

Hybrid Cloud Security

Presenter Name or Company Name & Date

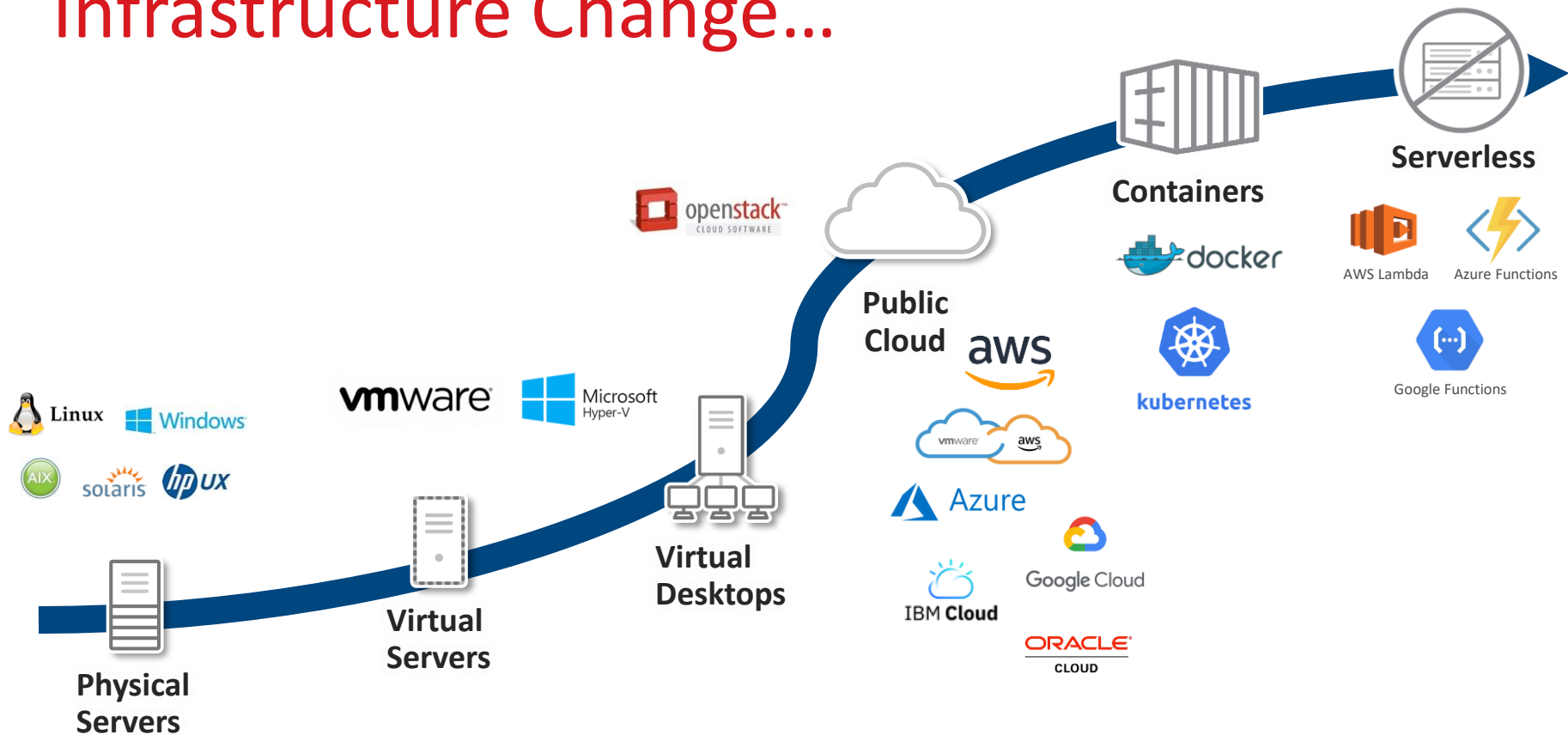




Part of a connected threat defense strategy



Infrastructure Change...



Hybrid Cloud Evolution



1. Cloud Birth



2. Cloud Chaos



3. Cloud Harmony

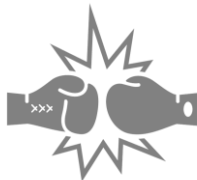


4. Hybrid Groove

Security
Decision
Making



BU Led, Driven by
Time to Market



IT, Security, Cloud
Ops conflict



Cloud and Data
Center Silo's



Aligned, integrated
and fast

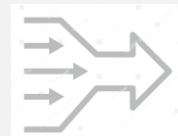
Security &
Compliance
Posture



Inconsistent,
High Risk



Complicated, High
Risk, Not Scalable



Streamlined, Lower
Risk, Scalable



Consistent, Full
Visibility, Faster Audits

Operational
Cost



Experimental Spend



Most Expensive

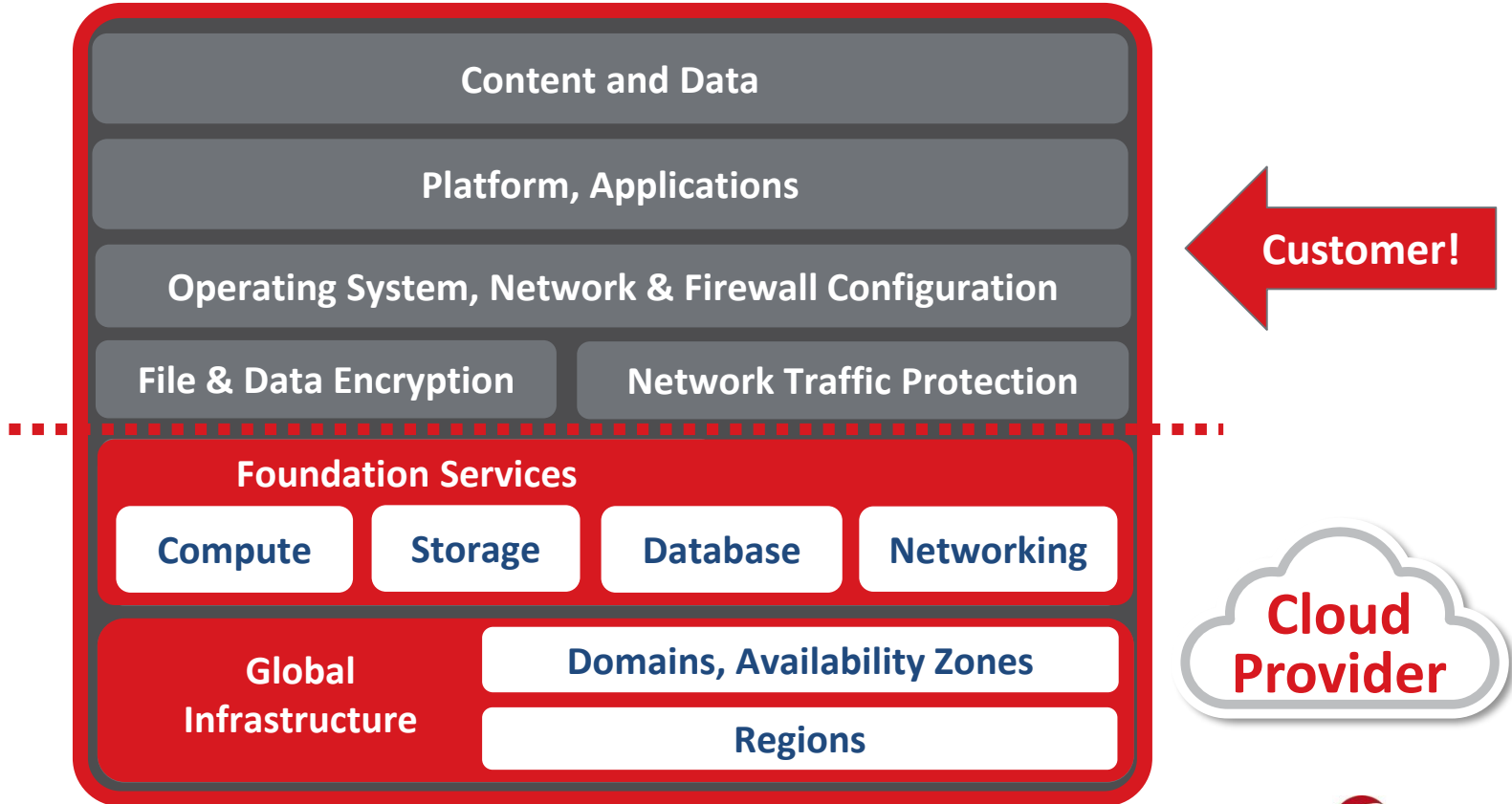


Contained, Sustainable



Optimized

Security is a Shared Responsibility



Deep Security Helps You...



BE POWERFUL

Protect against vulnerabilities, malware & unauthorized changes



GET STREAMLINED

Consistent protection and visibility, optimized for every part of your hybrid cloud



GO AUTOMATED

Connected security that fits seamlessly into Dev and Ops processes to minimize friction & ensure adoption

Why Do I Need Specialized Workload Security?



Threats

- Network attacks
- Vulnerabilities
- Malware
- Open-source



Compliance

- PCI DSS
- HIPAA
- GDPR
- Internal

Deep Security Helps You...



BE POWERFUL

Protect against vulnerabilities, malware & unauthorized changes



GET STREAMLINED

Consistent protection and visibility, optimized for every part of your hybrid cloud



GO AUTOMATED

Connected security that fits seamlessly into Dev and Ops processes to minimize friction & ensure adoption


Container Image Scanning



- Vulnerabilities
- Malware
- Compliance
- Sweeping & Hunting

Continuous image scanning

Network Security



- Intrusion Prevention
- Firewall
- Vulnerability Scanning

Stop network attacks, shield against vulnerabilities

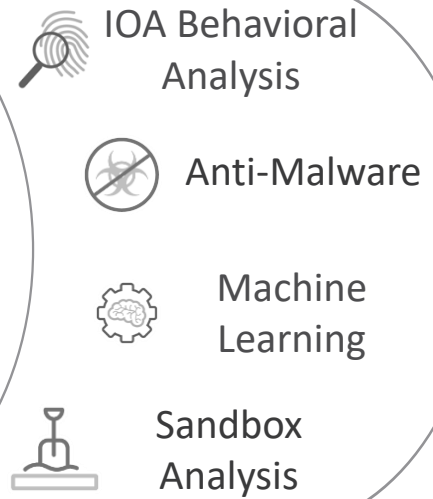
System Security



- Application Control
- Integrity Monitoring
- Log Inspection

Lock down systems & detect suspicious activity

Malware Prevention



- IOA Behavioral Analysis
- Anti-Malware
- Machine Learning
- Sandbox Analysis

Stop malware & targeted attacks

Stages of a Threat



Cloud



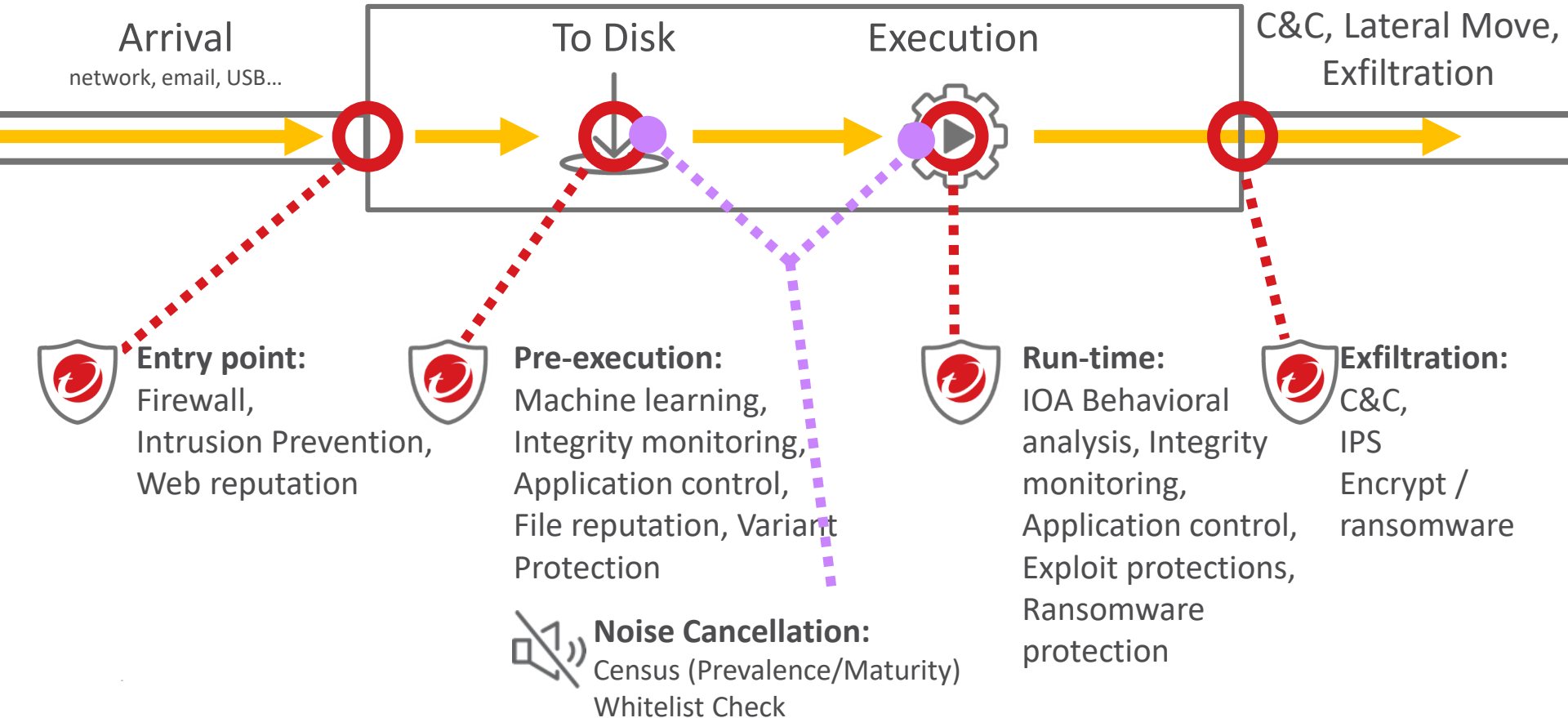
Containers



Data Center



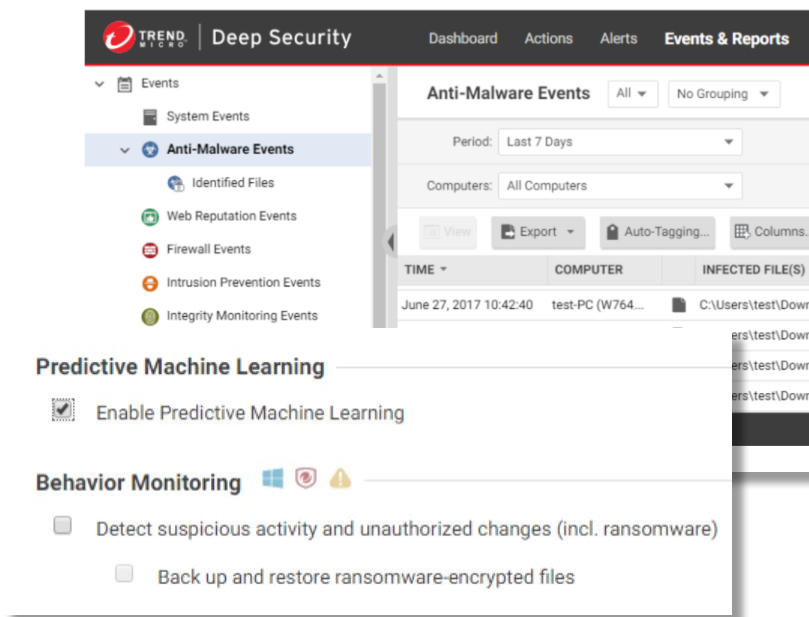
Virtual Server



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



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 interface. The main window is titled "Unrecognized Software" and shows a list of software items detected on various hosts. A context menu is open over the first item, listing options: "Change By Process" (with path /home/computer/desktop/executables), "Change By User" (with user root), and "Change Event Time" (with date May 5, 2016). The software list includes items like "Database.php", "create.php", "size.php", "write.php", "write_rows.php", "saftc.sh", and "wget". Each item has columns for "Date Detected", "Installed By", and "Action" (Allow/Block). A bar chart at the top shows the number of occurrences over time. The right sidebar shows system information for the host 192.168.2.173, including hostname, display name, last IP used, platform, policy, ruleset, and agent version.

