Machine Translated by Google



Vision One - Endpoint Security

Optimize your endpoint, server, and cloud workload security outcome

INSTRUCTOR

Market and Challenges

Machine Translated by Google

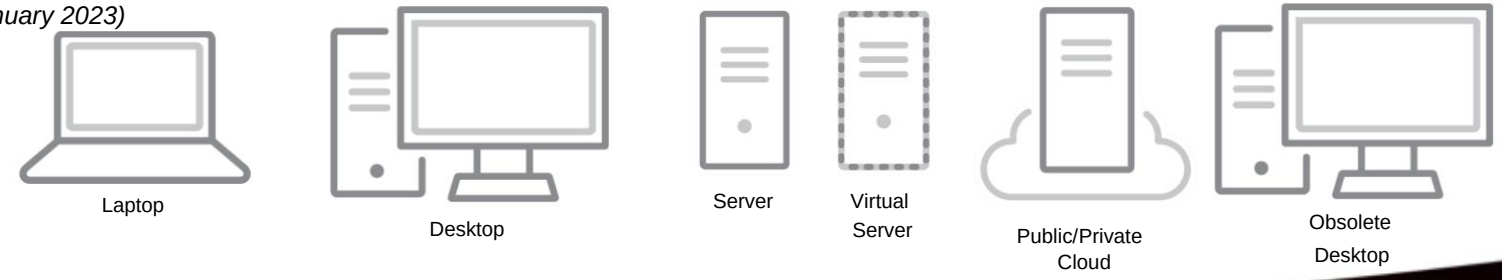
Server Workloads & User Endpoints Facing Different Threats

According to Gartner,[1] "An end-user endpoint is regularly exposed to threats via email, websites, cloud services or USB drives.

Instead, threat actors target servers through software and configuration vulnerabilities, lateral movement, and stolen employee credentials.

These differences in threat exposure create the need for security requirements. distinct security and protection strategies for end-user endpoints and server workloads."

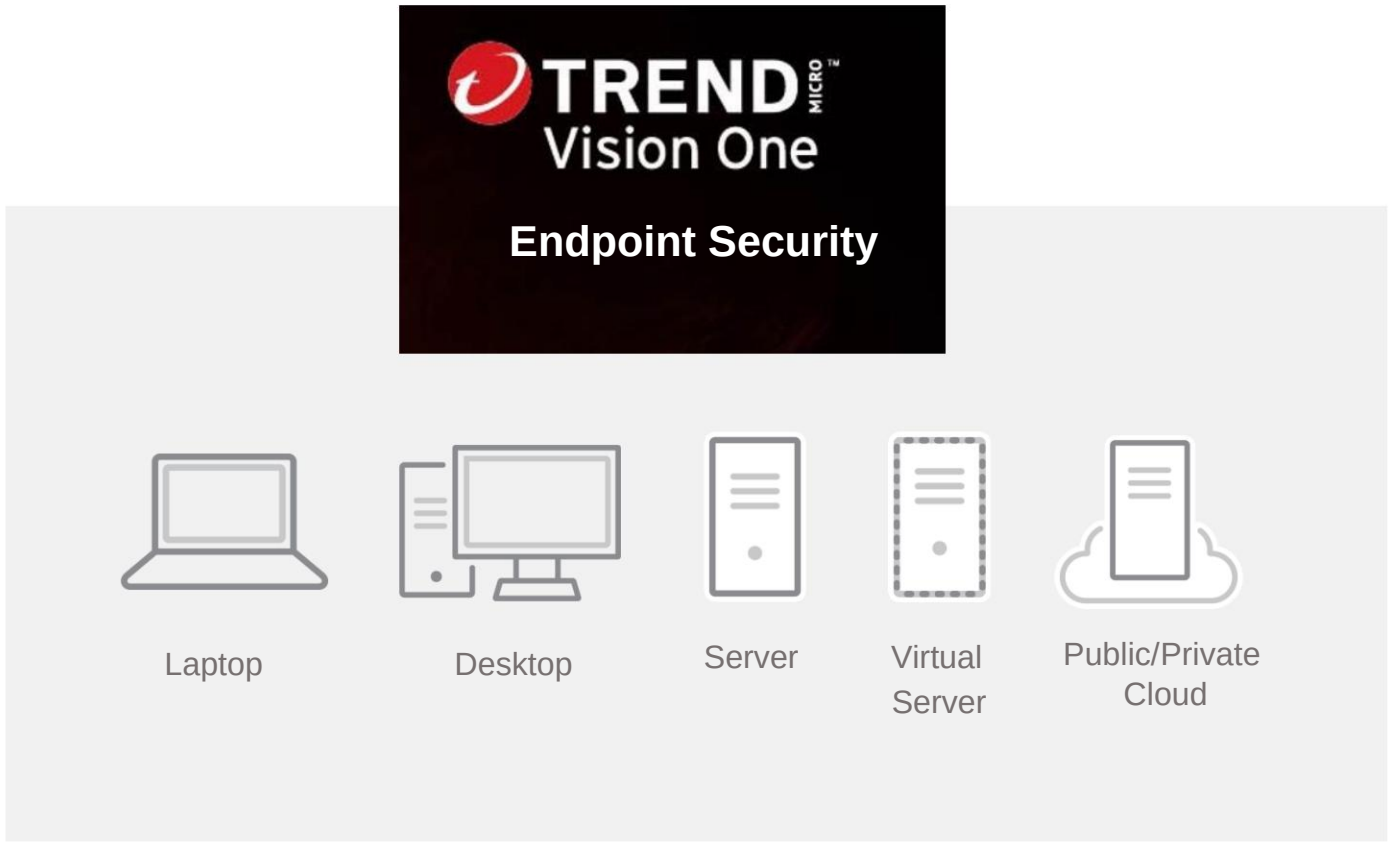
1. Gartner, Prioritizing Security Controls for Enterprise Servers and End-User Endpoints (Evgeny Mirolyubov, Peter Firstbrook, January 2023)



Why “Vision One - Endpoint Security”?

Machine Translated by Google

Vision One - Endpoint Security



- Security designed specifically for endpoint, server, and cloud workloads.
- Secure, cloud and hybrid data center
- Single console for visibility and management; protection and EDR
- Connected workflow IT/SecOps
- Part of the Vision platform One; easy expansion to other native security solutions, XDR, and ASRM

Machine Translated by Google

Why Vision One Endpoint Security



Best safety result



Less complexity

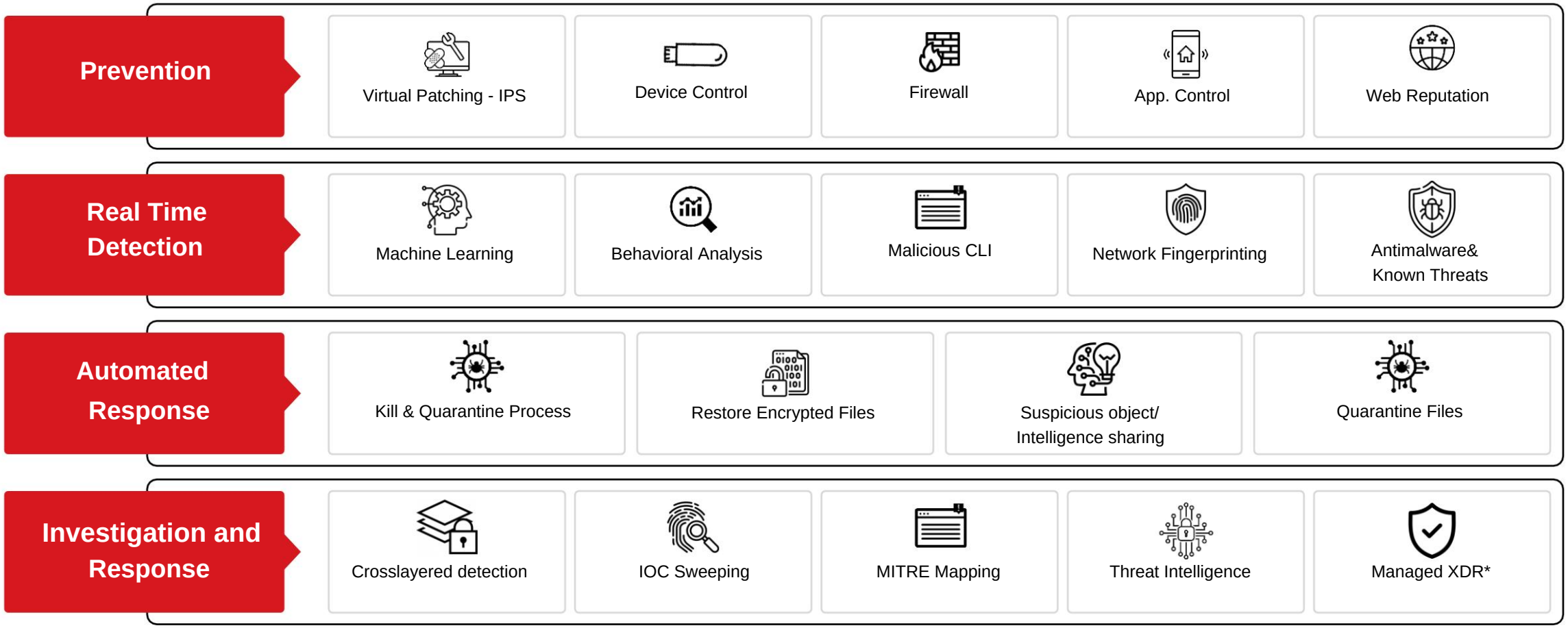


Accelerate your supplier consolidation process

Machine Translated by Google

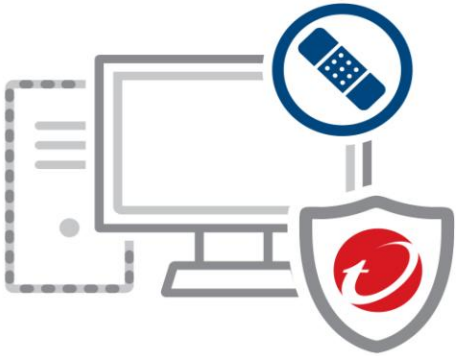
Comprehensive Threat Protection

From layered prevention to detection and response



Machine Translated by Google

Protection from the exploitation of Vulnerabilities of the Operating System and Applications



Virtual Patch (IPS)

Protect yourself from vulnerabilities up to that the vendor patch is available.

