

# Seamless Security in the Age of Cloud Services: Securing SaaS Applications & Cloud Workloads



Kimmo Vesajoki, Country Manager Finland & Baltics

Trend Micro EMEA Ltd.





**Cross-generational blend of  
threat defense techniques**

**Intelligently applies the  
right technique at the right  
time**

**Powered by global  
threat intelligence**

# Solving Real Customer Problems

## IT Dynamics



Increasingly sophisticated threats



Shift to the cloud



Changing user behavior

## Customer Pain



Recovering from high impact attacks



Existing defenses stagnant and ineffective



Complexity & lack of visibility

## XGen Endpoint Security



Maximum Protection



Minimum Impact



Proven Security Partner

# XGen Endpoint Security



## Maximum Protection

Cross-generational blend of threat defense techniques



## Minimum Impact

Central visibility & control, lower false positives and efficient threat defense



## Proven Security Partner

Innovative and timely response to changing threat landscape

# There is no silver bullet...



**“History has clearly shown that no single approach will be successful for thwarting all types of malware attacks. Organizations and solution providers have to use an adaptive and strategic approach to malware protection.”**

**- Gartner EPP Magic Quadrant 2016**

# Pros & Cons of New Threat Techniques

## Application Whitelisting



Blocks all unknown apps



Only stops EXEs

## Behavior Analysis



Recognizes behavior



CPU intensive

## Exploit Protection



Blocks vulnerabilities that threats exploit



Can't block threats that don't exploit app/OS vulnerabilities

## Machine Learning



EXE file detection



Higher false positives, needs to be trained with specific file types

**No silver bullet; combine techniques to get best of all worlds**



# The Right Technique at the Right Time

With its cross-generational blend of threat defense techniques including high-fidelity machine learning, Trend Micro™ XGen endpoint security is always adapting to identify and defeat new ransomware and other unknown threats.

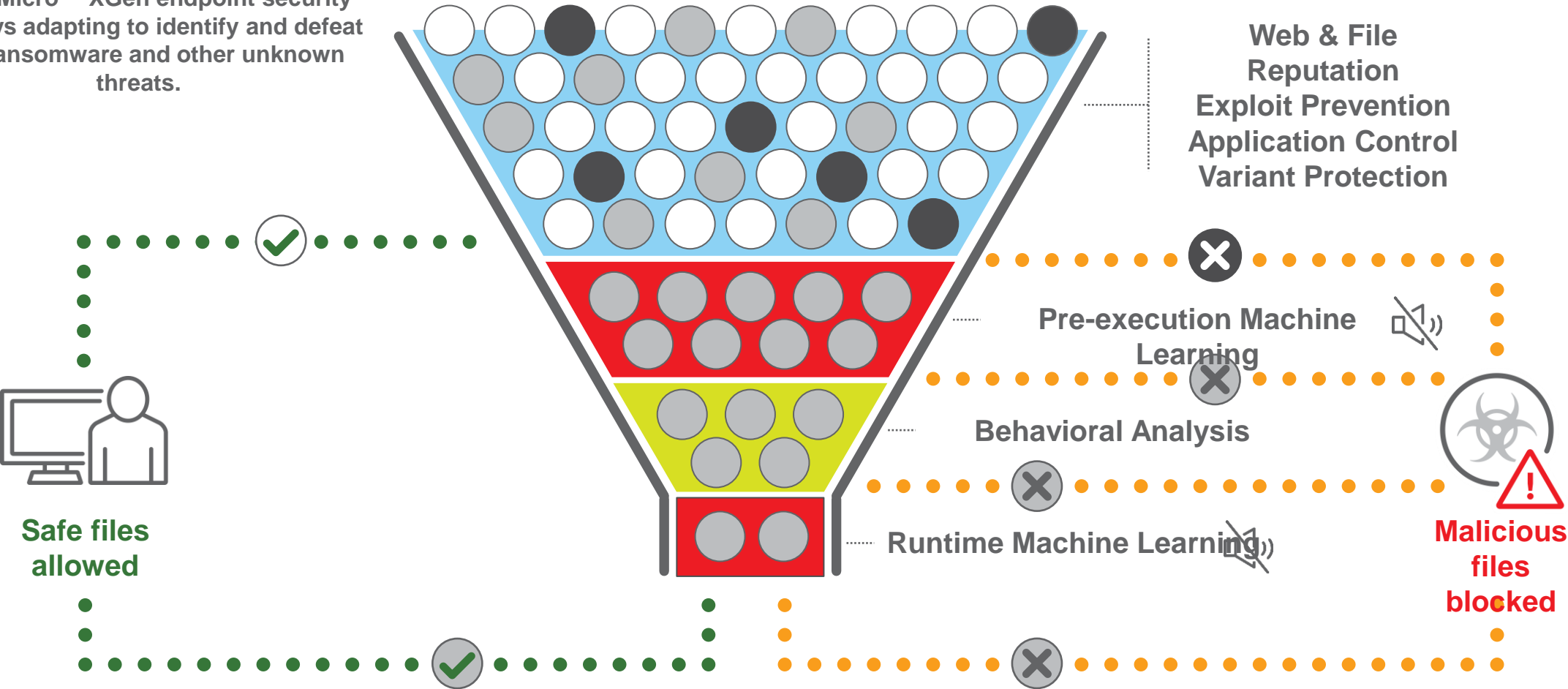
LEGEND

Known Good Data

Known Bad Data

Unknown Data

Noise Cancellation



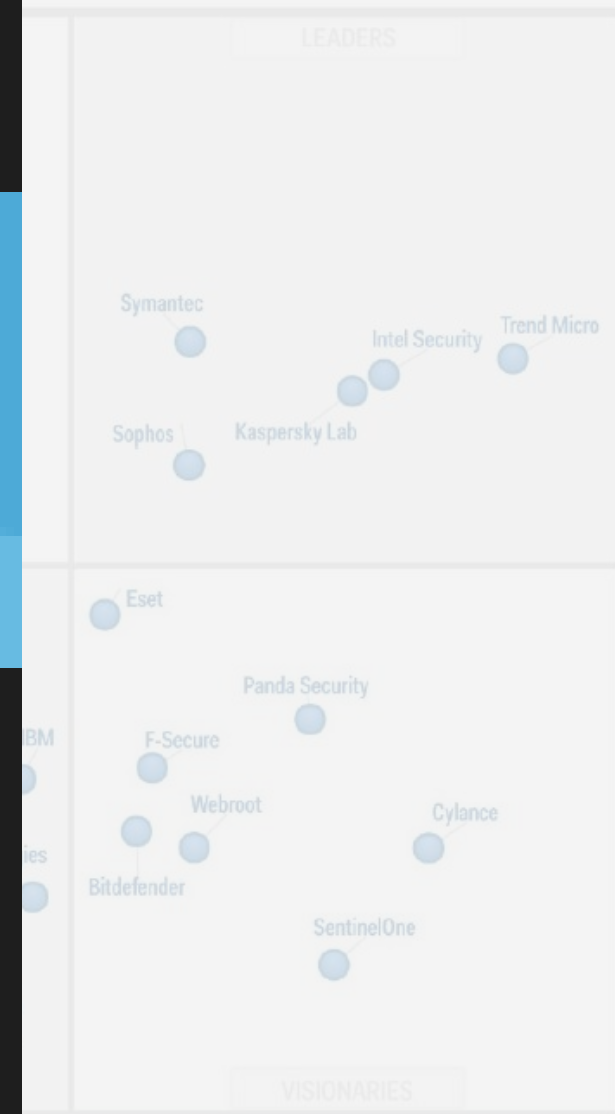
Trend Micro offers best protection against modern threats

Leader  
14 straight years

# FORRESTER®

## WAVE LEADER 2016

### Endpoint Security Suites



Gartner Magic  
Endpoint Protec





“Increasingly,  
organizations are asking  
**what can’t go to the cloud,**  
rather than what can...”