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



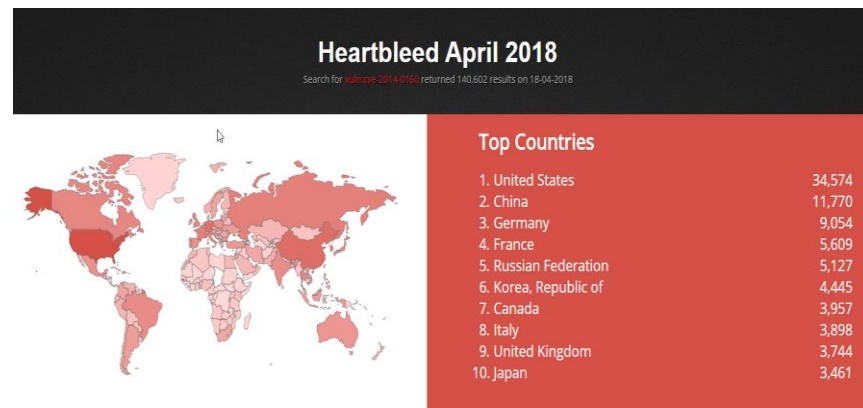
kubernetes



Struts™ 2



Windows



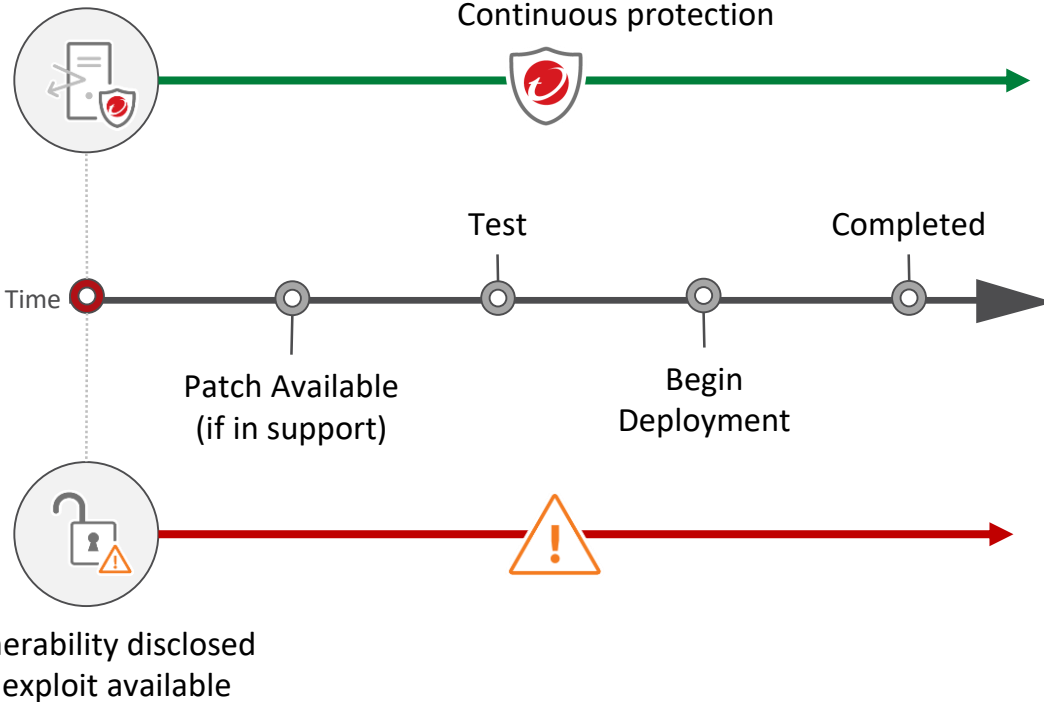
Reduce Operational Impacts

- 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)

Virtual patch available



Accelerate Incident Response

What was affected?

What was added?

Where did it spread?



PREVENT

Assess potential vulnerabilities and proactively protect workloads from threats



DETECT

Detect advanced malware and suspicious behavior that evades standard defenses



RESPOND

Respond to detections with remediation options and workflow integrations



INVESTIGATE

Gain operational visibility, and investigate threat severity and impact

DEMISTO

ArcSight

now

IBM
Radar

splunk



SWIMLANE

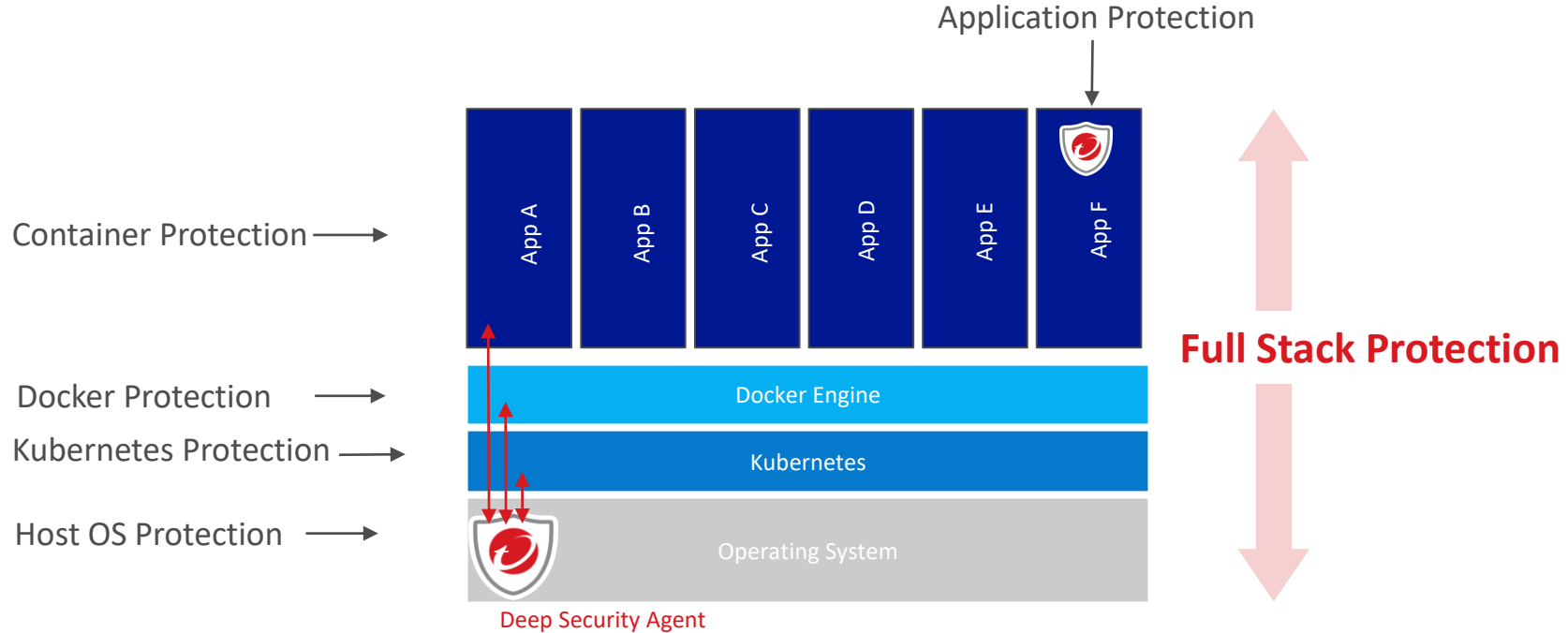
sumologic



TREND
MICRO

Deep Security for Containers

Runtime Protection for Docker Deployments

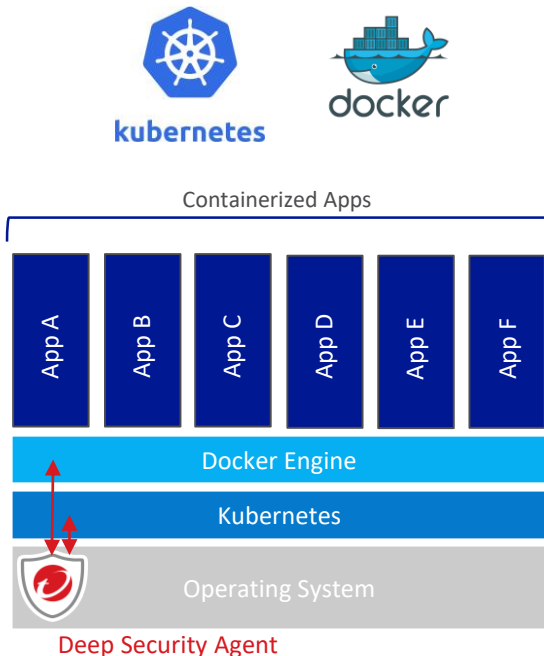


Physical, Virtual or Cloud Container Nodes

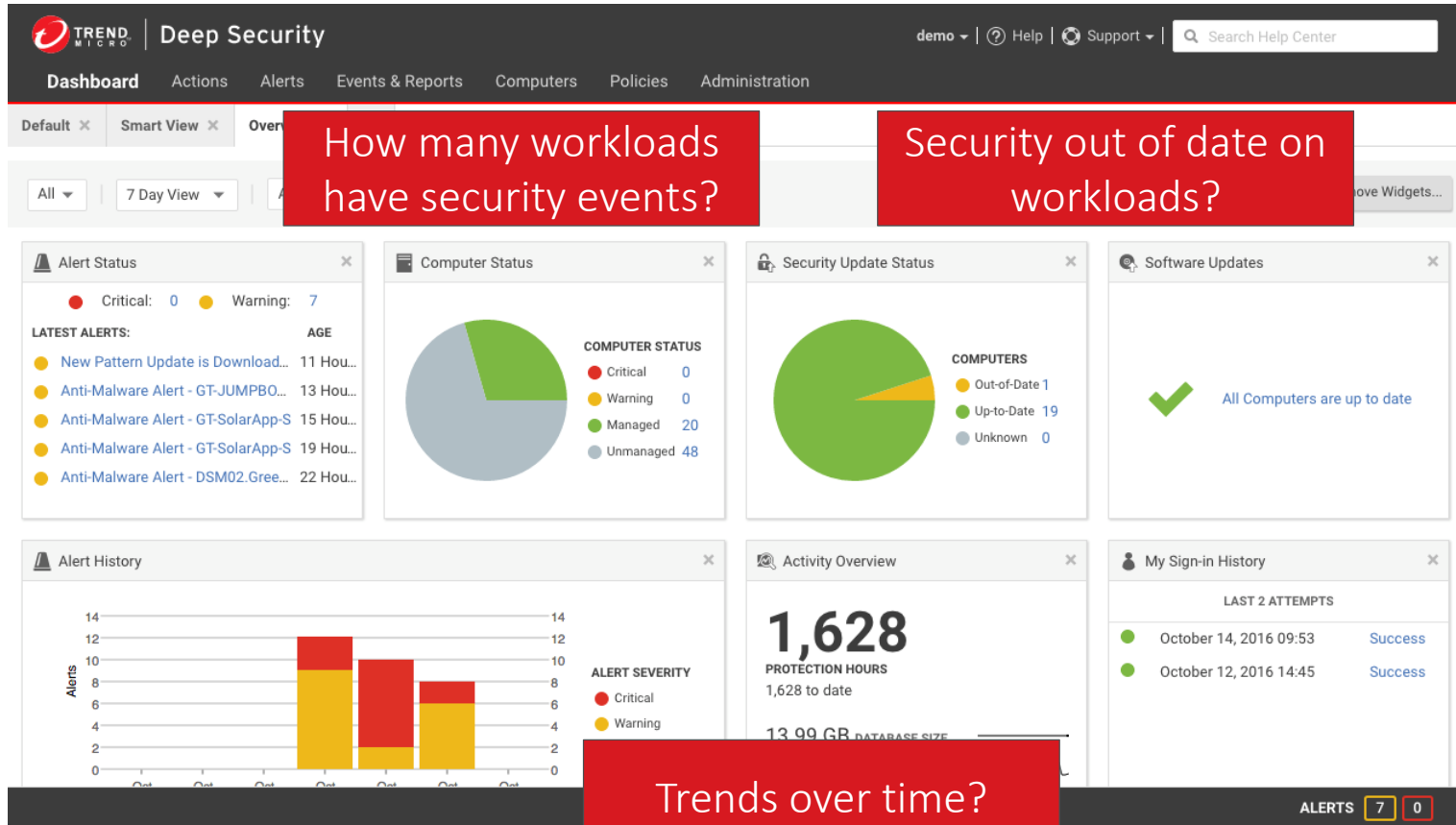
Detecting Container Platform Attacks

Docker and Kubernetes Protection

- Attackers may target Docker and Kubernetes to execute attacks
 - Image execution
 - Networking and Microsegmentation
 - Authentication bypass
- Deep Security monitors key objects to detect compromised Docker and Kubernetes instances
 - Software upgrades, downgrades or removal
 - Attribute changes for binaries
 - Running processes
 - Critical files
 - IPtables rules
 - Permissions for key directories



At-a-glance Dashboards: Runtime



Container Image Scanning



Continuous image scanning

Network Security



Stop network attacks, shield against vulnerabilities

System Security



Lock down systems & detect suspicious activity

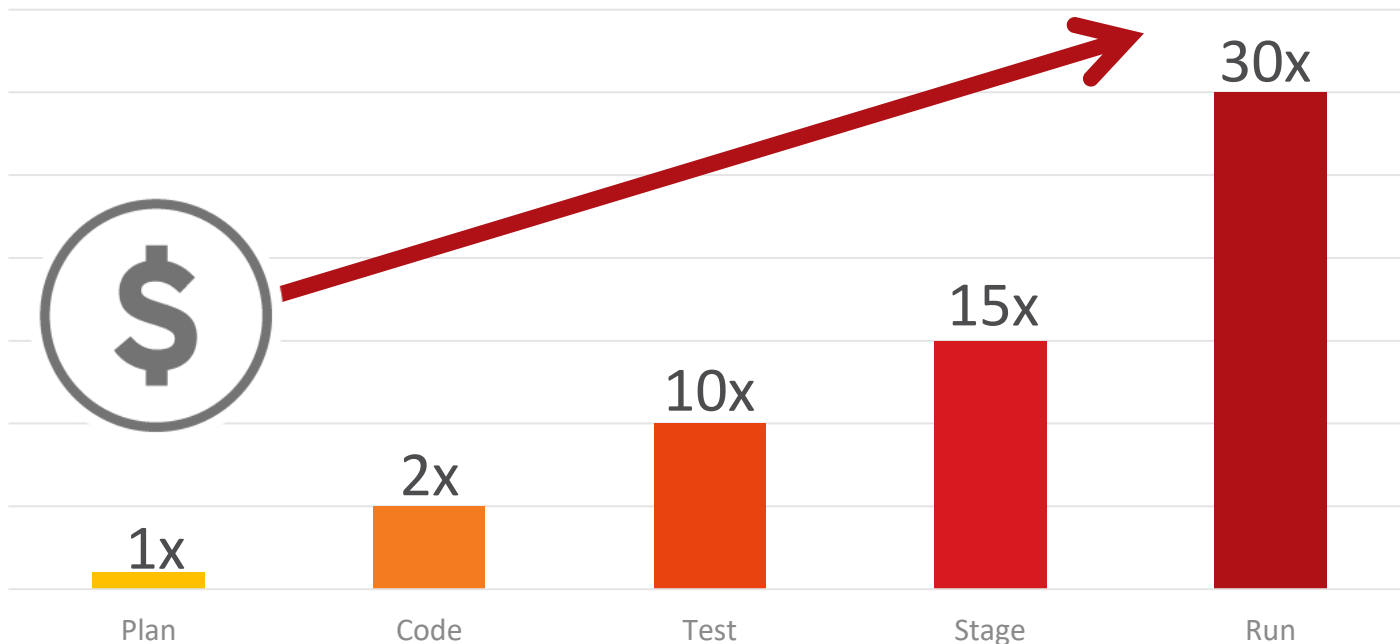
Malware Prevention



Stop malware & targeted attacks

When You Apply Security 'Controls' Matters

Resolution Cost – Workflow Stage



Security Across the Application Lifecycle



Deep Security Smart Check

Continuous
image scanning

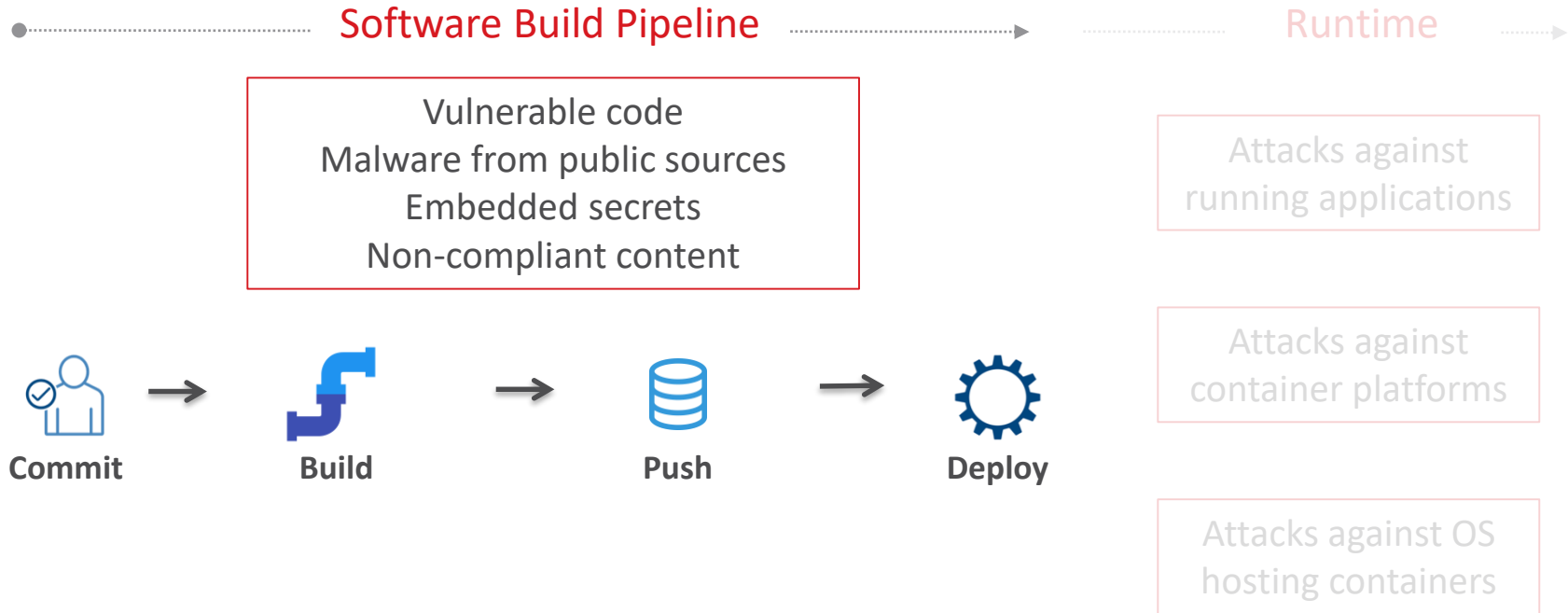
Shift Left to protect the software build pipeline