Protect automatically the newly discovered vulnerabilities the few hours of its discovery.

With the support of Trend Zero Day Initiative (ZDI), market leader in public disclosure during the last 14 years.

Machine Translated by Google

Creado y optimizado para servidores y cargas de trabajo en la nube

We meet the unique needs of servers, cloud workloads, and security of runtime containers, unlike other providers that use user endpoint capabilities for servers and workloads.

Network Security



Intrusion Prevention



Firewall



Vulnerability Scanning

System Security



Application Control



Integrity Monitoring



Log Inspection

Malware Prevention



Anti-Malware



Behavioral Analysis



Machine Learning

Detection & Response (activity monitoring)



Detect



Respond



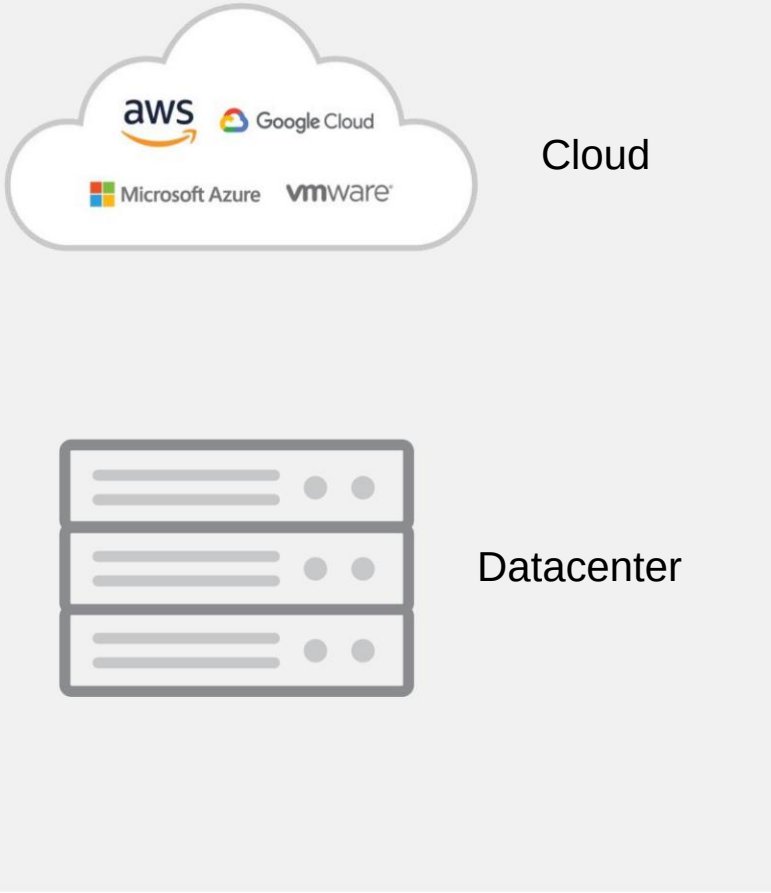
Investigate

Machine Translated by Google

Protect your Hybrid Cloud

TREND MICRO Vision One

Endpoint Security



Cloud native, SaaS-based platform

Hybrid and multi-cloud support

Protection tailored for server/cloud workload

Machine Translated by Google

Protect Your Linux Platform

Broad platform support extending across extensive builds

Linux and hundreds of kernels Linux

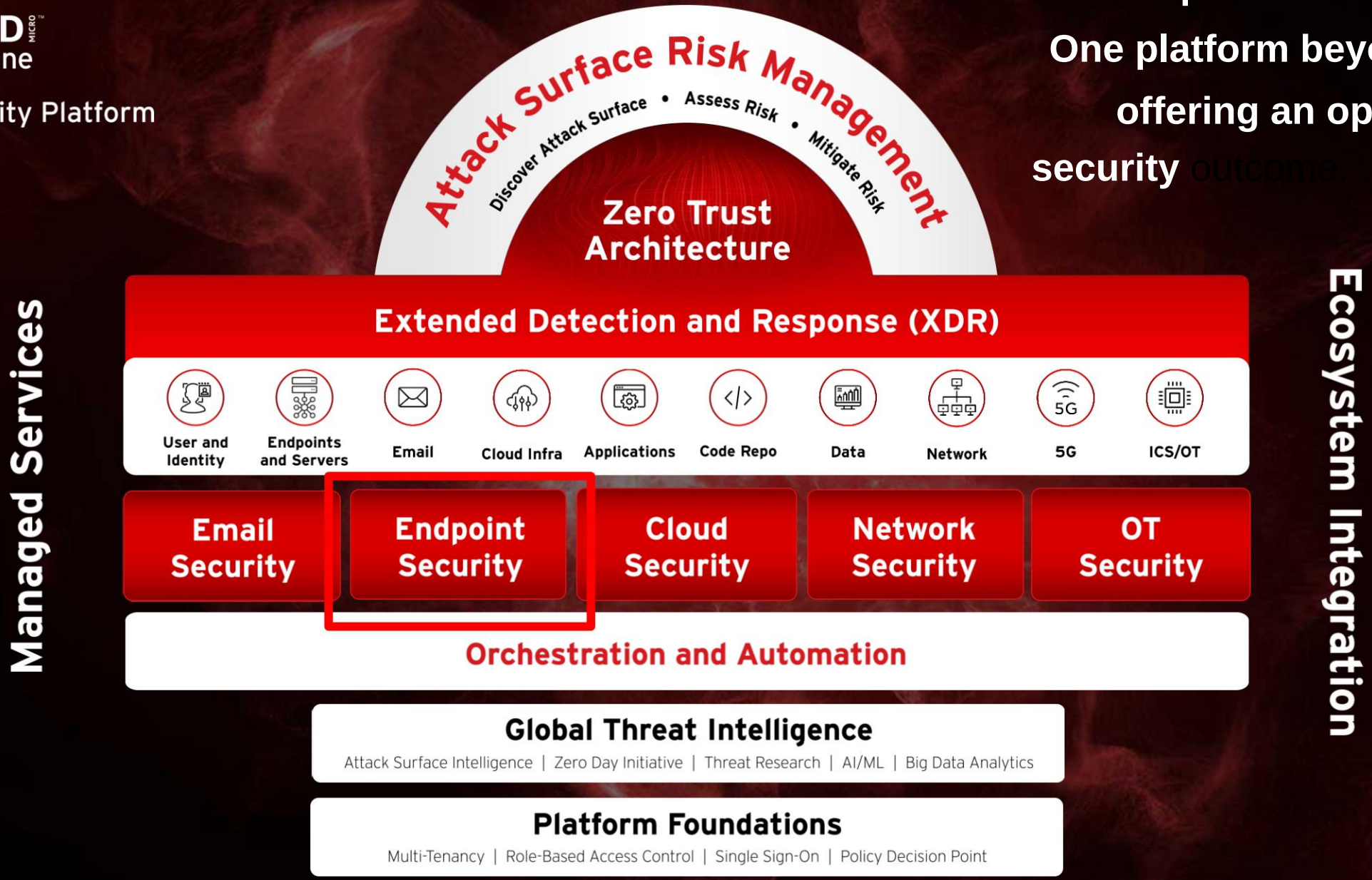


Machine Translated by Google

TREND MICRO Vision One

Cybersecurity Platform

It is part of the Vision One platform beyond EDR, offering an optimal security outcome.



Machine Translated by Google

Trend Vision A platform that delivers tangible results

Better Protected



He suffered half as many attacks successful in the last 12 months.

Detecting Quicker



2.2x more likely to detect a breach data or a successful attack in a few days or less

Responding Completely



60% less likely to report Re-propagation of attacks

Source: Trend Micro Vision One Economic Benefits Analysis, 2021

Machine Translated by Google

Why EDR/XDR on endpoints?

Most attacks interact with corporate endpoints during the breach lifecycle.

Detect: Security analysis finds hidden threats among endpoint telemetry. IOC Sweep

Investigate: What happened inside the endpoint? How did it spread? What tactics/techniques are used?

Respond Examples: Isolate,stop process, delete/restore files



Going Further with Other XDR

Layers: Where Did the Threat Originate?

Where else is this threat found in my network, workloads, email?

Machine Translated by Google

EDR/XDR for Servers and Cloud Workloads



SIEM



Log Inspection Alert: Possible SSH Server Attack (or Version Harvesting) Source: 3.211.84.114



Alerts don't tell the whole story .

This is probably one step of many...

What's the big picture?

Was the attacker successful?

Detect: High-fidelity detections were correlated with different security controls and activities to tell a complete story. IOC Sweep : **Investigate:** Full visibility into activities helps answer questions such as: What happened within the workload?

How did it spread?

Activity Data: •

User account activity

- Processes
- Commands executed
- Network connections
- Files Created/Accessed •

Registry Modifications



Machine Translated by Google

Broader detection for workloads

Environments





Platforms



Telemetry Data

Host activities

Process, File, Network, User Account, Container

Application-level logs

OS Platform System/Audit event logs

Windows service logs (PowerShell service/Remote desktop/Terminal Service)

Web Server/FTP/Database/Mail Server logs

Security Events/Anomalies/Changes

Newly Installed software/changes

Application components changes

Indicators of attack (IOAs)

Known attack footprints

Analysis

XDR

Managed XDR

Detection

Investigation & Response

Machine Translated by Google

Why Vision One Endpoint Security?