# Many choices...



Google Cloud Platform



# Many choices...

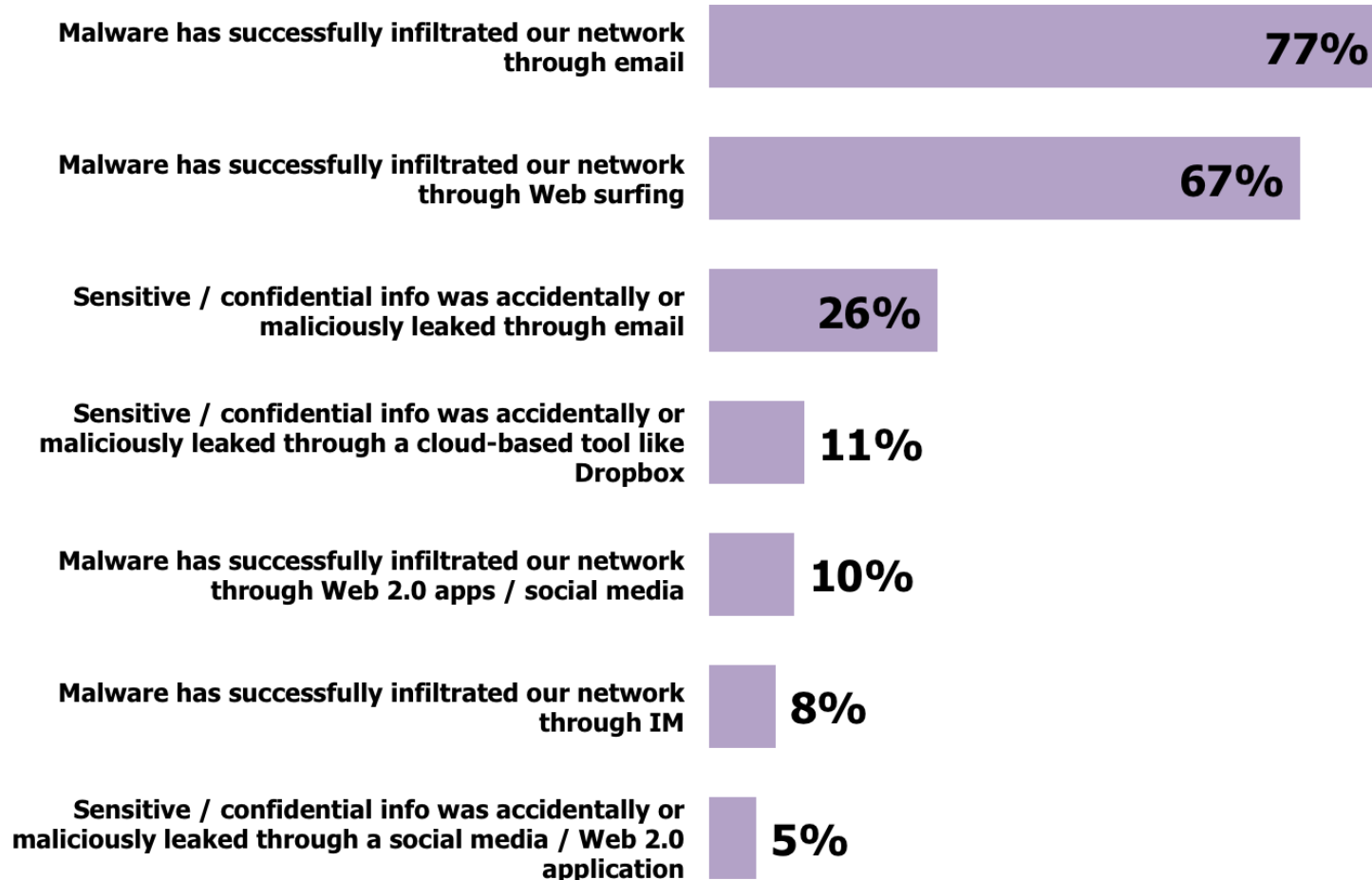


# Many Companies Gradually Move to Cloud Office

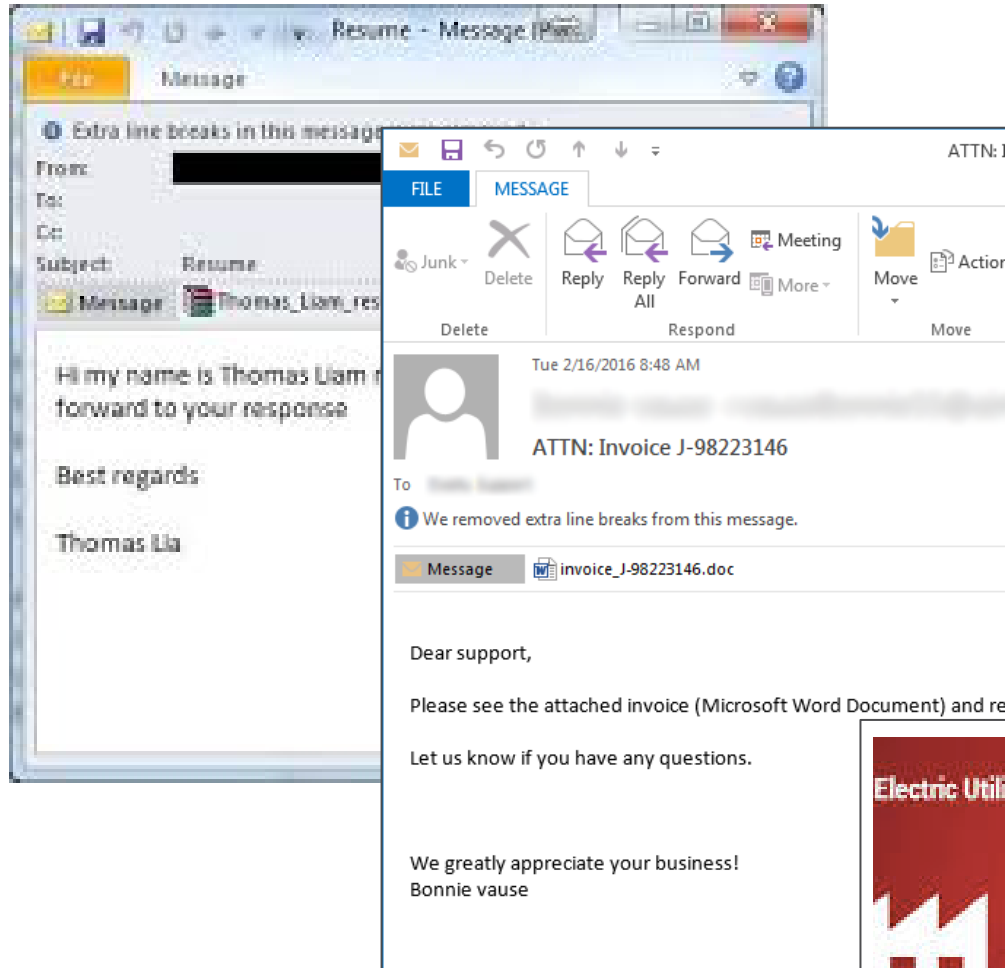
- Intermediate stage to full cloud deployment
- May always keep group of users on premises
- Want equivalent protection without extra management



# Most organizations have been infected with malware from email



# Majority of Ransomware via Malicious Emails



- Common email hooks are here is an invoice or my resume
- Often use weaponized executable, script, html, scr, zip, Office, PDF files
- Leverage Dridex (Smart macro attack)
- May be a URL leading to ransomware



## Ransomware Virus Shuts Down Electric and Water Utility

The Hacker News - 2 days ago

Ransomware has become an albatross around the neck, targeting businesses, hospitals, ...

