

Wiki Webinar - Hoe ransomware voorkomen?

Stefaan Van Hoornick, Hybrid Cloud Security Specialist, Trend Micro

Luc Horré, Rcloud Manager, Realdolmen





- Welcome
- The current threat landscape
- Cloud One – Workload security
- Realdolmen offering
- Q&A

CYBER SECURITY

NMSU FIREWALL ONLINE INFORMATION NETWORK PHISHING THREATS BREACHES PRIVACY SOFTWARE SECURITY ENCRYPTION ACCESS FIREWALL INTERNET SSN AUDIT COMPUTERS USER INTRUSION VULNERABILITY BOT ACCOUNTS MALWARE TRACKING PASSWORD CRYPTOGRAPHY

firewall

hacker target trojan virus spyware phishing internet hacking malware intruder infection

spam networks attack cyber groups crime infected international terrorism

protection safe

password firewall data lock security

security

safety privacy communications technology protection



Introduction: Trend Micro

- 6000+ employees in over 50 countries
- Headquartered in Japan, Tokyo Exchange Nikkei Index
- Annual sales of approximately \$1.3B US, consistently profitable
- Customers include 45 of top 50 global corporations
- **30 years** focused on making “A World Safe for Exchanging Digital Information”



Enterprise



Midsize Business



Small Business



Consumers

500k commercial customers & 250M+ endpoints protected

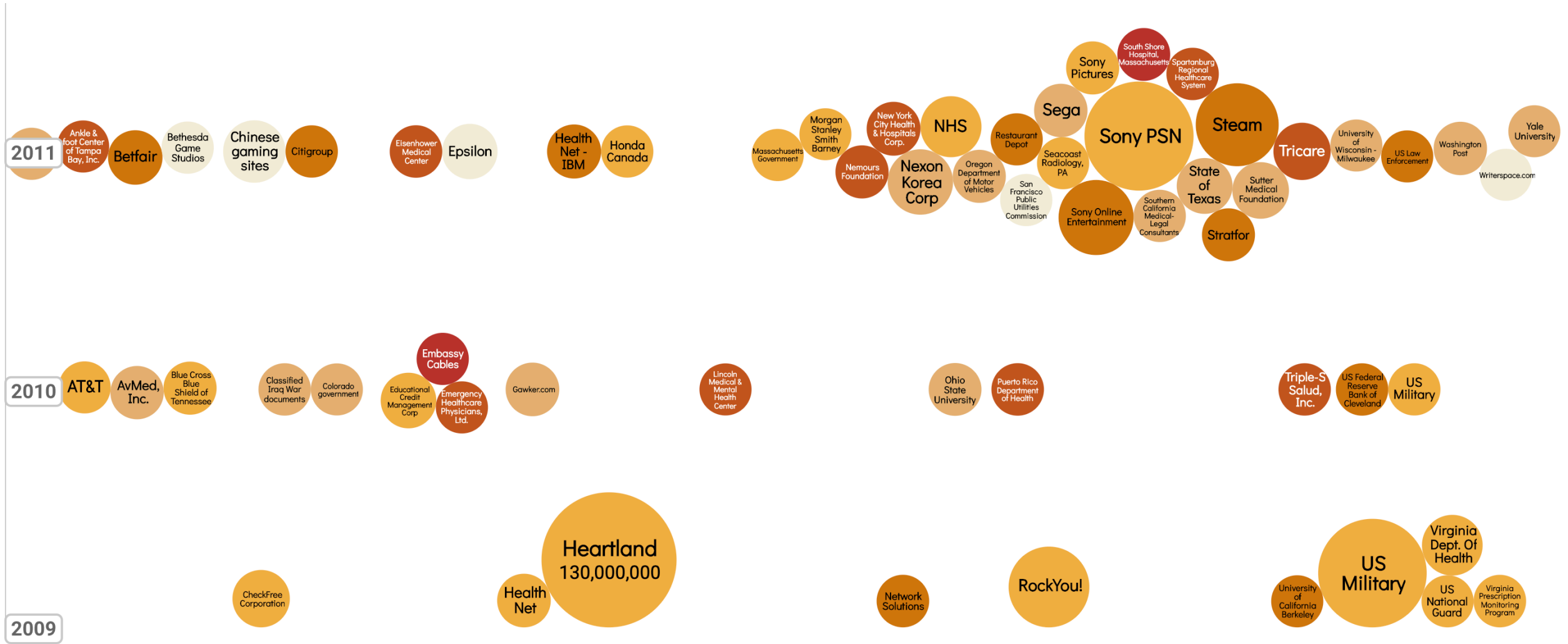
Threat Landscape



The threat landscape is **evolving**



Hacks and Vulnerabilities 2009->2011



Source - <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

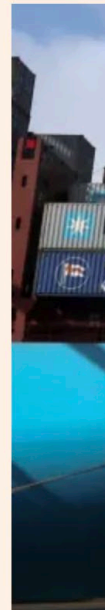
A continuous Battle: WannaCry, Petya, Bad Rabbit, ...

Moller-Maersk nuts cost of cyber attack at up



'Petya' ransomware attack: what is it and how can it be stopped?

}8



Maersk reit

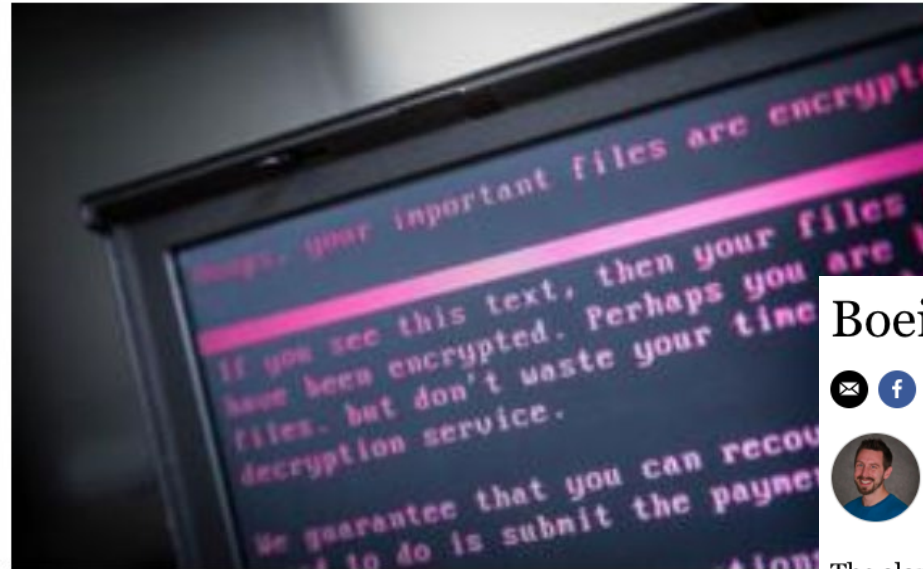
Richard M

A cyber
shippin

conglomerate said on Tuesday

'Bad Rabbit' ransomware strikes Ukraine and Russia

24 October 2017 | Technology



Companies have been crippled by global cyberattack, the second major ransomware crime in two months. We answer the key questions



