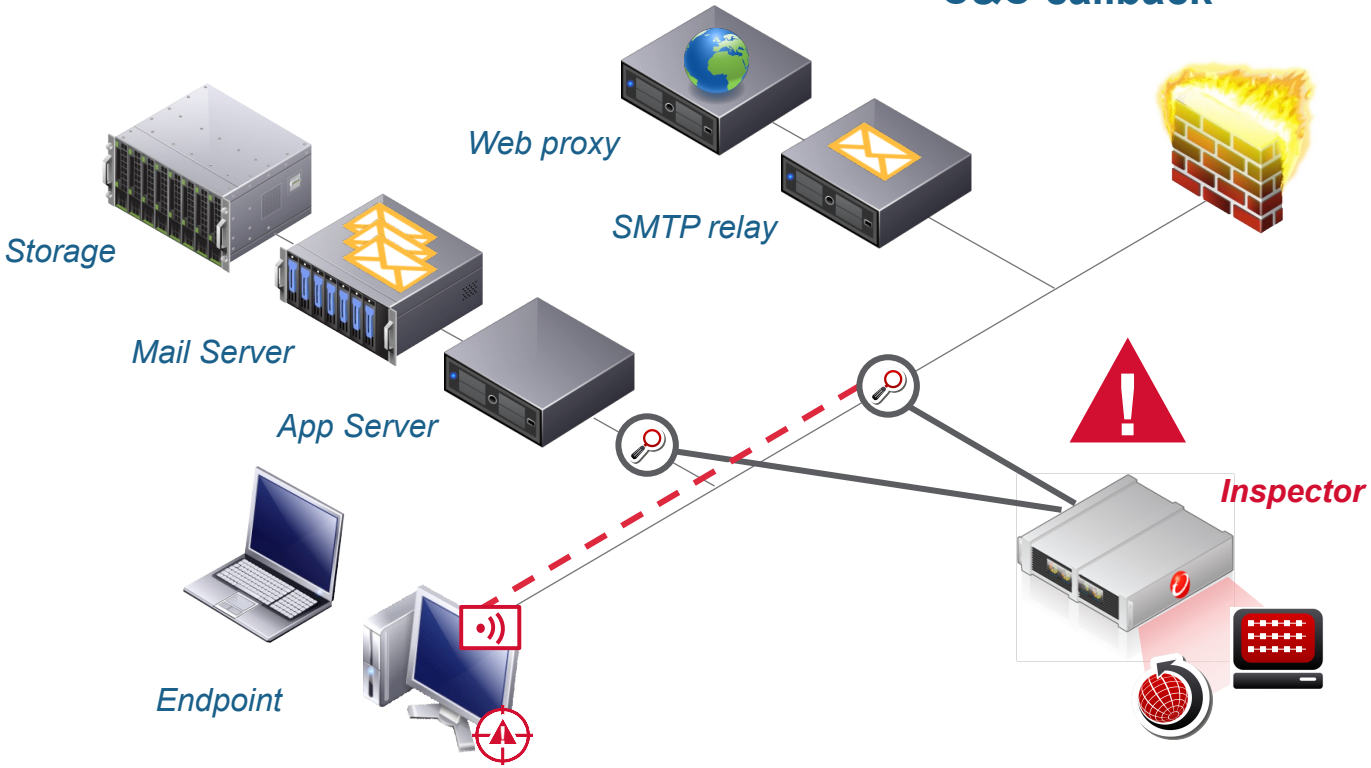
Lateral movement

C&C callback



Dynamic blacklist

af12e45b49cd23...
48.67.234.25:443
68.57.149.56:80
d4.mydns.cc
b1.mydns.cc
...



Create your **Custom Defense**

Analyzer

- External sandbox system
- Automatic Analysis Labs
- Manual & API submission tools
- Multi-box (*5 nodes, 100k files/day)*

Integrated into

Trend Micro solutions

Threat profil export
(IOC, hash)

API & scripting

Email Inspector

- Email reputation & attachment analysis
- Embedded URL analysis in VA
- MTA (inline) or BCC (monitor) mode
- Up to 2M mails/day per box

Threat Intelligence Center

- Central event dashboards
- Custom searches & reports
- Central alerting and reporting

Get a complete picture of targeted attacks

Deep Discovery Endpoint Sensor

Context-aware endpoint solution designed to speed the **discovery**, **investigation** and **response** to security incidents

Accelerate you response process

- Confirm **endpoint infiltration** alerts from network security
- See which endpoints have specific malware or **C&C activity**
- Discover full context and **spread of an attack**

