
A New Approach
Unified Security
Haider Pasha, CISSP, C|EH, CCIE
Director, Security Strategy
Emerging Markets
Symantec

# Our Biggest Security Challenges

Maintain Security and Compliance as business models change

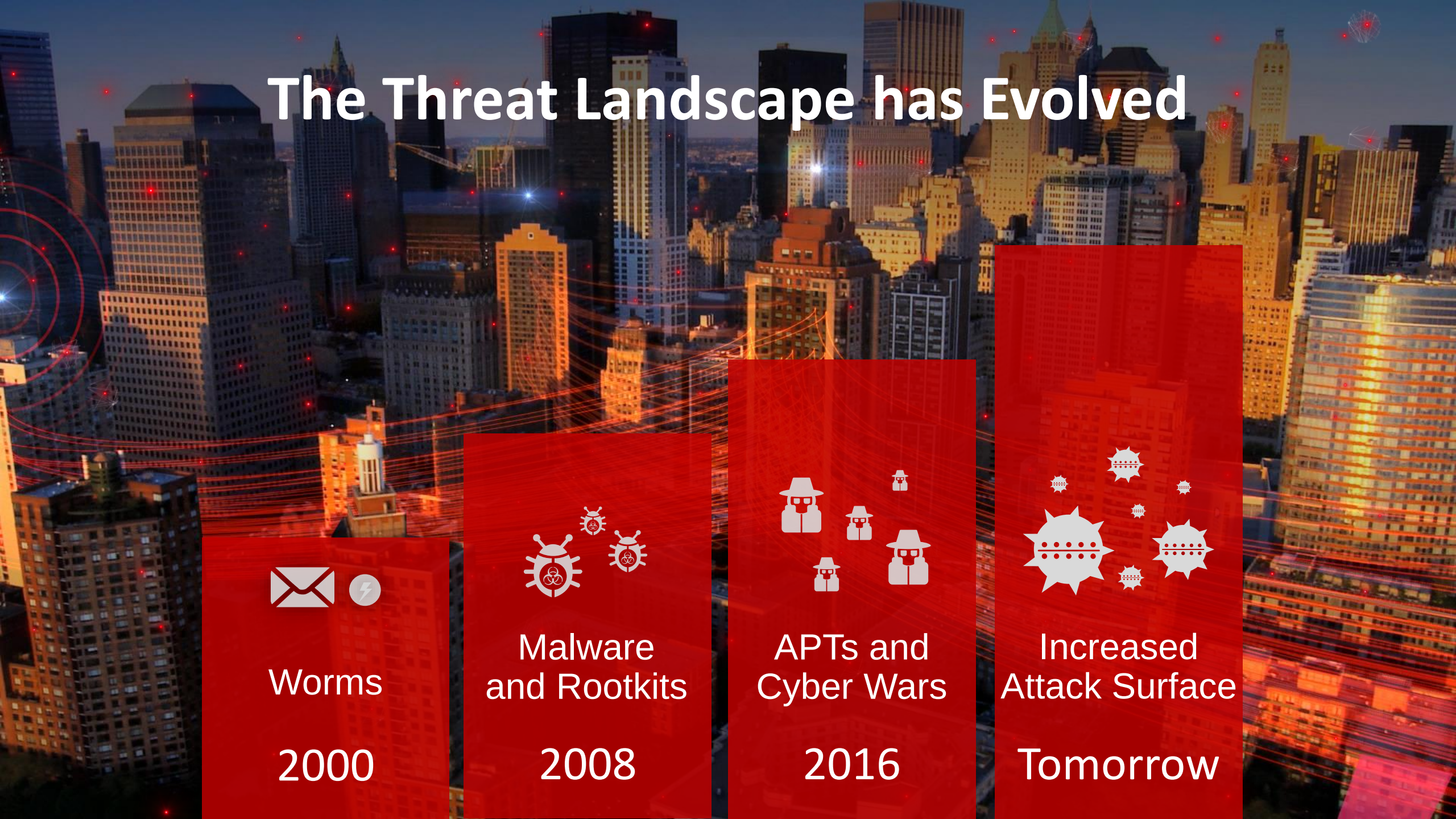
(Staying Agile)