Boeing Is The Latest WannaCry Ransomware Victim



Lee Mathews, CONTRIBUTOR

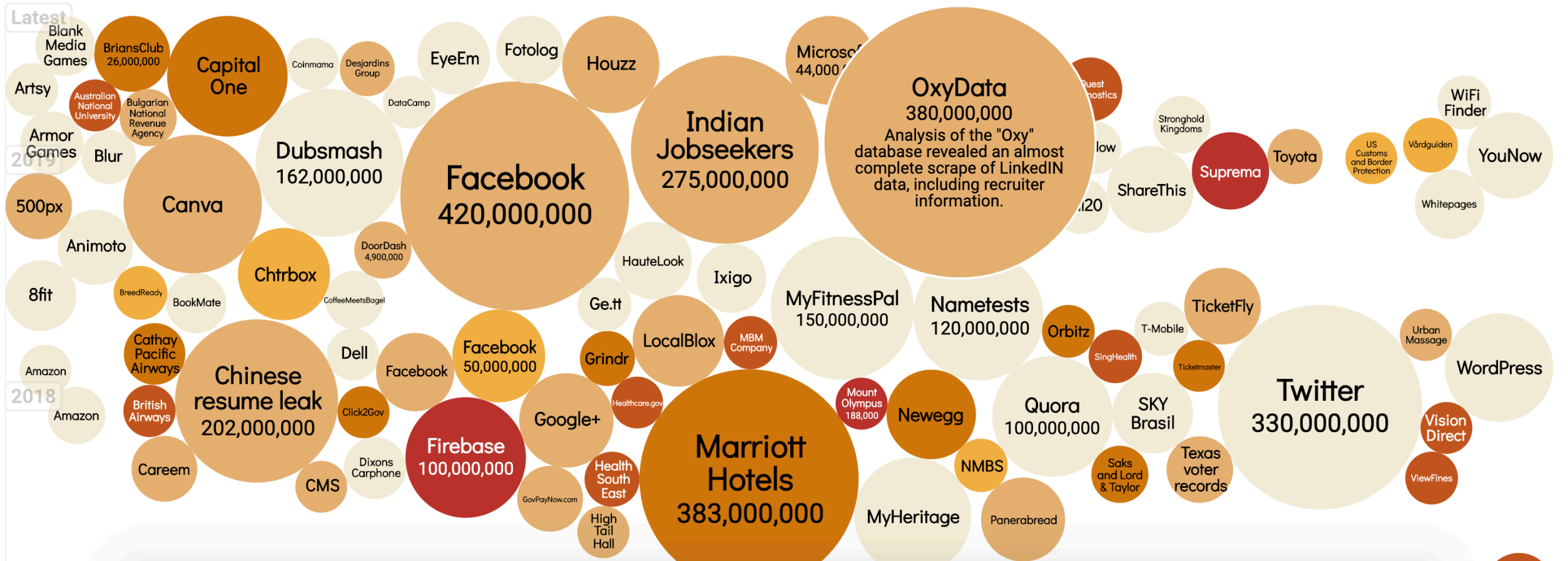
Observing, pondering, and writing about tech. Generally in that order. [FULL BIO](#)

Opinions expressed by Forbes Contributors are their own.

The alarm bells were blaring this week at Boeing. In the early hours Wednesday morning, computers on the aerospace giant's network were being attacked by the WannaCry virus.

▲ The website homepage of British advertising company WPP after it was targeted by international cyber-attack 'Petya'. Photograph: Benjamin Fathers/AFP/Getty Images

Hacks and Vulnerabilities 2018 -> 2020



Some Recent attacks

Le CHU de Rouen a bien été victime d'une cyberattaque criminelle



OLIVIER JA

Pour l

La cybe
assure
d'inform

"On est revenus au papier-stylo" : le CHU de Rouen victime d'une attaque informatique générale



Par **franceinfo**
Radio France
Mis à jour le 16/11/2019 | 19:10

Le CHU de Rouen a été victime dans la soirée du vendredi 15 novembre d'une gigantesque attaque informatique, qui empêche toujours samedi d'avoir accès au dossier des patients, rapporte [France Bleu Normandie](#). L'attaque provoque de sérieux ralentissements dans le traitement des patients. Lorsque elle a été détectée, le personnel du CHU de Rouen a décidé d'arrêter le système d'information, "pour éviter que l'attaque ne se propage partout", explique le service de communication de l'hôpital. Mais alors, impossible pour le personnel soignant de créer des fiches pour les patients qui arrivent, de suivre les malades ou de communiquer entre services, etc.

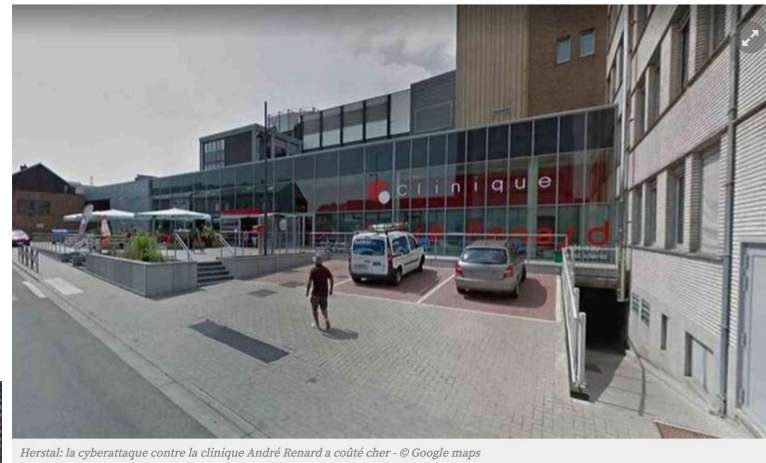
Seule solution : "On est revenus au papier-stylo, cela a compliqué énormément les choses, absolument tout est informatisé", détaille Evelyne Bourgeois, agent de service hospitalier et secrétaire locale à la CGT. "Heureusement, il y avait des médecins ce matin pour faire des prescriptions, car on n'avait plus rien. Pareil pour les repas, ils sont commandés par informatique, donc là ça a été compliqué. Certains ont des régimes très particuliers."

Le CHU déjà victime d'une cyberattaque

Dans l'après-midi du samedi 16 novembre, tous les logiciels étaient soumis à des analyses, menées par les trente personnes du service informatique du CHU. "On redémarre progressivement après analyse de chaque logiciel", rassure l'hôpital. "Mais il n'est pas sûr que tout soit opérationnel dimanche". Ce qui devrait compliquer encore un peu plus la tâche du personnel hospitalier, encore moins fourni le dimanche. "On est en effectif minimum", déplore Evelyne Bourgeois. "Il y aura des médecins de garde, mais ça va être compliqué."