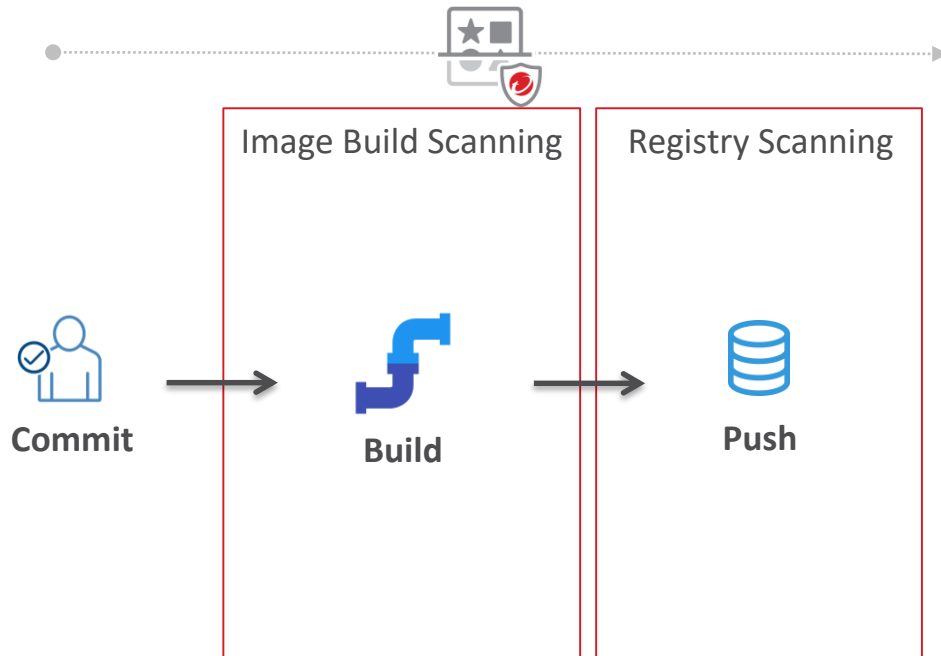
Deep Security

Runtime workload
and container
security

Software Build Pipeline Risks



Pipeline Scanning with Deep Security Smart Check



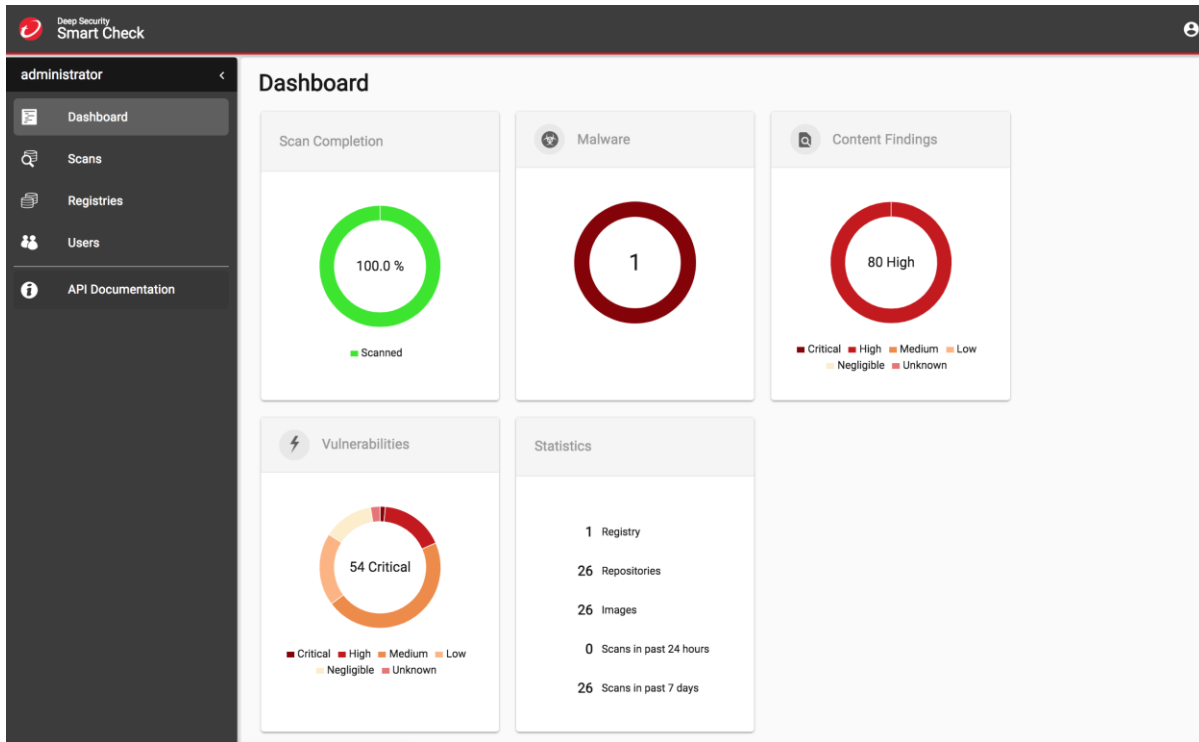
- Advanced Scanning and Detection:
 - Vulnerabilities
 - Malware
 - Embedded Secrets
 - IoCs (sweeping)
 - Policy Compliance
- Continuous protection:
 - Build-time scanning for earliest detection and lowest cost remediation
 - Continuous registry scanning
 - Latest Threat Intelligence

At-a-glance Dashboards: Image Scanning

Have all our images been scanned?

Do any items need attention?

What has been scanned?



Scans

	us.gcr.io/argus-deploy/eicar:latest	576fa32e	2018-12-26 11:54
	1		
	us.gcr.io/argus-deploy/vscan:latest	c1667174	2018-12-26 11:56
	28 Medium + 42 Other		
	us.gcr.io/argus-deploy/squid:latest	71e5d0e3	2018-12-26 11:54
	4 High + 7 Other		
	us.gcr.io/argus-deploy/auth:latest	b867743c	2018-12-26 11:52
	us.gcr.io/argus-deploy/jm-nginx:latest	a4fb1545	2018-12-26 11:54
	17 High + 109 Other		
	us.gcr.io/argus-deploy/db:latest	05e2f457	2018-12-26 11:53
	1 high		
	32 High + 141 Other		
	us.gcr.io/argus-deploy/sc-success-sample:latest	69abf719	2018-12-26 11:52
	1 medium		
	us.gcr.io/argus-deploy/sc-failure-sample:latest	964485a3	2018-12-26 11:50
	2 High + 5 Other		
	us.gcr.io/argus-deploy/clair:latest	817ad70d	2018-12-26 11:51
	10 high		
	3 Medium + 1 Other		
	us.gcr.io/argus-deploy/contentsourcecan:latest	fd9280ed	2018-12-26 11:41

LEADER in vulnerability discovery
since 2007, with **1449**
vulnerabilities reported in 2018



TOP REPORTER of Microsoft &
Adobe vulnerabilities worldwide



Threats



Vulnerabilities
& Exploits



Targeted
Attacks



AI &
Machine Learning



IoT



OT / IIoT



Cybercriminal
Undergrounds



Future Threat
Landscape

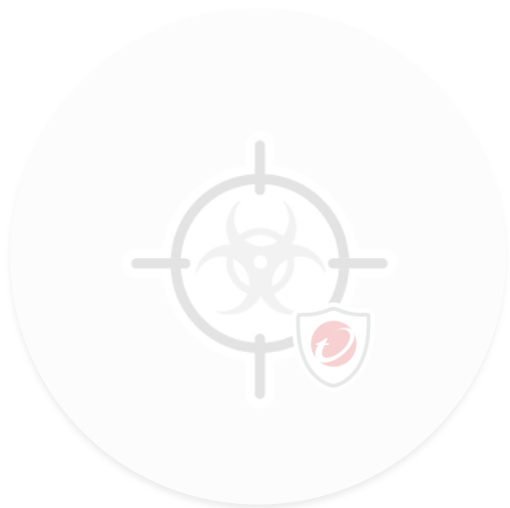


Accelerated compliance

- Multiple controls with central management & reporting
- Protect legacy environments
- Consistent security across the hybrid cloud



Deep Security Helps You...



BE POWERFUL

Protect against vulnerabilities, malware & unauthorized changes



GET STREAMLINED

Consistent protection and visibility, optimized for every part of your hybrid cloud

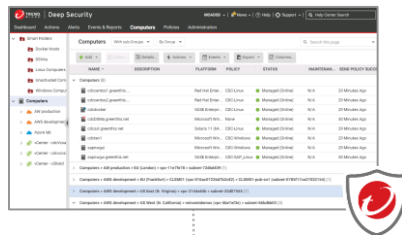


GO AUTOMATED

Connected security that fits seamlessly into Dev and Ops processes to minimize friction & ensure adoption

Built for the Hybrid Cloud

Deep Security



Data Center



Public Cloud



Containers

vmware®

NUTANIX™

Microsoft
Hyper-V

aws

Azure

Google Cloud

docker

kubernetes

RED HAT
OPENSIFT

Deep Security Optimized for Cloud



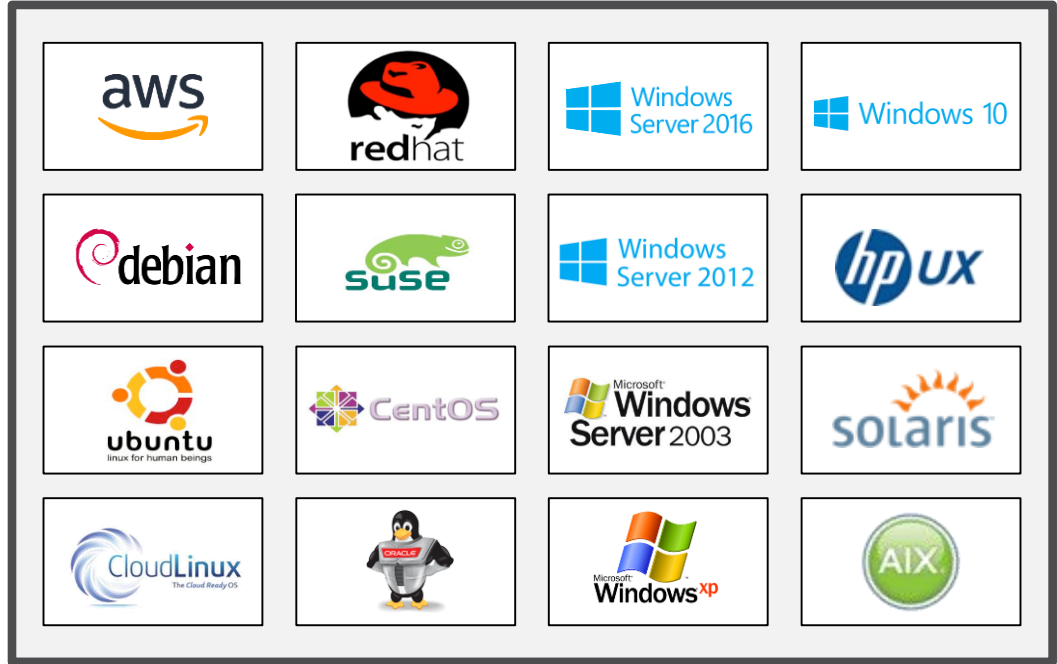
- Azure and AWS Marketplace pay-as-you-go billing and consumption contracts
- Integration for auto-detect & rapid protection
- Quick starts & templates
- AWS & Azure sellers incented to partner
- Complement & integrate with existing AWS, Azure, and Google Cloud toolset



Google Cloud

No More Platform Support Issues

Thousands of supported kernels with rapid updates



Discovery & Visibility Across Your Hybrid Cloud

The screenshot displays the Trend Micro Deep Security interface. The top navigation bar includes the logo, 'Deep Security' title, and navigation links for MOADSD, News, Help, and Support. Below this is a secondary navigation bar with 'Dashboard', 'Actions', 'Alerts', 'Events & Reports', 'Computers', 'Policies', and 'Administration'. The left sidebar shows a tree view of 'Smart Folders' including Docker Hosts, DSVAs, Linux Computers, Unactivated Computers, and Windows Computers. The 'Computers' folder is selected and expanded, showing a list of 8 computers. A red callout box highlights the text: 'Smart folders for customized views across physical, virtual, cloud, containers'. Another red callout box at the bottom left says: 'Visibility within each environment'. The main table lists computers with columns for NAME, DESCRIPTION, PLATFORM, POLICY, STATUS, MAINTENAN..., and SEND POLICY SUCC... The table shows various operating systems like Red Hat Enterprise Linux, SUSE Enterprise Linux, Microsoft Windows, and Solaris 11, all with a 'Managed (Online)' status. Breadcrumbs at the bottom show the path: Computers > AWS development > EU (Frankfurt) > CLSM01 (vpc-016ac07226d7b2c82) > CLSM01-pub-sn1 (subnet-0785f17ce27032154) (1).

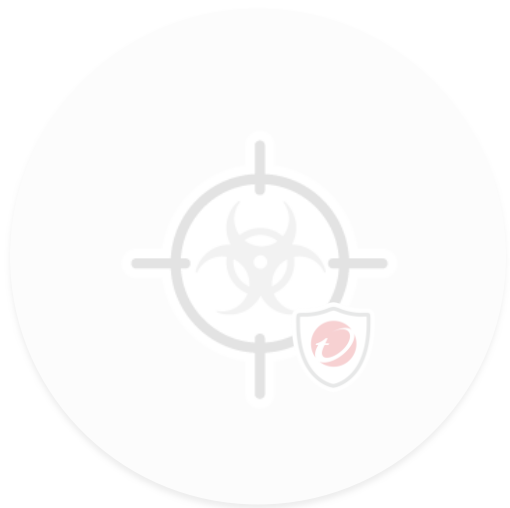
Smart folders for customized views across physical, virtual, cloud, containers

Visibility within each environment

NAME	DESCRIPTION	PLATFORM	POLICY	STATUS	MAINTENAN...	SEND POLICY SUCC...
cdccentos1.greenthis...		Red Hat Enter...	CDC-Linux	Managed (Online)	N/A	29 Minutes Ago
cdccentos2.greenthis...		Red Hat Enter...	CDC-Linux	Managed (Online)	N/A	29 Minutes Ago
cdcdocker		SUSE Enterpri...	CDC-Linux	Managed (Online)	N/A	29 Minutes Ago
cdcDSMa.greenthis.net		Microsoft Win...	None	Managed (Online)	N/A	30 Minutes Ago
cdcsol.greenthis.net		Solaris 11 (64...	CDC-Linux	Managed (Online)	N/A	29 Minutes Ago
cdcten1		Microsoft Win...	CDC-Windows	Managed (Online)	N/A	29 Minutes Ago
sapnwgui		Microsoft Win...	CDC-Windows	Managed (Online)	N/A	29 Minutes Ago
nwgw.greenthis.net		SUSE Enterpri...	CDC-SAP_Linux	Managed (Online)	N/A	30 Minutes Ago

Computers > AWS development > EU (Frankfurt) > CLSM01 (vpc-016ac07226d7b2c82) > CLSM01-pub-sn1 (subnet-0785f17ce27032154) (1)

Deep Security Helps You...



BE POWERFUL

Protect against vulnerabilities, malware & unauthorized changes



GET STREAMLINED

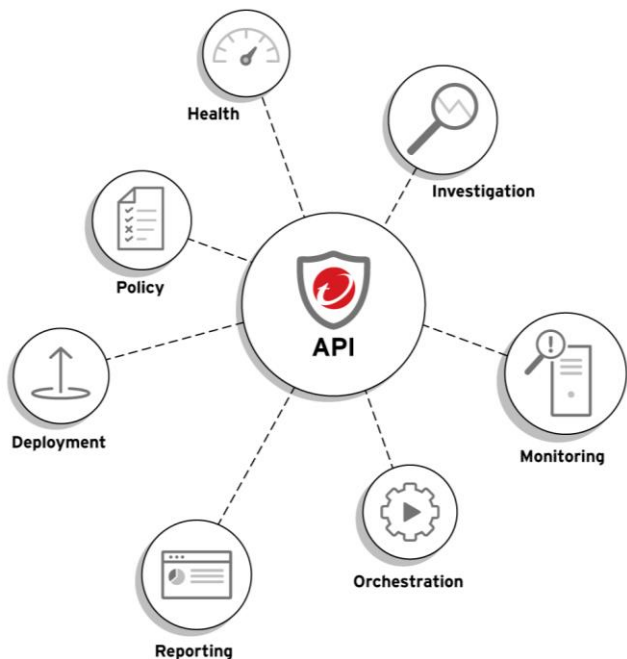
Consistent protection and visibility, optimized for every part of your hybrid cloud



GO AUTOMATED

Connected security that fits seamlessly into Dev and Ops processes to minimize friction & ensure adoption

Accelerate Security Automation



Security Automation - policy creation, and updates

Deployment Automation - security at scale

Reporting Automation - customizable compliance reports and leading SIEM integration

Monitoring Automation - operational and security health of your environment

Orchestration Automation - integrate with your pipeline tools, SOAR tools, etc.

