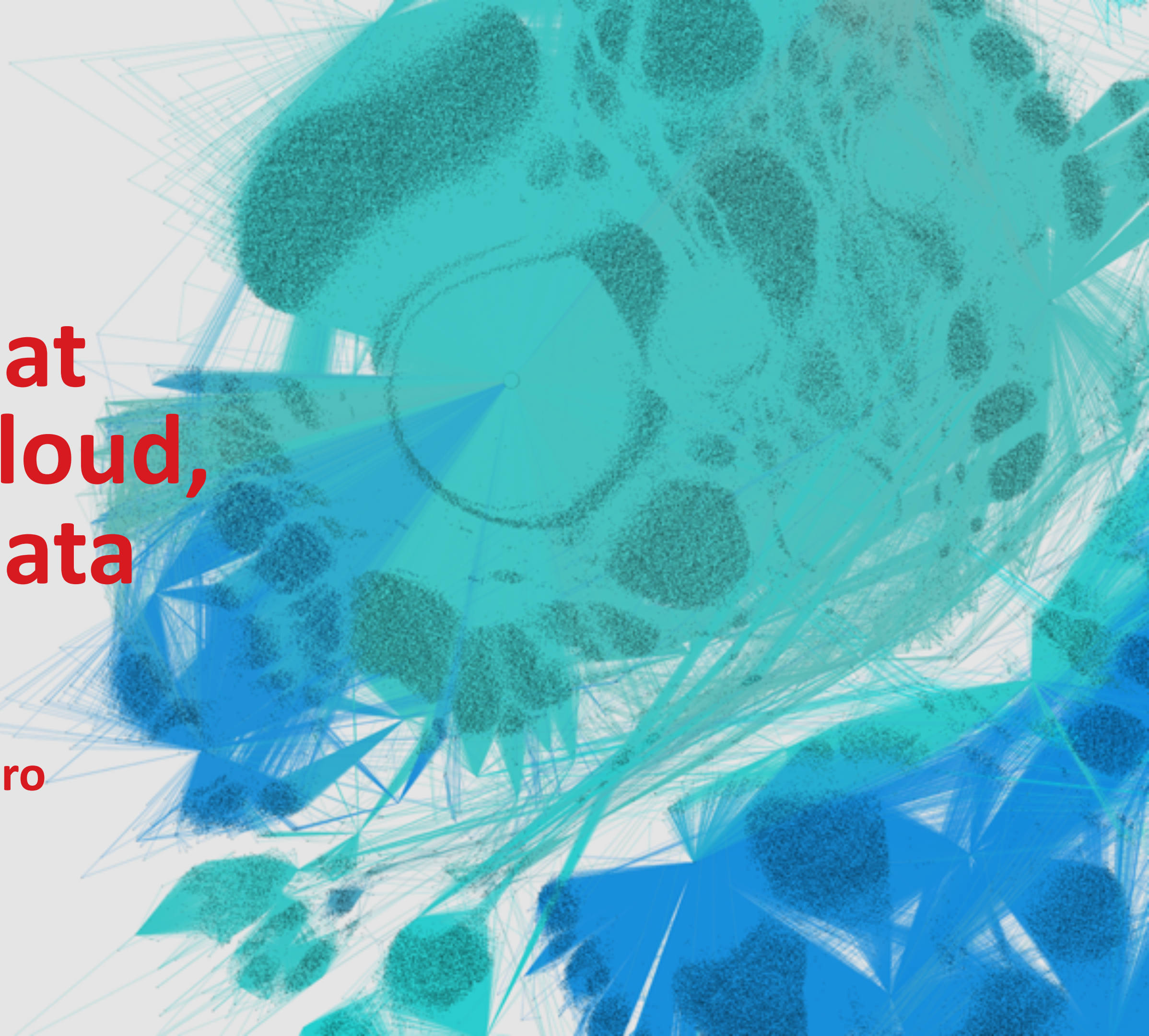
TREND MICRO

Cybersecurity at the speed of cloud, dealing with data and identity

Albert Kramer
Technical Director Trend Micro

IRMAC, Nov 20th



IT Security Facing Heightened Risk

Digital extortion will get more “creative” (GDPR $, smear campaigns)

Every unsecure **home device** is an entry point into the enterprise network

Business email compromise will go two levels down the org chart

More **cloud-related vulnerabilities** will be discovered (Kubernetes, Docker images…)