'Dit was de grootste cyberaanval op een Belgisch ziekenhuis tot nu toe'

Herstal: la cyberattaque contre la clinique André Renard a coûté cher



Herstal: la cyberattaque contre la clinique André Renard a coûté cher - © Google maps

François Braibant

Publié le vendredi 05 avril 2019 à 09h21

[/al-op-een-belgisch-ziekenhuis-tot-nu-toe~be89ac9e/e-victime-d-une-cyberattaque-criminelle.N908414](#)

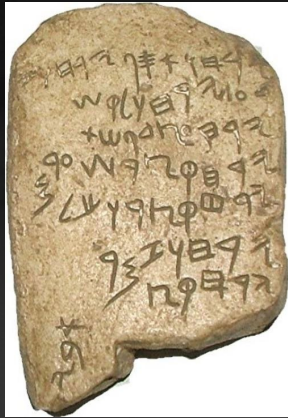


Source
<https://www.franceinfo.fr>
<https://www.franceinfo.fr>

What to do?



Total Isolation



Pen & paper



Insurance fee

OR



Setup "Secure by design" safeguards

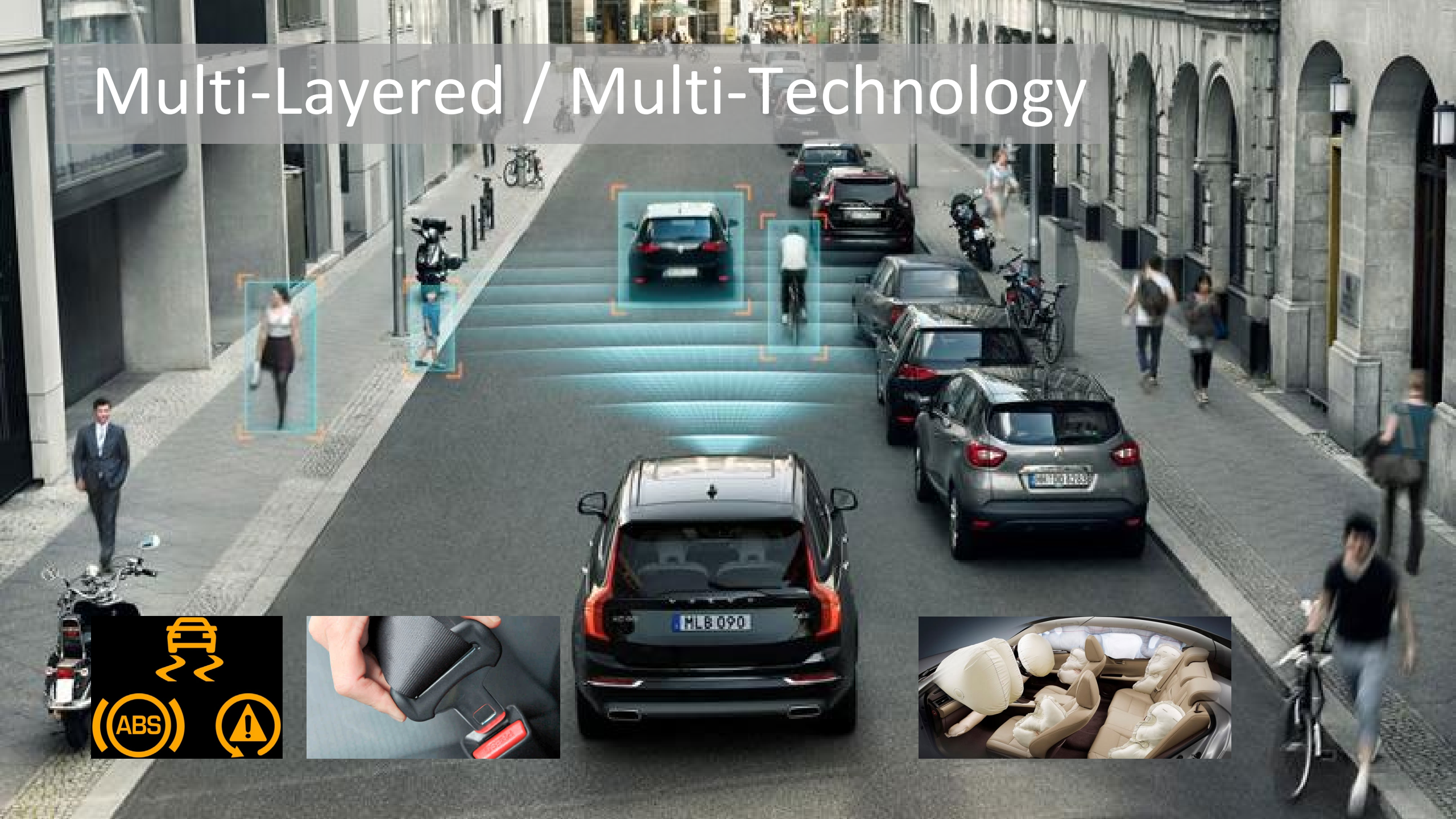


Reduce reaction time between detection and response (Do you know that you are breached?)