GET /computers

REQUEST SAMPLES

Java Python JavaScript

```
import com.trendmicro.deepsecurity.ApiClient;
import com.trendmicro.deepsecurity.Configuration;
import com.trendmicro.deepsecurity.auth.ApiKeyAuth;
```

```
import com.t
import com.t
import com.t
```

```
public clas
```

```
public st
```

```
// Setup
ApiClient
default
```

```
// Authen
ApiKey
Default
```

```
try {
    defa
} catch
```

```
System
    e.printStackTrace();
}
```

```
// Initialization
// Set Any Required Values
```

```
ComputersApi instance = new ComputersApi();
Boolean overrides = false;
String apiVersion = "v1";
try {
```

Automation Center

API first for hybrid cloud environments

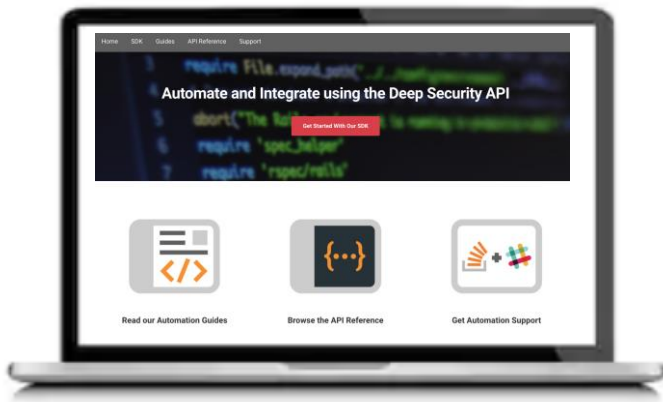
Find - a solution to my problem by searching on Google

Learn - simple guides and example

Code - full RESTful API documentation. Examples of code

Verify - guidance around how to use applications to test APIs

Get Help - Stack Overflow, GitHub, and Trend Help



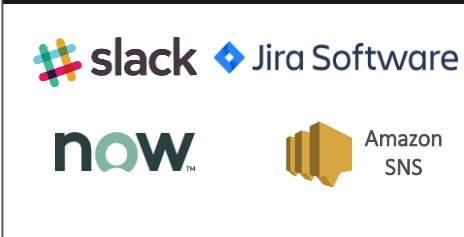
“Using Deep Security, we were able to improve our efficiency with Docker containers to realize savings for our AWS licenses and compute costs ,”
Todd Williams – Manager SecOps at MEDHOST

Automation With Pipeline & Workload Security

Pipeline Management & Deployment



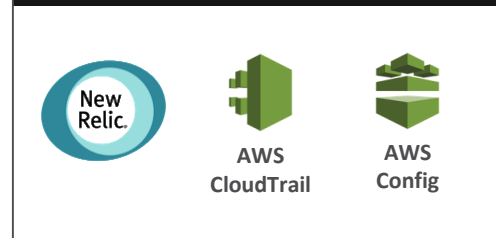
IT Service Management



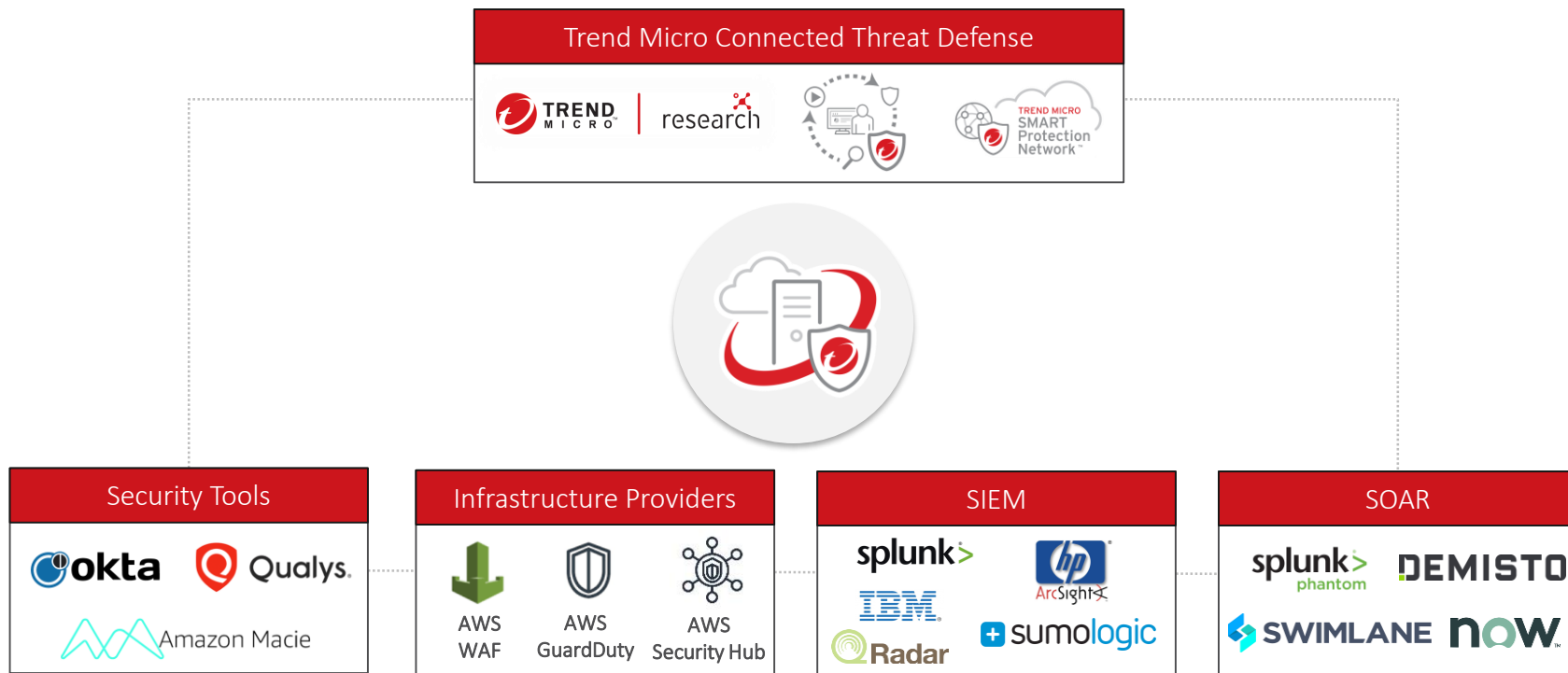
Environments



Monitoring Tools



Automate Threat & Information Sharing





Gartner®

2019
Market Guide for
Cloud Workload
Protection Platforms

Free Download

8 of 8

Core Controls*

+

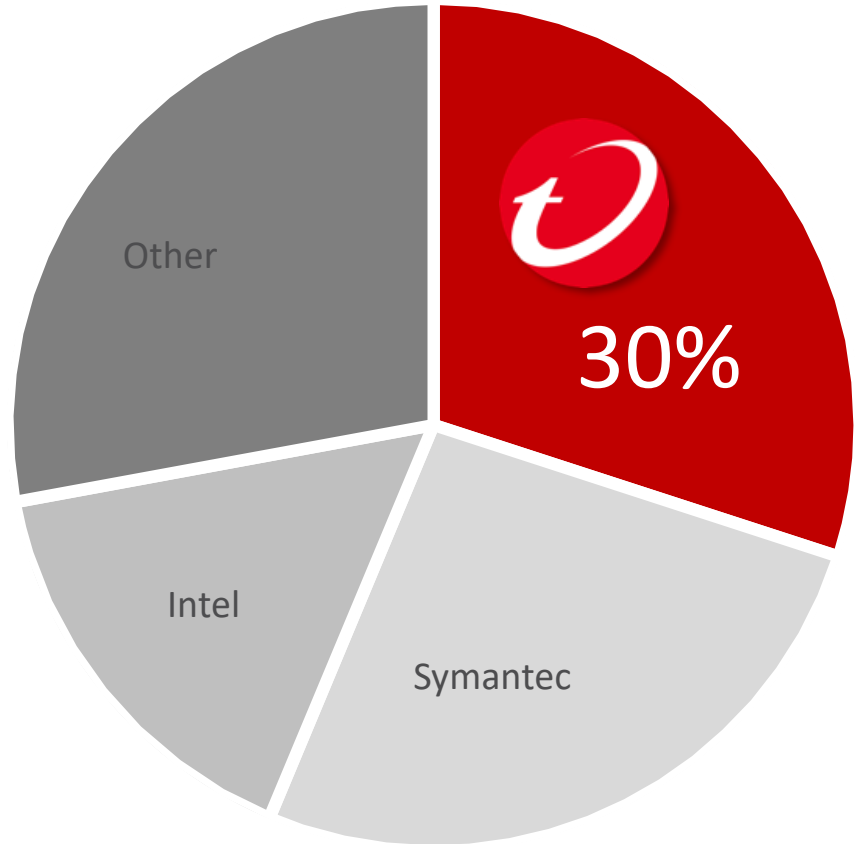
21 of 25

Additional Criteria*

Trend Micro delivers the
most cloud security
controls and criteria of
all security vendors*

* As assessed by Trend Micro

The **MARKET LEADER**
in server security for 7
straight years



Security Wants To...



BE POWERFUL

Protect against vulnerabilities, malware & unauthorized changes



GET STREAMLINED

Consistent protection and visibility, optimized for every part of your hybrid cloud



GO AUTOMATED

Connected security that fits seamlessly into Dev and Ops processes to minimize friction & ensure adoption

DevOps & Automation with Deep Security



Hybrid Cloud Evolution



1. Cloud Birth



2. Cloud Chaos



3. Cloud Harmony

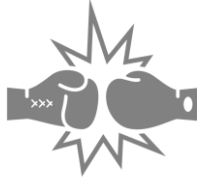


4. Hybrid Groove

Security
Decision
Making



BU Led, Driven by
Time to Market



IT, Security, Cloud
Ops conflict



Cloud and Data
Center Silo's



Aligned, integrated
and fast

Security &
Compliance
Posture



Inconsistent,
High Risk



Complicated, High
Risk, Not Scalable



Streamlined, Lower
Risk, Scalable



Consistent, Full
Visibility, Faster Audits

Cost



Experimental Spend



Most Expensive

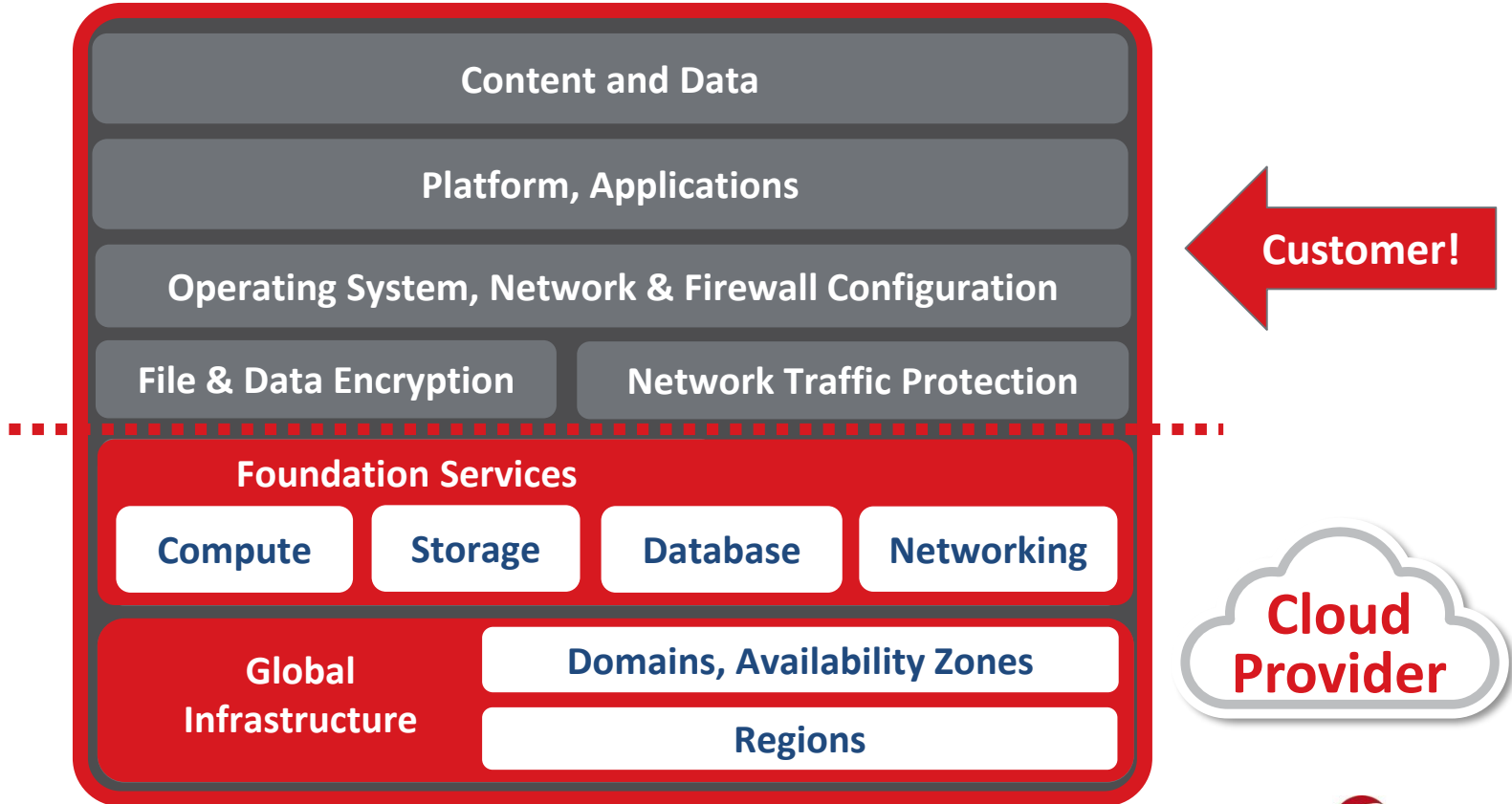


Contained, Sustainable



Optimized

Security is a Shared Responsibility



Why You Need to Care About Security...



Threats

- Network attacks
- Vulnerabilities
- Malware
- Open-source



Compliance

- PCI DSS
- HIPAA
- GDPR
- Internal

DevOps Wants To...



BUILD SECURE

Designed into processes as the speed of business changes



SHIP FAST

Provide synergy between IT Security and DevOps



RUN ANYWHERE

Increased visibility and speed of response across environments

Deep Security Helps You...