Best safety result



Less complexity

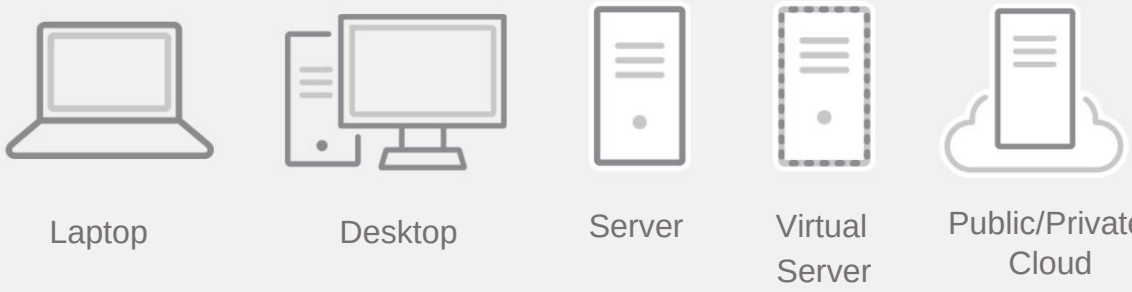


Accelerate your supplier consolidation process

Machine Translated by Google

One platform, one console





What is it?

Single panel (inventory, detections, actions of mitigation, management of policies)

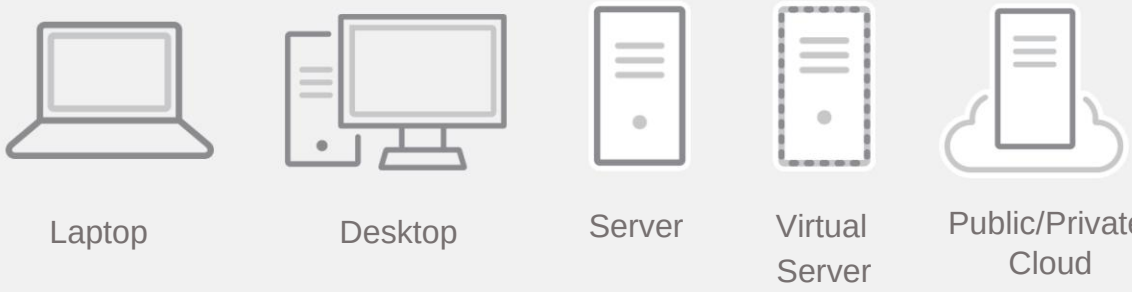
Common RBAC, policy management, licensing, and more

Connected workflows and automation

Machine Translated by Google

One platform, one console





Benefits

Centralized visibility, response, and management

Reduce complexity;
Increase efficiency

Optimize your IT and security Operations Workflow

Machine Translated by Google

Why Vision One Endpoint Security?



Best result of security



Less complexity



Accelerate your consolidation process suppliers

Machine Translated by Google

Accelerate your supplier consolidation process

According to Gartner1, "75% of organizations are looking to consolidate security vendors."

A solution for your endpoint, server and Workload security.

Simplify operation, fewer tools/suppliers to manage.

Increase efficiency, more time for strategy initiatives.

Streamline your IT/security operations workflow, no more silos.

Single platform with native endpoint, email, network, IT/OT, cloud security + MDR services for expand your security team.

1. Gartner, Emerging Tech: The Impact of Emerging Trends on Security Solution Demand Published (Rustam Malik, October 2022)

Machine Translated by Google

Why Vision One Endpoint Security



Best safety result

Superior prevention, detection, and response for user endpoints , servers, and cloud workloads

Hybrid and multi-cloud support

Industry-leading threat intelligence and timely protection against vulnerabilities

Recognized industry leader



Less complexity

Single panel (inventory, detections, mitigation, policies)

Common RBAC, policy management, licensing, and more across the platform

Connected IT/Security Operations

Workflow



Accelerate your supplier Consolidation trip

"75% of organizations are chasing

"security vendor consolidation" (Gartner)

Single platform: endpoint, email, network, cloud, OT

MDR Service to expand your security team

Industry Leadership

Machine Translated by Google

2022 Gartner Magic Quadrant for Endpoint Protection Platforms1 (EPP)



Named a Leader by Gartner in this category since 20222 19 times in a row

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from: https://resources.trendmicro.com/Gartner-Magic-Quadrant-Endpoints.html

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be constructed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

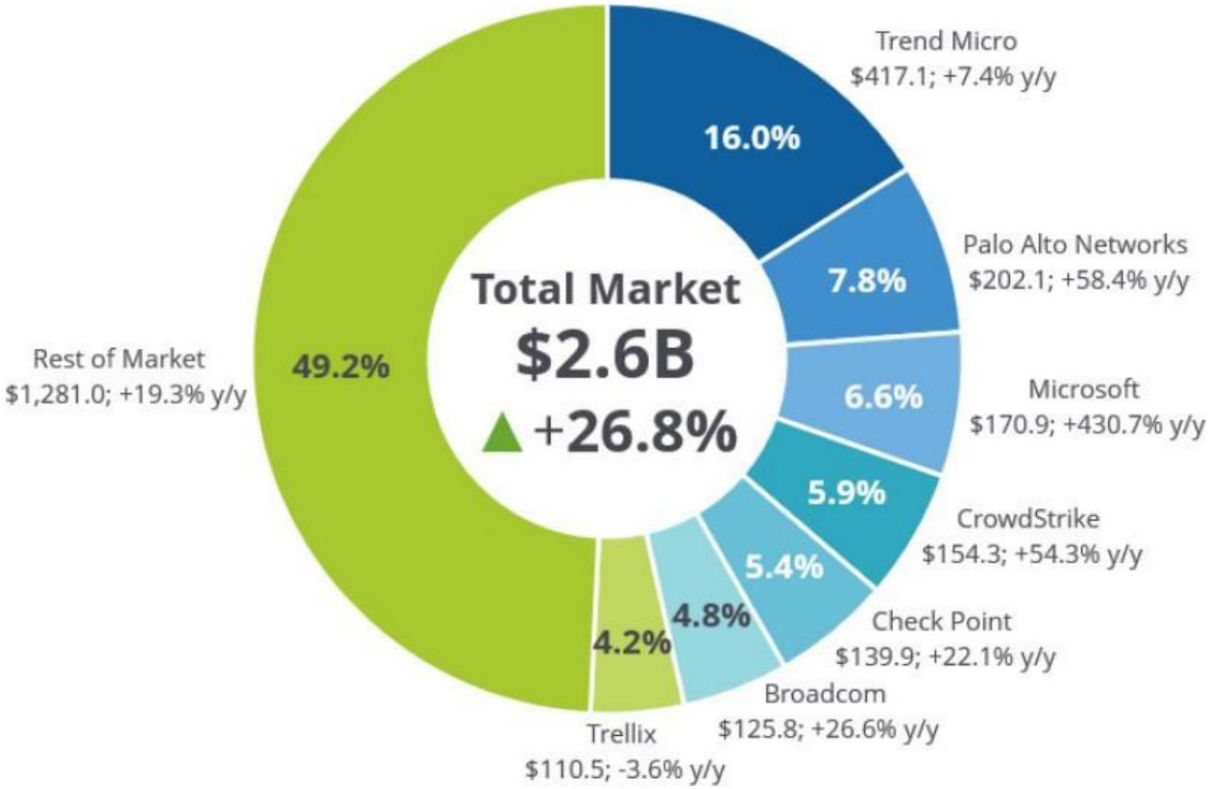
1 Gartner "Magic Quadrant for Endpoint Protection Platforms," by Peter Firstbrook, Chris Silva, December 2022

2 Under the names of "Magic Quadrant for Endpoint Protection Platforms," and previously, "Magic Quadrant for Enterprise Antivirus"

(Enterprise Antivirus 2Q02MQ: Room for Improvement, Magic Quadrant for Enterprise Antivirus, 1H03, Magic Quadrant for Enterprise Antivirus, 2006, "Magic Quadrant for Endpoint Protection Platforms" from 2007onwards)

Machine Translated by Google

IDC Worldwide Cloud Workload Security Market Shares, 20221



Ranked

#1

for Cloud Workload Security

Market Share

for the 5th consecutive year

1. IDC, Worldwide Cloud Workload Security Market Shares, 2022:A Shifting Landscape, #US50197823,May 31, 2023.

Machine Translated by Google

THE FORRESTER WAVETM

Endpoint Security Software as a Service - Q2 2021



The Forrester WaveTM is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Machine Translated by Google

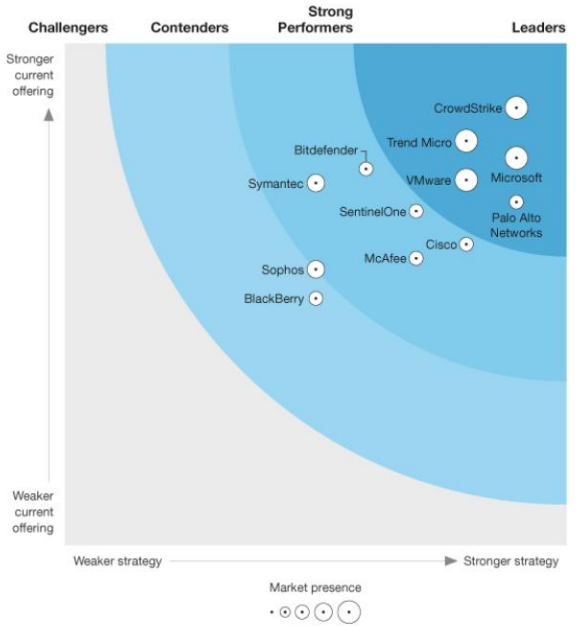
A Leader in XDR and its Building Blocks



The Forrester New Wave™ Extended Detection and Response, Q4 2021



The Forrester Wave™: Endpoint Detection and Response, Q2 2022



The Forrester Wave™: Endpoint Security Software as a Service, Q2 2021

"The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to "change."