Stay ahead of the threat landscape (Staying Proactive)

Reduce complexity and fragmentation of security solutions

(Staying Simple)

# The Threat Landscape has Evolved



Worms

2000

Malware and Rootkits

2008

APTs and Cyber Wars

2016

Increased Attack Surface

Tomorrow

# *There's a Vulnerability for everything…*









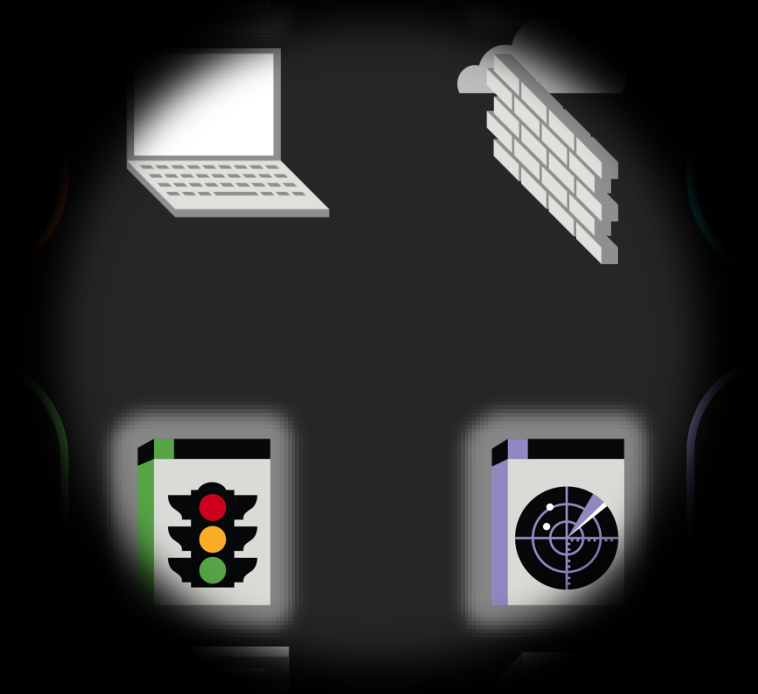


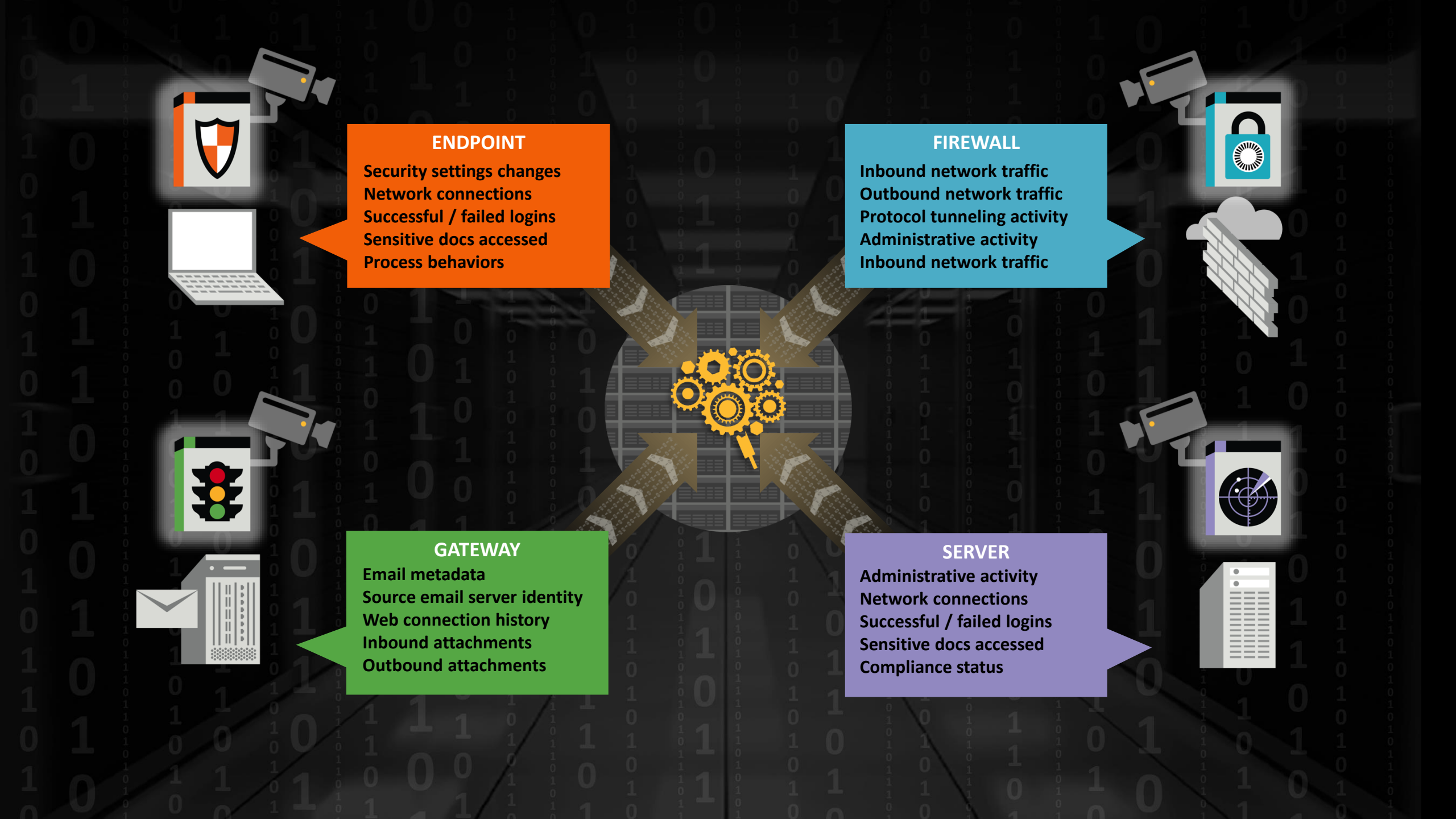


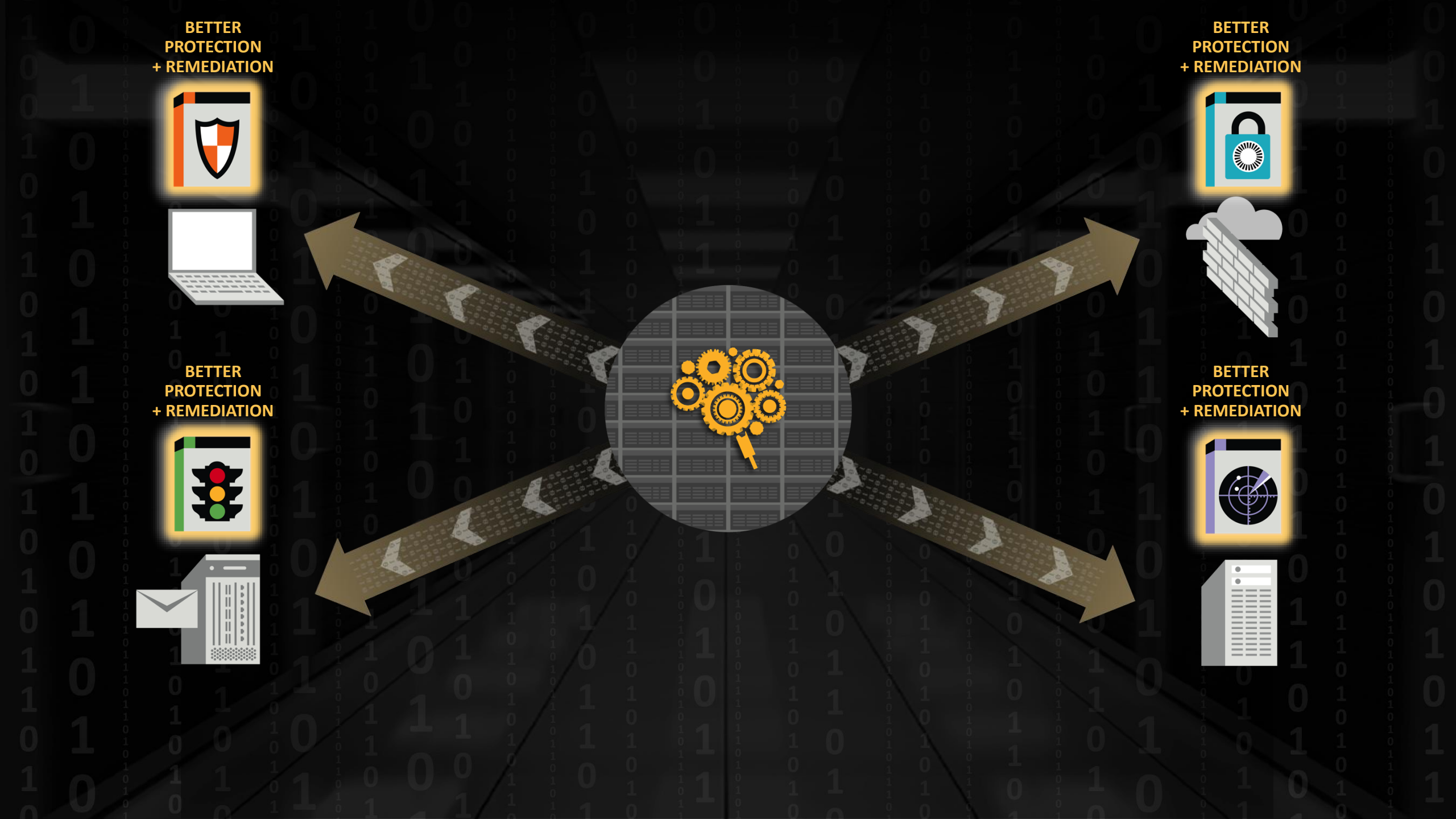

…

http://www.csoonline.com/article/2835080/data-breach/15-of-the-scariest-things-hacked.html

Your **Digital Shadow** grows with every online interaction!




ENDPOINT
Security settings changes
Network connections
Successful / failed logins
Sensitive docs accessed
Process behaviors
FIREWALL
Inbound network traffic
Outbound network traffic
Protocol tunneling activity
Administrative activity
Inbound network traffic
GATEWAY
Email metadata
Source email server identity
Web connection history
Inbound attachments
Outbound attachments
SERVER
Administrative activity
Network connections
Successful / failed logins
Sensitive docs accessed
Compliance status


BETTER
PROTECTION
+ REMEDIATION
BETTER
PROTECTION
+ REMEDIATION
BETTER
PROTECTION
+ REMEDIATION
BETTER
PROTECTION
+ REMEDIATION


BENCHMARKING ACROSS PEERS
A
B
INDUSTRY-SPECIFIC ATTACK CAMPAIGNS
GLOBALLY INFORMED DEVICE RISK
?
Many we have not thought of yet


BUILD/ACQUIRE
PARTNER
COLLECT
3rd Party
3rd Party
INCIDENT MANAGEMENT
INCIDENT INVESTIGATION
INTERACTIVE ANALYTICS
RISK ANALYSIS & REDUCTION

Your company gets a tip from a law enforcement agency that they may be under attack