# Attack Migration Through Email

## *Internal* Phishing Attacks

- Less common but even more important to detect
- Indicator of an attack already in progress

## Example: Financial Times attack

- Phishing emails sent internally from a compromised user
- IT sent warning to users with a link to change their password
- Attackers re-sent IT's email with their own phishing link!

From: [REDACTED]@ft.com>  
Date: 17 May 2013 10:30  
Subject: Change Your Email Password Immediately  
To:

Over the past 24 hours we have seen a large number of Phishing emails being sent within the organisation. These emails are being sent from addresses within the company, therefore look safe, however are not as their accounts have potentially been compromised. In all cases the email has included a link, which when clicked on asks the individual to re-confirm their Google details.

**ACTION:** Please change your password immediately using this [link](#).

If you wish to implement increased security on your Google account, please consider implementing a 2<sup>nd</sup> level of authentication via Google's 2-step Verification process. Instructions are available [here](#) or via your local Service Desk, who can also answer any queries or concerns.

IT Service Desk  
Financial Times  
4th Floor  
One Southwark Bridge  
London SE1 9HL  
Tel: [REDACTED]



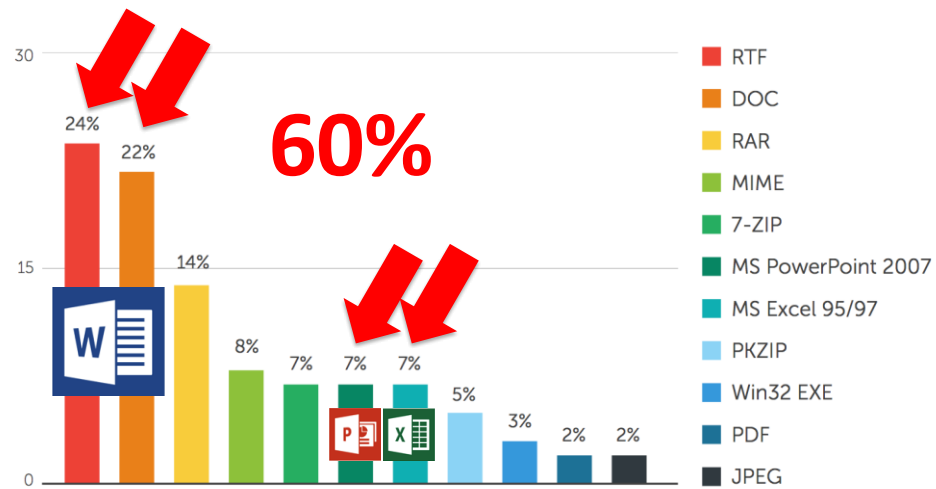


# Advanced Malware Difficult to Detect

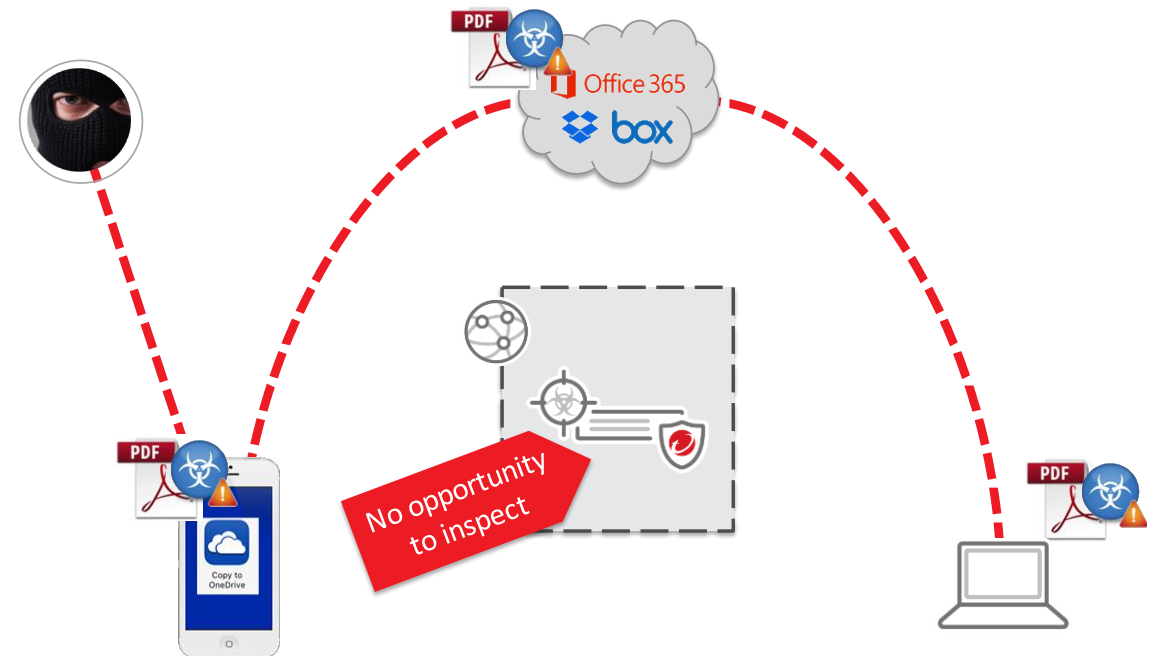
# 90%

of malware is  
used only once

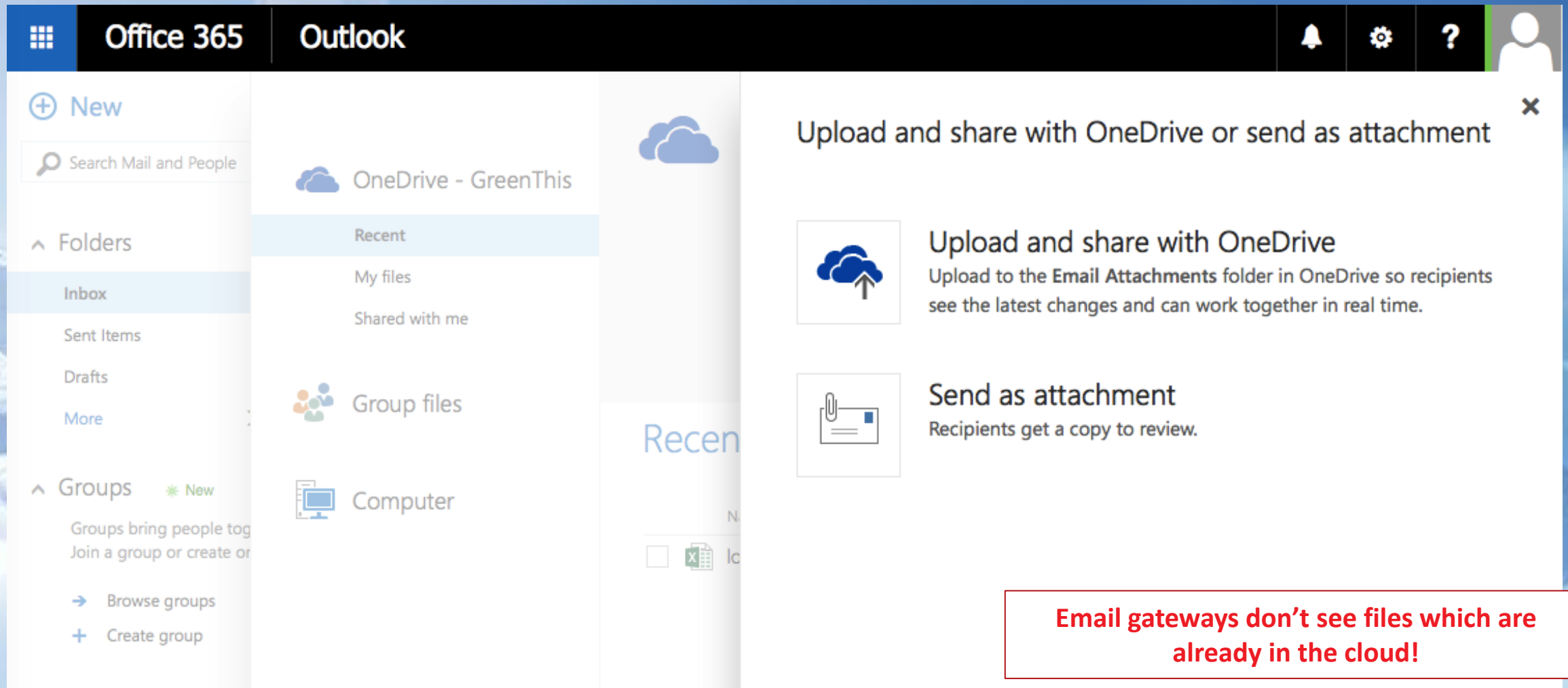
## MS Office files with malware used in 60% targeted attacks