BUILD SECURE

Designed into processes as the speed of business changes



SHIP FAST

Provide synergy between IT Security and DevOps

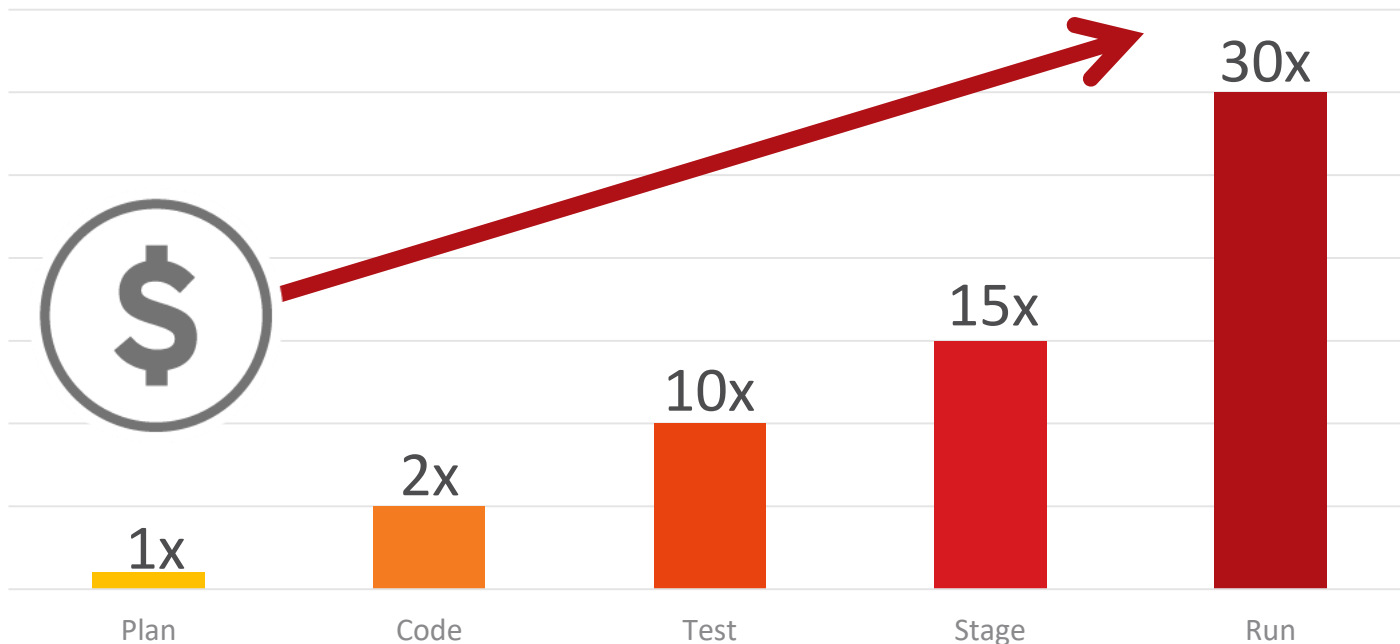


RUN ANYWHERE

Increased visibility and speed of response across environments

When You Apply Security 'Controls' Matters

Resolution Cost – Workflow Stage



Security Across The Application Lifecycle



Deep Security Smart Check

Continuous
image scanning

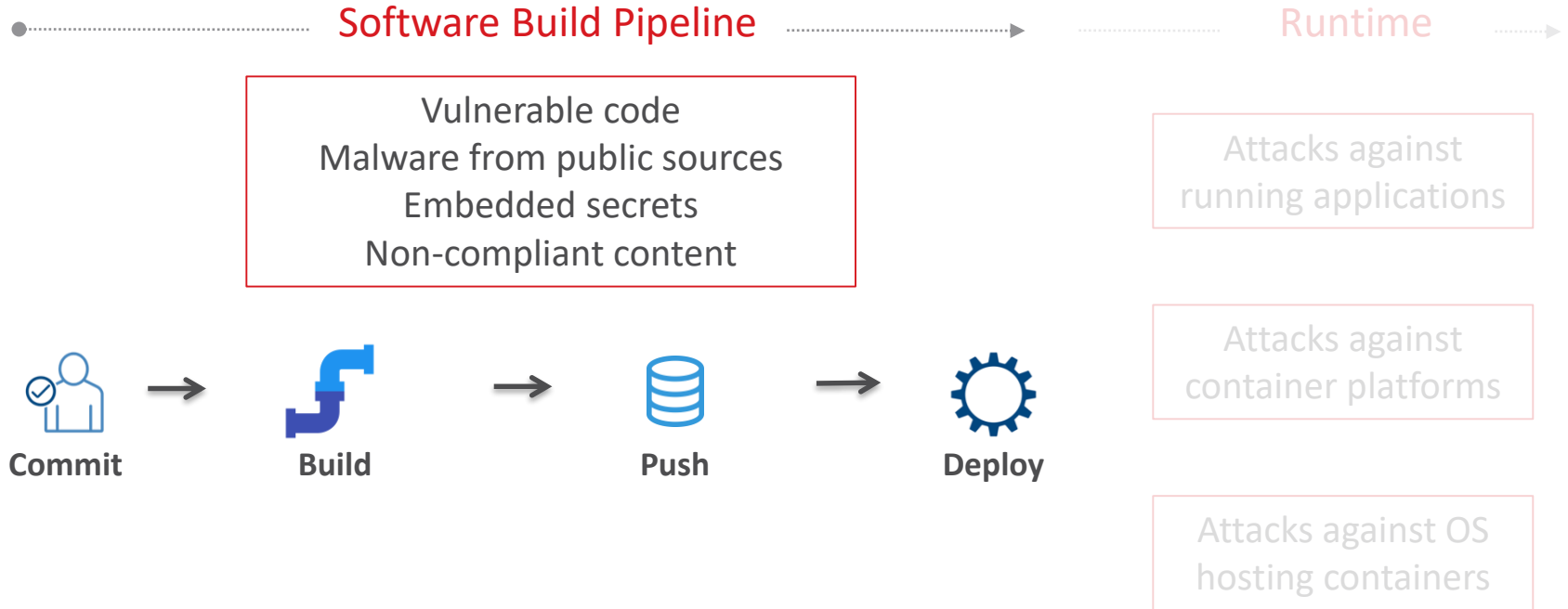
Shift Left to protect the software build pipeline



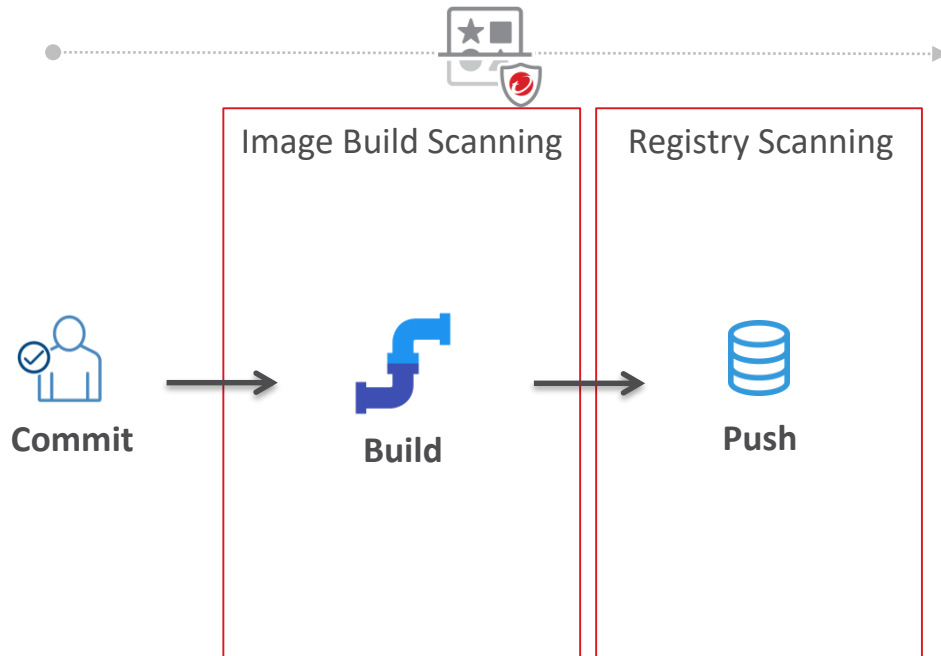
Deep Security

Runtime workload
and container
security

Software Build Pipeline Risks



Pipeline Scanning with Deep Security Smart Check

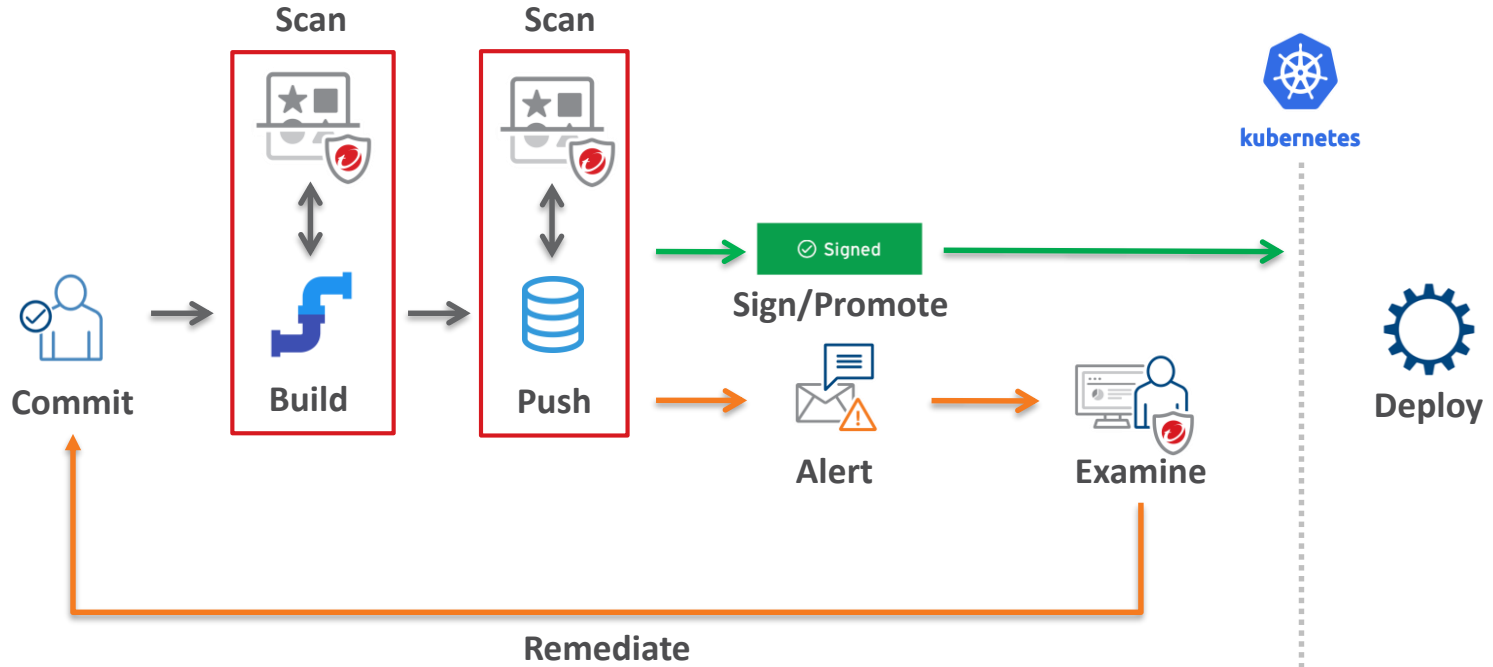


- Advanced Scanning and Detection:
 - Vulnerabilities
 - Malware
 - Embedded Secrets
 - IoCs (sweeping)
 - Policy Compliance
- Continuous protection:
 - Build-time scanning for earliest detection and lowest cost remediation
 - Continuous registry scanning
 - Latest Threat Intelligence

Find Security Issues in the Build Pipeline

Continuous scanning of container images for malware, vulnerabilities, and secrets

Image Assertion – Approve containers for deployment

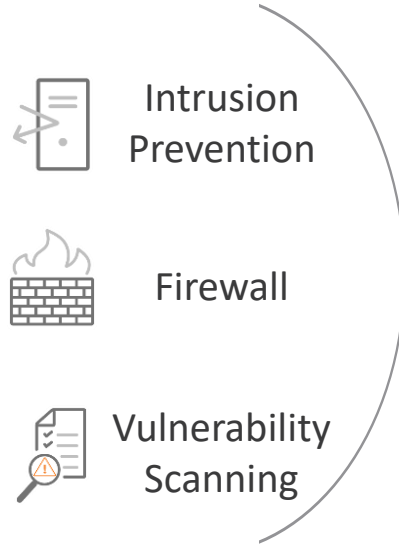


Container Image Scanning



Continuous image scanning

Network Security



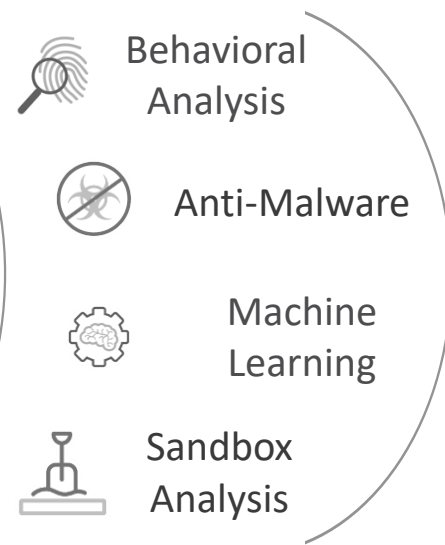
Stop network attacks, shield against vulnerabilities

System Security



Lock down systems & detect suspicious activity

Malware Prevention



Stop malware & targeted attacks

DevOps Can Help With Compliance

- Security capabilities to satisfy security and compliance teams
- Reduce the number of application rebuilds
- Consistent security across the hybrid cloud



Deep Security Helps You...



BUILD SECURE

Designed into processes as the speed of business changes



SHIP FAST

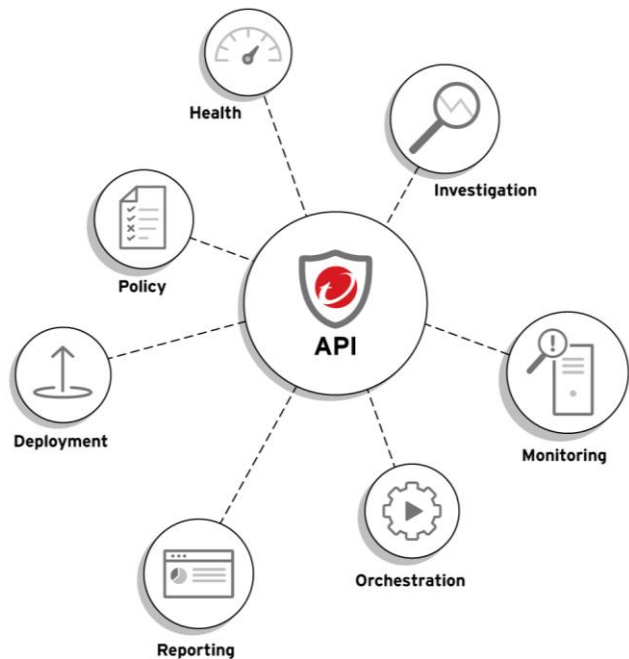
Provide synergy between IT Security and DevOps



RUN ANYWHERE

Increased visibility and speed of response across environments

Accelerate DevOps with Security Automation



Security Automation - policy creation, and updates

Deployment Automation - security at scale

Reporting Automation - customizable compliance reports and leading SIEM integration

Monitoring Automation - operational and security health of your environment

Orchestration Automation - integrate with your pipeline tools, SOAR tools, etc.

```
import com.trendmicro.deepsecurity.ApiClient;
import com.trendmicro.deepsecurity.Configuration;
import com.trendmicro.deepsecurity.auth.ApiKeyAuth;
```

```
import com.t
import com.t
import com.t
```

```
public clas
```

```
public st
```

```
// Setup
ApiClient
default
```

```
// Auther
ApiKey
Default
```

```
try {
    defa
} catch
```

```
System
    e.printStackTrace();
}
```

```
// Initialization
```

```
// Set Any Required Values
```

```
ComputersApi instance = new ComputersApi();
```

```
Boolean overrides = false;
```

```
String apiVersion = "v1";
```

```
try {
```

Security Designed for DevOps

API first for hybrid cloud environments

Find - a solution to my problem by searching on Google

Learn - simple guides and example

Code - full RESTful API documentation. Examples of code

Verify - guidance around how to use applications to test APIs

Get Help - Stack Overflow, GitHub, and Trend Help



“Using Deep Security, we were able to improve our efficiency with Docker containers to realize savings for our AWS licenses and compute costs.”

Todd Williams – Manager SecOps at MEDHOST

Deep Security Helps You...



BUILD SECURE

Designed into processes as the speed of business changes



SHIP FAST

Provide synergy between IT Security and DevOps

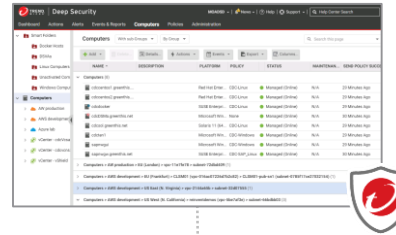


RUN ANYWHERE

Increased visibility and speed of response across environments

Built for the Hybrid Cloud

Deep Security



Data Center



Public Cloud



Containers

vmware®

NUTANIX™ Microsoft Hyper-V

aws Azure Google Cloud

docker

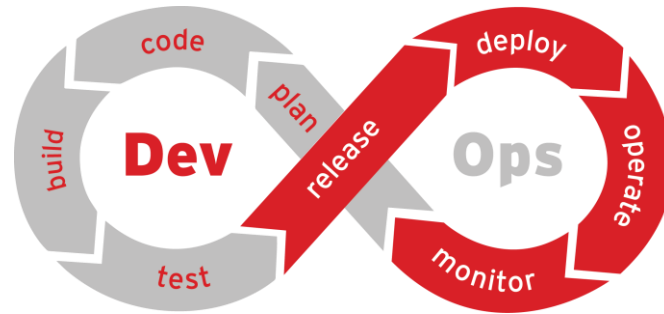
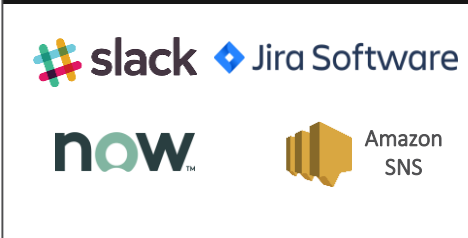
kubernetes RED HAT OPENSIFT

Automation With Pipeline & Workload Security

Pipeline Management & Deployment



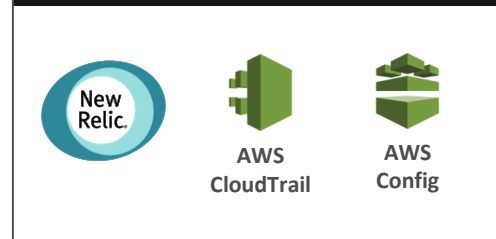
IT Service Management



Environments

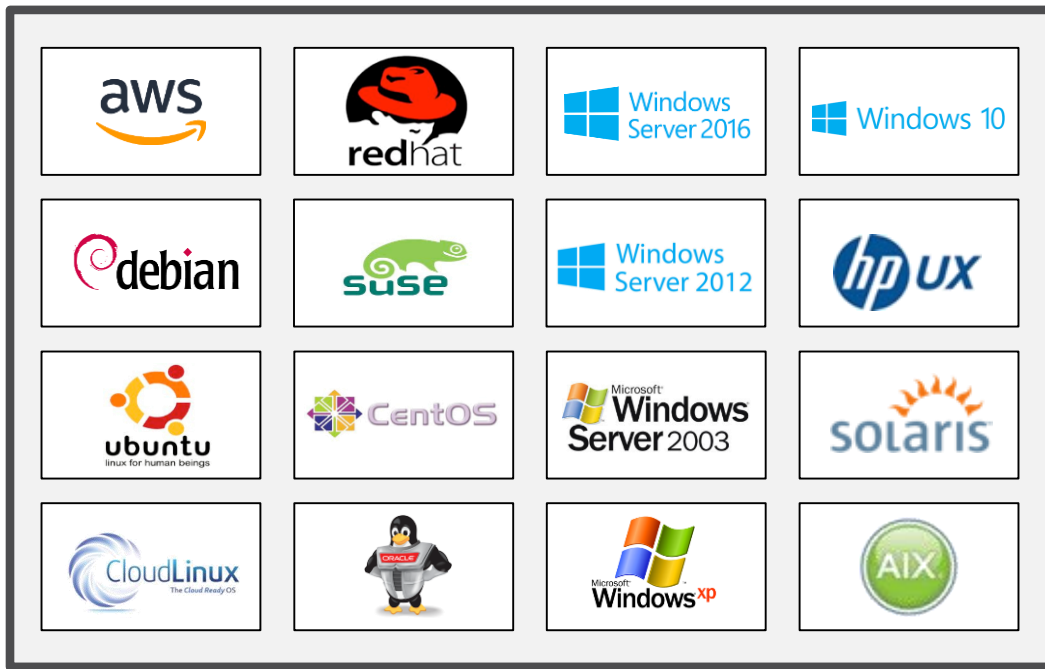


Monitoring Tools



Deploy on Any Platform

Thousands of supported kernels with rapid updates



Deep Security Helps You...