Automation will be a new wrinkle in **business process compromise**

Real-life attacks will increase on Industrial Control Systems **(ICS)**

Gaining Meaningful Visibility is Challenging

>10 thousand

Daily security alerts received by >55%
of IT Security professionals

Overwhelming number of alerts, hard to discover unknown threats

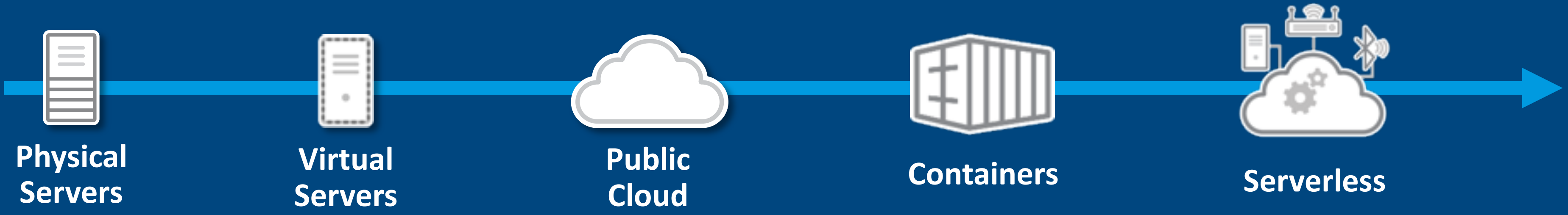
25+

# of individual security technologies
used by >50% of enterprises

Silos of visibility with limited understanding of risk posture

Source: 1. SC Media Survey, 2018, 2. ESG, OCT 2017

> “Now every company is a software company” -FORBES



Physical Servers

Virtual Servers

Public Cloud

Containers

Serverless

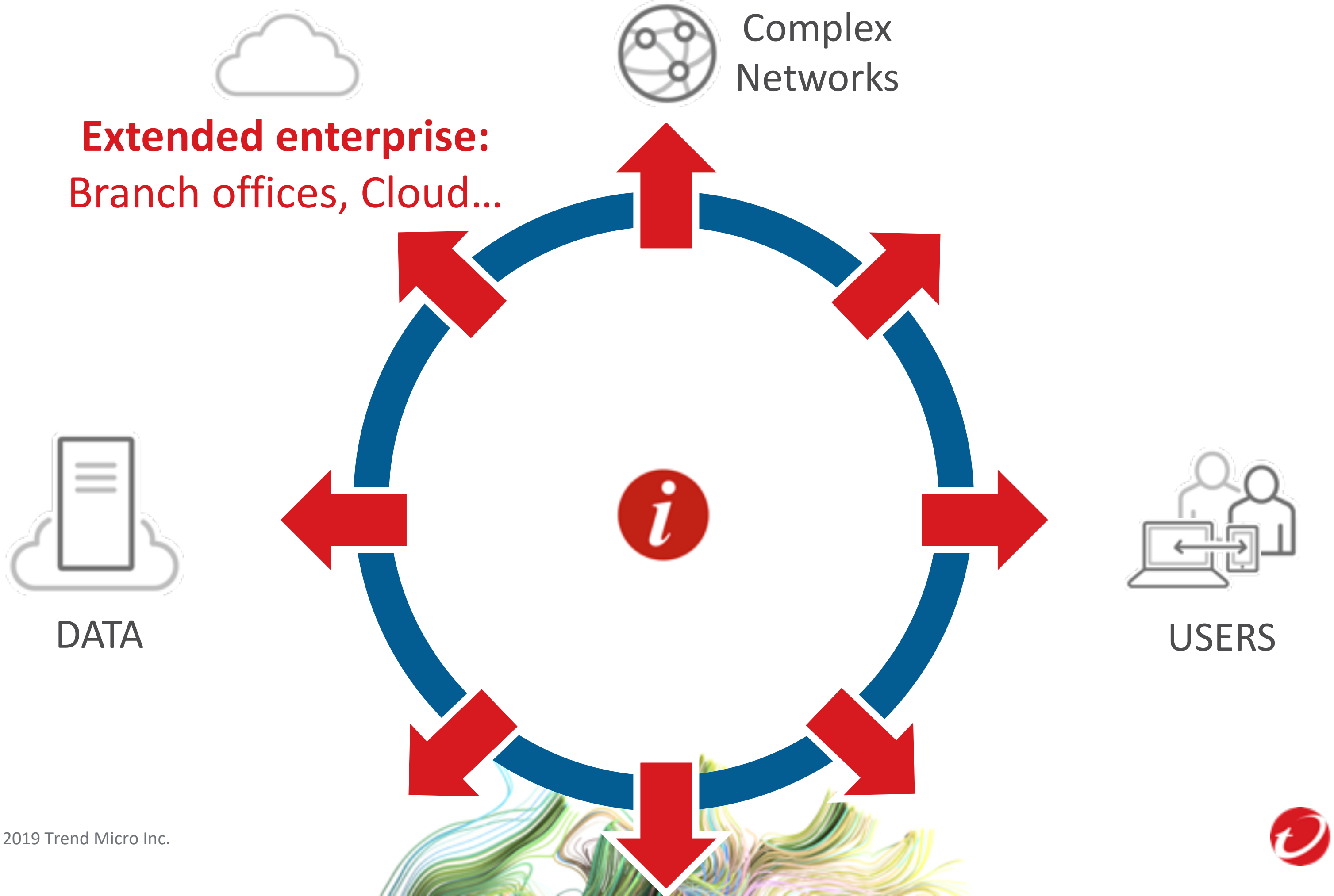
What is most important?

DATA

USERS

The right Data
The right Information

The right People



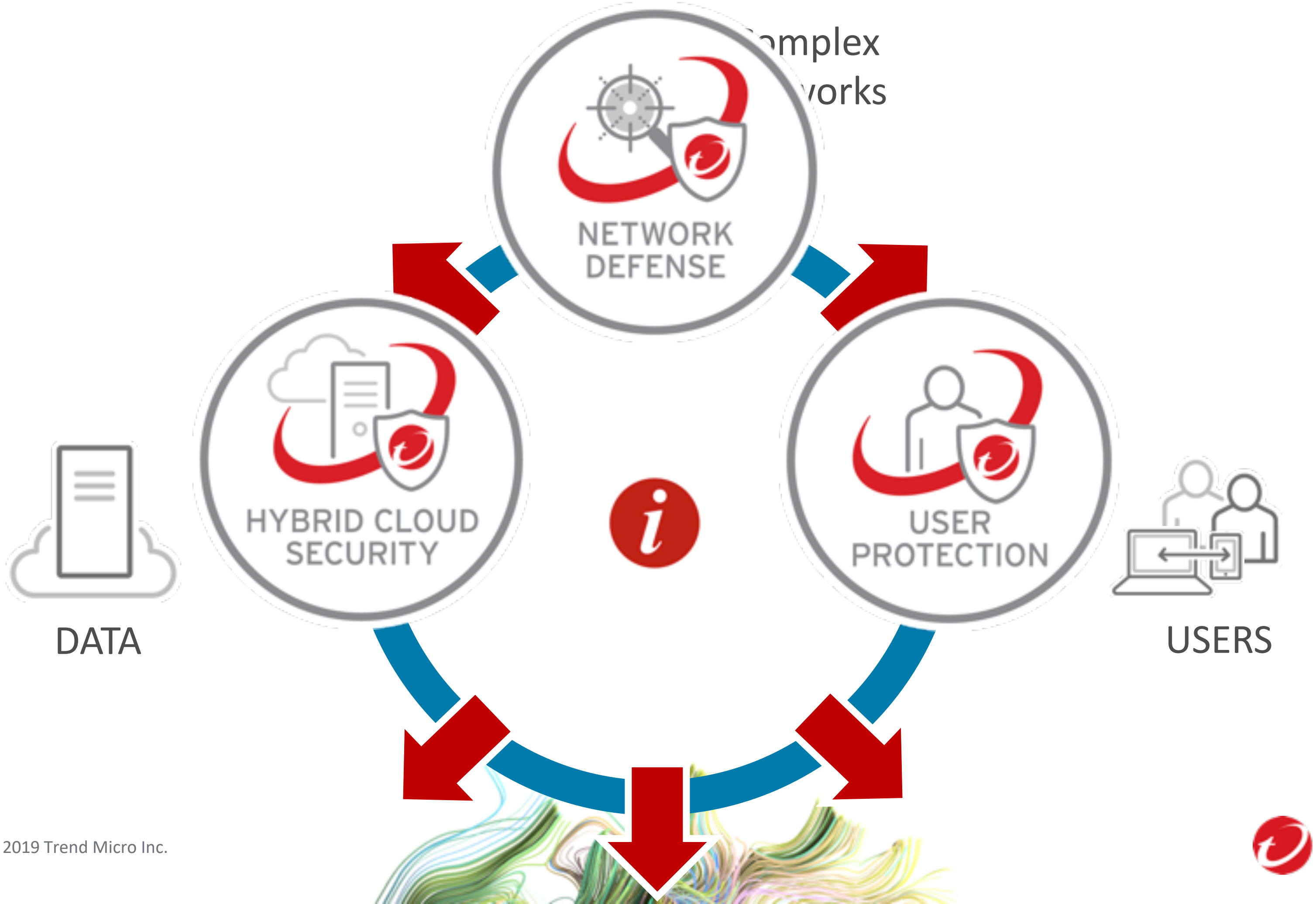
Complex Networks

Extended enterprise:

Branch offices, Cloud…

DATA

USERS


omplex
vorks
NETWORK DEFENSE
HYBRID CLOUD SECURITY
USER PROTECTION
DATA
USERS

Users are More Mobile, Productive, Liberated

70% work remotely at least one day per week[1]

“BYOC” is the new “BYOD”

In 2019, **70%** of MS Office users will be using Office 365[2]

1. IWG survey, 2018, 2. www.onmsft.com, Oct 2017

RISK: Traditional Defenses Are Now Ineffective

Email still primary attack vector:

- +269% in **phishing** (including SaaS)
- +28% in **business email compromise,** now beyond CEO

Unsecured home devices provide entry point to enterprise

By 2020, 1/3 successful attacks will be on **shadow IT** resources[2]

Digital extortion more “creative” (GDPR $, smear campaigns)

Sources: Trend Micro Research 2018 Roundup Report and 2019 Predictions Report, 2. 2016 Gartner Security Prediction

Users Need “Things”

Entitlements – The *things* tied to a user (hardware, licenses, access, etc.)