## Network Breach Detection Systems help but miss traffic between off- network devices and SaaS services



# User behavior changing: Email Attachments → Cloud File Sharing



The screenshot shows the Microsoft Office 365 Outlook interface. The top navigation bar includes the Office 365 logo, the Outlook title, and icons for notifications, settings, help, and a user profile. The left sidebar contains a 'New' button, a search bar for 'Mail and People', and a list of folders including 'Inbox', 'Sent Items', 'Drafts', and 'More'. Below the folders are 'Groups' and 'Computer' sections. The main content area displays the 'OneDrive - GreenThis' account with a 'Recent' list. A dialog box titled 'Upload and share with OneDrive or send as attachment' is open, offering two options: 'Upload and share with OneDrive' (which allows for real-time collaboration) and 'Send as attachment' (which provides a static copy for review).

Office 365 Outlook

New

Search Mail and People

Folders

Inbox

Sent Items

Drafts

More

Groups

Groups bring people together. Join a group or create one.

Browse groups

Create group

OneDrive - GreenThis

Recent

My files

Shared with me

Group files

Computer

Upload and share with OneDrive or send as attachment

Upload and share with OneDrive

Upload to the Email Attachments folder in OneDrive so recipients see the latest changes and can work together in real time.

Send as attachment

Recipients get a copy to review.

Email gateways don't see files which are already in the cloud!

# What are Users Uploading to the Cloud?



**Compliance data? Sensitive information?**

# Why do I need to supplement the security included with Office 365?

- Exchange Online is designed and SLA backed to catch 100% known malware


## ▲ Anti-malware protection

Using multiple anti-malware engines, Exchange Online offers multilayered protection that's designed to catch all known malware. All messages transported through the service are scanned for malware (viruses and spyware). If malware is detected, the message is deleted. Notifications may also be sent to end users.

- But 90% malware infects only 1 device.  
*Only 10% malware is known.*
- Every customer needs a strategy to deal with unknown malware



21,883,981  
threats detected  
worldwide



921,741,474  
email messages and  
files scanned worldwide

# Complimenting Office 365's Built in Security for Better Overall Protection

	Office 365 includes	Trend Micro Cloud App Security Adds
Antispam	<input checked="" type="checkbox"/>	
Antimalware	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Document exploit detection to find malware hidden in office files		<input checked="" type="checkbox"/>
Risk-based sandbox behavioral analysis of suspicious files/attachments to detect zero day malware	E5 plan only	<input checked="" type="checkbox"/>
URL scanning within email attachments/shared files		<input checked="" type="checkbox"/>
DLP for Email, OneDrive for Business, SharePoint Online	E3, E5 plans only	<input checked="" type="checkbox"/>

# Securing SaaS-based applications

## Trend Micro Cloud App Security



 Office 365

 Exchange  
 SharePoint

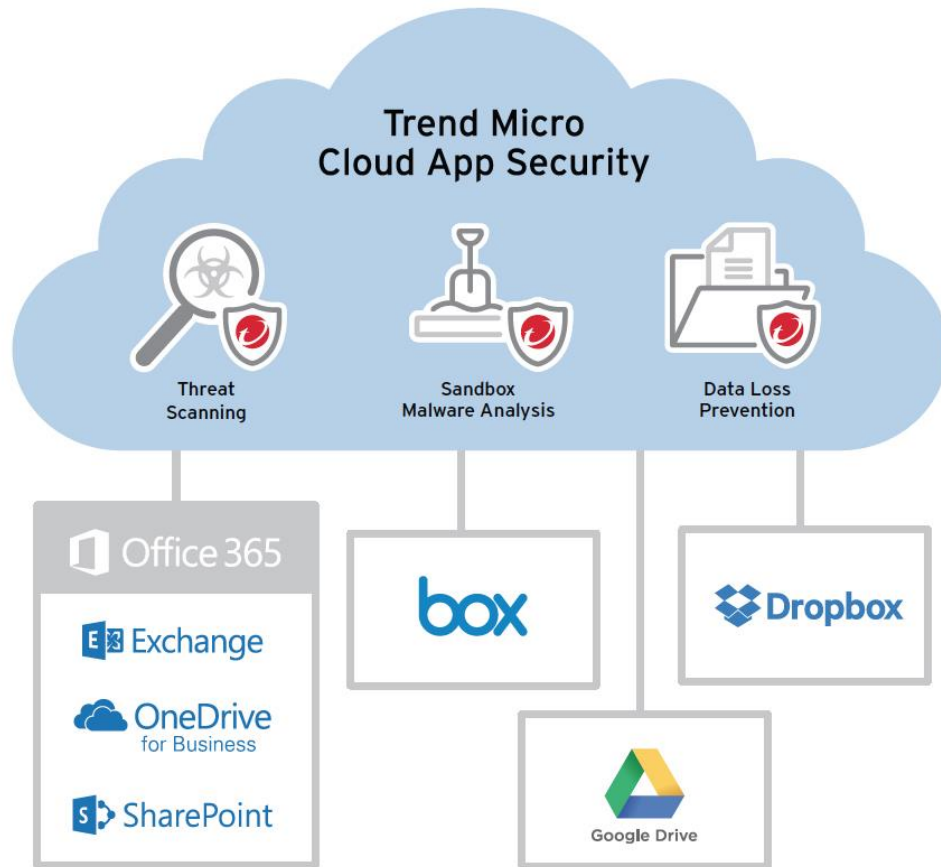
 OneDrive  
for Business

 box

 Dropbox

 Google Drive

# Securing SaaS-based Applications



## Advanced Threat Detection

- Finds zero-day and hidden threats
- Sandbox file analysis in the cloud
- Web reputation for URLs in email/files

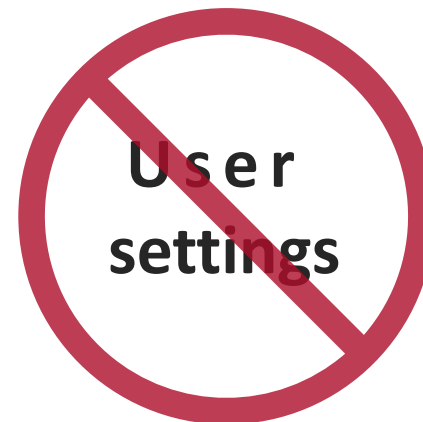
## Data Loss Prevention (DLP)

- Discovery and visibility into confidential data usage.
- DLP enforcement for cloud file sharing
- 240 customizable templates



# Simple and Elegant Integration with SaaS Services

- Direct cloud-to-cloud integration using vendor's API's
- No impact to user/admin functionality
- Supports all devices, anywhere
- Fully automatic setup (above 5000 users contact Trend Micro for best practices)



# Cloud App Security Service Delivery



- 99.9% Available
- US & EMEA sites are not interconnected

A light blue world map with white outlines of continents and countries, serving as a background for the slide.