BUILD SECURE

Designed into processes as the speed of business changes



SHIP FAST

Provide synergy between IT Security and DevOps



RUN ANYWHERE

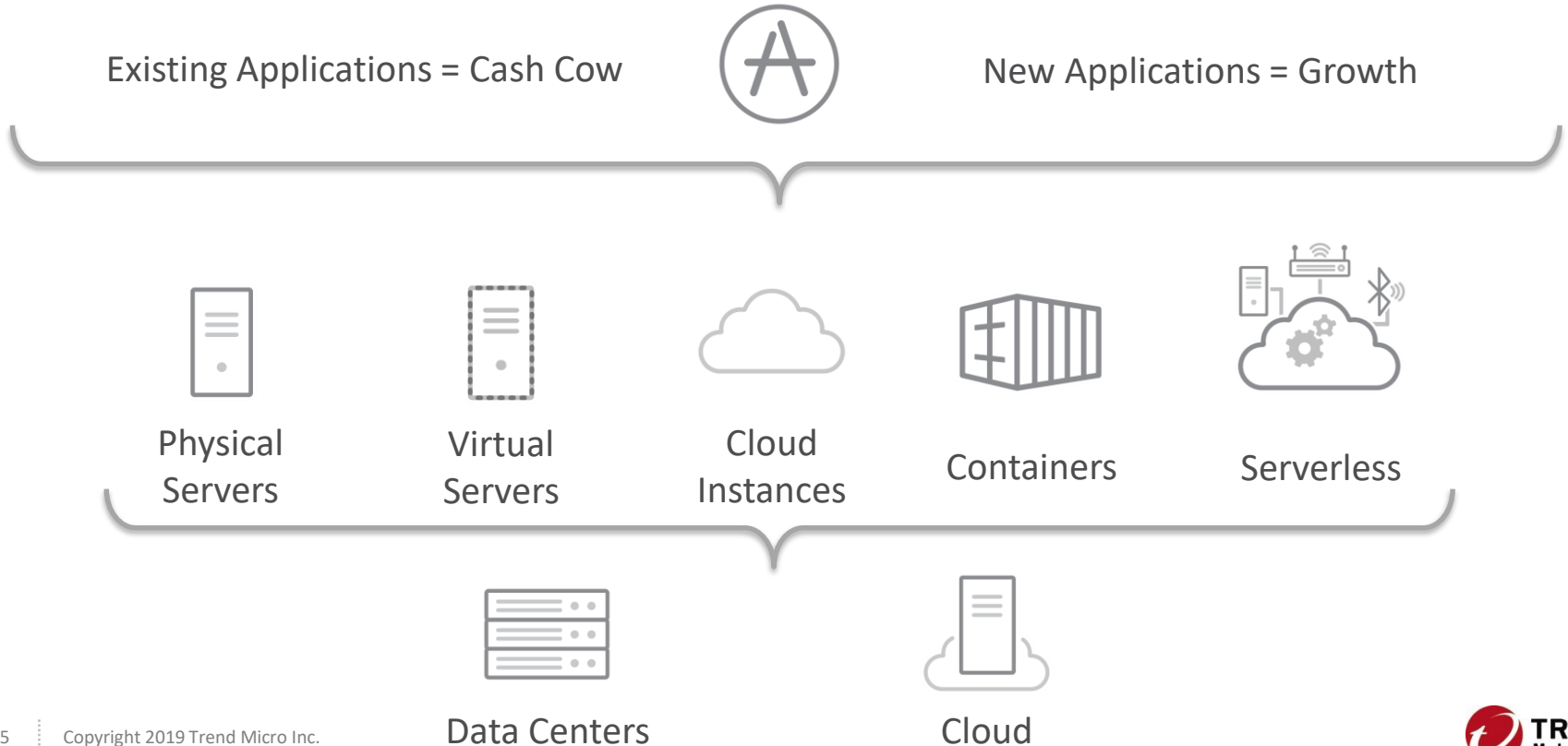
Increased visibility and speed of response across environments



trendmicro.com/hybridcloud

Additional Detail Slides

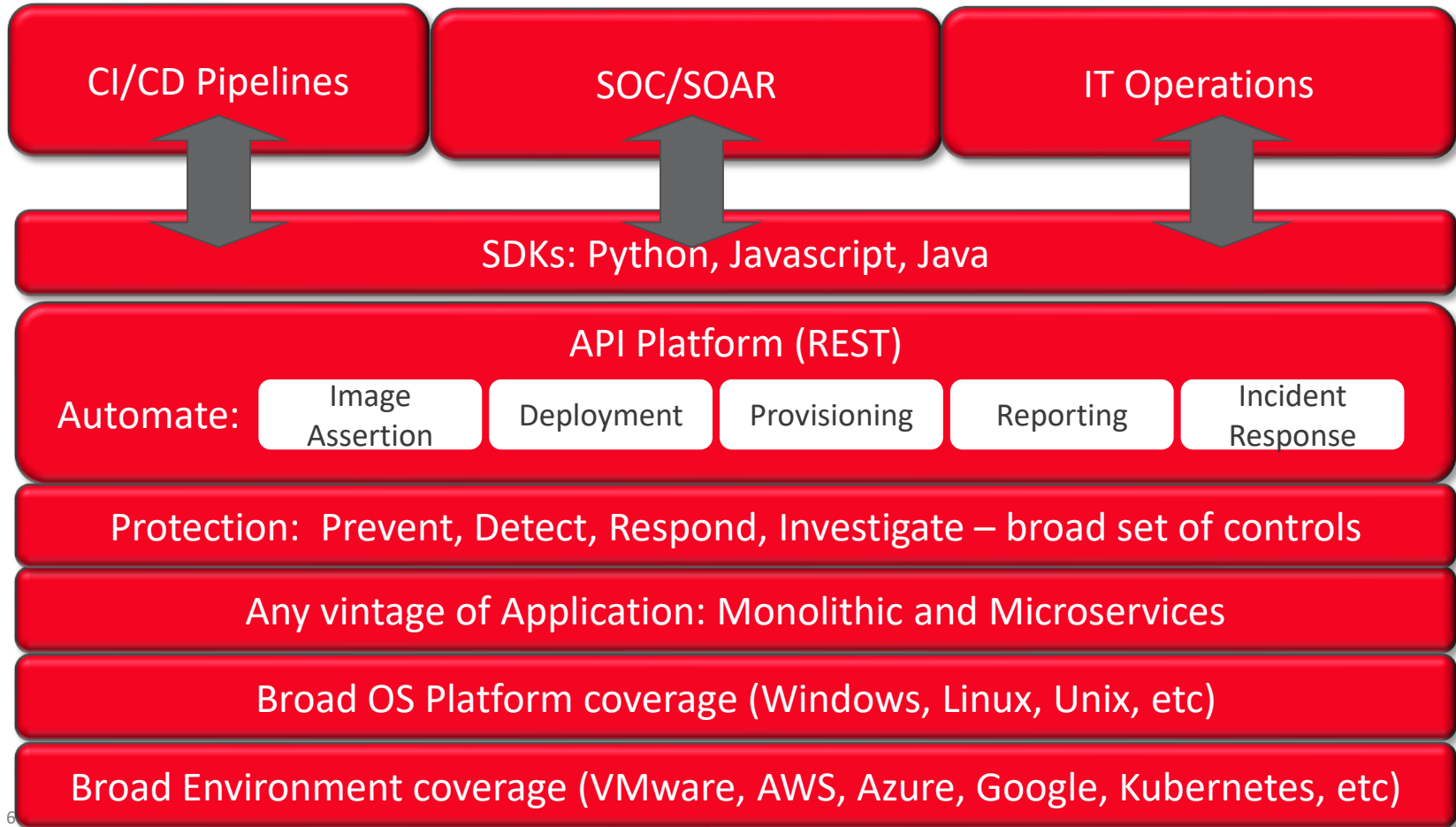
It's a Hybrid Cloud World



How Have Applications Changed?

	Existing Applications = Cash Cow	New Applications = Growth
App Architecture	monolithic	microservices
Scale	vertical, some horizontal	horizontal
Change Frequency	few times per year to monthly	multiple times per day
Deployment Model	pets (long-lived)	cattle (short-lived)
Security Operations	scheduled, manual, runtime	automated CI/CD pipeline + runtime
Security Tools	traditional, manual, static	APIs, cloud-friendly

Automated Security



Hybrid Cloud Security Solution



Software Build Pipeline

Runtime

Container Image Scanning

Network Security

System Security

Malware Prevention



Vulnerability Scanning
Malware Detection
Secrets & Compliance

Intrusion Prevention
Firewall
Vulnerability Scanning

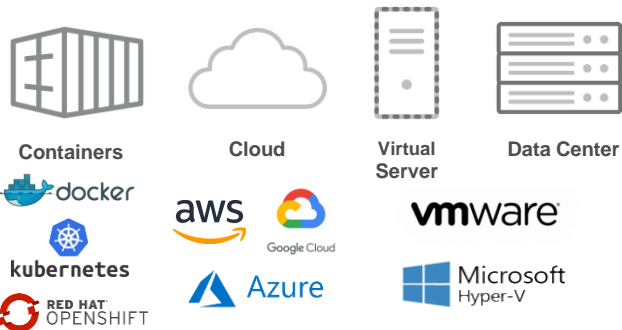
Application Control
Integrity Monitoring
Log Inspection