Priority Cybersecurity

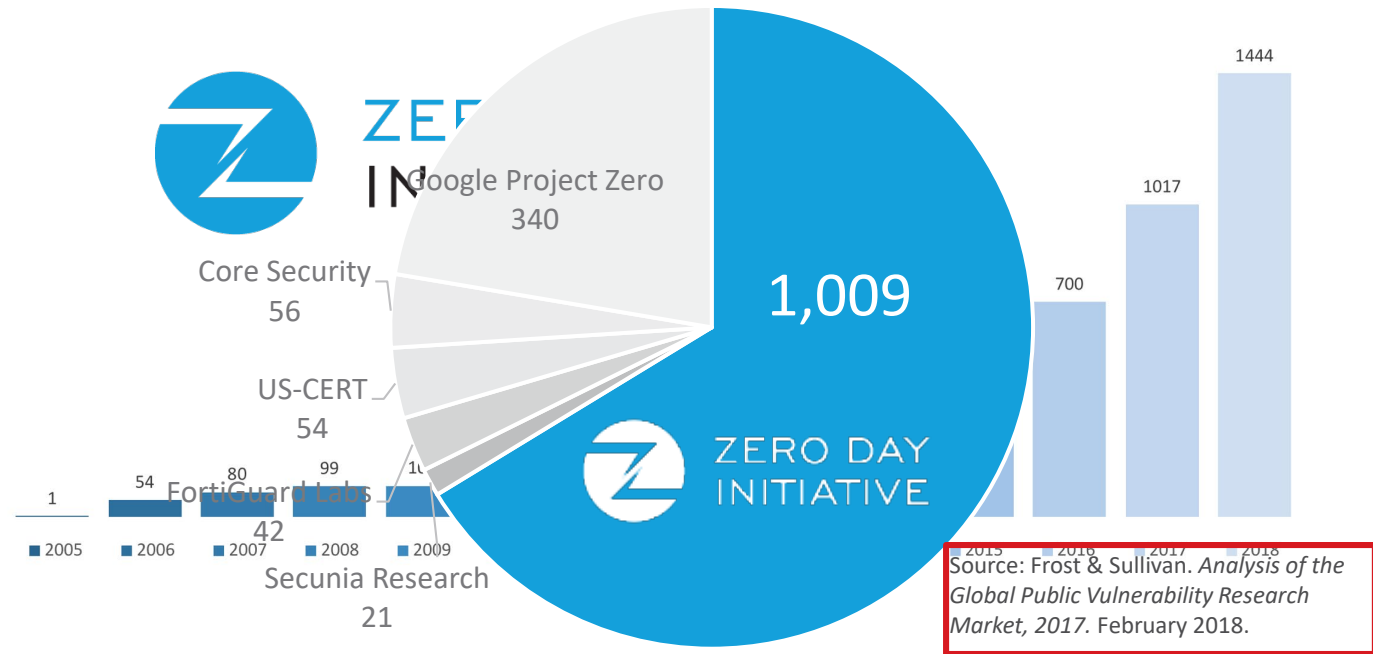
Multi-Layered / Multi-Technology



...powered by the Best Threat intelligence in the world.

LEADER in vulnerability discovery since 2007 with **66.3%** of vulnerabilities reported in 2017 verified vulnerabilities in 2017

TOP REPORTER in vulnerability discovery since 2007 of Microsoft & Adobe vulnerabilities worldwide



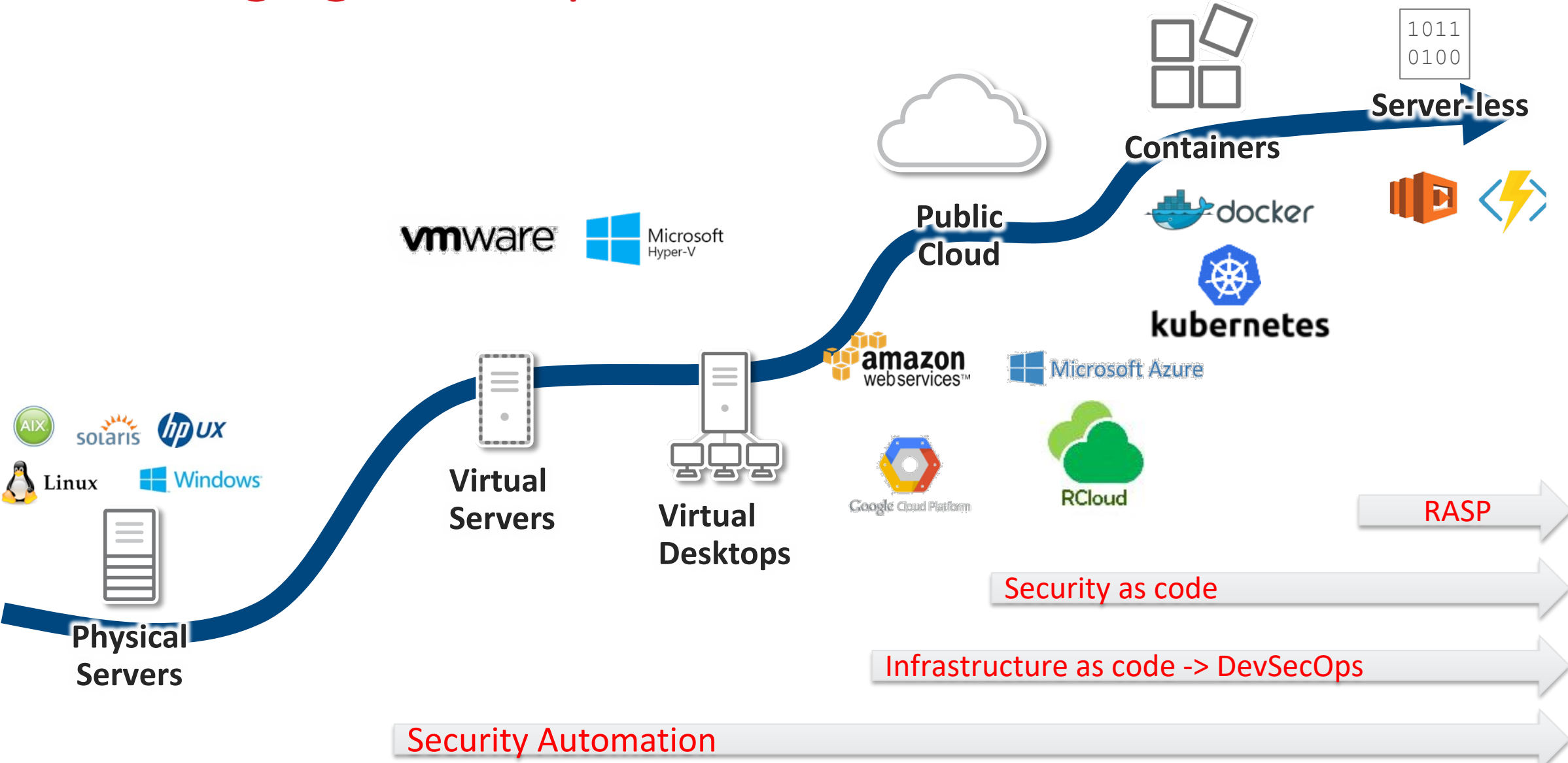
- Threats
- Vulnerabilities & Exploits
- Targeted Attacks
- AI & Machine Learning
- IoT
- OT / IIoT
- Cybercriminal Undergrounds
- Future Threat Landscape



Cloud & Datacenter Security



The changing landscape of server workloads



Strategic Priorities for Cloud Builders

Cloud Native Applications

- Deliver fast, iterate often



- Infrastructure as code

- Cloud leverage: code re-use, multi-source and public code repositories



Containers

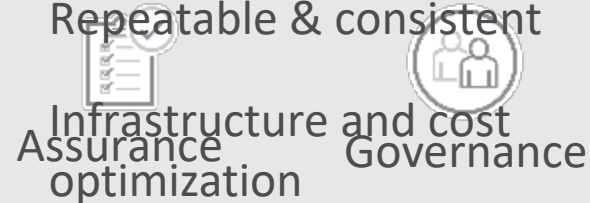
Serverless



How do you secure such a complex & fast-paced environment?