Attributes – Flags that indicate which *things* a user should have under which circumstances

Provisioning – Granting entitlements to a user account

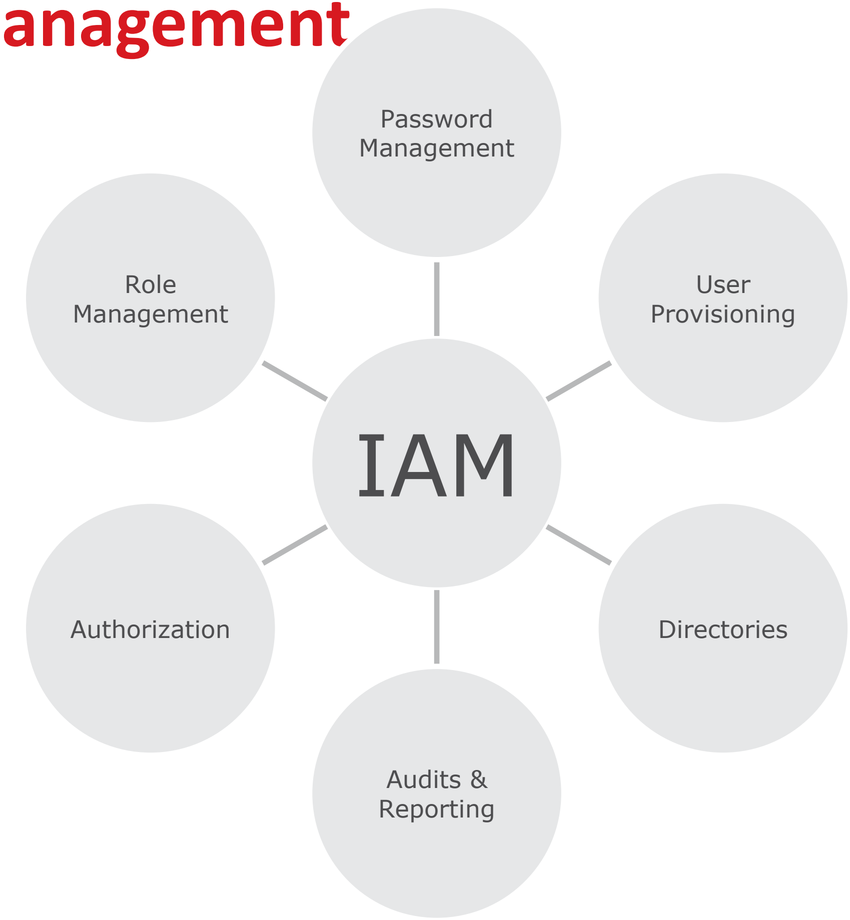
Deprovisioning – Removing entitlements from a user account