Machine Translated by Google

MITER Engenuity ATT&CK Evaluations(Enterprise 2022)

Trend Micro Proves Exceptional Attack Protection

Trend Micro Vision One recorded the following impressive results

100%

Detector of **all 19 attack steps**
In the evaluation – highly enriched telemetry for better investigations

105 out of 109

Provided clear visibility of attack methods providing **96.33% coverage** – this broad visibility allows customers to have a clear picture of the attack and respond faster

Ranked #1

In the **protection category** – ensuring that attacks are prevented early in the attack lifecycle

100%

(#1 performer)

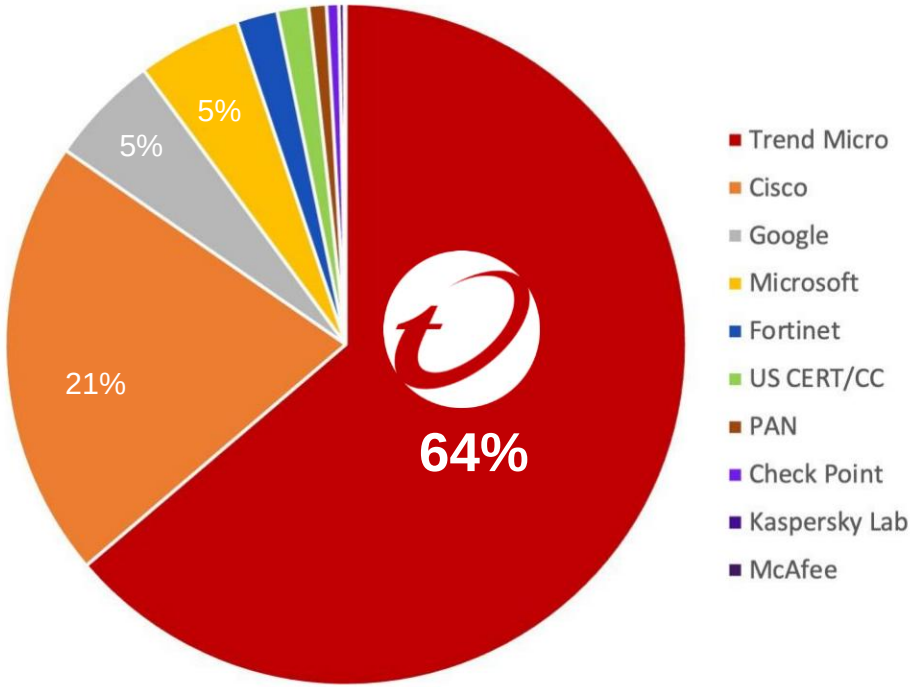
of attacks against the Linux host detected and prevented, capturing a simulated attack – especially important considering Linux is the most used OS in cloud-native applications

Machine Translated by Google

Market Leader in Vulnerability Disclosure

ZERO DAY INITIATIVE

- **10,000+** independent vulnerabilities researchers
- Market leader in the public disclosure market for past 14 years, discovering & reporting **64% of the vulnerabilities** in 2021
- **Most** disclosed high impact vulnerabilities (critical + high severity)

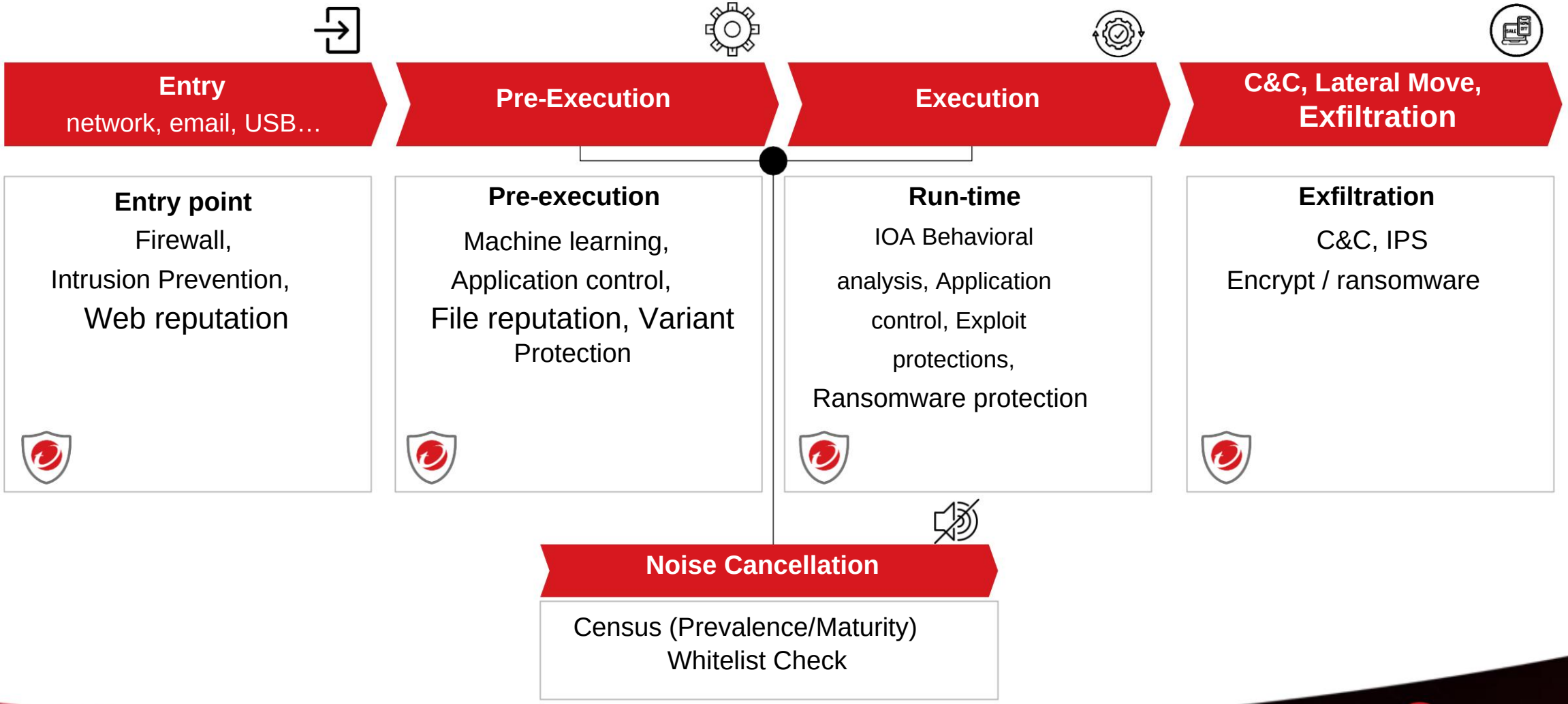


Source: Quantifying the Public Vulnerability Market, Omdia, May 2022

Layered Security

Machine Translated by Google

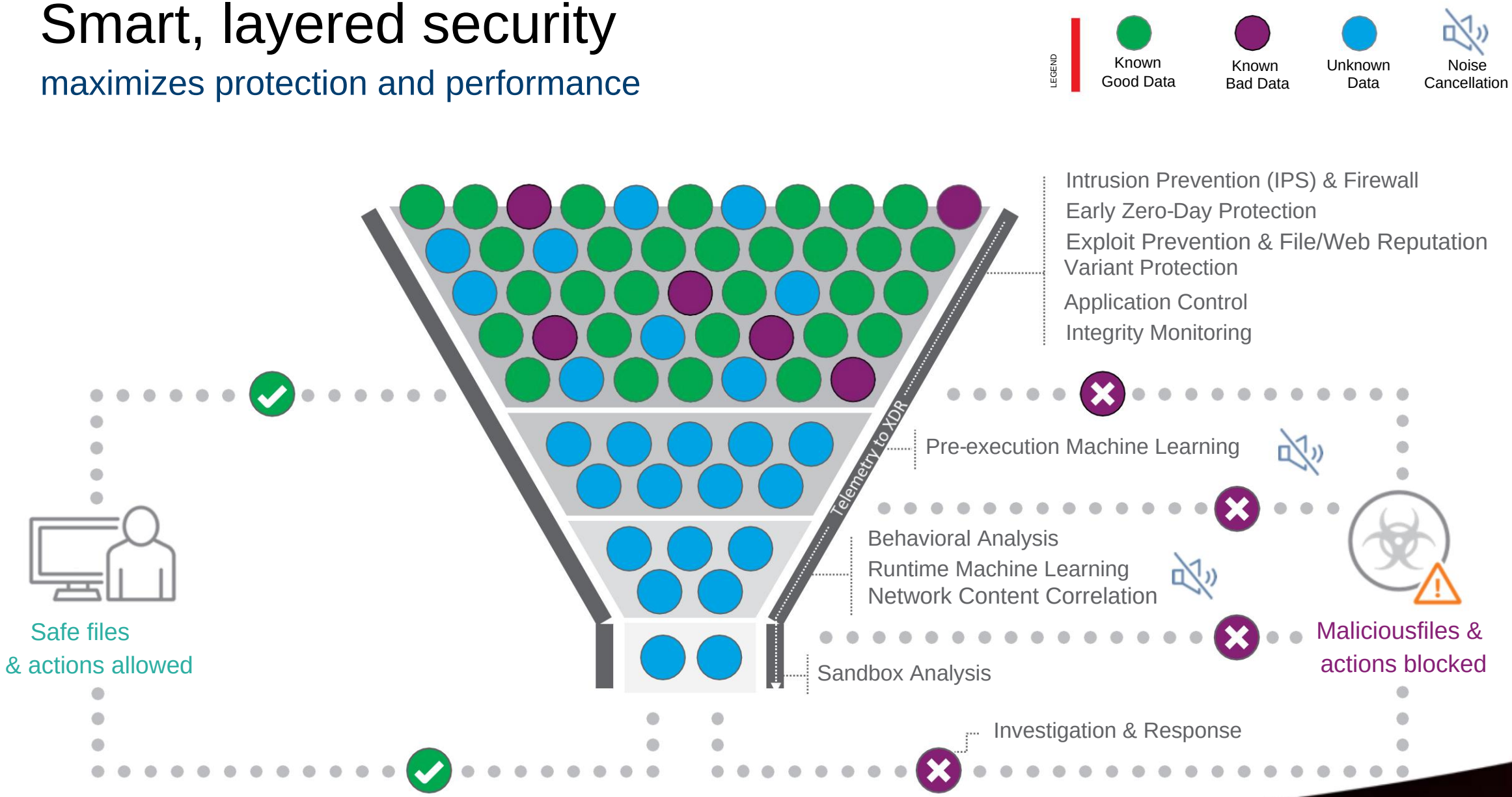
Layered security for every stage of an attack