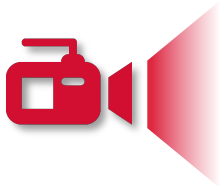
Get a full picture of threats

- **Records** detailed system activities
- Performs **multi-level search** across endpoints
- Uses rich search criteria
- **Compatible with any AV** security solution

TREND MICRO

Catch all endpoint activities & Make the story of the attack
Deep Discovery Endpoint Sensor

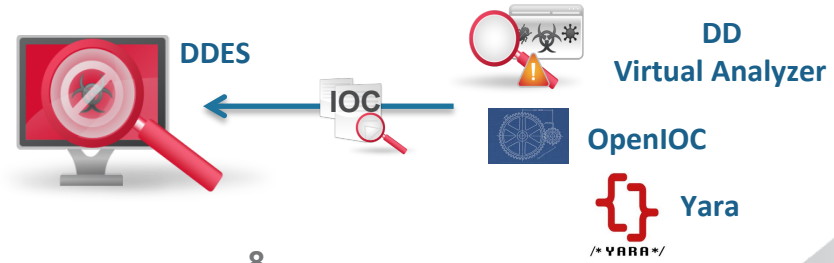
Record all events across **endpoint and network** to filter out "Ghost Alert" noise and re-classify **alert severity with REAL threat**



File changes/dropped
Registry changes
User account modification
URL request
Connection to direct IP
DNS resolution…

Adaptive **Investigation** empowers InfoSec **immediate incident responses** rather of relying on vendor solution delivery