Cloud Operational Excellence

- Repeatability & consistency
- Infrastructure and cost optimization
- Multi-cloud
- Cloud Center of Excellence (CCOE)



- Position not a customer
- Hybrid cloud is the norm




Cloud Migration

Trend Micro Cloud One.™

Security Services for Cloud Builders

Cloud Native Application Delivery



DevOps

Cloud Storage Cloud Workloads

Containers Serverless

Cloud Operational Excellence

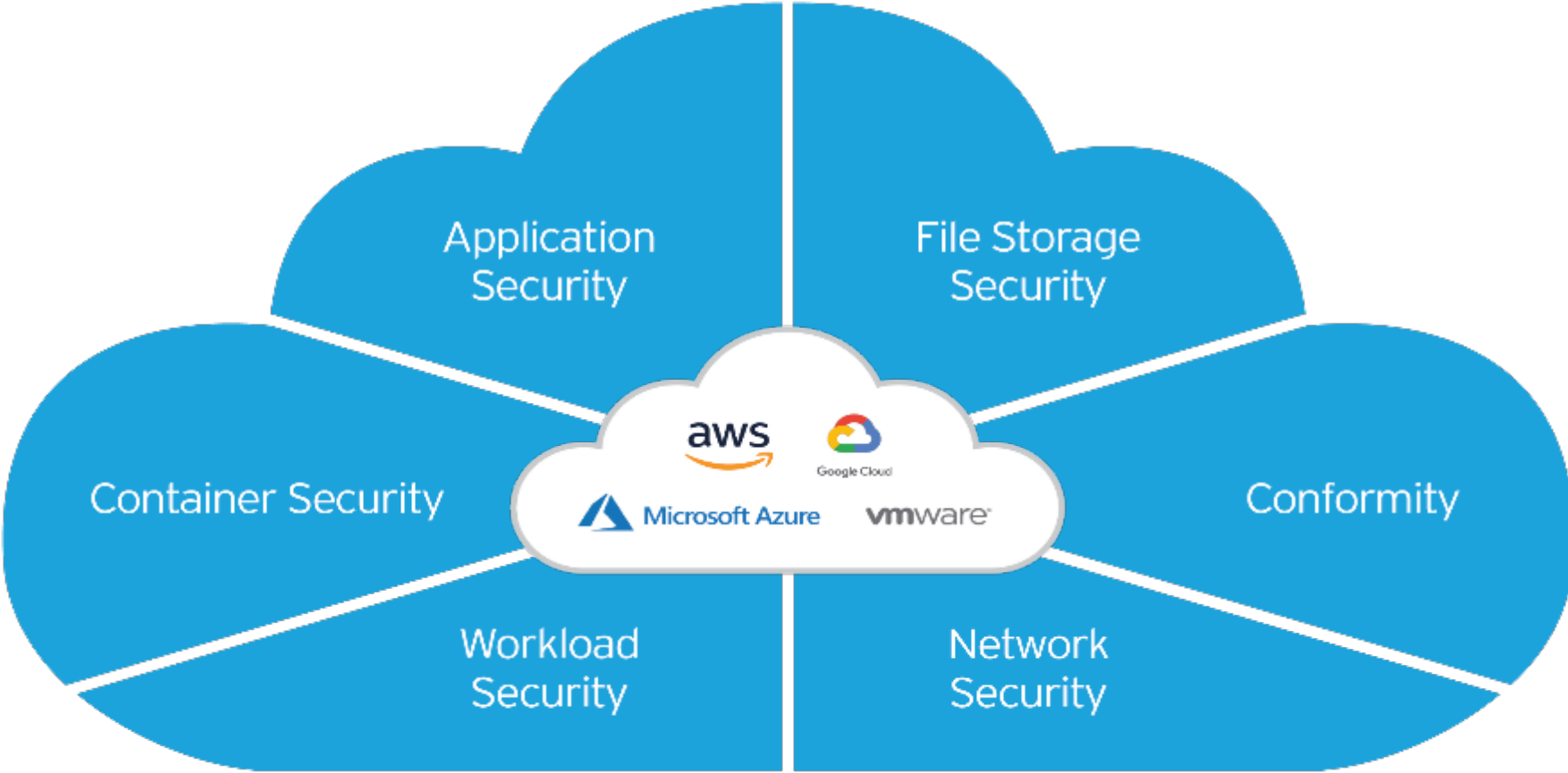
Assurance Governance

Compliance



Physical Virtual Cloud

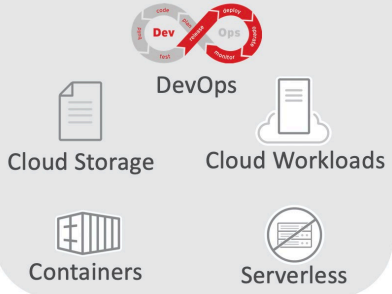
Cloud Migration



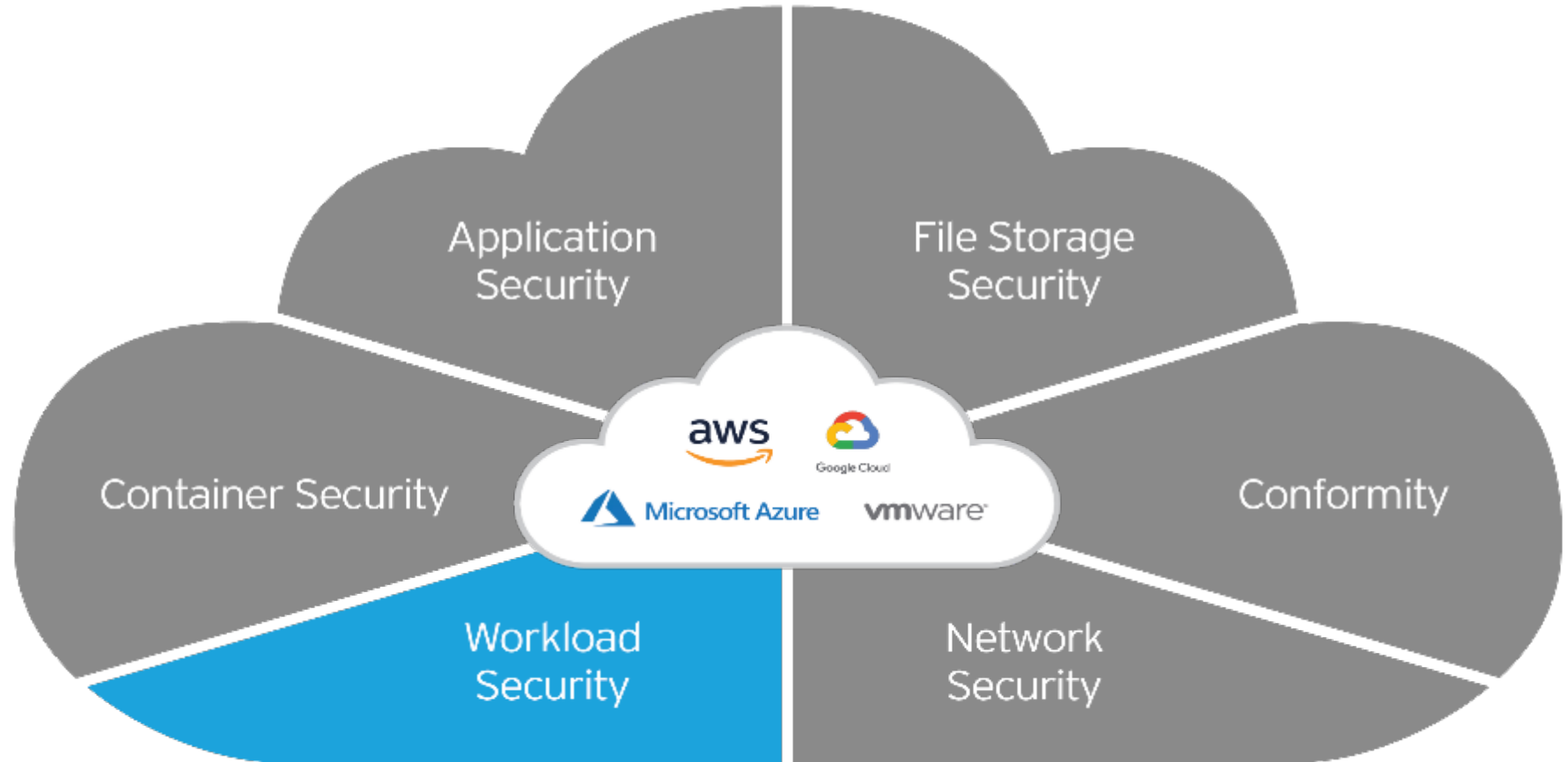
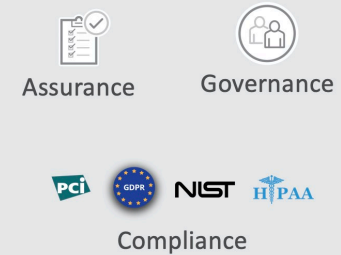
Trend Micro Cloud One.TM