USERS: Identity and Access Management

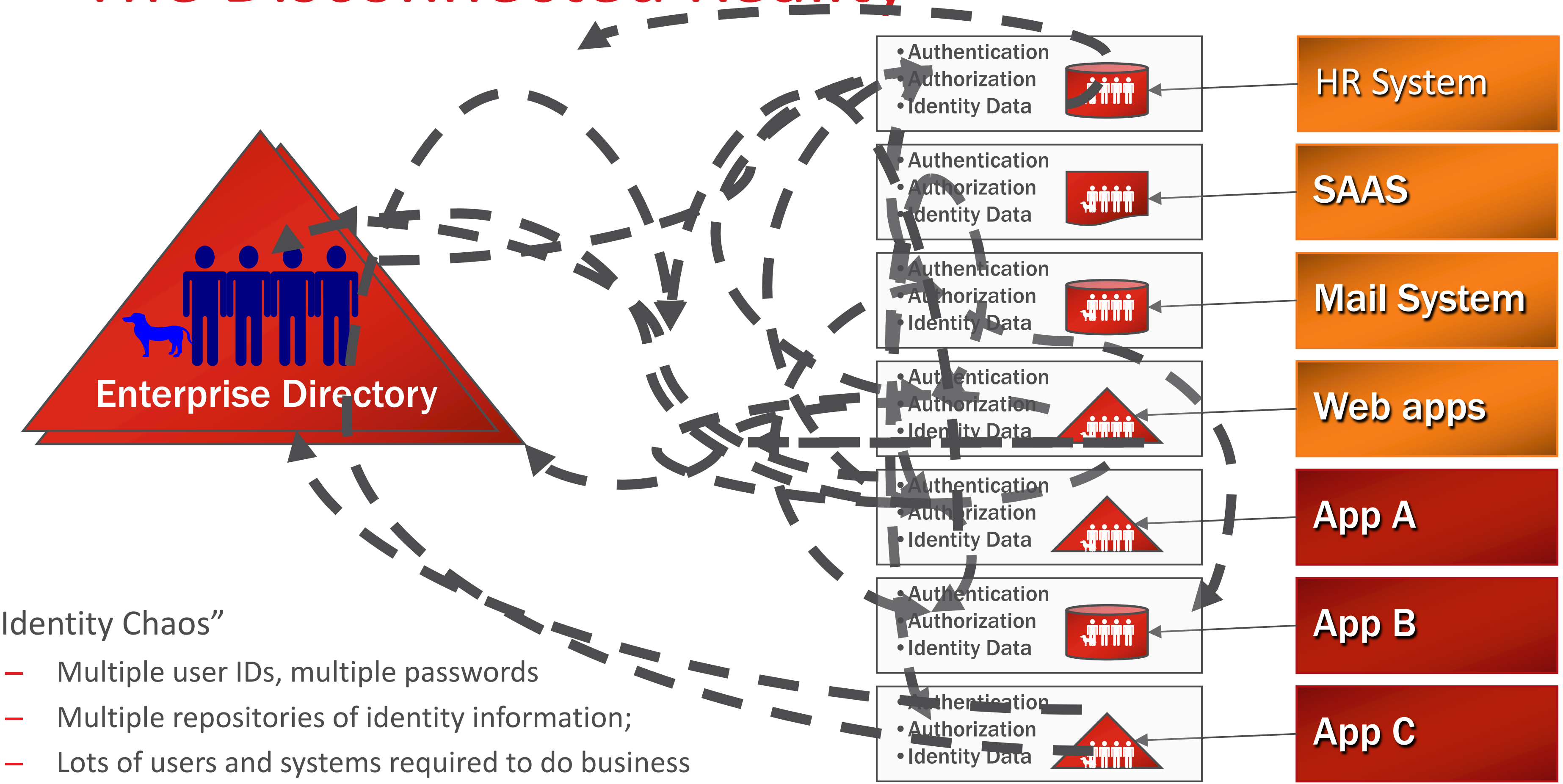
Authentication

Authorization

Accounting



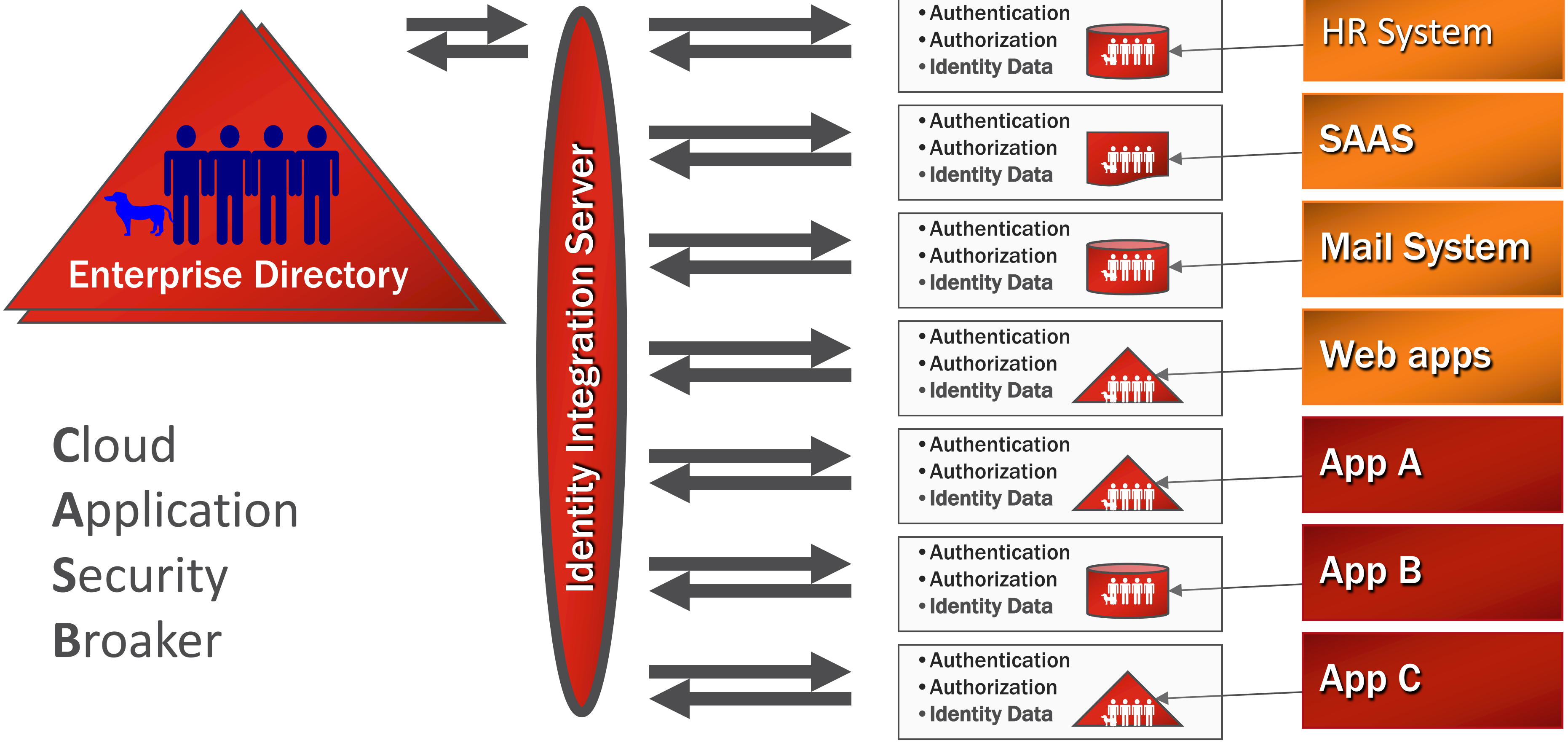
The Disconnected Reality



“Identity Chaos”

– Multiple user IDs, multiple passwords
– Multiple repositories of identity information;
– Lots of users and systems required to do business
– Decentralized management, ad hoc data sharing

Identity Integration



Enterprise Directory

Identity Integration Server

- Authentication
- Authorization
- Identity Data

- Authentication
- Authorization
- Identity Data

- Authentication
- Authorization
- Identity Data

- Authentication
- Authorization
- Identity Data

- Authentication
- Authorization
- Identity Data

- Authentication
- Authorization
- Identity Data

- Authentication
- Authorization
- Identity Data

HR System

SAAS

Mail System

Web apps

App A

App B

App C

Cloud

Application

Security

Broaker

What about Threats?

- Malware
- Vulnerabilities
- Data leakage
- Targeted attacks
- Malicious email
- Spam
- Old code
- Exposed applications

Detection & Response Beyond the Endpoint

Email

Network

Endpoints

Traditional Servers

Cloud Workloads

Containers

With more context, events that seem benign on their own suddenly become meaningful indicators of compromise, so you can detect threats earlier