# Real World Protection Statistic

*Cloud App Security scanned **691M** email/files and detected an additional **6.2 million malicious files/URLS** between July'15 and Aug'16. **58 thousands** malicious files/URLS are ransomware related.*

Source: Cloud App Security service operation portal.

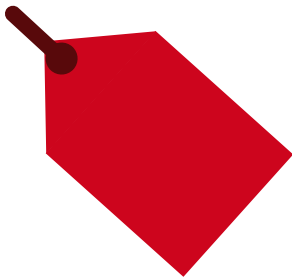
# Cloud Security Challenges



**Visibility**



**Agility**

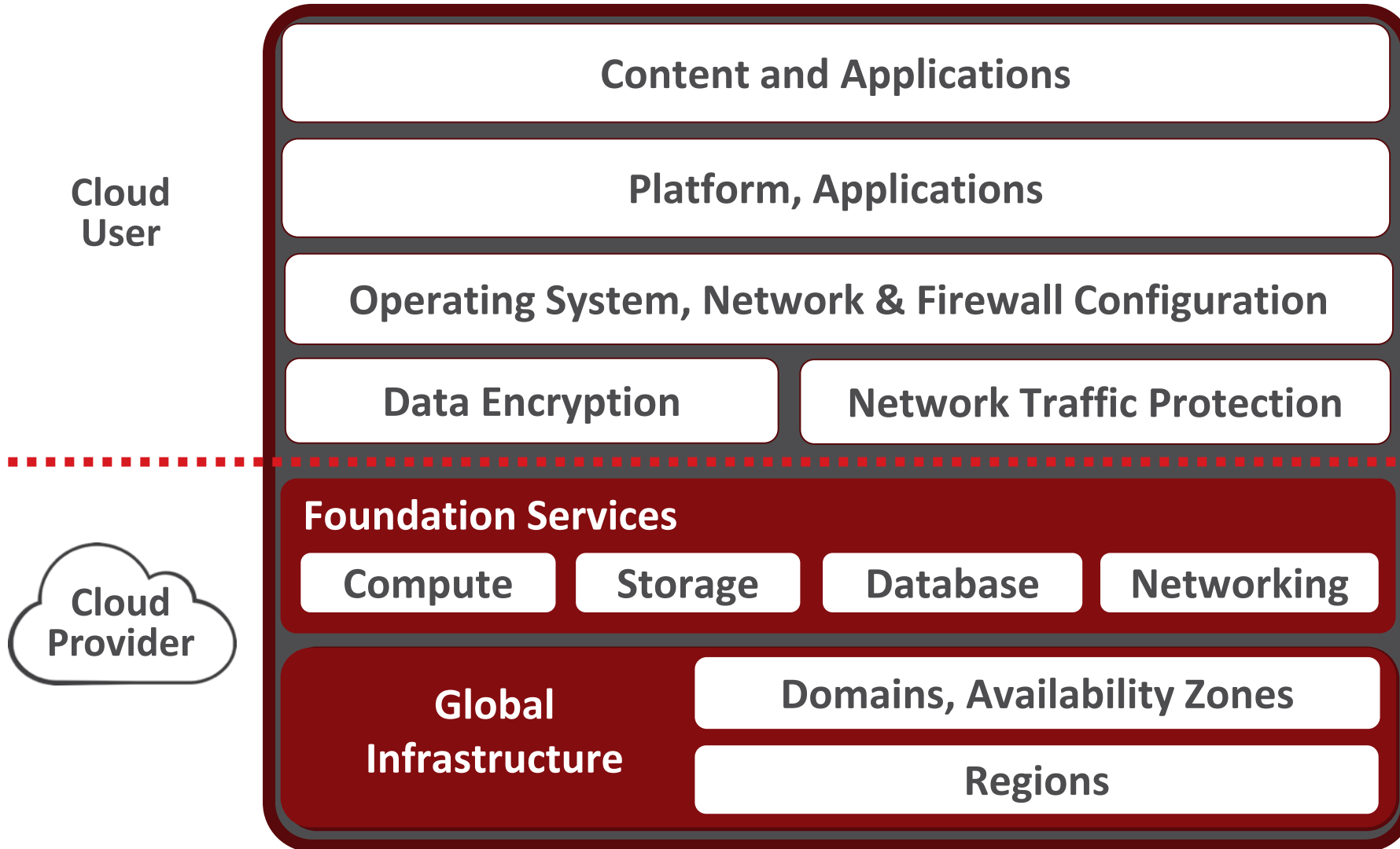


**Purchasing**



**Compliance**

# Cloud Security is a Shared Responsibility



Cloud providers deliver a secure infrastructure.

But YOU need to protect what you put IN the cloud—your workloads.

# Why do I need additional security in the cloud?

## Threats:



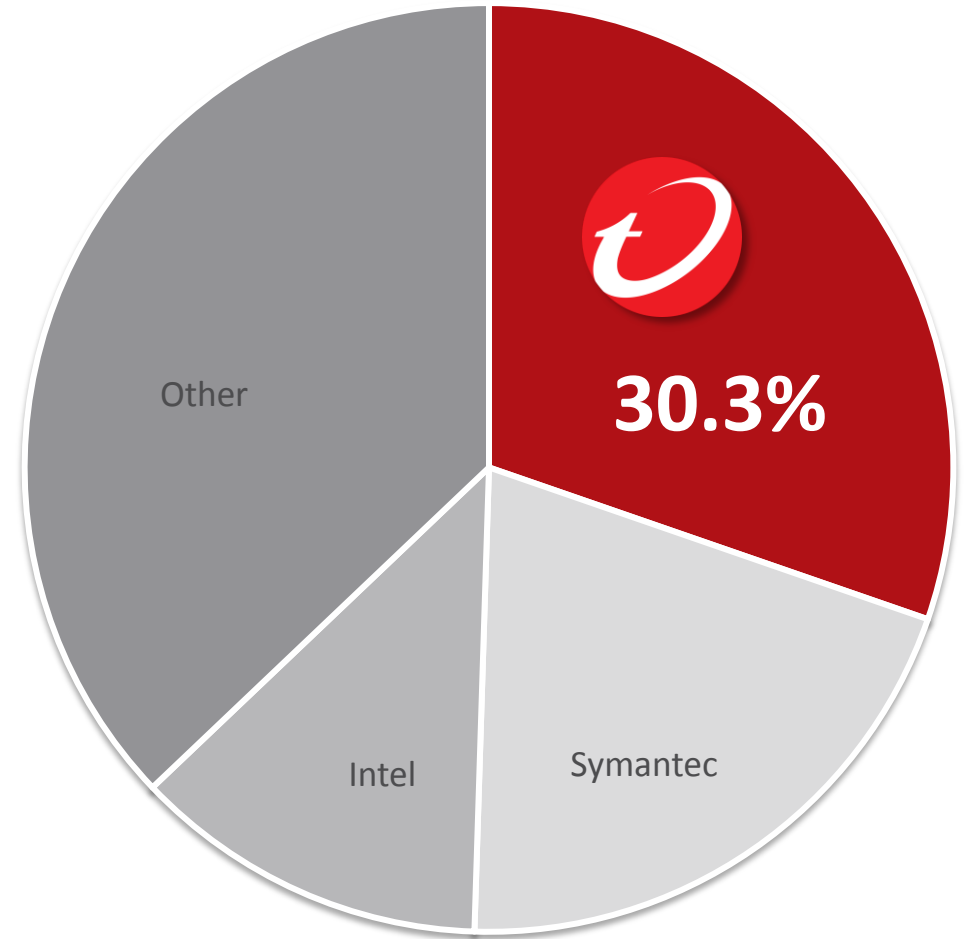
- Network attack
- Vulnerabilities
- Malware
- Insider threats