Security Services for Cloud Builders

Cloud Native Application Delivery



Cloud Operational Excellence

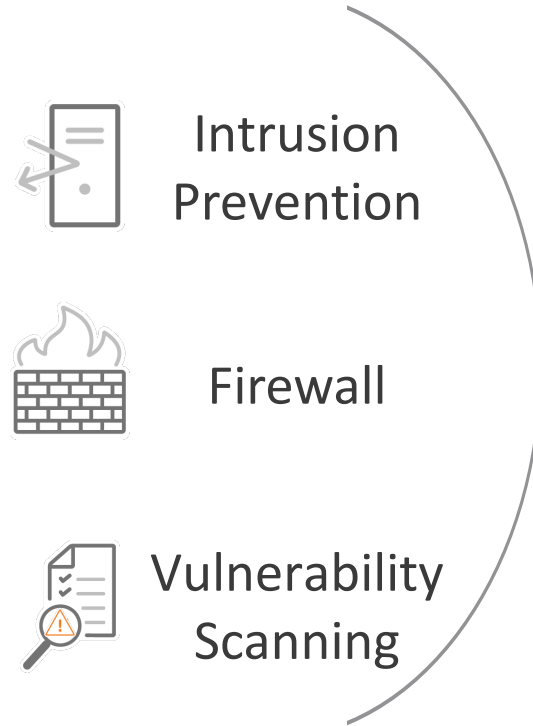


Container Image Scanning



Continuous image scanning

Network Security



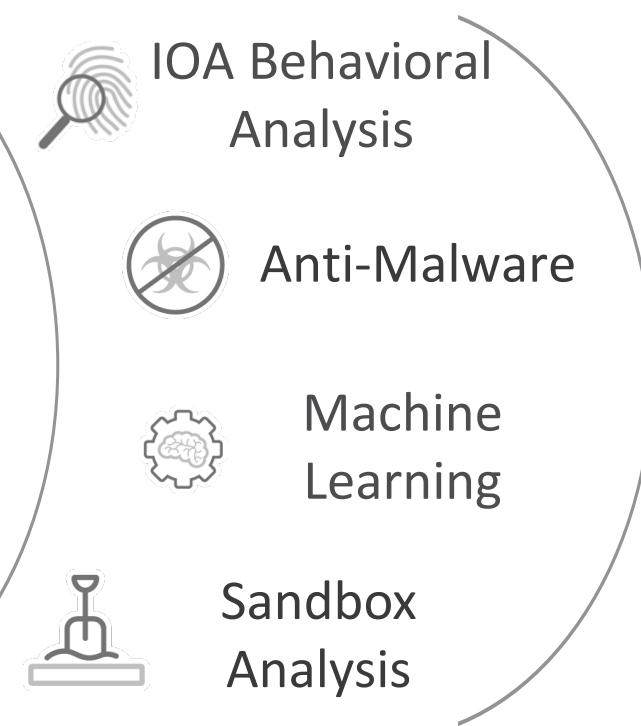
Stop network attacks, shield against vulnerabilities

System Security



Lock down systems & detect suspicious activity

Malware Prevention

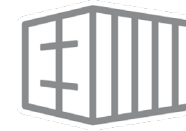


Stop malware & targeted attacks

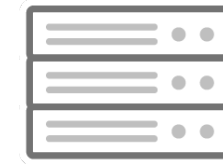
Stages of a Threat



Cloud



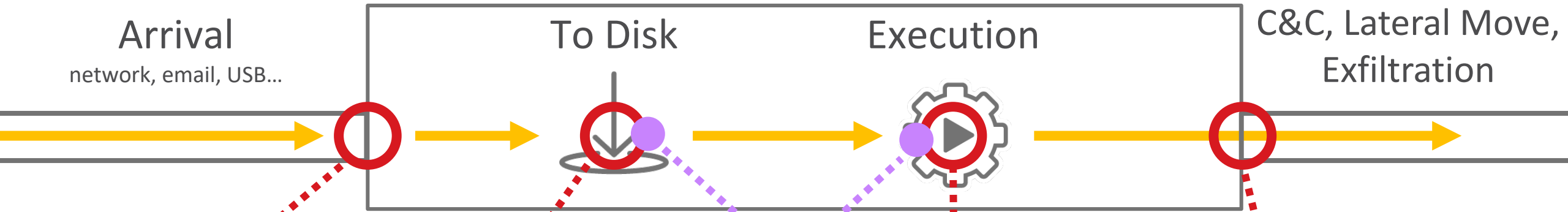
Containers



Data Center



Virtual Server



Arrival

network, email, USB...