Machine Translated by Google

Smart, layered security

maximizes protection and performance

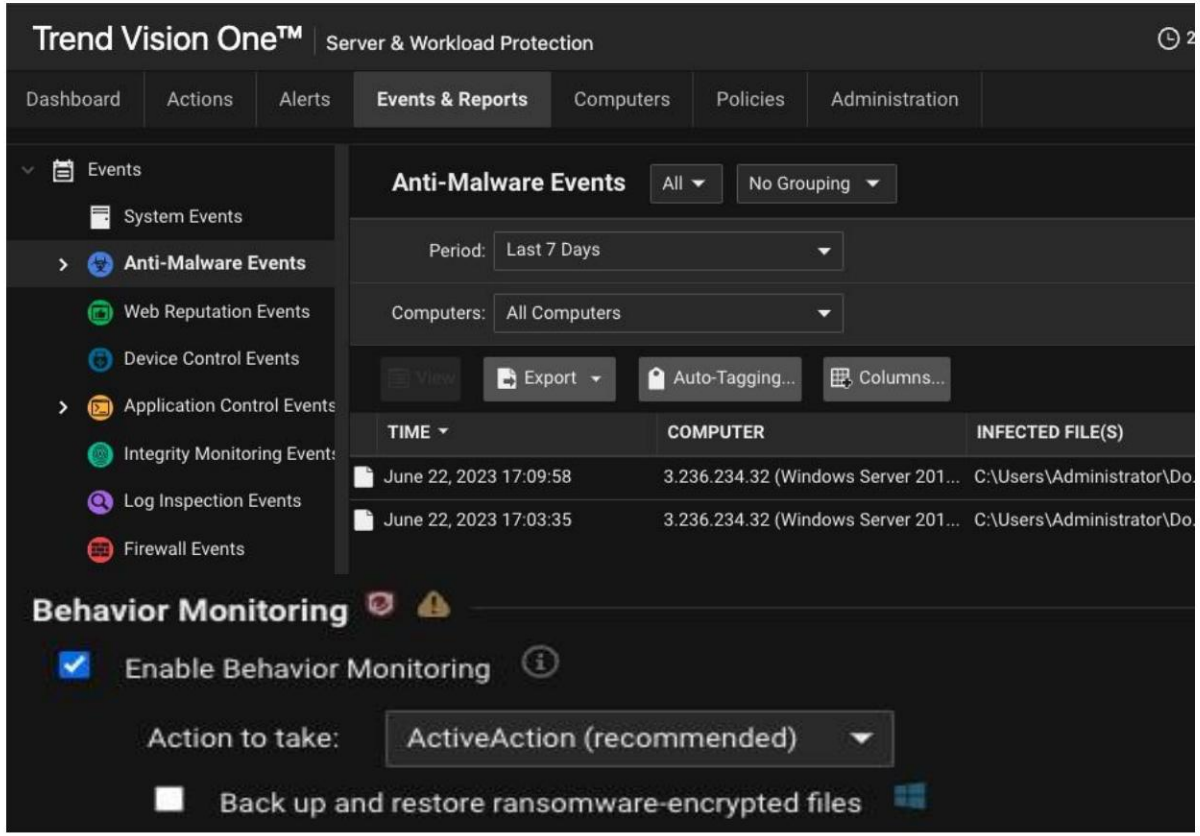


Machine Translated by Google

Detecting emerging security risks

Protection against malware, ransomware, and unknown threats

- Protects against frequent attacks
- Detects known emerging zero-day and a stranger
- Performs an in-depth analysis of the Windows files
- Look for suspicious behavior or indicators of attack (IOA)
- Blocks attempts to obfuscate/encrypt files by unknown processes, kills the process, and restores files
- Application whitelist to block allowed files/applications



Machine Translated by Google

Stop unauthorized changes

Application Control

- Full visibility of the executables of the host
- Application blocking (Windows and Linux)
- Automatic updater whitelist trust
- Support continuous application change with automation

- Respond quickly to threats newly discovered hash-locked (e.g., IOC)

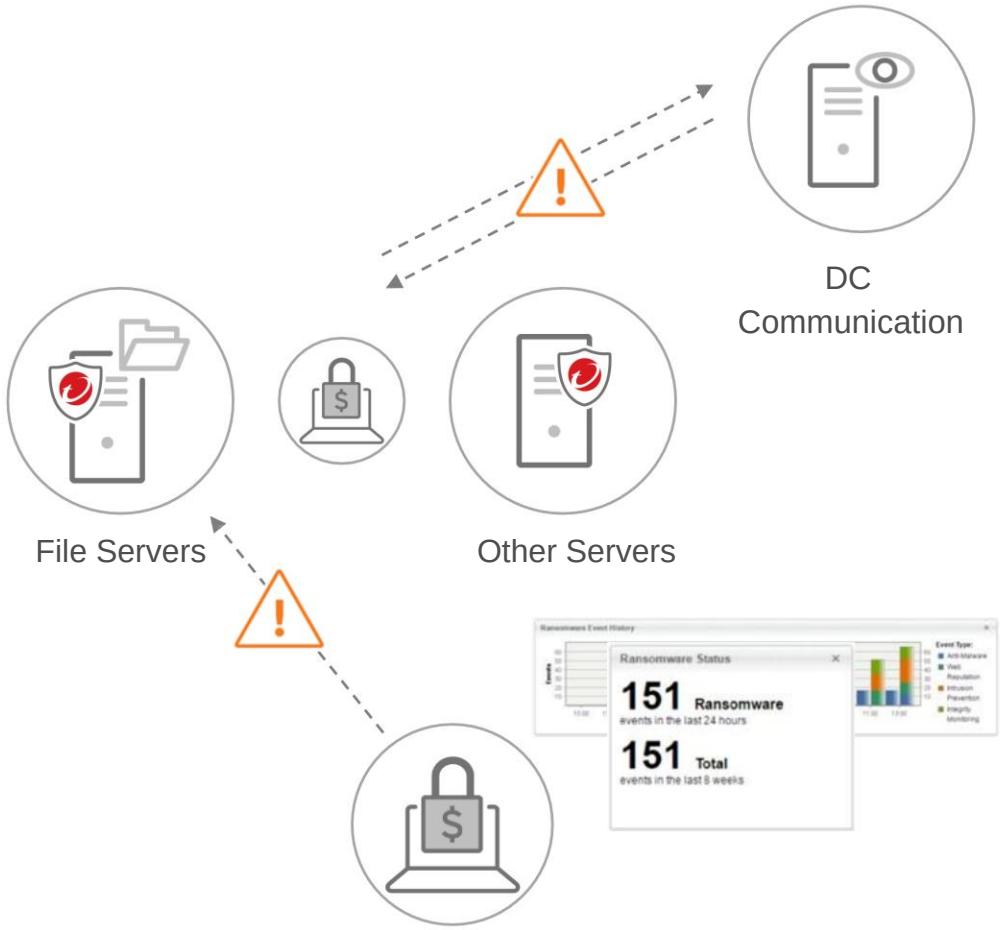


Machine Translated by Google

Stop Ransomware

Use layered security to:

- Stop ransomware on endpoints with advanced malware prevention that includes behavioral monitoring and machine learning
- Lock down your endpoints with application control
- Protect yourself from network attacks with IPS
- (vulnerabilities protection)
- Stop lateral movement and detect command and control (C&C) traffic



Suite Types

Machine Translated by Google

Trend Vision One – Endpoint Security offerings

	Core	Essentials	Pro
Primary endpoint type	User endpoints and basic servers	User endpoints and basic servers	Critical endpoints including servers and workloads
Windows, Linux and Mac OS	●	●	●
Antimalware, behavioral analysis, machine learning, web reputation	●	●	●
Device control	●	●	●
DLP	●	●	
Firewall	●	●	●
App control	●	●	●
Intrusion prevention – IPS (OS)	●	●	●
Virtualization protection	●	●	●
EDR-XDR		●	●
Intrusion prevention – IPS (server application)			●
Integrity monitoring / log Inspection			●
	Core	**Essentials**	**Pro**
Email Security	+	+	+
Mobile Security	+	+	+
Network Security	+	+	+
Cloud Security	+	+	+
Zero Trust Secure Access	+	+	+
MDR / Service One		+	+
Attack Surface Risk Management (ASRM)		+	+