Anti-Malware
Behavioral Analysis Machine Learning
Sandbox Analysis

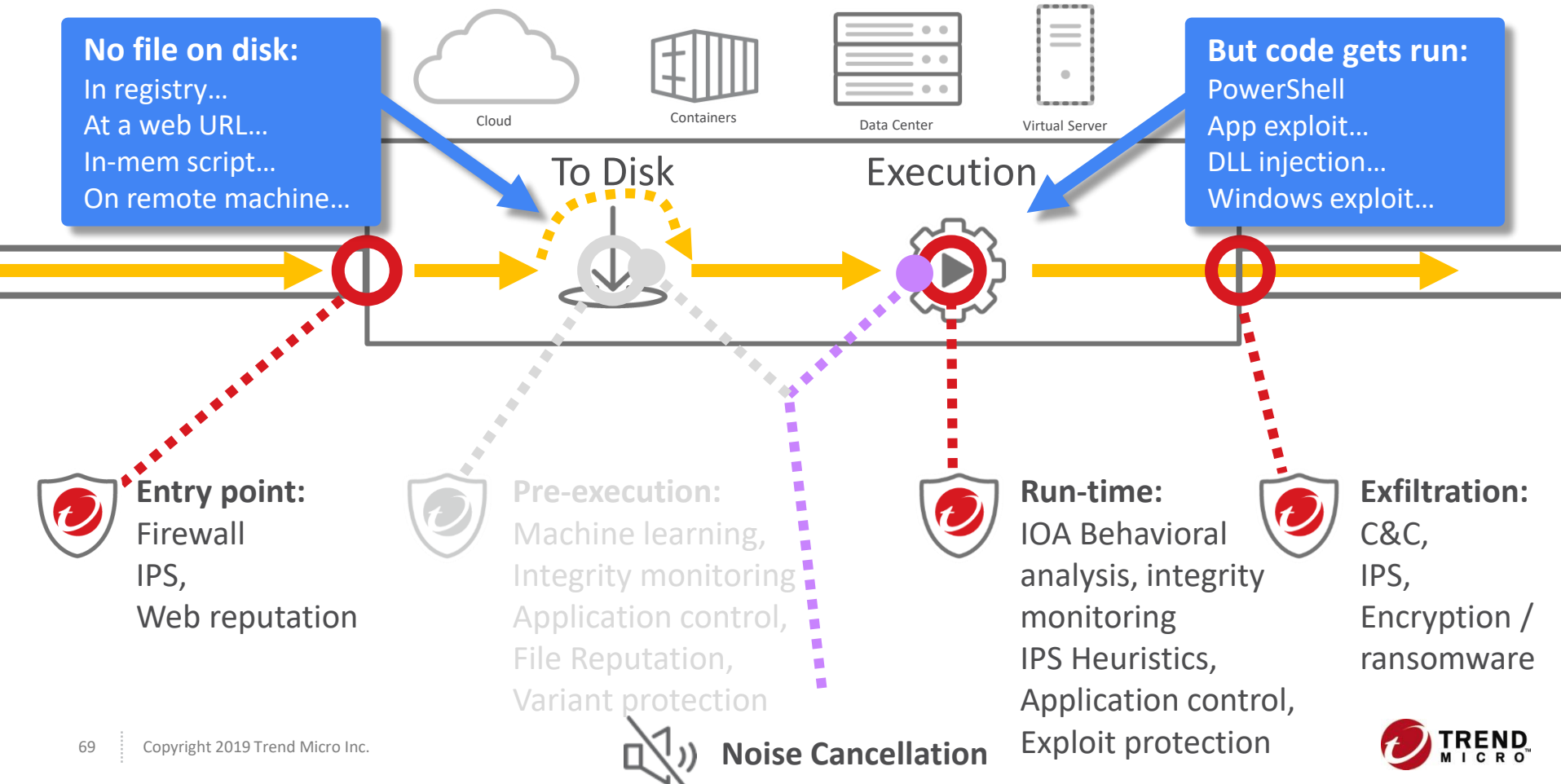
Environments

Platforms

API & Integrations



Defending Against Fileless Malware



Protect Against Advanced Threats

LEGEND



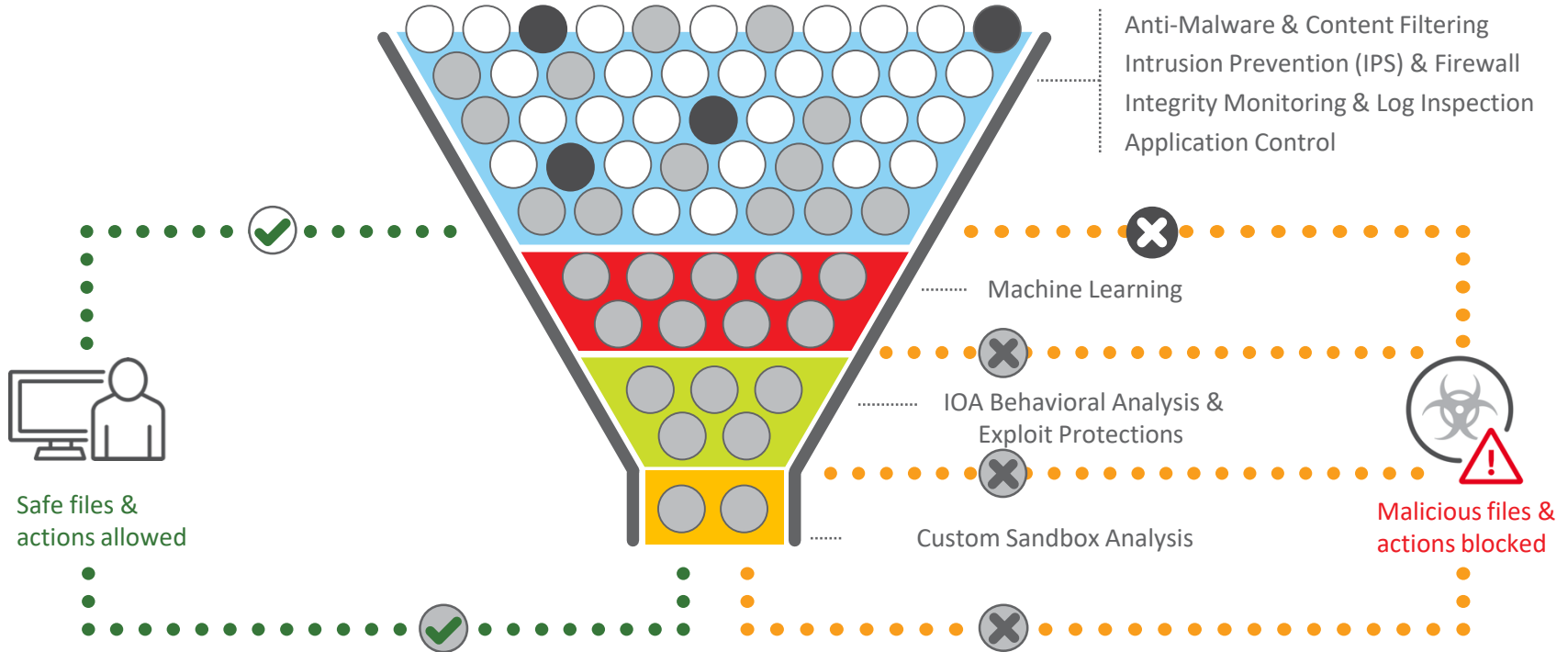
Known Good



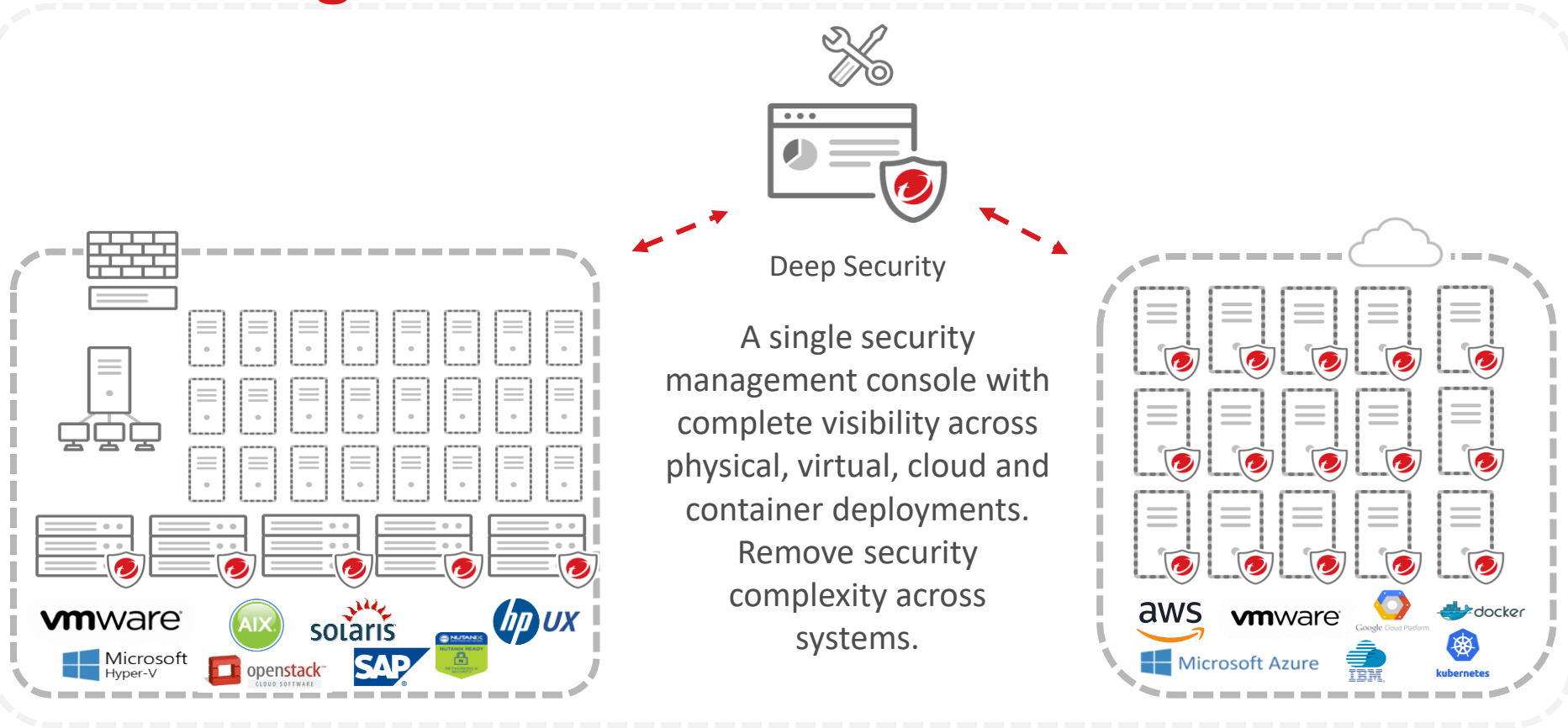
Known Bad



Unknown



Securing Business Transformation

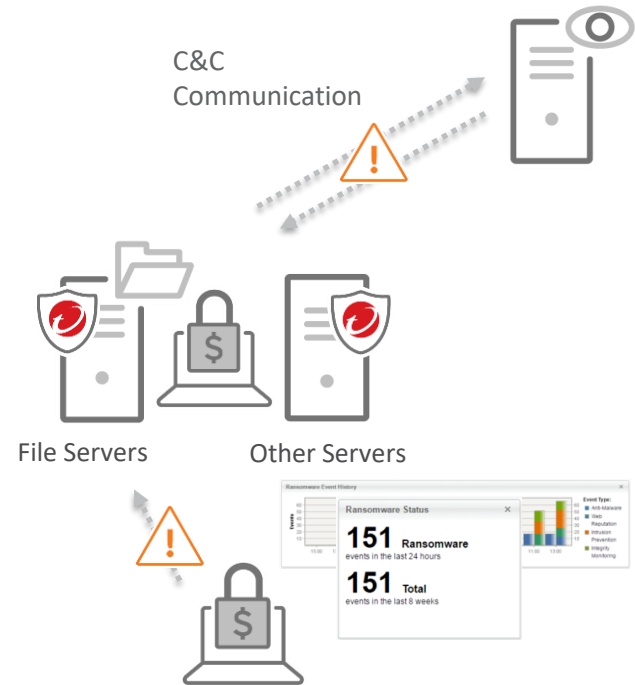


Stop Ransomware



Use layered security to:

- Stop ransomware on servers with advanced malware prevention that includes behavioral monitoring and machine learning
- Lock down Windows & Linux servers with application control
- Shield from network attacks with IPS, including the protection of network file shares (over SMB)
- Stop lateral movement and detect command & control (C&C) traffic



Uncover Suspicious System Changes

File integrity monitoring and log inspection

- Identify and report on important security events
- Monitor files, libraries and services for changes
- Creates a secure configuration baselines
- Suspicious events highlighted in dashboard without sorting through logs



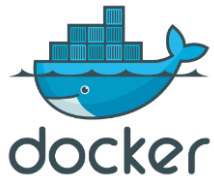
File Integrity



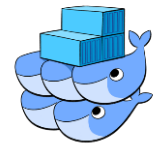
Log Inspection

Extend to Docker Containers

- Secure the host AND Docker containers running on it
- Get consistent security across all workloads

A screenshot of the Trend Micro Deep Security console. The interface is dark-themed with a navigation bar at the top containing "Dashboard", "Actions", "Alerts", "Events & Reports", "Computers", "Policies", and "Administration". The "Computers" section is active, showing a "Smart Folders" sidebar on the left with a red box around "Docker Hosts". The main content area displays "Docker Hosts" with a table of hosts. A tooltip is visible over the table, showing a green checkmark, a Docker icon, and the IP address "10.203.183.41".

NAME	POLICY	STATUS
10.203.183.41		Managed



Accelerate Compliance & Enhance Security



SANS/CIS TOP 20 CRITICAL SECURITY CONTROLS	
1. Inventory of Authorized & Unauthorized Devices	11. Secure Configurations for Network Devices
2. Inventory of Authorized & Unauthorized Software	12. Boundary Defense
3. Secure Configurations for Hardware & Software on Mobile Devices, Laptops, Workstations, & Servers	13. Data Protection
4. Continuous Vulnerability Assessment & Remediation	14. Controlled Access Based on the Need to Know
5. Controlled Use of Administrative Privileges	15. Wireless Access Control
6. Maintenance, Monitoring, & Analysis of Audit Logs	16. Account Monitoring & Control
7. Email and Web Browser Protections	17. Security Skills Assessment & Appropriate Training to Fill Gaps
8. Malware Defenses	18. Application Software Security
9. Limitation and Control of Network Ports, Protocols, and Services	19. Incident Response Management
10. Data Recovery Capability	20. Penetration Tests & Red Team Exercises

10 of 20 requirements



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
Regularly update anti-virus software	User
Maintain secure systems and applications	Shared
Limit 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

8 of 12 requirements



OWASP

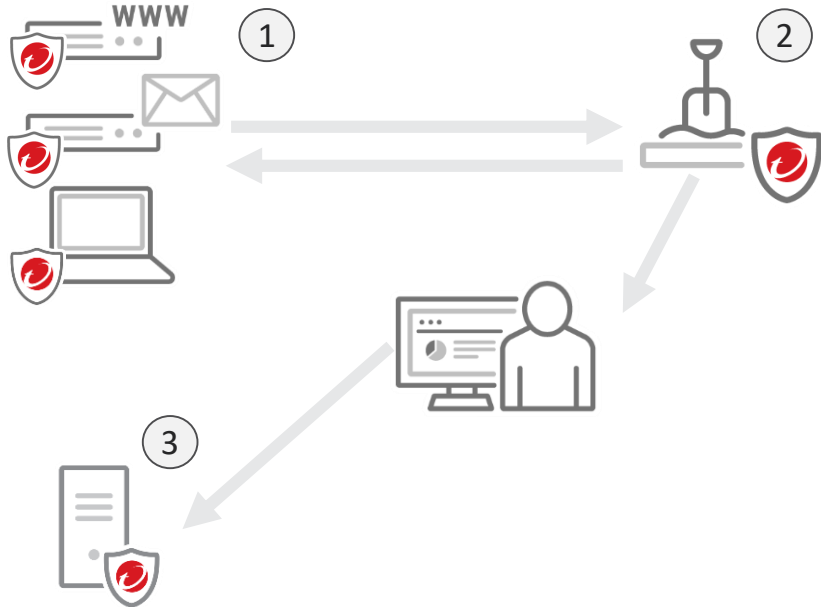
OWASP	OWASP TOP 10	DEEP SECURITY COVERAGE
A1	Injection	IPS; generic protection
A2	Broken Authentication and Session Management	Not covered
A3	Cross-Site Scripting (XSS)	IPS; generic protection
A4	Security Misconfiguration	Not covered; attack can't be distinguished from normal traffic
A5	Sensitive Data Exposure	IPS; coverage for specific vulnerabilities
A6	Broken Access Control	IPS; ensure crypto weaknesses are not exploited
A7	Security Logging and Monitoring	Not covered; attack can't be distinguished from normal traffic
A8	Denial of Service (DoS)	Not covered; attack can't be distinguished from normal traffic
A9	Using Known Vulnerable Components	Not covered; attack can't be distinguished from normal traffic
A10	Unvalidated Redirects and Forwards	Not covered; attack can't be distinguished from normal traffic

6 of 10 requirements



Automated Discovery and Rapid Response to Threats

Connected Threat Defense

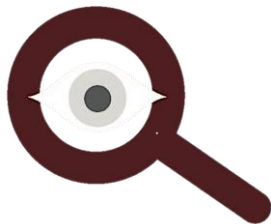


1. Endpoint and gateway agents send suspicious files to network sandbox
2. Sandbox detects malicious nature of file
3. Real-time signatures (SO) pushed to all workloads, endpoints and gateways via Control Manager

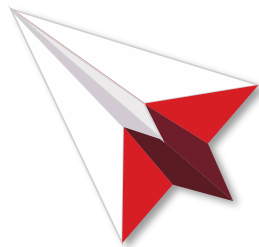


Security Challenges In The Cloud

Visibility



Agility



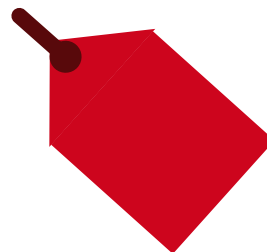
Tools



Compliance

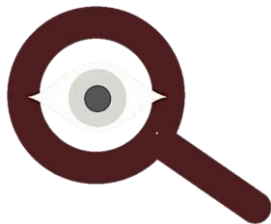


Purchasing

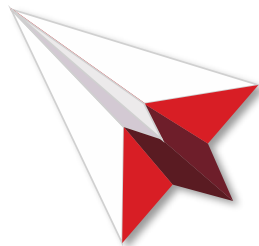


Security Challenges In The Cloud

Visibility



Agility



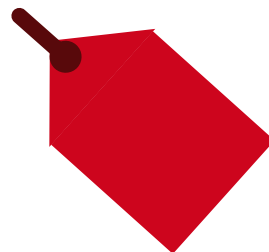
Sec
Dev Ops



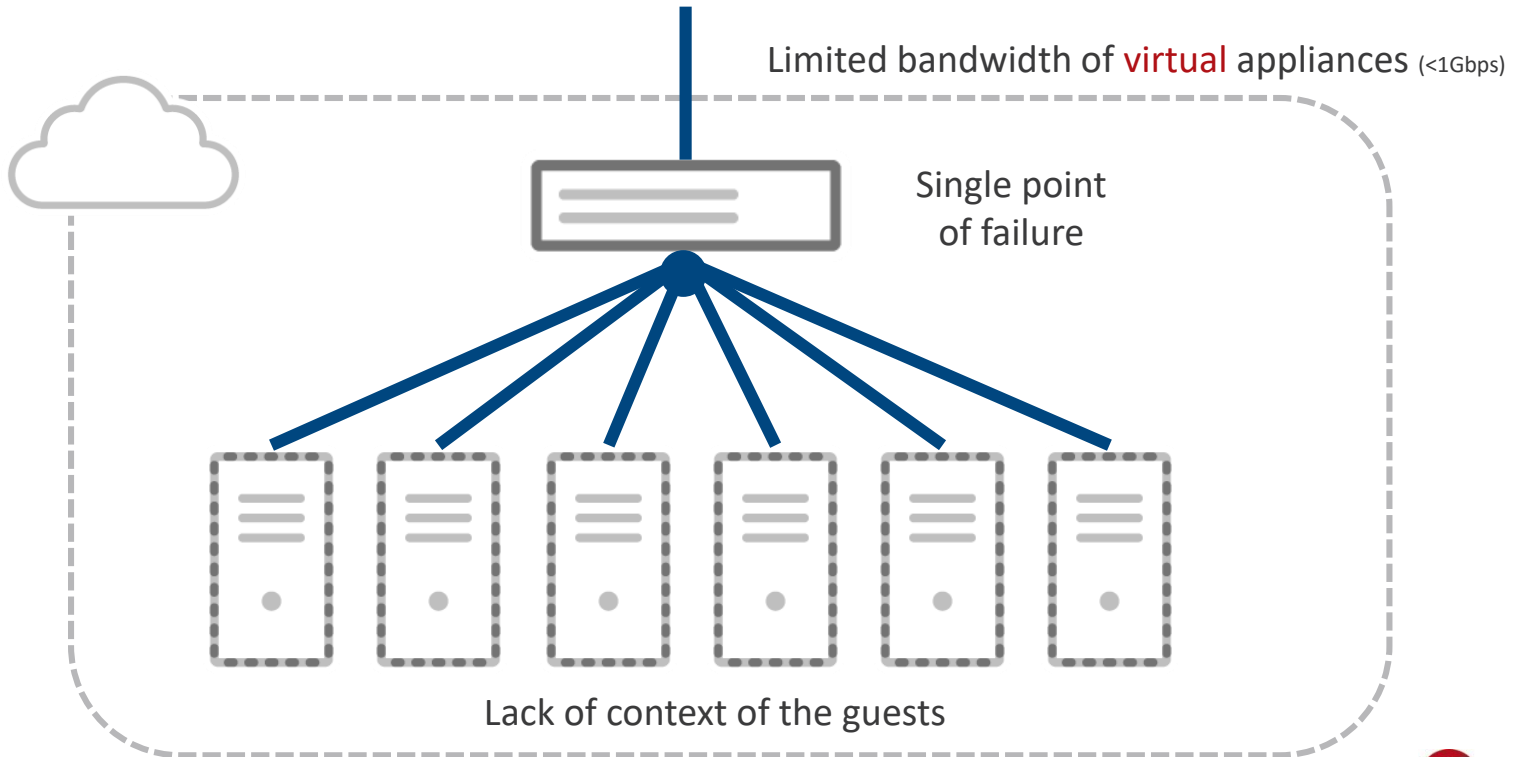
Compliance



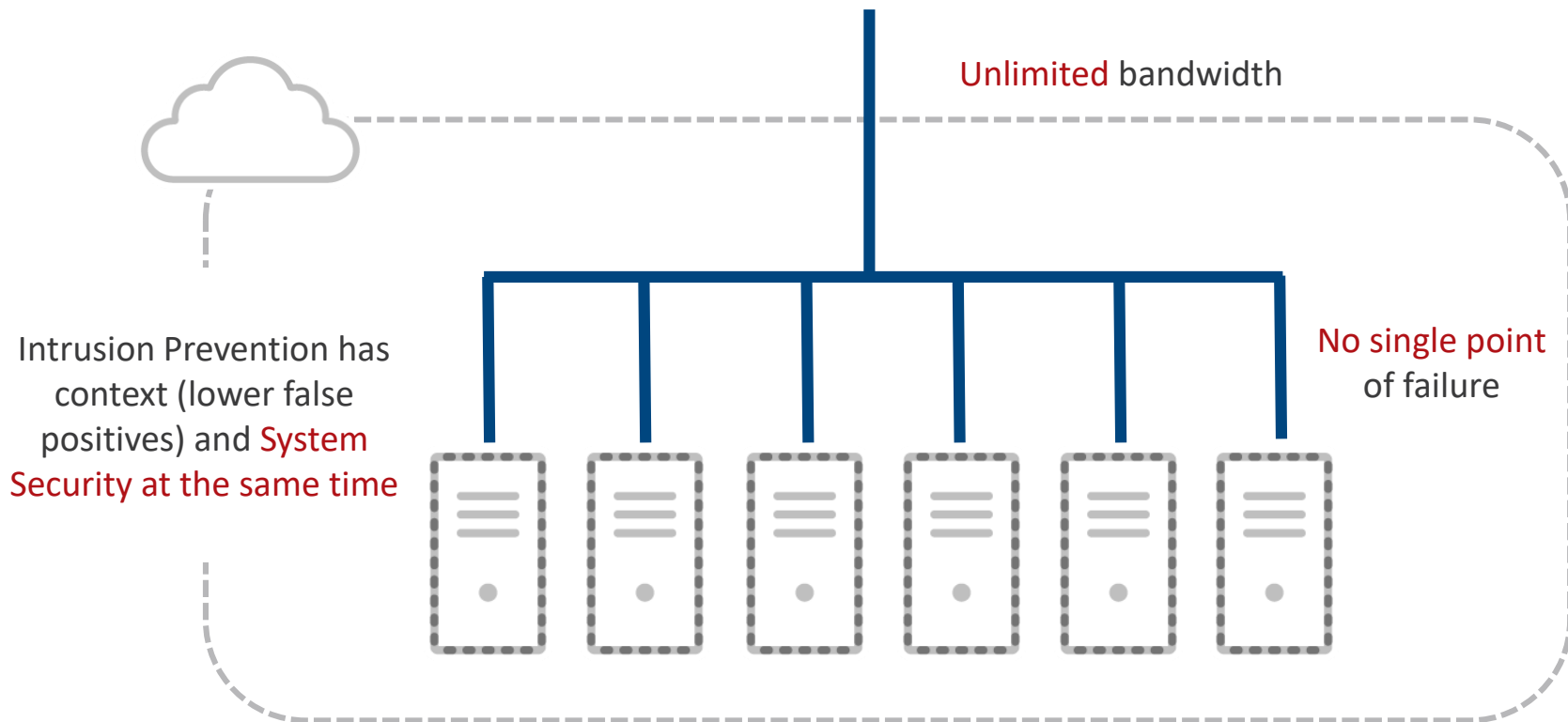
Purchasing



Perimeter Approaches Don't Translate To The Cloud



Host-based IPS Best For The Cloud



Market-leading Vision & Partnerships




TREND MICRO
SMART
Protection
Network™

Threat
Intelligence



First with
vShield
support





First with
Hypervisor-
based
protection




Deep
Security
in the private
& public cloud



Support for
next
generation
networking
with file &
network
security





Visibility across
data center ops
& security



Security
available in
major cloud
marketplaces



Security built
into cloud
managed
service offerings



Securing
microservices,
Docker
Containers,
applications &
serverless
functions



Deep Security is Optimized for AWS



- AWS marketplace - simply billing, consumption contracts
- Auto-detect instances and rapidly protect them
- Broadest platform and kernel support
- Quick Start Reference Deployment Guide, including CloudFormation templates
- Member of SaaS partner program
- Container Competency Center