## Compliance:



- PCI DSS
- HIPAA
- Internal

# Protect more servers than anyone else



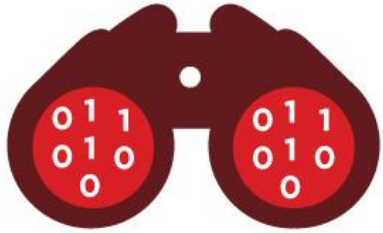


# Best Practices for Securing AWS Workloads\*



- Understand Your Shared Responsibilities
- Get Visibility of Cloud-based Workloads
- Bake Security Into Workloads from Development
- Adopt a "No Patch" Strategy for Live Environments
- Use AWS Security Groups but Leverage a Third-Party Firewall for Advanced Functionality
- Adopt a Workload-Centric Security Strategy

# Deep Security delivers



Intrusion Detection  
& Prevention



DevOps friendly  
Security



Actionable Insight



Advanced Security  
Functionality



Virtual Patching

**All in a  
single,  
host-based  
tool**

# Bake security into workloads

- Full visibility into cloud workloads from a central dashboard
- Automate policy creation and management via API, scriptable components, or central UI
- Deep Security delivers broadest OS and kernel support
- Works with configuration management tools like Chef, Puppet, Saltstack

**Make DevSecOps a reality**



# Virtually patch to speed protection

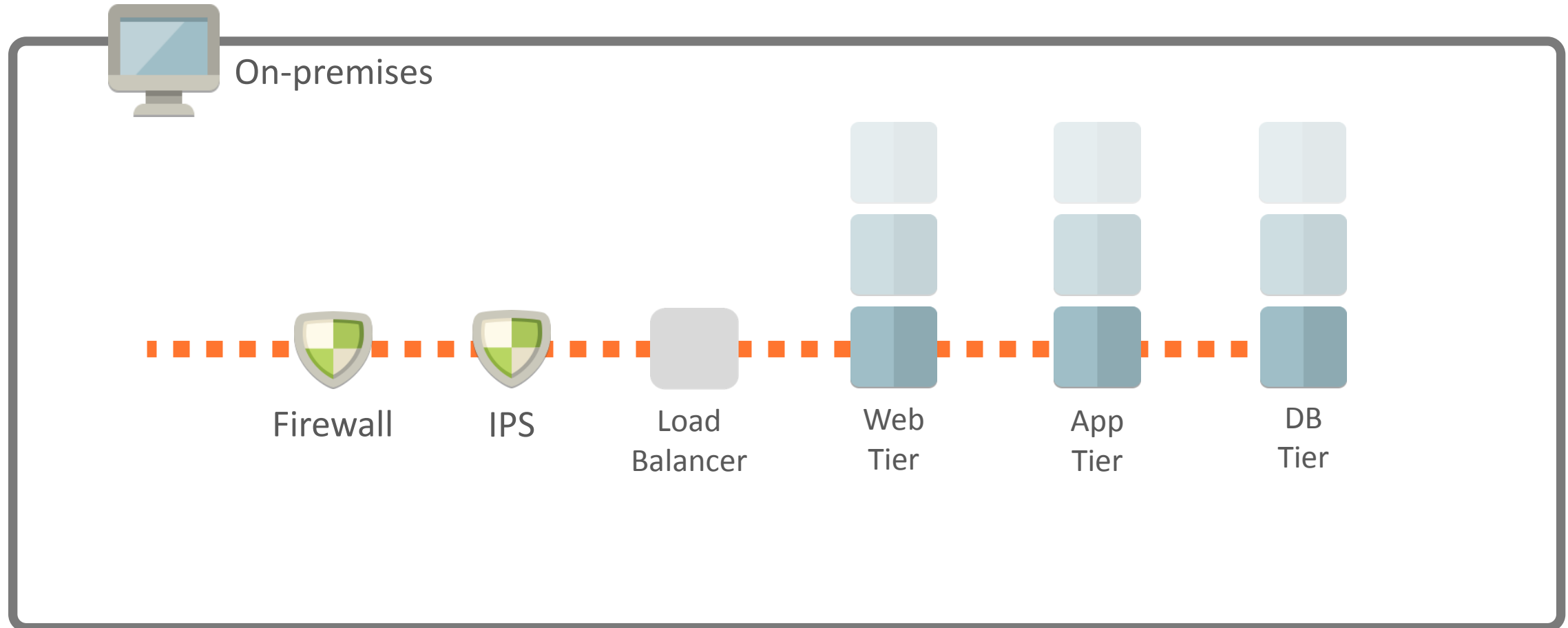
- Prevent exploit of zero-day vulnerabilities (Shellshock, Heartbleed)
- Reduce the risk of ransomware attacks on your workloads
- Reduce need for emergency patching
- Buy time to resolve the core issue with a new deployment – adopt a “no patch for live workloads” strategy
- Deep Security delivers ‘virtual patches’ to quickly protect workloads through IPS until updates can occur



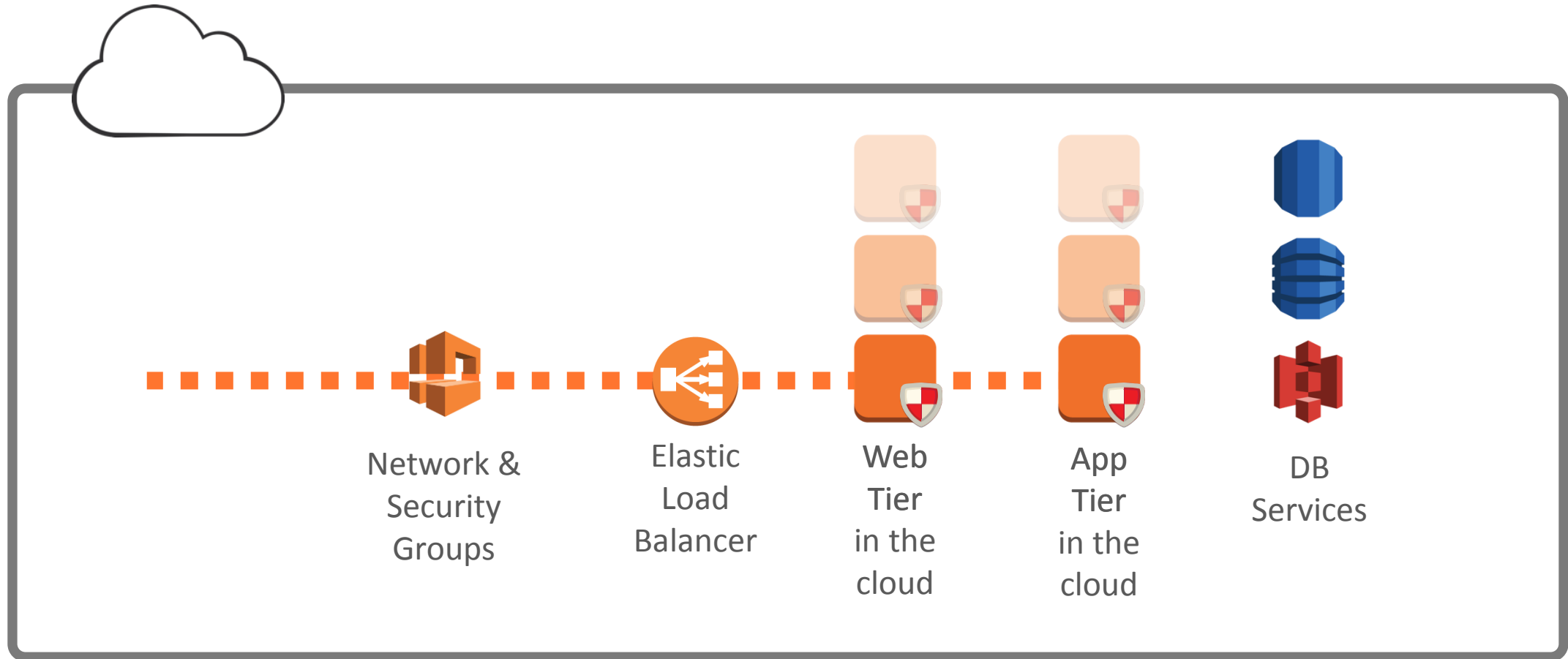
**Speed vulnerability response with virtual patching**