+ indicates add-on option

Managed XDR: Expert MDR Service

Expert Threat Hunting

Cutting-edge techniques with verification and Enrichment by experts in threats



24x7 Monitoring & Detection

Continuous monitoring and routine sweeping endpoint, server, network, and email

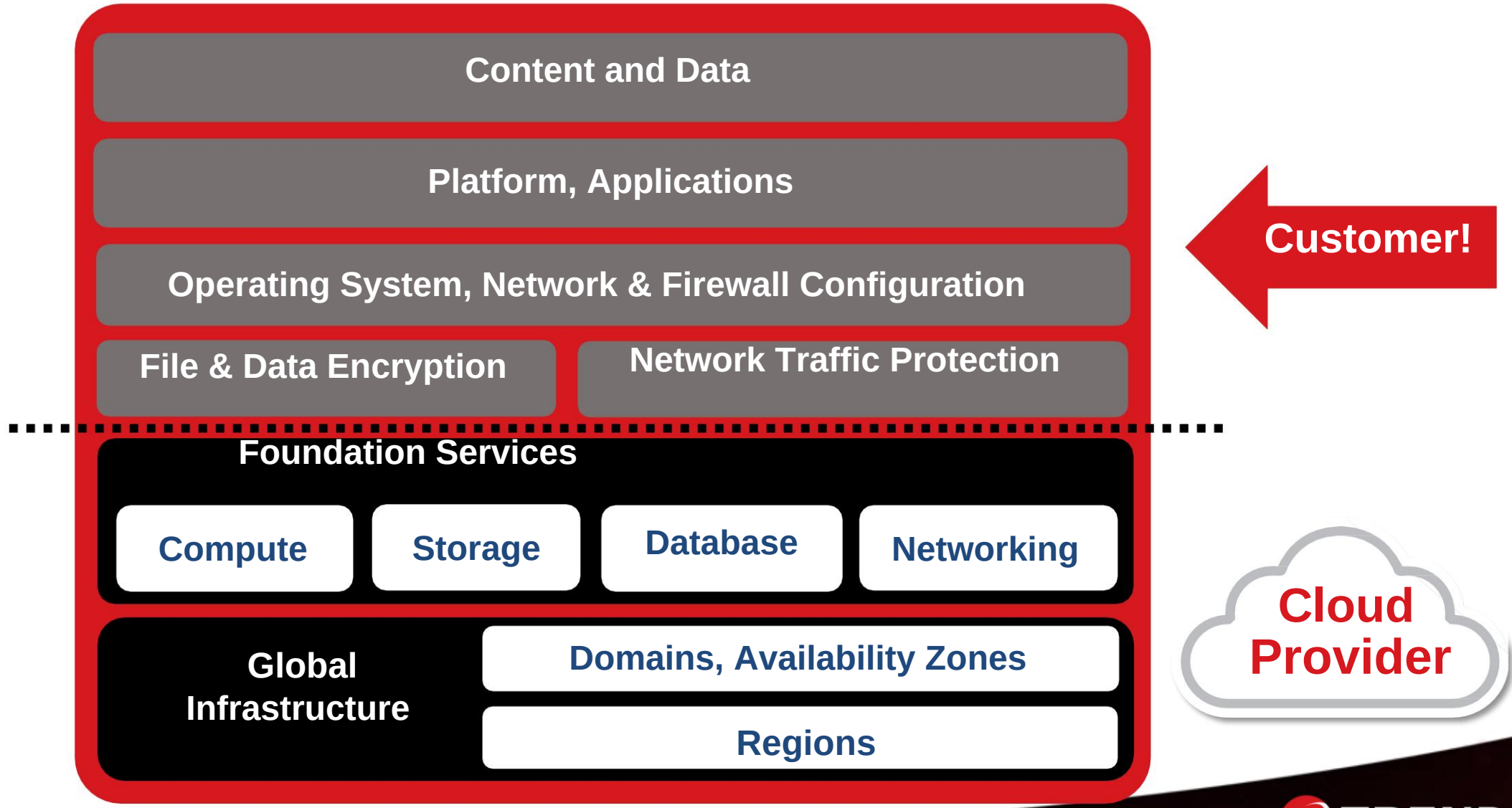
Rapid Investigation and Mitigation

Detailed response plan and remote actions through Trend products Micro

Vision One Endpoint Security PRO

Machine Translated by Google

Safety is a shared responsibility



Machine Translated by Google

Key Business Needs



All your environments covered...

• Discovery and visibility across multiple cloud providers • Application protection across physical, virtual, and container environments • Broadest operating system support, including legacy operating systems • Demonstrate compliance with regulatory requirements, GDPR, HIPAA and more



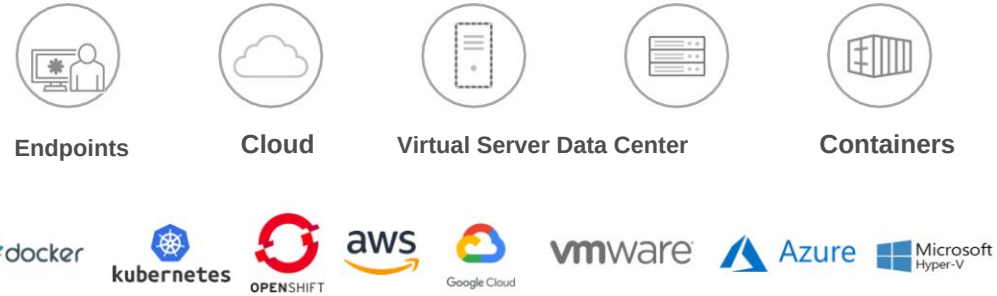
Automated detection and protection at scale • Comprehensive detection and protection capabilities that address the latest threats and are consolidated to eliminate the need for multiple point solutions • Speed of protection backed by Trend Research • API for easy integration • Integration with other security tools

Machine Translated by Google

Specifically designed for a variety of different environments

On-premises, cloud, or hybrid; new or legacy

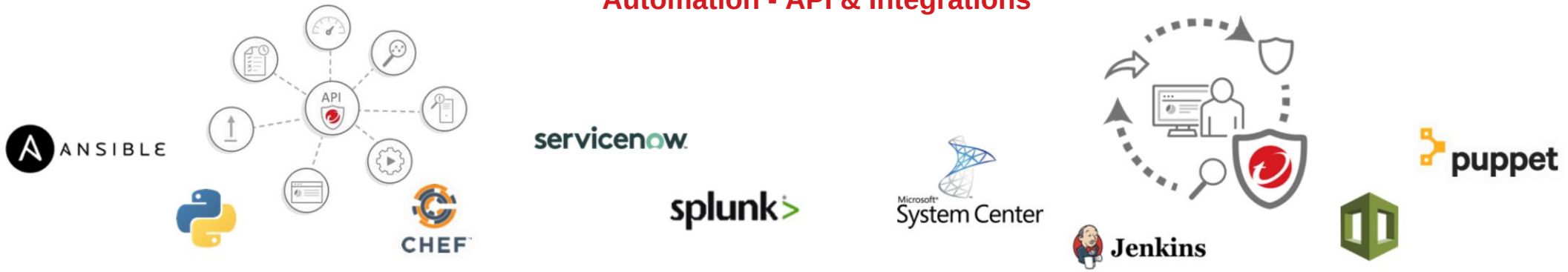
Environments



Platforms



Automation - API & Integrations

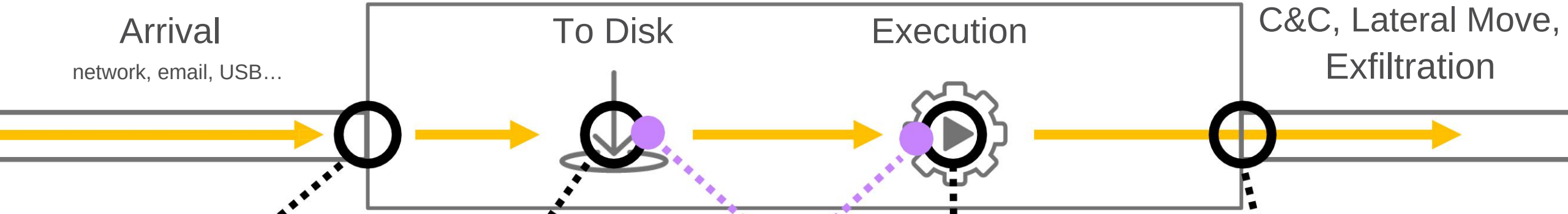


User endpoints, cloud workloads, VMs, containers & serve

Machine Translated by Google

Stages of a Threat





Entry point:

Firewall,
Intrusion Prevention,
Web reputation

Pre-execution:

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

Noise Cancellation:

Census (Prevalence/Maturity)
Whitelist Check

Run-time:

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

Exfiltration:

DC,
IPS
Encrypt /
ransomware

Machine Translated by Google

Uncover Suspicious System Changes

File integrity monitoring and log inspection

• Identify and report on important security events • Monitor changes, libraries, and services • Create a secure configuration baseline • Suspicious events highlighted in the unclassified dashboard

the records



File Integrity



Log Inspection

Machine Translated by Google

Accelerate Incident Response

Server & Cloud Workload EDR

What was affected?

What was added?

Where did it spread?







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 the severity and impact of threats

DEMISTO

ArcSight

now

IBM Radar

splunk>

SWIMLANE

M-XDR

sumologic

TREND MICRO

Machine Translated by Google

Powerful threat detection

What was affected?

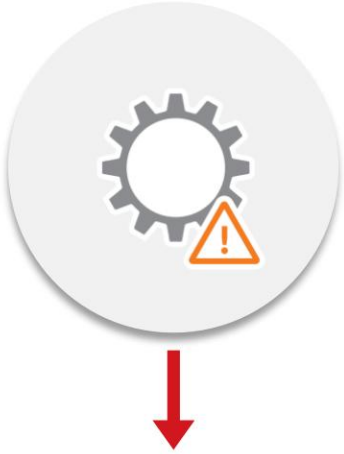


Detect IOAs and unexpected changes to files and systems with Integrity Monitoring

Analyze suspicious system logs with Log Inspection.