They have only one lead: The name of a single file

msnsrv.exe

# File Telemetry

## What is the file?

# Behavioral and Incursion Telemetry

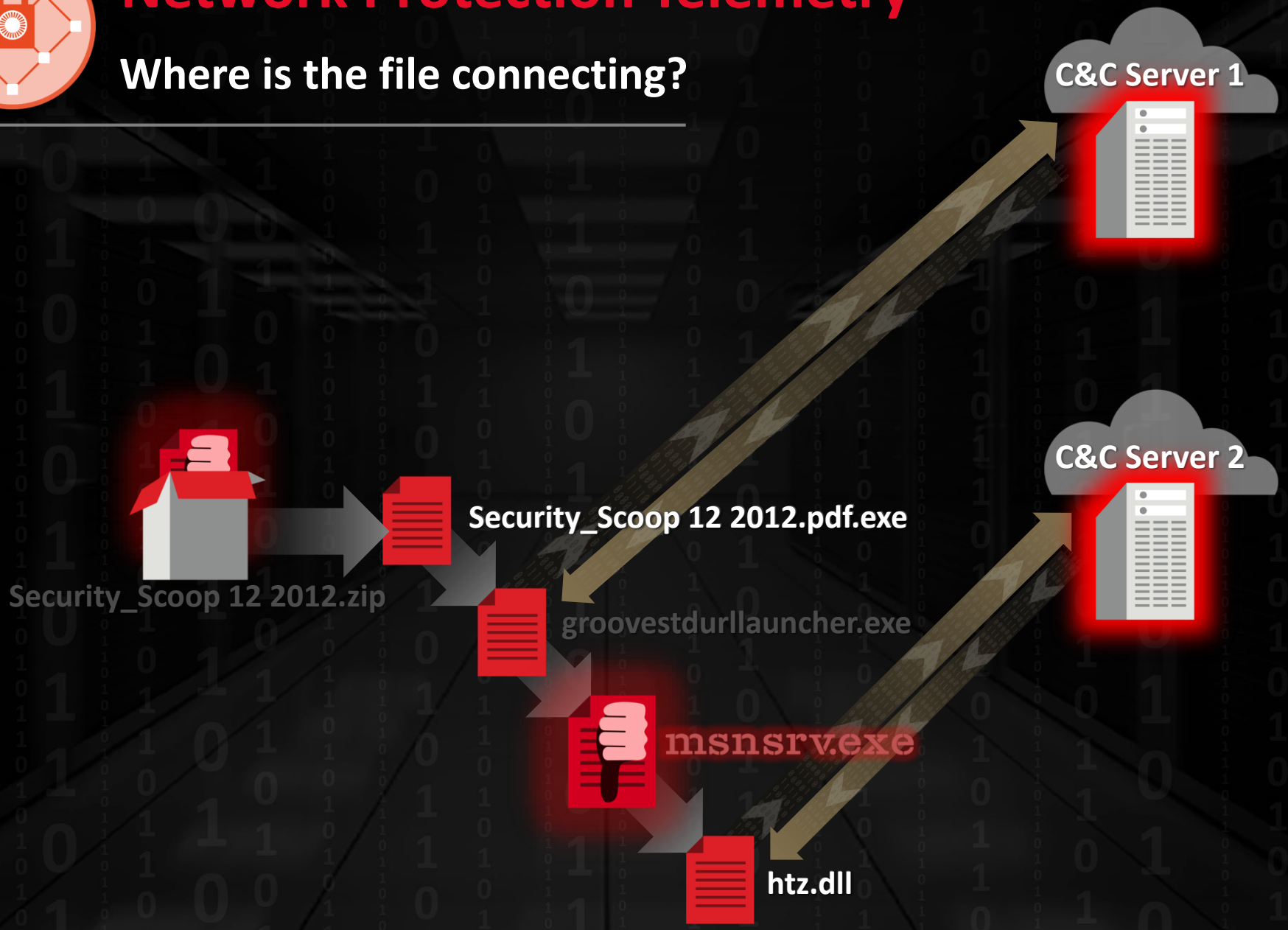
## What is the “lineage” of the file?