# Traditional on-premises security

Applied at the perimeter



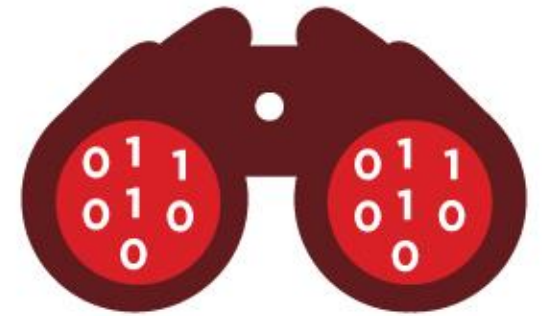
# Build a workload-centric security strategy



Avoid bottlenecks with Deep Security's automated host-based protection

# Prevent network attacks

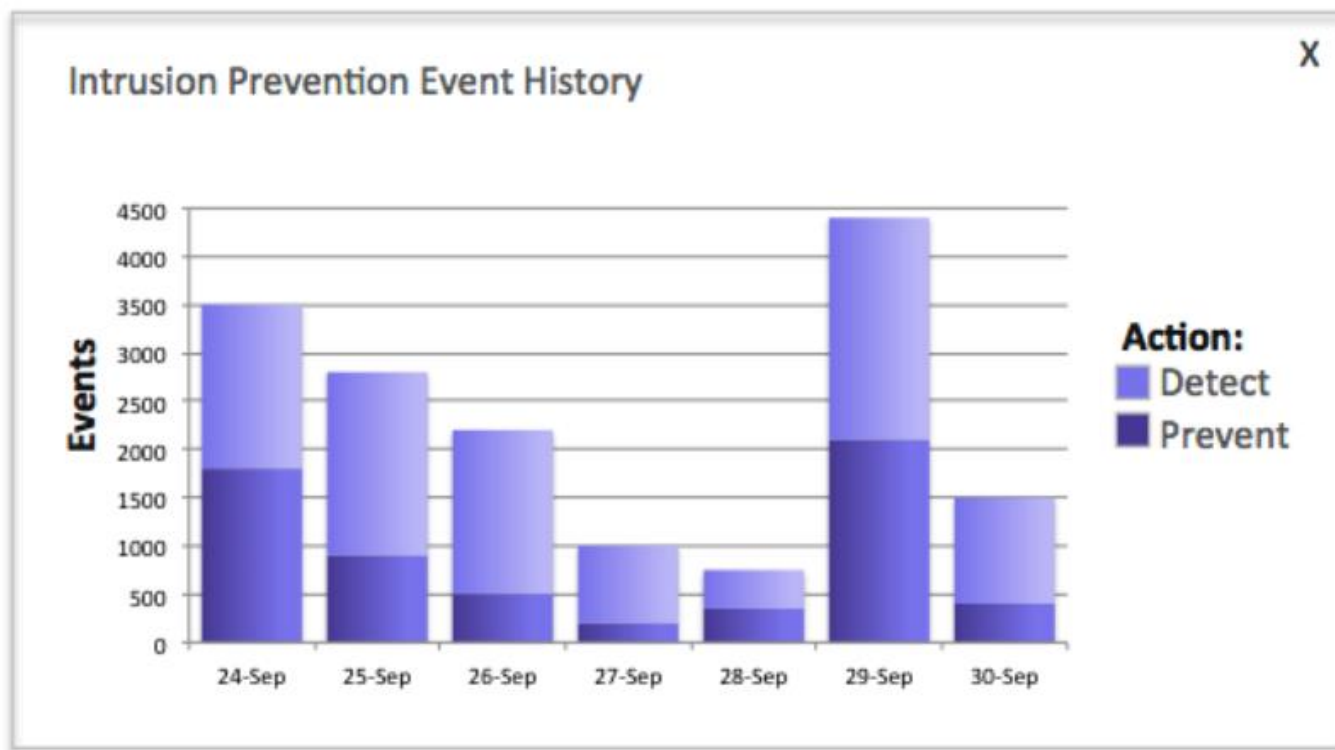
- Proactively protect your systems and applications with Intrusion prevention (IPS)
- IPS **prevents** attacks by examining network packets for malicious or unexpected traffic
- Deep Security provides full stack, host-based IPS that stops attacks **before** they reach applications, including new attacks like ransomware



**Don't just detect attacks, prevent them**



# Defend against network & application attacks



*Deep Security on Sept 30<sup>th</sup>, 2014, at a customer managing 100+ cloud instances*

5 days after publication:

**766 attacks blocked!**

1 year later:

**70,000+ attacks blocked**  
by the service

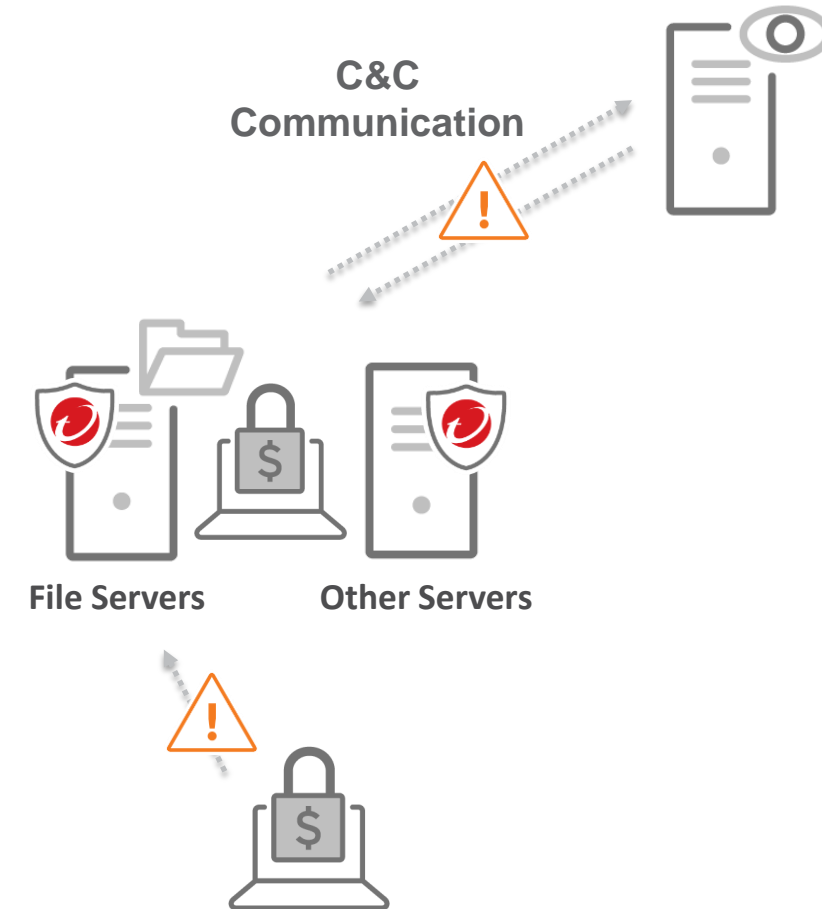
# Ransomware in the Modern Data Center

- An overall, multi-layered approach to lowering risk makes the most sense across the enterprise
- Attacks typically focused on users, but spreads to servers through file shares
- Some new attacks (ex: SAMSAM) are focusing on unpatched and vulnerable servers, requiring enterprises to pay a ransom to return to normal operations