PROTECTING your DATA and USERS

Email

Network

Endpoints

Traditional Servers

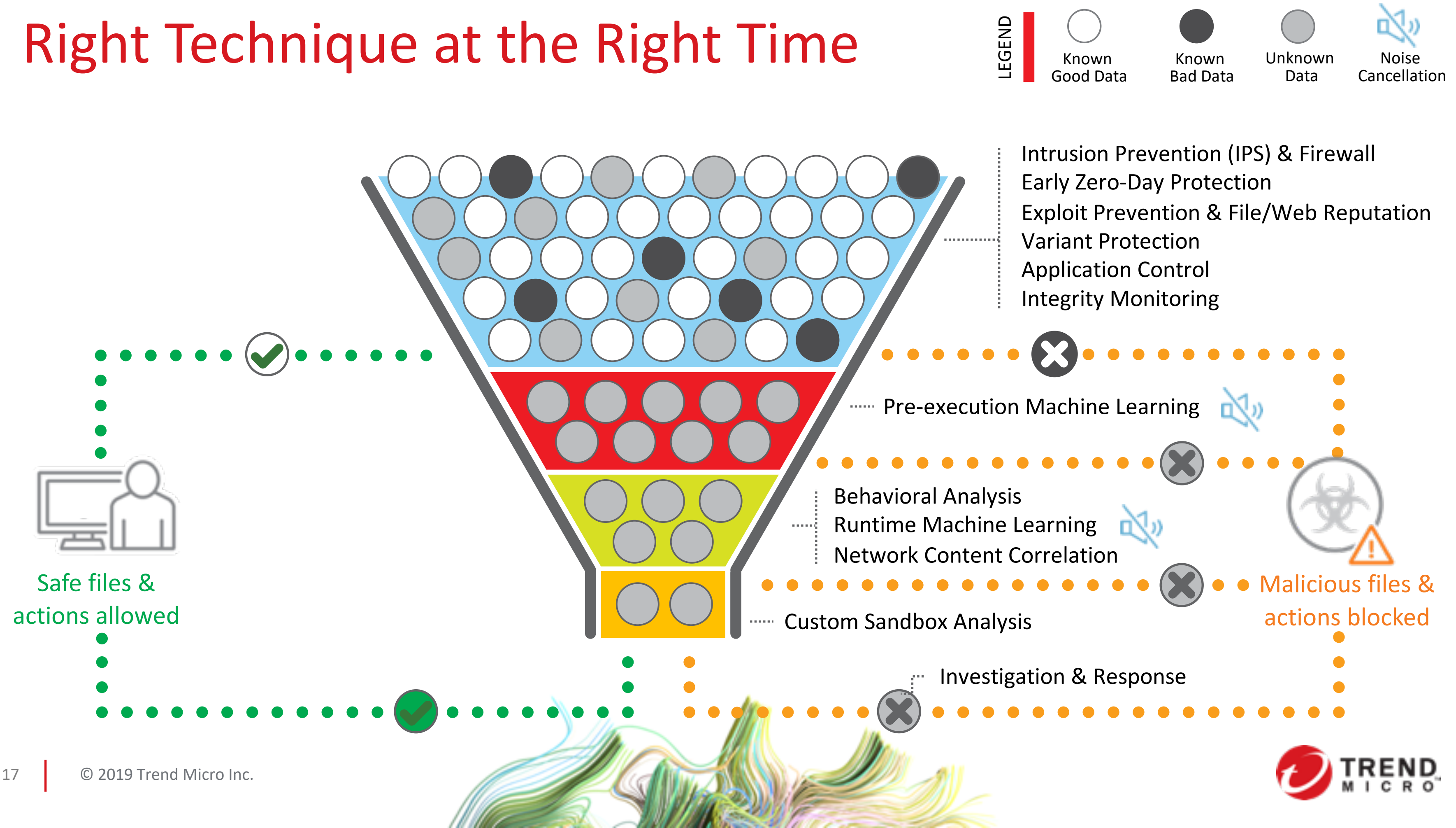
Cloud Workloads

Containers

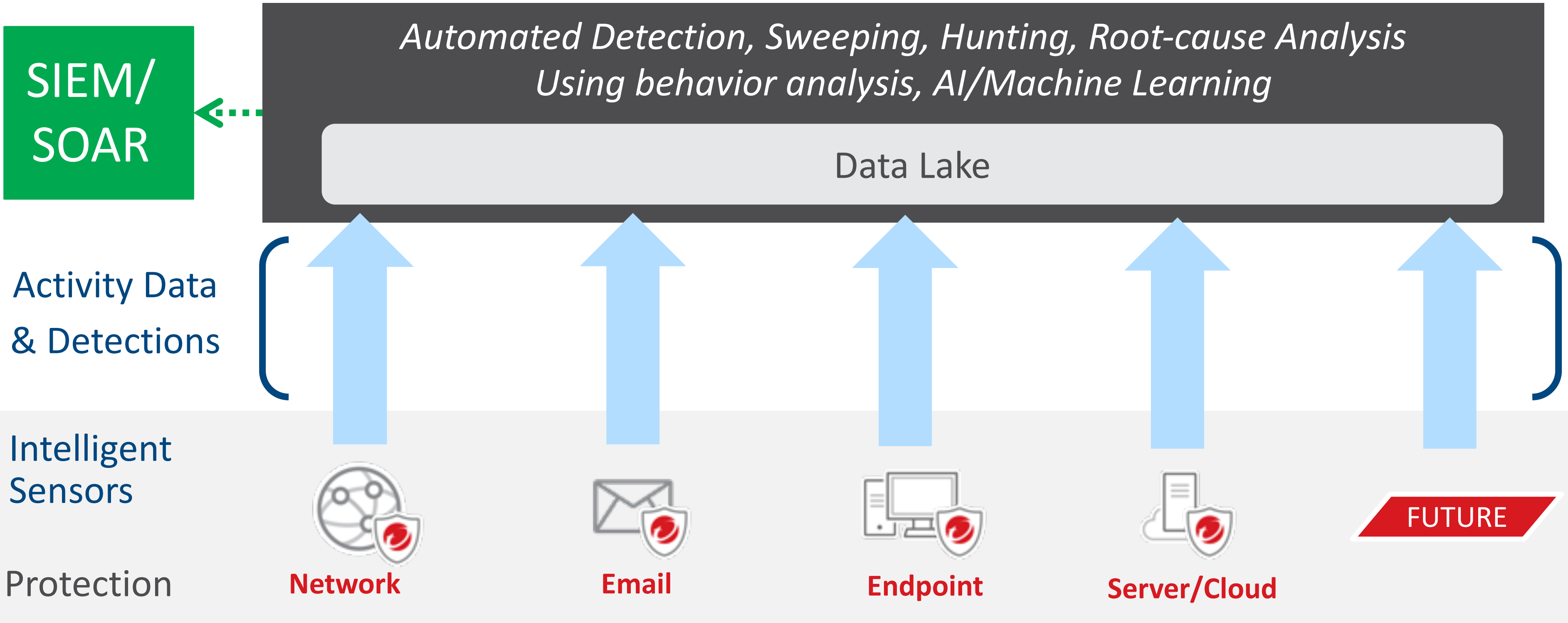
The more threats you prevent, the fewer you need to investigate and respond to

"An ounce of prevention is worth more than a pound of detection"

Right Technique at the Right Time


LEGEND
○ Known Good Data
● Known Bad Data
● Unknown Data
Noise Cancellation
Intrusion Prevention (IPS) & Firewall
Early Zero-Day Protection
Exploit Prevention & File/Web Reputation
Variant Protection
Application Control
Integrity Monitoring
Pre-execution Machine Learning
Behavioral Analysis
Runtime Machine Learning
Network Content Correlation
Custom Sandbox Analysis
Investigation & Response
Safe files & actions allowed
Malicious files & actions blocked

XDR - beyond Endpoint Detection and Response



SIEM/ SOAR

Automated Detection, Sweeping, Hunting, Root-cause Analysis
Using behavior analysis, AI/Machine Learning

Data Lake

Activity Data & Detections

Intelligent Sensors

Protection

Network

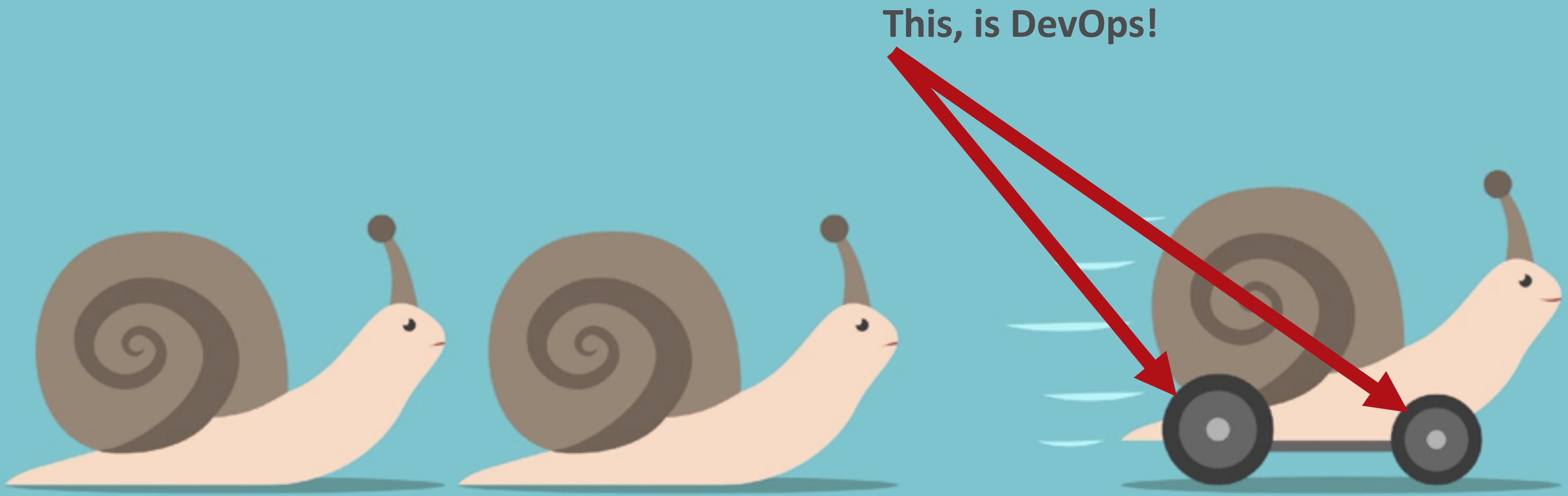
Email

Endpoint

Server/Cloud

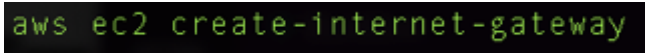
FUTURE

The only differentiator organizations have left…

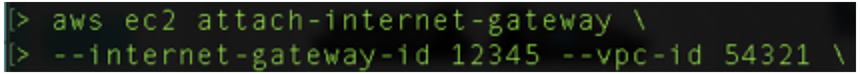


What does faster look like?

OR

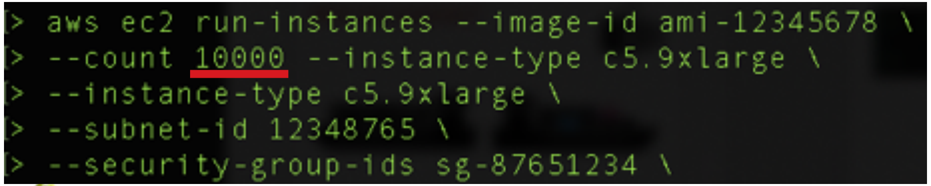


```
aws ec2 create-internet-gateway
```



```
> aws ec2 attach-internet-gateway \
> --internet-gateway-id 12345 --vpc-id 54321 \
```