# Hosted Email Telemetry

## How did the file get in?

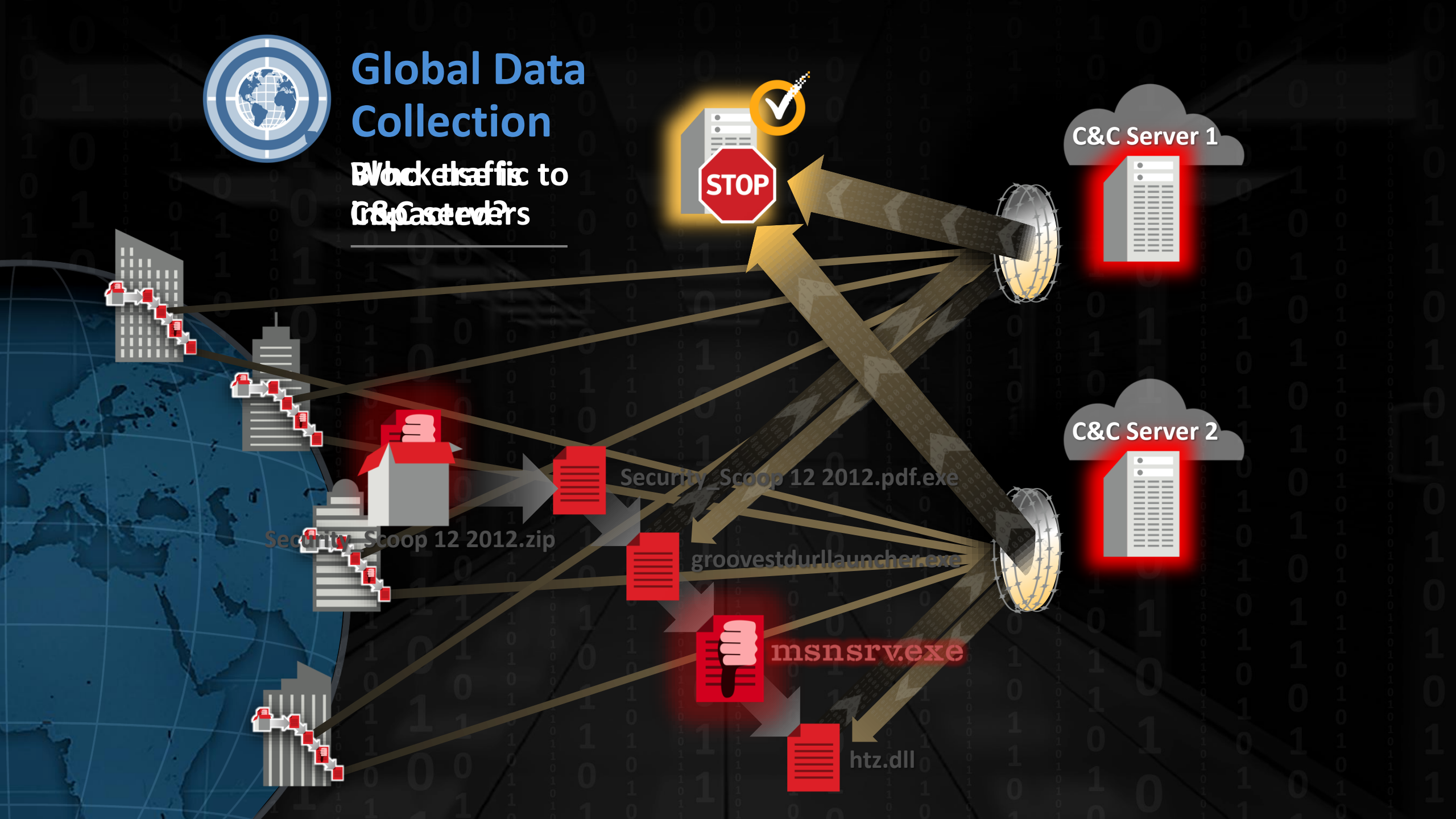
# Network Protection Telemetry

## Where is the file connecting?



# Global Data Collection

Block traffic to C&C servers




Shipping
Aerospace
Defense
Telecom
Think Tanks

# How do we do this?

Massive Sensor Network

Big Data Platform and Analytics

Experts

# UNIFIED SECURITY
## VISION

Symantec will deliver a
**unified security intelligence platform**

**that leverages** the combined **visibility** and **intelligence**
**of all of our offerings** (augmented by 3rd-party data)

to **block**, **detect**, and **remediate attacks**,
**protect information**,
and **reduce risk**, better than anyone else.


Symantec