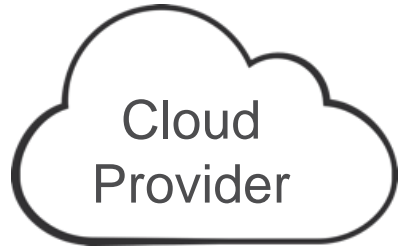
PAY  
OR  
ELSE!

# Ransomware Protection for Servers

- Anti-malware & web reputation for detection of malicious software & known-bad URLs, including ransomware
- Vulnerability shielding (through intrusion prevention) to prevent server compromise
- Lateral movement detection & prevention through intrusion prevention to stop the spread of infection
- Ransomware-specific:
  - Command & control (C&C) communication detection & alerting
  - Defending Windows & Linux file servers from ransomware-infected clients through detection of over-the-network suspicious file change activity



# Shared responsibility for compliance








## Facilities

Physical security of hardware









Network infrastructure

Virtualization infrastructure

-  File & System integrity monitoring
-  Intrusion detection & prevention
-  Firewall
-  Anti-malware
-  Vulnerability scanning & updating

# Accelerate PCI DSS compliance



PCI DSS Requirement	Responsibility
Install and maintain a firewall configuration to protect cardholder data	 Shared
Do not use vendor-supplied defaults for passwords or other security parameters	 Shared
Protect stored cardholder data	Shared
Encrypt transmission of cardholder data	User
use and regularly update anti-virus software	 User
Develop and maintain secure systems and applications	 Shared
Restrict access to cardholder data by business need to know	 Shared
Assign a unique ID to each person with computer access	 Shared
Restrict physical access to cardholder data	Cloud Provider
Track and monitor all access to network resources and cardholder data	 Shared
Regularly test security systems and processes	 Shared
Maintain a policy that addresses info security for all personnel	Shared

# What about GDPR?

## Recital 49 EU General Data Protection Regulation (EU-GDPR):

*“The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned.*

*This could, for example, include **preventing unauthorised access** to electronic communications networks and **malicious code distribution** and **stopping 'denial of service' attacks** and **damage to computer and electronic communication systems.**”*

# Deep Security - Optimized for the Cloud

Deep Security can secure cloud and hybrid deployments with a single platform



Seamless integration with leading cloud providers:

- Auto-detect instances and rapidly protect them
- Fully scriptable, including tools to automate provisioning and set up
- Host-based protection so security isn't a bottleneck



# Flexible purchase & deployment options

## Software-as-a-Service



Less work

## Marketplace



On AWS or Azure bill

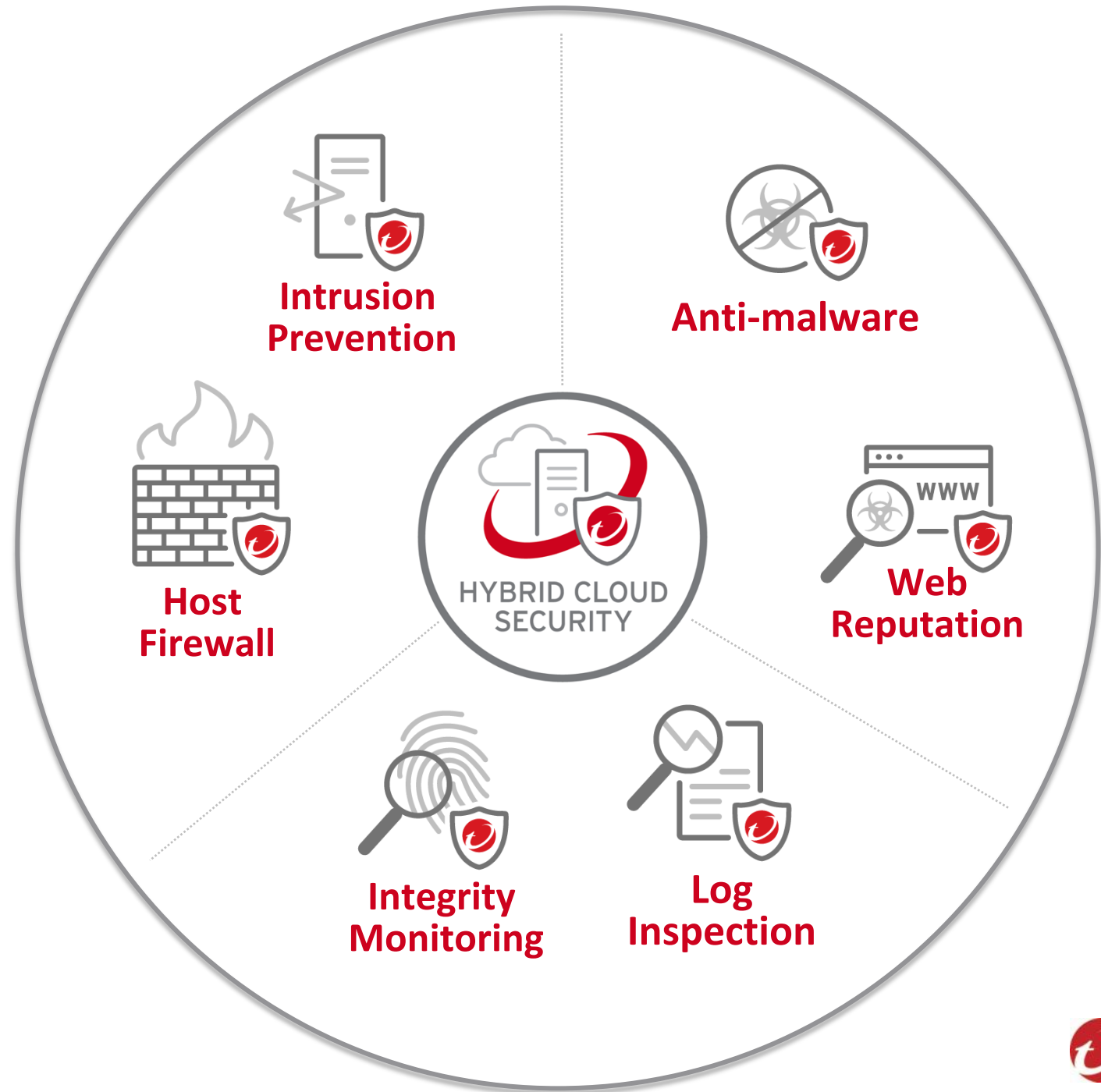
## Software



Hybrid Environment



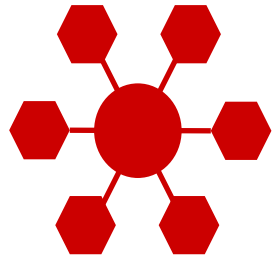
# Trend Micro Deep Security



# Why choose Trend Micro?



Scalable, automated security that fits



Single security console, multiple capabilities



Usage-based pricing



[trendmicro.com/cloud](https://trendmicro.com/cloud)