OR



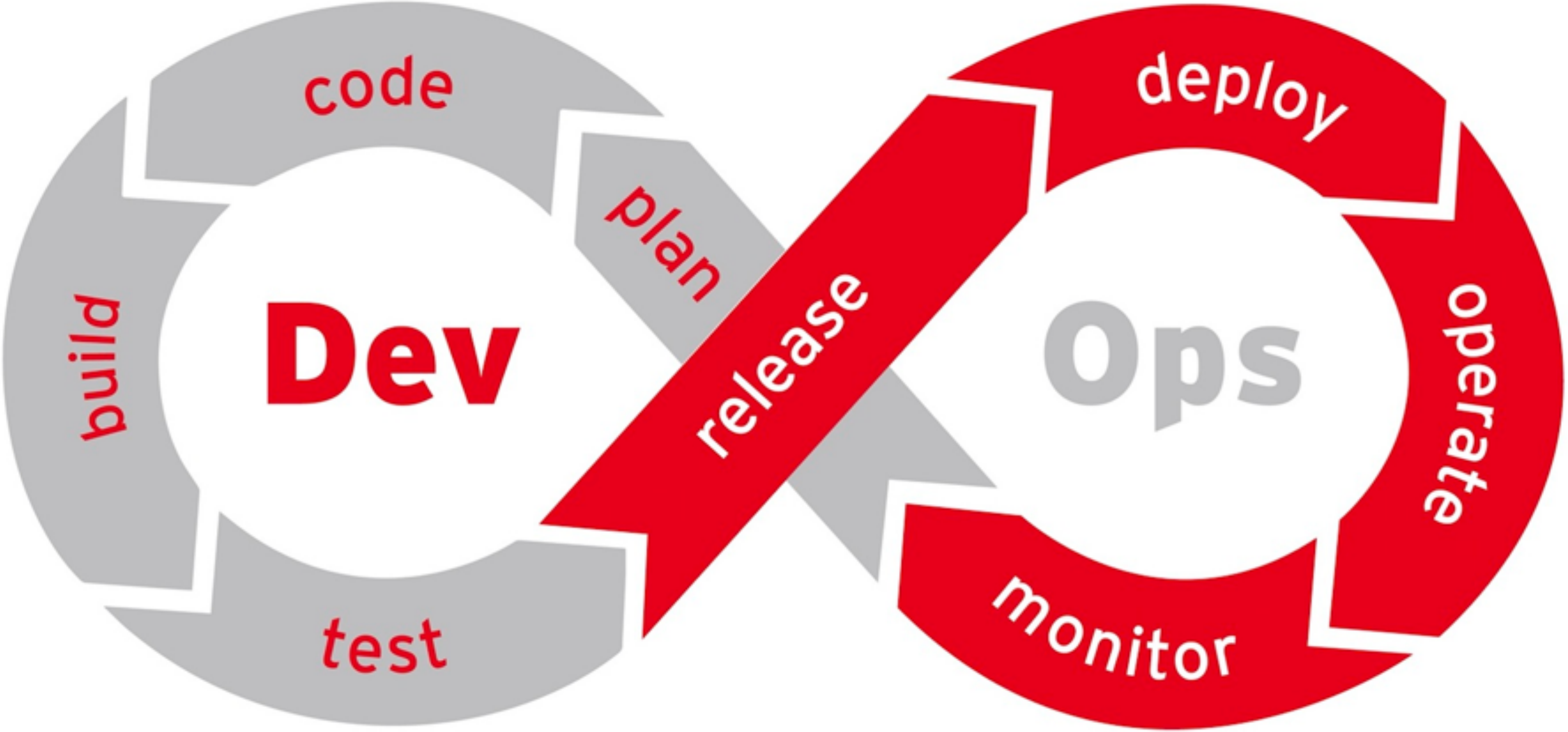
```
> aws ec2 run-instances --image-id ami-12345678 \
> --count 10000 --instance-type c5.9xlarge \
> --instance-type c5.9xlarge \
> --subnet-id 12348765 \
> --security-group-ids sg-87651234 \
```

What does faster look like?

kubernetes

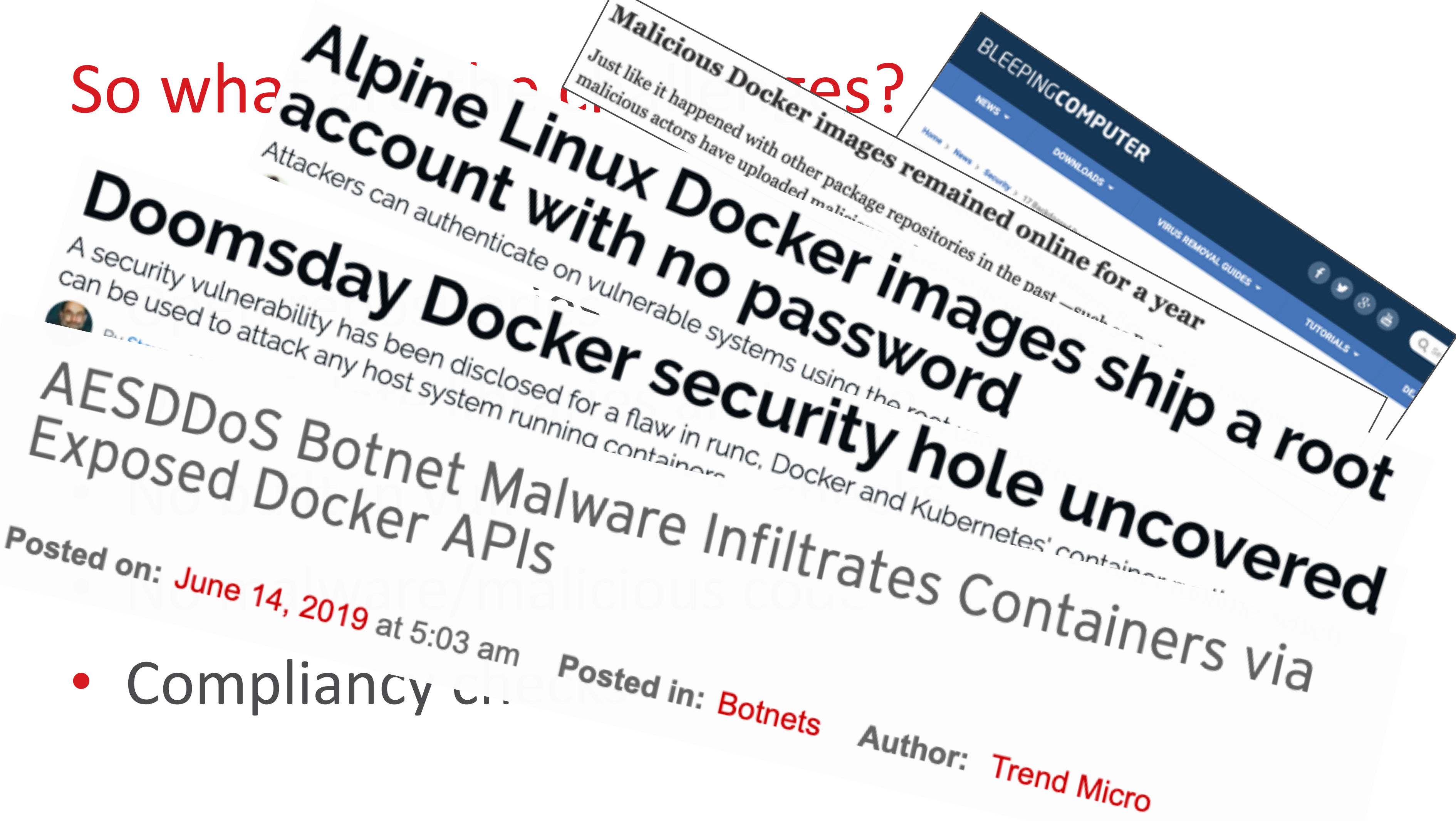
GitHub

Jenkins


code
plan
build
Dev
test
release
deploy
Ops
operate
monitor

Whoever Slows This Down is the Enemy

So wha… es?