To Disk

Execution

C&C, Lateral Move,
Exfiltration



Entry point:

Firewall,
Intrusion Prevention,
Web reputation



Pre-execution:

Machine learning,
Integrity monitoring,
Application control,
File reputation, Variant
Protection



Run-time:

IOA Behavioral
analysis, Integrity
monitoring,
Application control,
Exploit protections,
Ransomware
protection



Exfiltration:

C&C,
IPS
Encrypt /
ransomware

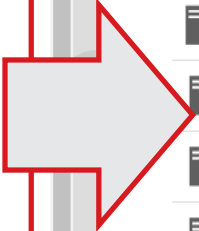


Noise Cancellation:

Census (Prevalence/Maturity)
Whitelist Check



- Smart Folders
- Computers
 - A vCenter - cdvcnsx.greenthis.net
 - Hosts and Clusters
 - Virtual Machines
 - AWS development
 - AWS production
 - Azure lab
 - GCP - DeepSecurityDemo
 - Production
 - deepsecuritydemo
 - Google Cloud
 - DSSC-20180707
 - vCenter - cdcVcsaNsx-T.greenthis.net



Computers With sub-Groups By Group Search this page

+ Add
Delete...
Details...
Actions
Events
Export
Columns...

NAME	PLATFORM	POLICY	STATUS	VERSION	SEND
Computers (8)					
cdcsol.greenthis.net	Solaris 11 (64 bit)	CDC-Linux	Managed (Online)	10.0.0.3059	April
cdcdocker	SUSE Enterprise Server 1...	CDC-Linux	Managed (Online)	11.2.0.147	April
cdccentos2.greenthis.net	Red Hat Enterprise 6 (64 ...	CDC-Linux	Managed (Online)	11.2.0.147	April
cdccentos1.greenthis.net	Red Hat Enterprise 6 (64 ...	CDC-Linux	Managed (Online)	11.2.0.147	April
sapnwgw.greenthis.net	SUSE Enterprise Server 1...	CDC-SAP_Linux	Managed (Online)	11.2.0.147	April
sapnwgui	Microsoft Windows Serv...	CDC-Windows	Managed (Online)	11.2.0.147	April
cdcten1	Microsoft Windows Serv...	CDC-Windows	Managed (Online)	11.2.0.147	April
cdcDSMa.greenthis.net	Microsoft Windows Serv...	None	Managed (Online)	11.2.0.147	April

Computers > A vCenter - cdvcnsx.greenthis.net > Hosts and Clusters > cdc_DC_NSX > cdc...

- Anti-Malware
- Web Reputation
- Firewall
- Intrusion Prevention
- Integrity Monitoring
- Log Inspection
- Application Control

Detect Emerging Security Risks

Predictive Machine Learning for zero-day/unknown threats

- Protects against prevalent server attacks
- Detects emerging known and unknown security risks at pre-execution time
- Performs in-depth Windows file analysis
- Utilizes Trend Micro Smart Protection Network
- Configured as part of the anti-malware settings

The screenshot displays the Trend Micro Deep Security interface. The top navigation bar includes 'Dashboard', 'Actions', 'Alerts', and 'Events & Reports'. The left sidebar shows a tree view with 'Events' expanded to 'Anti-Malware Events'. The main content area shows 'Anti-Malware Events' with filters for 'All' and 'No Grouping', a 'Period' of 'Last 7 Days', and 'Computers' set to 'All Computers'. A table below shows event details for 'June 27, 2017 10:42:40' on 'test-PC (W764...)' with an infected file at 'C:\Users\test\Down...'. Below the table, the 'Predictive Machine Learning' section has a checked 'Enable Predictive Machine Learning' checkbox. The 'Behavior Monitoring' section has two unchecked checkboxes: 'Detect suspicious activity and unauthorized changes (incl. ransomware)' and 'Back up and restore ransomware-encrypted files'.

Adds combined threat prevention and detection as part of the strong Deep Security layered security solution

Stop Unauthorized Changes

Application Control

- Full visibility of host executables
- Lock down applications and servers (Windows & Linux)
- Trusted updater automatic whitelisting
- Support continuous application change with automation
- Quickly respond to newly discovered threats with block by hash (e.g. IOCs)

The screenshot displays the Trend Micro Deep Security console. The main view is titled "Unrecognized Software" and shows a bar chart of activity over the last 7 days. Below the chart, a table lists 47 occurrences of unrecognized software, grouped by computer. The first group, "ec2-52-73-219-185.compute-1.amazonaws.com", has 41 occurrences and lists files like Database.php, create.php, and delete.php. The second group, "ec2-52-91-135-18.compute-1.amazonaws.com", has 5 occurrences and lists saifc.sh. The third group, "192.168.2.173", has 1 occurrence and lists wget. A modal window is open over the first group, showing options to "Change By Process" (with path /home/computer/desktop/executables), "Change By User" (root), and "Change Event Time" (May 5, 2016). The interface includes a navigation menu on the left with "Smart Folders" (Application Servers, Database Server, Web Servers, Computers) and a top navigation bar with "Dashboard", "Actions", "Alerts", "Events & Reports", "Computers", "Policies", and "Administration".

Vulnerabilities Don't Stop or Go Away



Heartbleed



WannaCry



Erebus



ZERO DAY
INITIATIVE

Trend Micro ZDI detected 1449 vulnerabilities in 2018. This powers unmatched timeliness for virtual patches.