- OpenIOC support
- Memory snapshot
- Registry snapshot
- Retrospective Replay



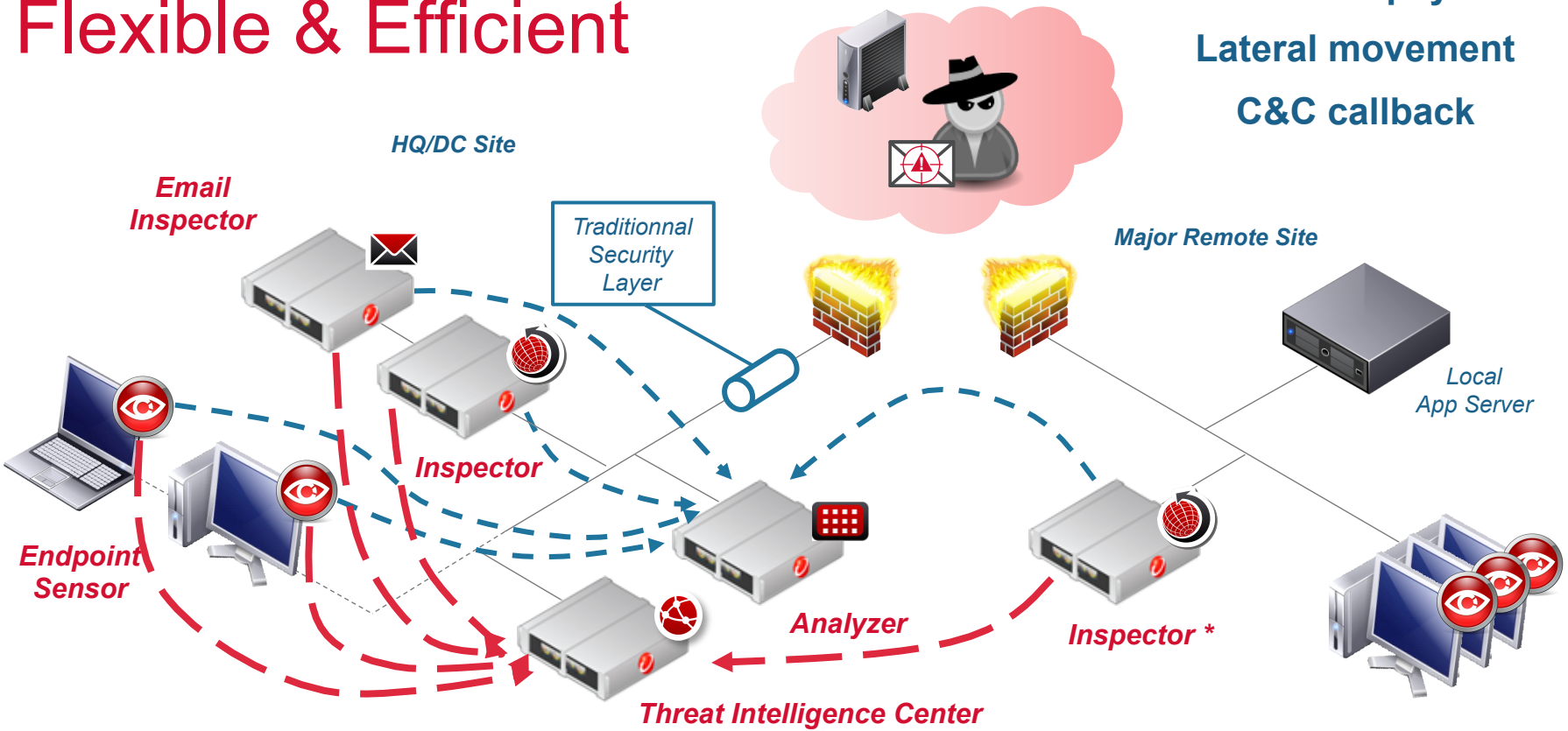
Deep Discovery

Flexible & Efficient

Infection & payload

Lateral movement

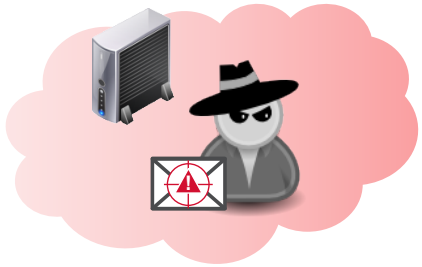
C&C callback

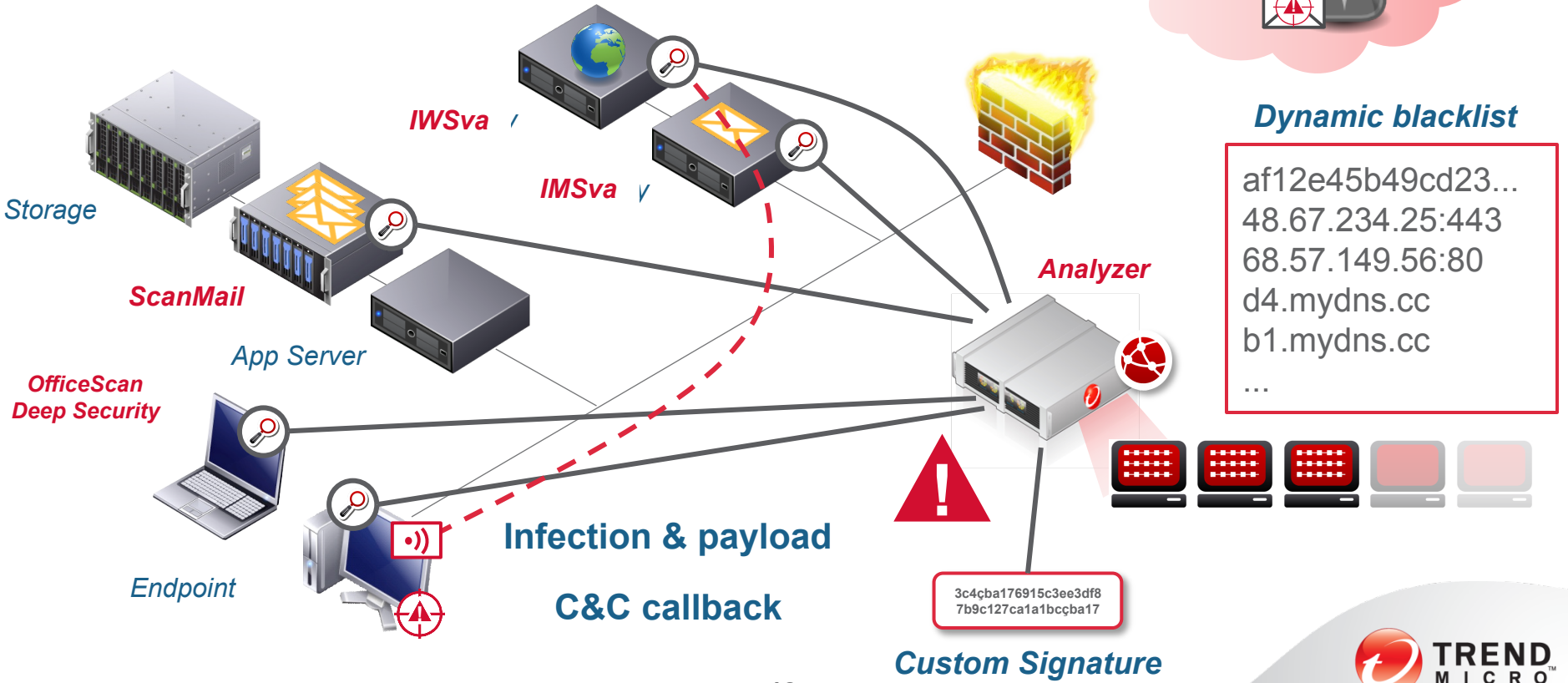


* Can be virtualized

Trend Micro Products

Integrated Advanced Protection





Demo-time!

TREND MICRO