Sandbox integration for suspicious documents

What was added?



Detect newly registered services or open ports running with Integrity Monitoring

Detect and prevent the execution of new software and processes with application control

Where did it spread?



Anomalous network traffic patterns with heuristic rules (smart)

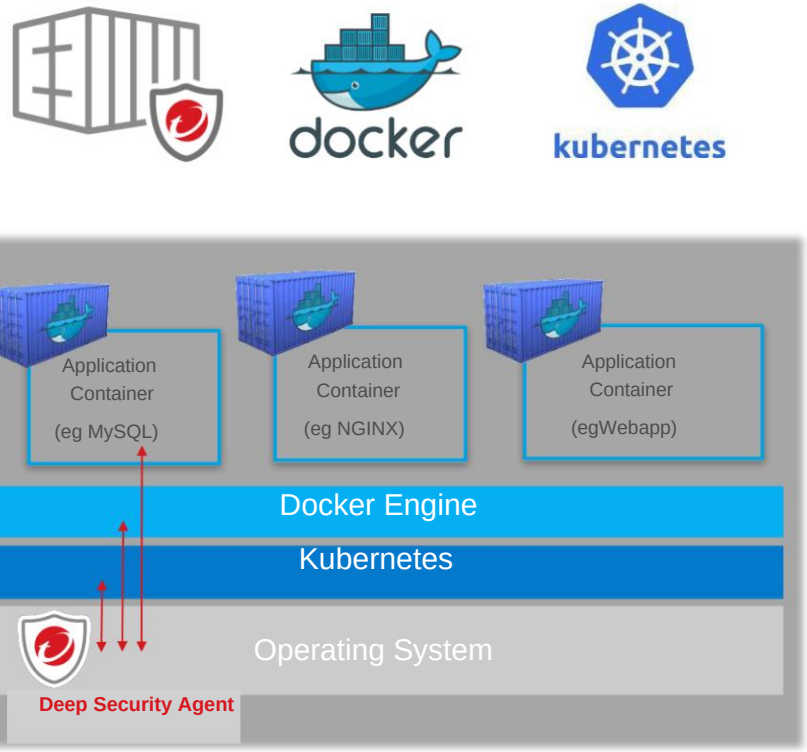
Process activity, files, connections network, registry, users and DNS

Machine Translated by Google

Detecting attacks on container platforms

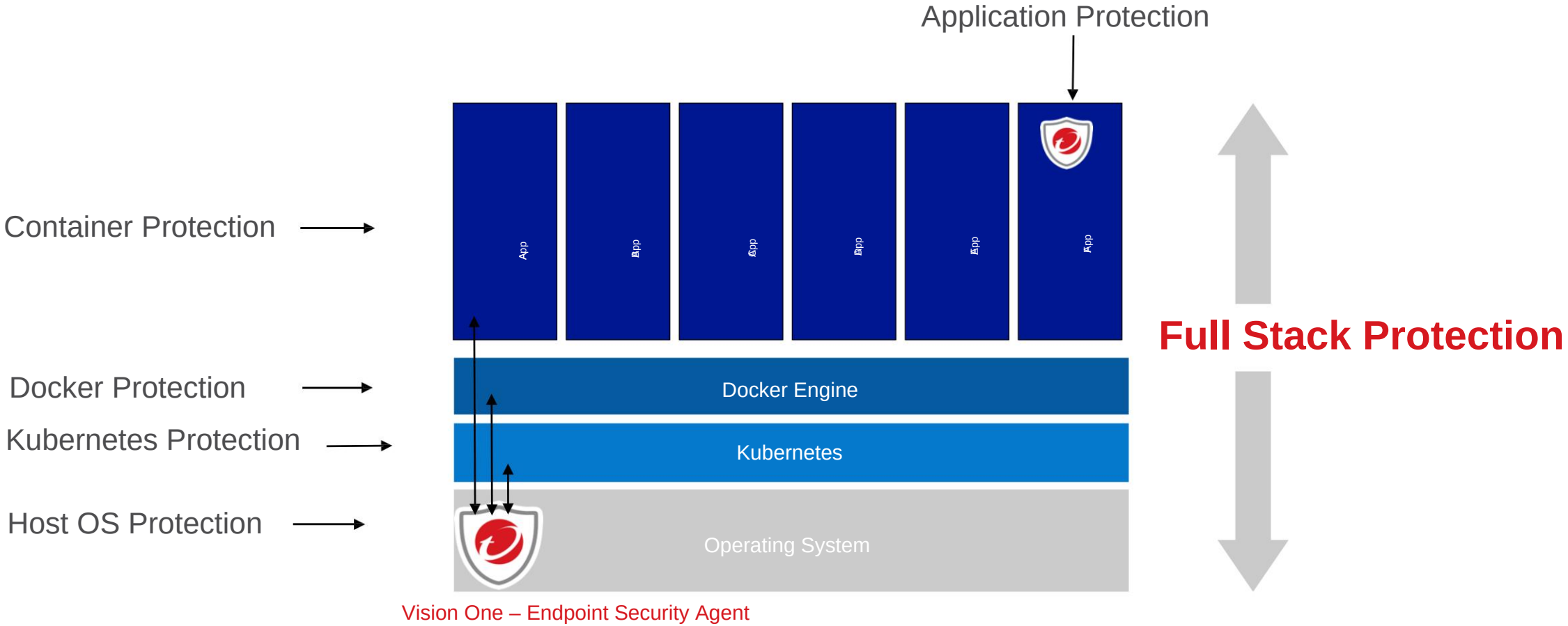
Docker and Kubernetes

- Automatic detection of Docker and Kubernetes
- Software change detection
- Upgrades, downgrades, deletions
- Monitoring binary files for attribute changes
- Monitor running processes
- dockerd, etcd, Kubelet, Kube-apiserver, etc.
- Detection of changes in critical files
- Configuration, certificates, keys, yaml files, etc.
- Monitor changes to iptables rules
  - Protect against unauthorized port changes
- Detect changes in permissions on key directories
- Inspect key events
- Eg. Prohibited action errors



Machine Translated by Google

Runtime Protection for Containers



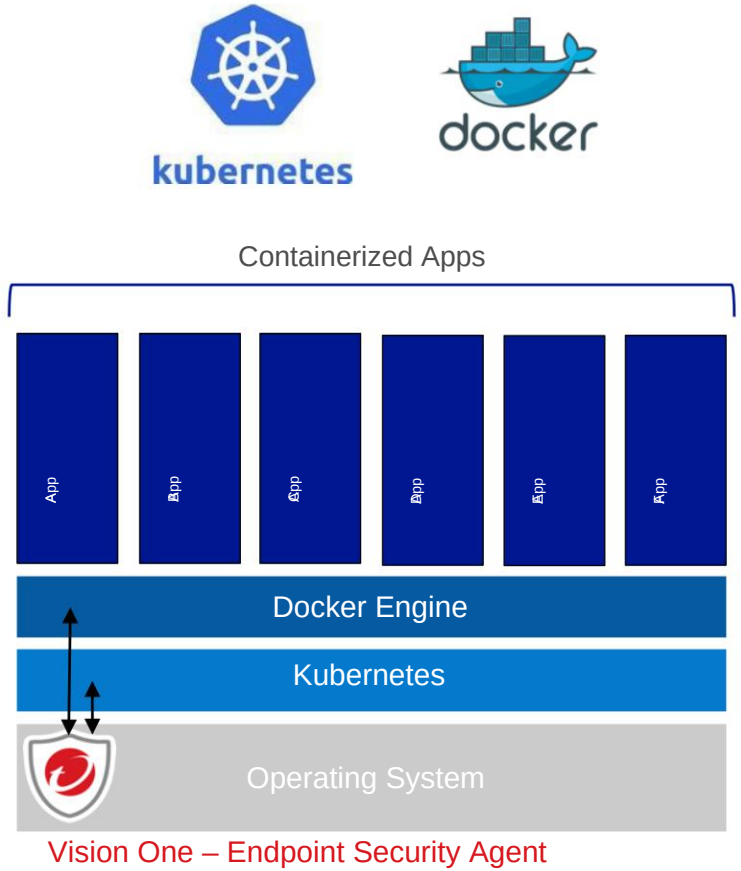
Physical, Virtual or Cloud Container Nodes

Machine Translated by Google

Detecting attacks on container platforms

Securing Docker and Kubernetes

Attackers can target Docker and Kubernetes to execute attacks • Image execution • Networking and micro-segmentation • Authentication bypass



Vision One – Endpoint Security Agent

Monitors key objects to detect instances of Docker and Kubernetes compromised

- Software updates, downgrades, or removals
- Changes in binary attributes
- Running processes • Critical files • IPtables rules • Permissions for key directories

Machine Translated by Google

Security driven by leading threat research

Cyber Threats & Exploits

Targeted Attacks

Vulnerabilities

AI & ML

IoT

OT / IIoT

Cybercriminal Undergrounds

Future Threat Landscape

450 researchers globally

Cloud and Container Research Team Examples:

Kubernetes API Server Denial of Service Vulnerability

Apache Tomcat Remote Code Execution Vulnerability

Kubernetes API Proxy Request Handling Privilege Escalation Vulnerability



Machine Translated by Google

Optimized for the cloud



- Marketplace Billing
- Hybrid cloud visibility across all environments
- Visibility of all cloud services
- Integration for automatic detection and automatic escalation of protection (up and down)
- Quick starts and templates
- Complement and integrate with existing toolsets from AWS, Azure, Google Cloud, and VMware Cloud