runC



kubernetes



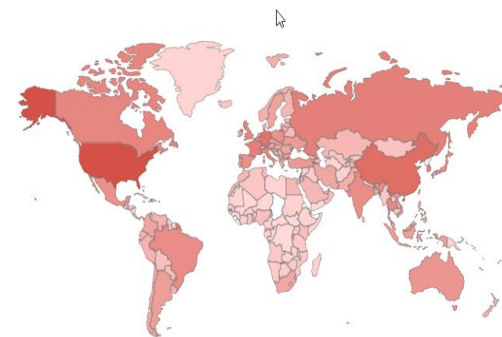
Struts™ 2



Windows

Heartbleed April 2018

Search for `vuln:cve-2014-0160` returned 140,602 results on 18-04-2018

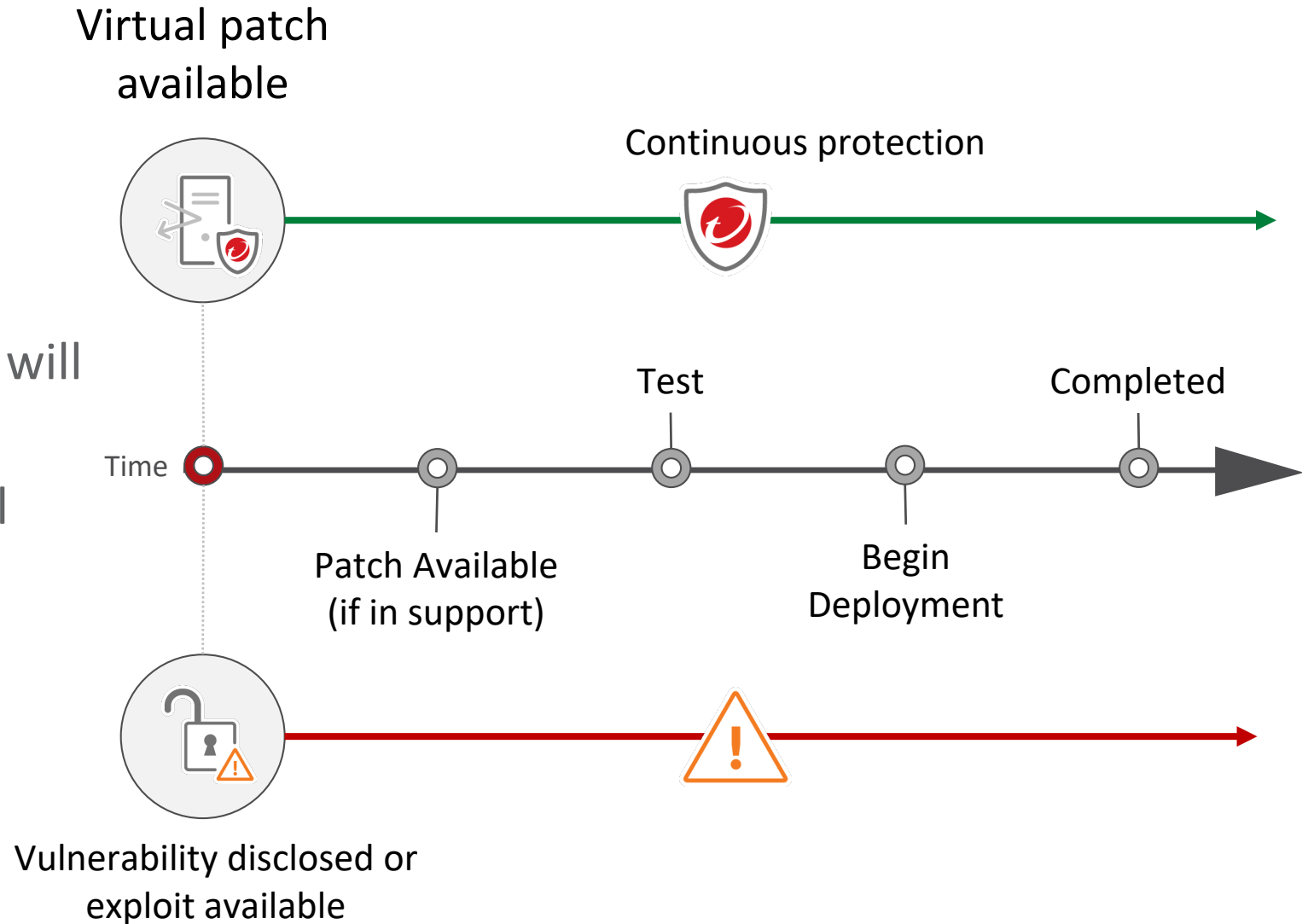


Top Countries

1. United States	34,574
2. China	11,770
3. Germany	9,054
4. France	5,609
5. Russian Federation	5,127
6. Korea, Republic of	4,445
7. Canada	3,957
8. Italy	3,898
9. United Kingdom	3,744
10. Japan	3,461

Reduce Operational Impacts

- Reduce operational costs of emergency & ongoing patching
- Protect systems where no patches will be provided
- Secure server and application-level vulnerabilities



WannaCry ransomware protection delivered in March, 2017, with enhancements at public disclosure (May 2017)

At-a-glance Dashboards: Runtime

The screenshot shows the Trend Micro Deep Security dashboard. At the top, there is a navigation bar with the logo and menu items: Dashboard, Actions, Alerts, Events & Reports, Computers, Policies, Administration. A search bar is on the right. Below the navigation bar, there are tabs for 'Default' and 'Smart View'. A red callout box asks 'How many workloads have security events?'. Another red callout box asks 'Security out of date on workloads?'. The dashboard contains several widgets: 'Alert Status' showing 0 Critical and 7 Warning alerts; 'Computer Status' showing a pie chart with 0 Critical, 0 Warning, 20 Managed, and 48 Unmanaged computers; 'Security Update Status' showing a pie chart with 1 Out-of-Date, 19 Up-to-Date, and 0 Unknown computers; 'Software Updates' showing a green checkmark and 'All Computers are up to date'; 'Alert History' showing a bar chart of alert counts over time; 'Activity Overview' showing 1,628 Protection Hours and 13.99 GB Database Size; and 'My Sign-in History' showing two successful sign-in attempts. At the bottom right, there is a summary bar with 'ALERTS 7 0'. A red callout box at the bottom asks 'Trends over time?'.

How many workloads have security events?

Security out of date on workloads?

Trends over time?

Cloud One Security Services



Software Build Pipeline

Runtime / Deployed

Image Scanning

Network Security

System Security

Malware Prevention



Vulnerability Scanning
Malware Detection
Sweeping & Hunting



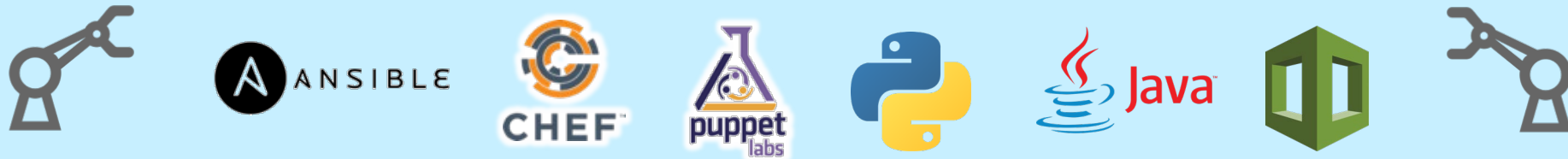
Intrusion Prevention
Firewall
Vulnerability Scanning



Application Control
Integrity Monitoring
Log Inspection



Anti-Malware
Behavioral Analysis Machine Learning
Sandbox Analysis



REALDOLMEN'S OFFERING

- As Reseller
- As Systems Integrator
- As Managed Service Provider



REALDOLMEN'S MSP OFFERING

- As Managed Service Provider
 - ▣ Product is running on RCloud as a multi-tenancy environment
 - ▣ 3 Packages are available
 - Malware prevention
 - System Security
 - Network Security
 - ▣ Pay as you go
 - ▣ Multi-cloud



New challenges

NEW IDEAS



HQ Realdolmen Huizingen

A. Vaucampsaan 42
1654 Huizingen
+32 2 801 55 55

www.realdolmen.com