Malicious Docker images remained online for a year

Just like it happened with other package repositories in the past —such as P
malicious actors have uploaded malicio

Alpine Linux Docker images ship a root account with no password

Attackers can authenticate on vulnerable systems using the root

Doomsday Docker security hole uncovered

A security vulnerability has been disclosed for a flaw in runc, Docker and Kubernetes' container
can be used to attack any host system running containers

By St

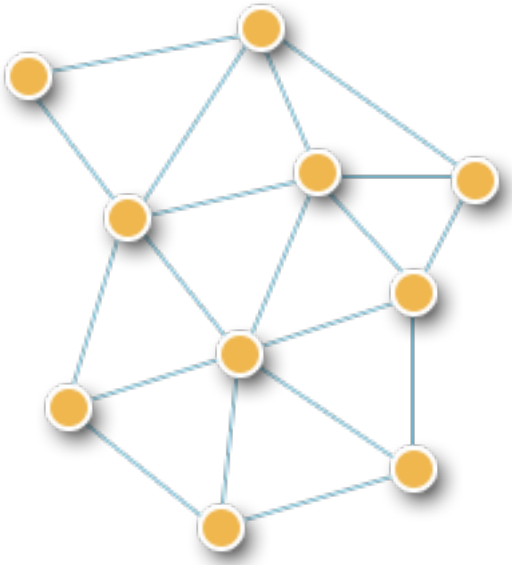
AESDDoS Botnet Malware Infiltrates Containers via Exposed Docker APIs

Posted on: June 14, 2019 at 5:03 am **Posted in:** Botnets **Author:** Trend Micro

- No … vulnerability ch…
- No malware/malicious code …
- Compliancy ch…

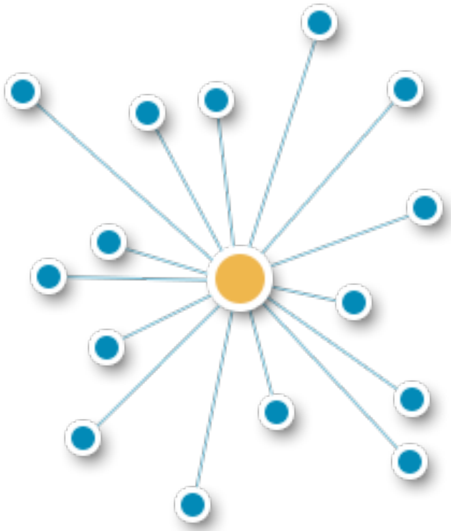
Operations: People, process & technology

Modern app teams look like this



VS

Security teams need visibility like this



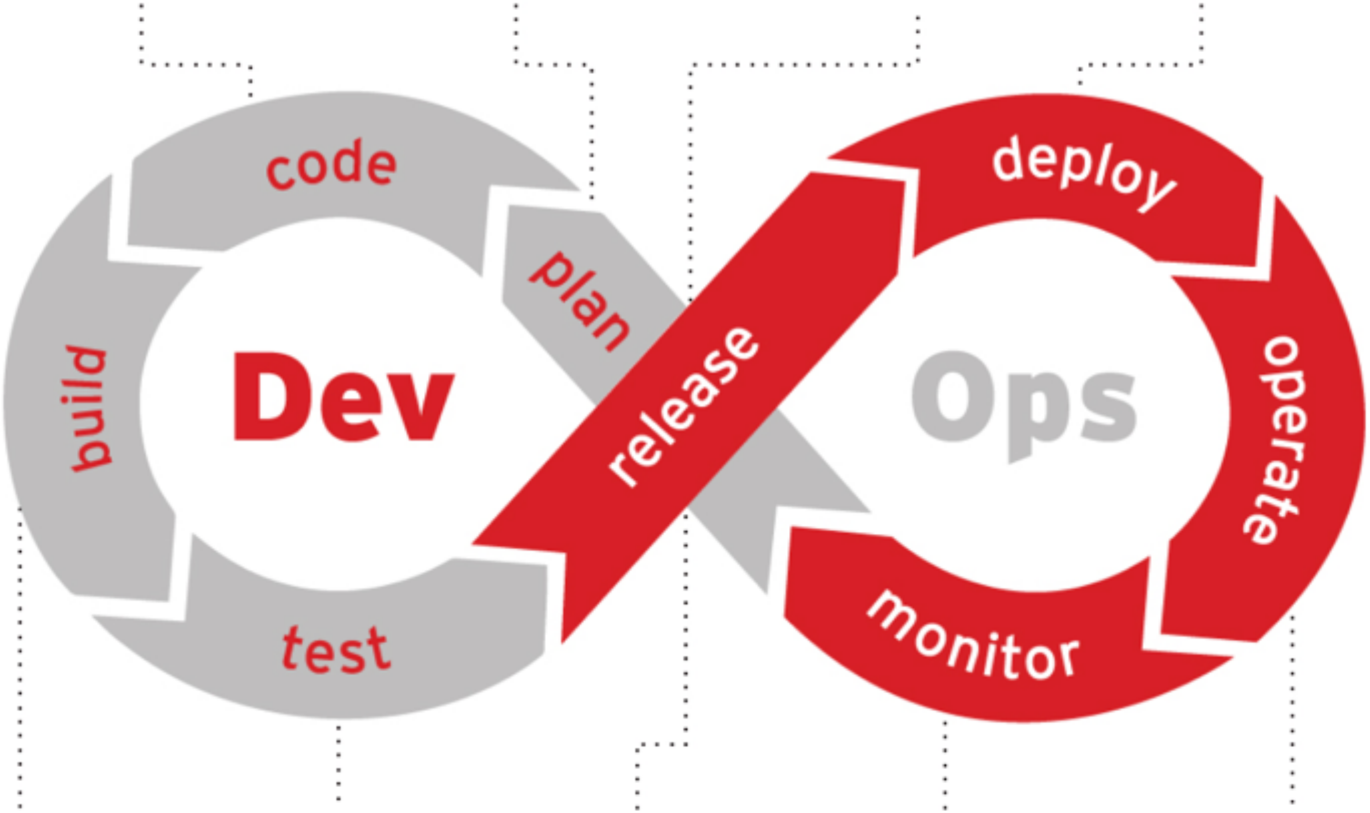
@hijinksensue

Validate patches and fixes from scan results

Details on Patches and Updates for remediation of newly discovered vulnerabilities

Kubernetes Integrations

Deep Security Protected Docker Hosts



Automated scanning of new build

Risk assessment for pipeline promotions

Image Assurance

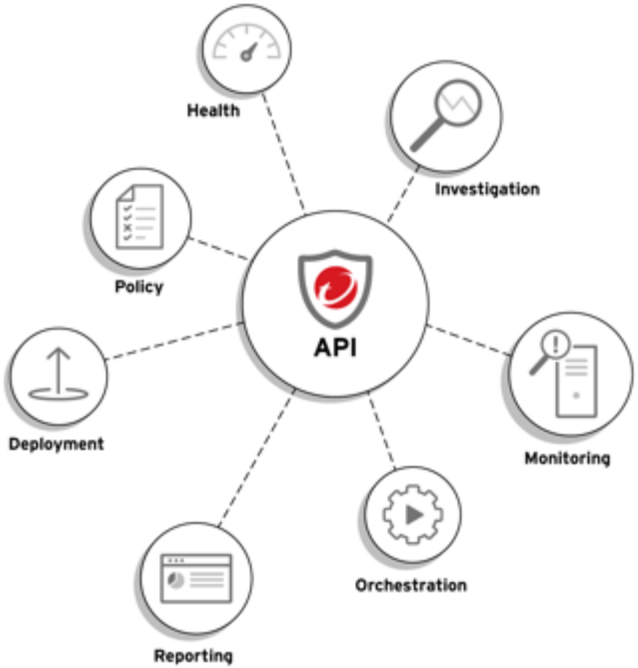
Continuous monitoring for Docker activity and new CVEs/malware

Runtime detection and prevention of exploits

TREND MICRO

Accelerate DevOps with Security Automation

"Security used to be thought of as an inhibitor to development, but not anymore. Our teams understand that security is built into the environment. The security team is helping to steer the effectiveness of cloud operations," Security Team - Infor