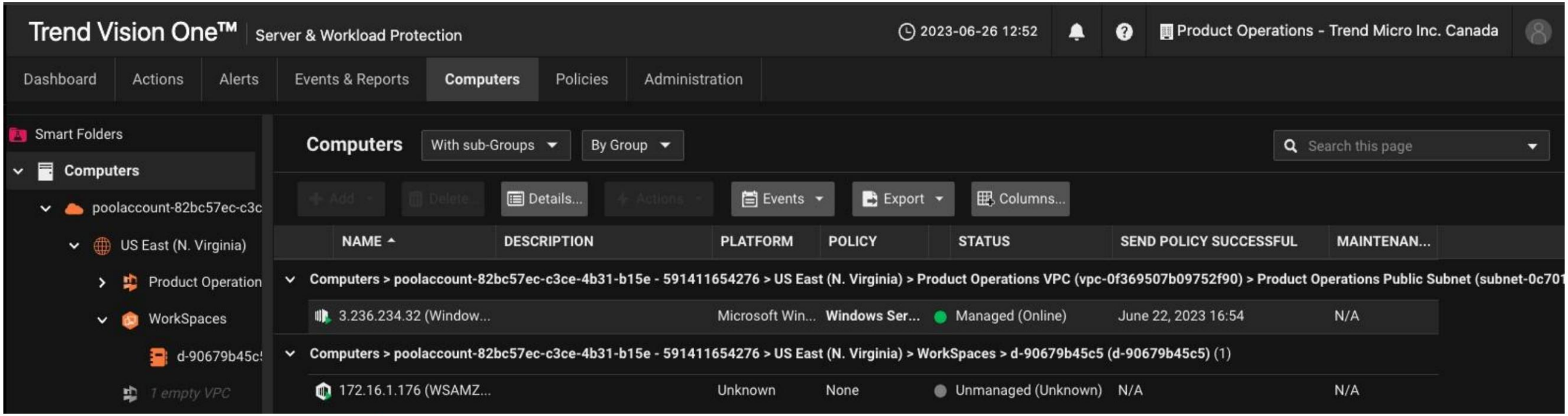
Google Cloud

vmware

Machine Translated by Google

Discovery and visibility across the hybrid cloud

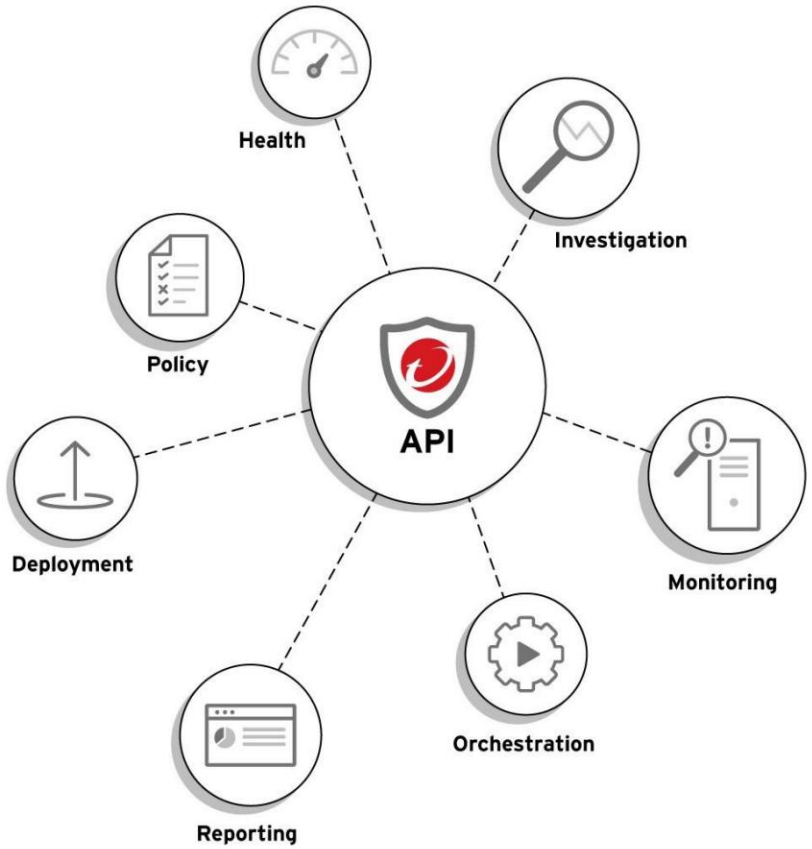
Smart Folders for custom views in physical, virtual, and cloud containers



Visibility within each environment

Machine Translated by Google

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 Status of Your Environment

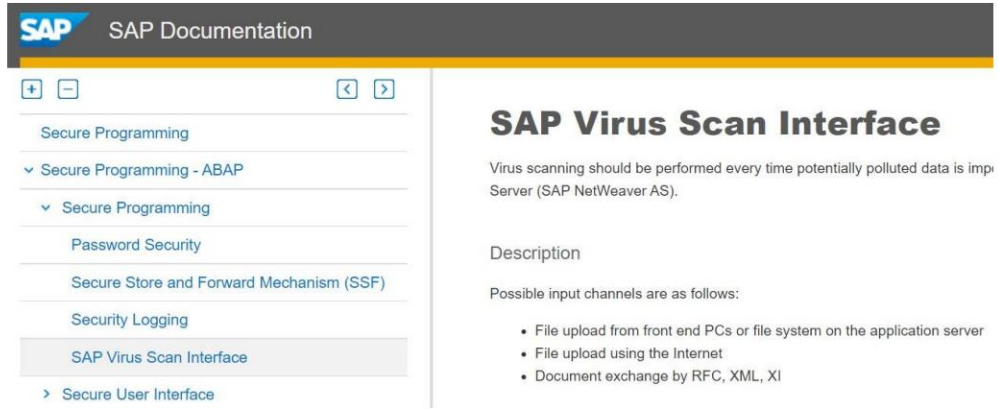
Orchestration Automation: Integrates with your pipeline tools, SOAR tools, etc.

Machine Translated by Google

SAP recommends using the NW-VSI interface

- The SAP interface allows external antivirus and security solutions to scan content uploaded to the SAP application
- Detects malicious file formats, file format classification, and active content within the file (e.g., scripts in files)

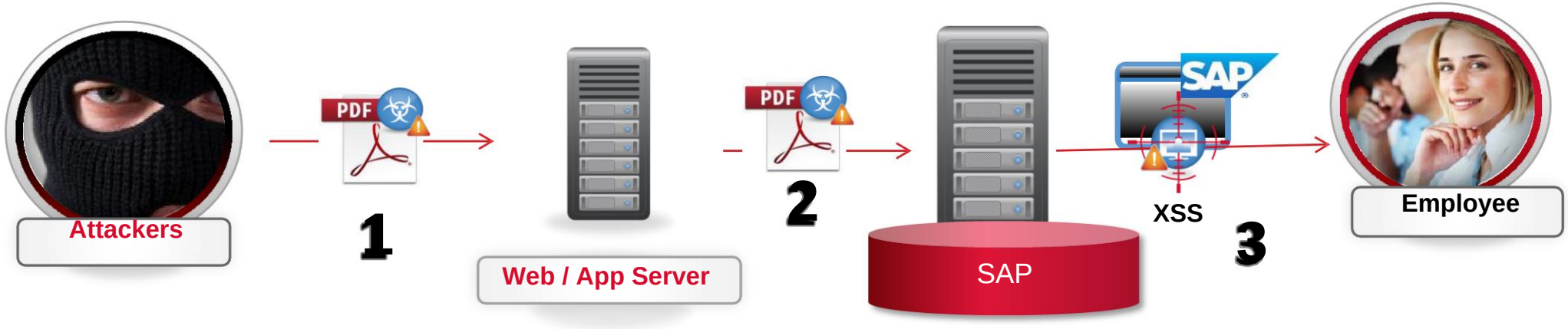
Provides antimalware scanning for SAP through a premium feature in the product



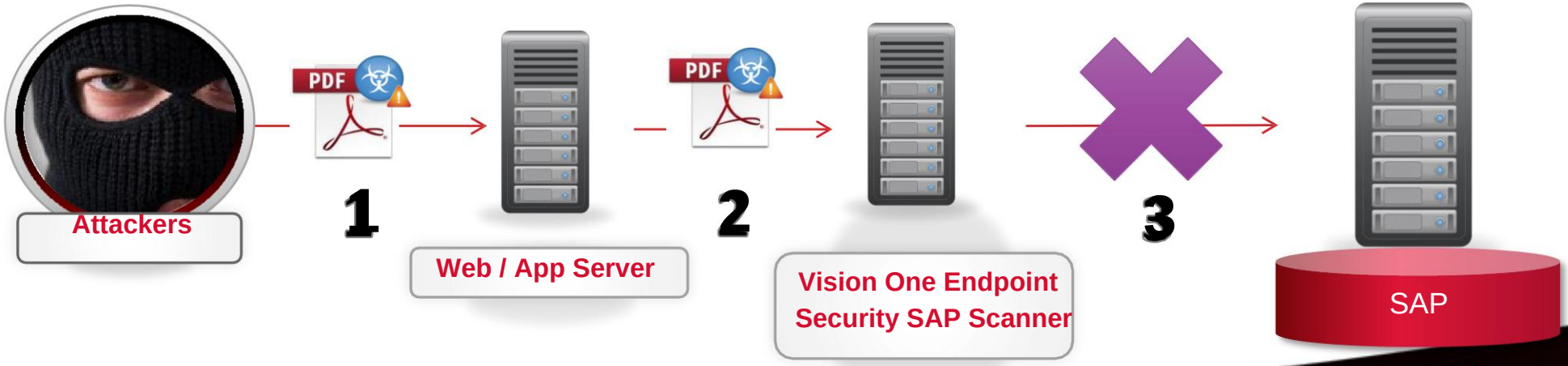
Machine Translated by Google

How do we help in SAP environments?

Before



After





Thank you!!!

©2023Trend Micro Inc.