Integrated with AWS Services

- AWS Security Hub
- Amazon SNS
- AWS WAF rules
- Amazon Macie
- Amazon GuardDuty
- AWS Config Rules
- CloudTrail



Deep Security is Optimized for Azure

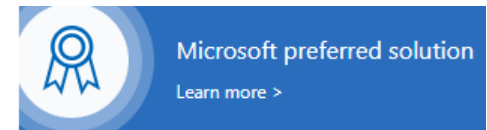


Trend Micro is Microsoft's leading Global security ISV driving Azure consumption

- Deep Security as a Service BYOL or pay-as-you-go available on the Azure Marketplace
- Auto-detect instances and rapidly protect them
- Fully scriptable, including PowerShell scripts to automate provisioning and set up
- Broadest platform and kernel support, IPS for Win 2008 EOS
- Optimized for container protection



Microsoft Partner
Gold Application Development



Deep Security is Optimized for VMware



- Partner of the Year (Global + Regional)
- Deep integration with VMware solutions (vSphere, vCloud, VDI, NSX, etc.)
- Broadest platform and kernel support
- #1 Security Partner for datacenter and cloud
- Launch Partner for VMware Cloud Marketplace

vmware®

Partner Innovation Award
2017 Global Winner

**PARTNER
READY**

VMWARE CLOUD
ON AWS



VMware Cloud Marketplace

BETA

How Does VMware Cloud on AWS Help Your Business?

VMware vSphere-based service running on the AWS cloud



Components of VMware Cloud on AWS

- Maintain existing investments
- Serviced and supported by VMware
- Retain existing architecture and tools
- Scale workloads instantly
- Utilize consistent deployment models

Introducing VMware Cloud on Amazon Web Services

with Trend Micro protection for workloads across the data center AND the cloud

Service and support by VMware

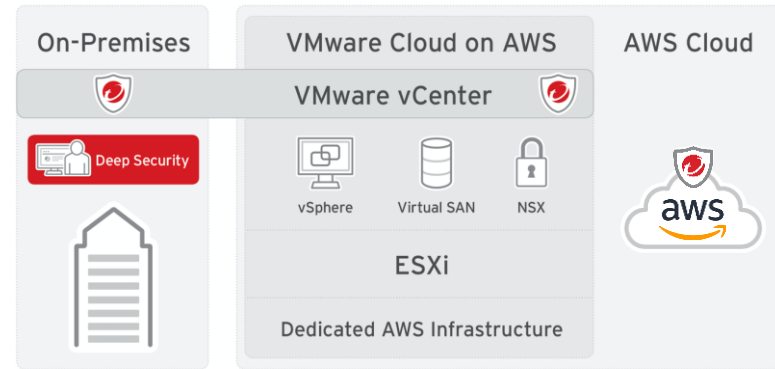
- Retain existing architecture and investments
- Scale workloads instantly
- Utilize consistent deployment models

Security and protection by Trend Micro

- Visibility of all workloads from one console
- Prevent known and unknown threats
- Automate deployments, policies, and controls
- Minimize point solution security tools
- Lower operational costs and maintenance



VMware vSphere-based service running on the AWS cloud

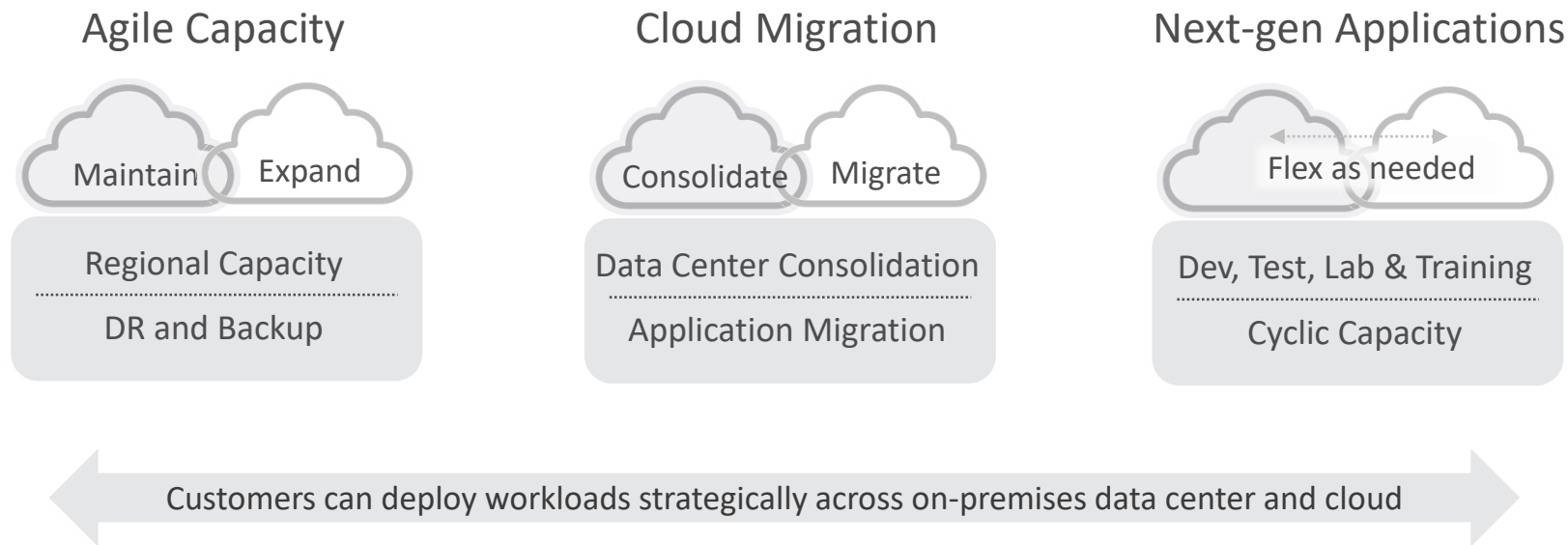


Components of VMware Cloud on AWS

Visit trendmicro.com/vmware/cloud

VMware Cloud on AWS

Use cases – easy glide path to the cloud



Certified For Key Environments AND For Security



aws partner network

Advanced
Technology
Partner

Security Competency

Government Competency

Public Sector Partner

Marketplace Seller

SaaS Partner



Level 1 Service Provider



Built On Proven Technology

Deep Security



Deep Security as a Service



Level 1 Service Provider

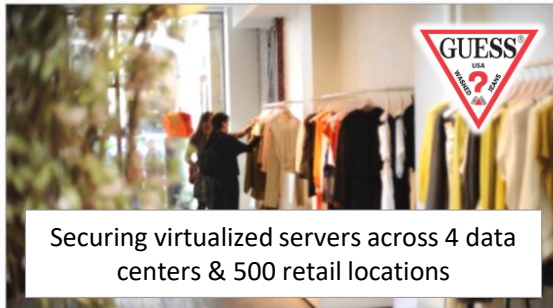


ISO 27001 Certified



ORION
HEALTH

Automates security on AWS while meeting HIPAA, HITRUST, & GDPR regulations



GUESS
USA
EST. 1981

Securing virtualized servers across 4 data centers & 500 retail locations



SQUARE ENIX

Automatically protecting workloads supporting millions of global customers



NASA

Securely migrates and scales in the cloud while reducing security operations costs



ESSILOR
SEEING THE WORLD BETTER

High performance security across virtualized and private cloud workloads



UNIVERSITY OF PITTSBURGH

Increasing operational efficiency & security for critical applications



WASHINGTON DEPARTMENT OF FISH AND WILDLIFE

Ensuring availability of important public data and protecting applications from attack



book my show

Securing the sale of millions of event tickets without impacting performance



matchmove

Complying with PCI with proven security that fits with cloud operations



infor

Automates security deployment and compliance using DevSecOps



TRC
Results you can rely on

Securely migrates applications to Docker containers on AWS



MEDHOST

Ensures protection across the hybrid cloud and containers



cloudticity
MEDICAL

Builds security into the CI/CD pipeline with automated protection



pivvot

Integrates security at pre-deployment and runtime for full lifecycle container protection



WORKS APPLICATIONS

Consolidates security across 6000 AWS & Docker instances from a single console



AWS Security Shared Responsibilities

			Deep Security	AWS
Cloud User Responsibility	Application Security	Access Control	??	??
		Configuration	??	??
		L4 Network Protection		some capabilities
		L7 Network Protection		??
		Application Integrity		??
		Log Security Intelligence		??
		Security Alerts		??
	Operating System Security	Access Control		??
		Configuration	??	??
		L4 Network Protection		some capabilities
		L7 Network Protection		??
		Malicious File Protection		??
		System Integrity		??
		Log Security Intelligence		??
Security Alerts		??		
Instance Configuration	Roles, Security Groups, Encrypted Volumes	AWS provides tools but is customer responsibility		
Services Controls	Authentication and User authorization	AWS provides tools but is customer responsibility		
AWS Responsibility	Hypervisor Controls	Access control, configuration	??	AWS
	Network Infrastructure Controls	Router/switch access control, configuration	??	AWS
	Physical Infrastructure Controls	Badge readers, alarm systems etc	??	AWS



Azure Security Shared Responsibilities

			Deep Security	Azure
Cloud User Responsibility	Application Security	Access Control	??	??
		Configuration	??	??
		L4 Network Protection	??	some capabilities
		L7 Network Protection	??	??
		Application Integrity	??	??
		Log Security Intelligence	??	??
		Security Alerts	??	??
	Operating System Security	Access Control	??	??
		Configuration	??	??
		L4 Network Protection	??	some capabilities
		L7 Network Protection	??	??
		Malicious File Protection	??	??
		System Integrity	??	??
		Log Security Intelligence	??	??
Security Alerts	??	??		
Instance Configuration	Roles, Security Groups, Encrypted Volumes	Azure provides tools but is customer responsibility		
Services Controls	Authentication and User Authorization	but is customer responsibility		
Azure Responsibility	Hypervisor Controls	Access Control, Configuration	??	Azure
	Network Infrastructure Controls	Router/switch Access Control, Configuration	??	Azure
	Physical Infrastructure Controls	Badge Readers, Alarm Systems etc	??	Azure

Simplify Purchasing And Deployment

Software-as-a-Service



Less work

Marketplace



Simplified Billing
Pay-as-you-go

Software



Hybrid Environment

Flexible Deployment On AWS

Software as a Service



Less work

AWS Marketplace



On the AWS bill

Software



Hybrid Environment

Flexible Deployment On Microsoft Azure

Software as a Service



Less work

Azure Marketplace



On the Azure bill

Software



Hybrid Environment

What Deployment Is Best For You?

	SaaS	Software
Available in AWS/Azure Marketplace	Azure and AWS	Yes (Pay or BYOL)
Hourly Pricing available	Yes	Yes
Helps meet compliance	Yes	Yes
Fits into DevOps	Yes – API, Scriptable	Yes – API, Scriptable
Management of Security Infrastructure	Trend Micro	Customer's responsibility
Security Data Location	Trend Micro	In Customer's Environment
Procurement Methods	Azure & AWS Marketplace Annual License	Azure & AWS Marketplace Traditional license
Best for:	Pure Cloud Large or Small Teams Easy Procurement	Hybrid IT Easy Procurement

Deep Security for AWS Deployment Overview

	SaaS	Software
Available in AWS Marketplace	Yes	Yes
Hourly Pricing available	Yes	Yes
Helps meet compliance	Yes	Yes
Fits into DevOps	Yes – API, Scriptable	Yes – API, Scriptable
Management of Security Infrastructure	Trend Micro responsibility	Customer's responsibility
Security Data Location	Trend Micro	In Customer's Data Center
Ways to procure	AWS Marketplace Credit Card Annual License	AWS Marketplace Traditional license
Best for:	Pure Cloud Large or Small Teams Easy Procurement	Hybrid IT Easy Procurement

Deep Security for Azure Deployment Overview

	SaaS	Software
Available in Azure Marketplace	Yes	Yes (BYOL)
Hourly Pricing available	Yes	No
Helps meet compliance	Yes	Yes
Fits into DevOps	Yes – API, Scriptable	Yes – API, Scriptable
Management of Security Infrastructure	Trend Micro responsibility	Customer's responsibility
Security Data Location	Trend Micro	In Customer's Data Center
Ways to procure	Azure Marketplace Annual License	Azure Marketplace Traditional license
Best for	Pure Cloud Large or Small Teams Easy Procurement	Hybrid IT Easy Procurement

Procurement Flexibility – It's A Benefit!



Buy How You Want

- Consumption
- Annual Subscription
- Perpetual



Buy Where You Want

- Your favorite channel
- Azure and AWS MP
Line item on cloud bill

Choose the model that best fits your operational, procurement and accounting needs

Deep Security As A Service Hourly Pricing

Choose from:

Deep Security
as a Service

 Windows Azure
Marketplace

 aws marketplace

Smaller
workloads

\$0.01 /hour

Mid-sized
workloads

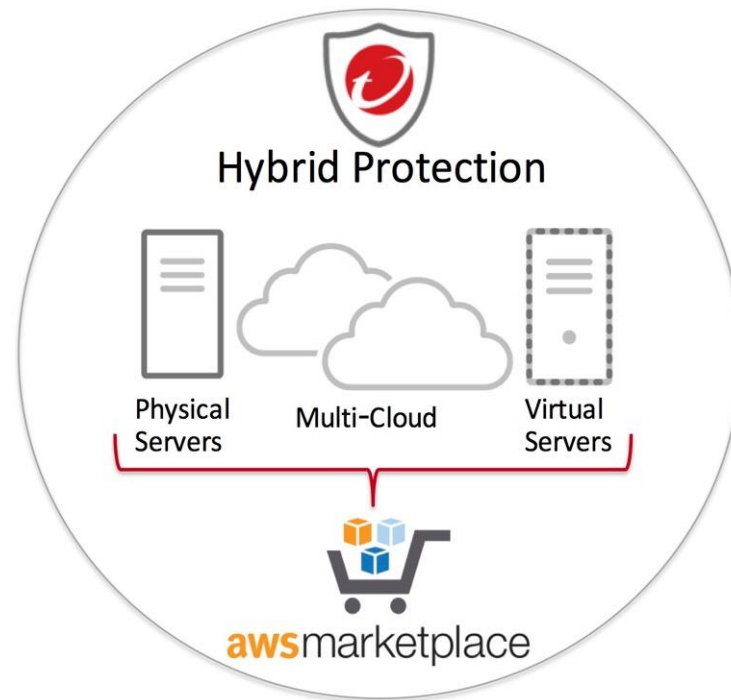
\$0.03 /hour

Very large
workloads

\$0.06 /hour

Simplifying Multi-cloud Procurement

- Protect Hybrid Cloud workloads (other cloud and on-premises) with Deep Security in the AWS Marketplace
- Simplify procurement with all security costs on your AWS bill



Usage-based Pricing on the AWS Marketplace

*Trend Micro as a Service
starting at 1¢ per hour*



Micro, Small,
Medium
(1 core)
\$0.01 /hour

Large
(2 cores)
\$0.03 /hour

Xlarge
and above
(4 cores +)
\$0.06 /hour

For data centers - all computers in Deep Security Manager that are not from a cloud connector are \$0.06/hour

Usage-based Pricing on the Azure Marketplace

*Trend Micro as a Service
starting at 1¢ per hour*



Micro, Small,
Medium
(1 core)
\$0.01 /hour

Large
(2 cores)
\$0.03 /hour

Xlarge
and above
(4 cores +)
\$0.06 /hour

For data centers - all computers in Deep Security Manager that are not from a cloud connector are \$0.06/hour