Security Automation - policy creation, and updates

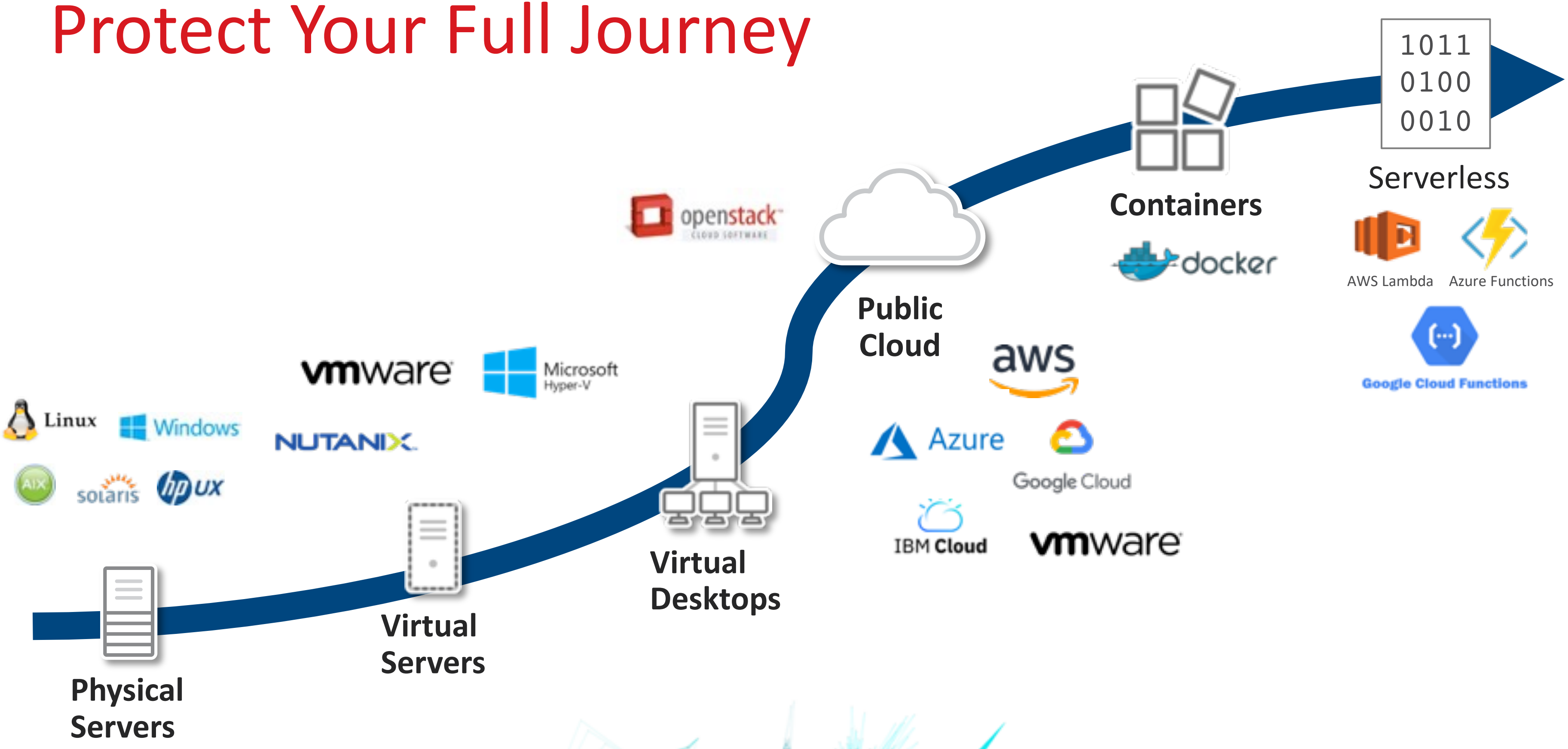
Deployment Automation - security at scale

Reporting Automation - customizable compliance reports and leading SEIMs integration

Monitoring Automation - operational and security health of your environment

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

Protect Your Full Journey



Physical Servers

Virtual Servers

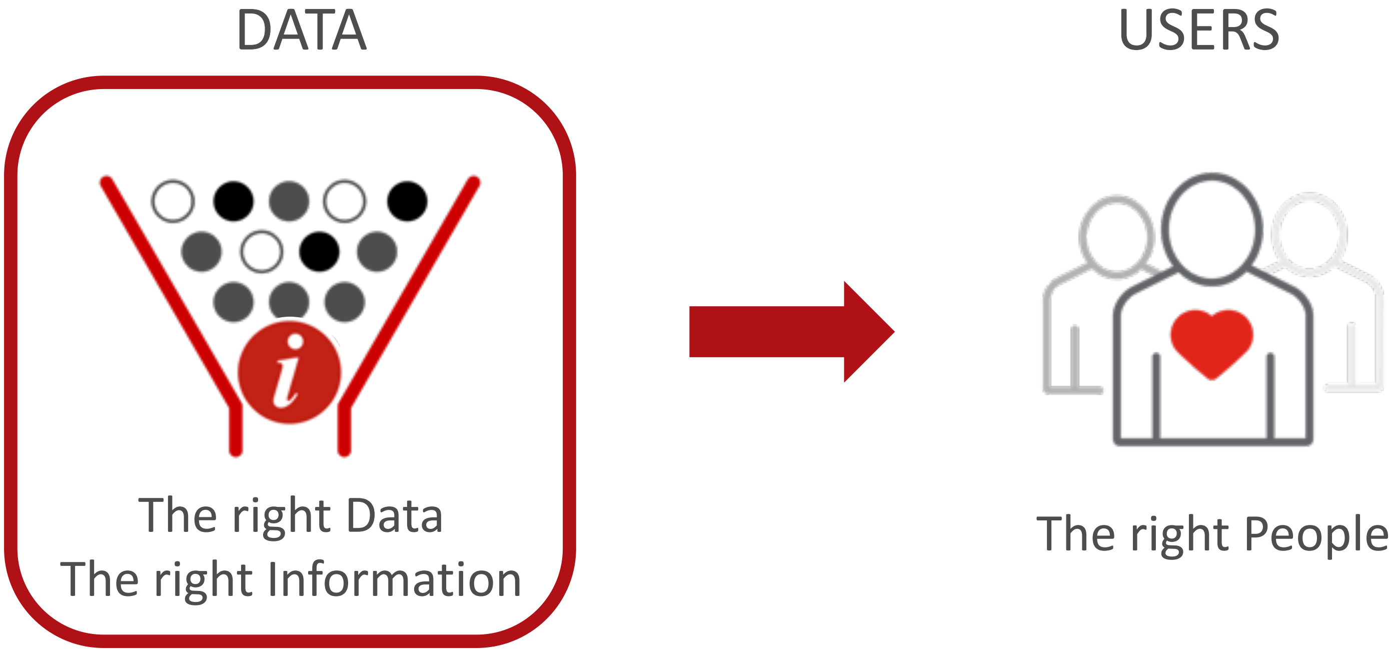
Virtual Desktops

Public Cloud

Containers

Serverless

Remember?



DATA

The right Data
The right Information

USERS

The right People

Key takeaways!

- Identify the user
- Give only access when needed
- Implement monitoring and visibility
- Protect the user > beyond endpoint
- Protect the data > beyond endpoint

- Embrace DevOps
- Use machine learning / AI
- Bring security as close as possible
- Consolidate as much as possible
- Automate everything
- Bring in expertise / services
- USER AWARENESS! (training and programs)

https://trendmicro.com/cloud

THE ART OF CYBERSECURITY

Automated hybrid cloud workload protection via calls to Trend Micro APIs. **Created with real data by Trend Micro threat researcher and artist Jindrich Karasek.**