Trend Micro Cloud One™

Cloud Security Simplified

Wuthikrai R.
Security Consultant, Trend Micro (Thailand) Co., Ltd.

The Perfect Storm for Cloud Security

Exploding set of cloud infrastructure services

Multiple teams making infrastructure & security decisions

DevOps increasing velocity of application delivery

More demanding compliance requirements

New vectors for breaches

Too many security tools

Strategic Priorities for Cloud Builders

Cloud Native Application Delivery

- Deliver fast, iterate often
- Infrastructure-as-code
- Code leverage: code re-use, open-source and public code repositories

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

Cloud Operational Excellence

- Repeatable & consistent
- Infrastructure and cost optimization
- Multi-cloud
- Manage risk

- Transition, not a cut-over
- Hybrid cloud is the norm

Cloud Migration

Trend Micro Cloud One™

Security Services Platform for Cloud Builders

Cloud Native Application Delivery

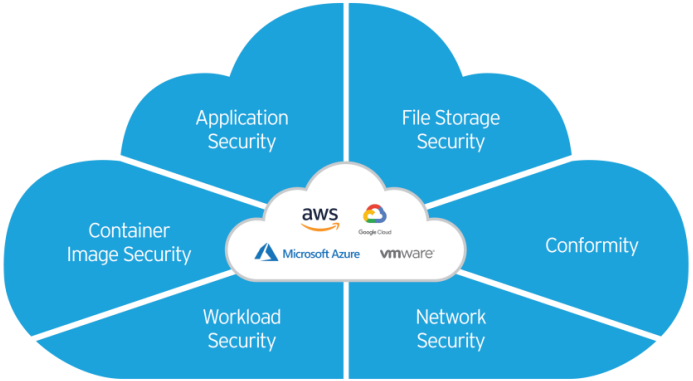
DevOps

Cloud Storage

Cloud Workloads

Containers

Serverless



Cloud Operational Excellence

Assurance

Governance

PCI GDPR NIST HIPAA

Compliance

Physical Virtual Cloud

Cloud Migration

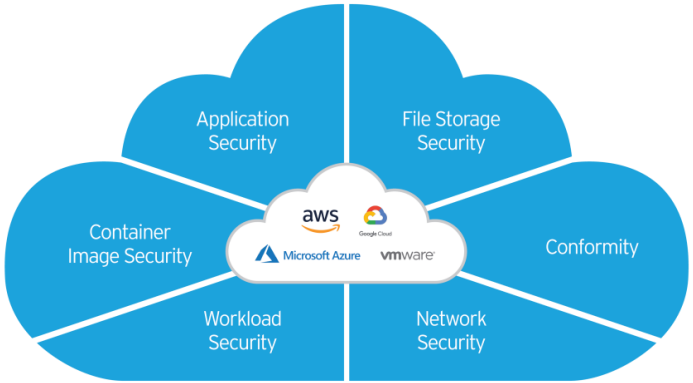
TREND MICRO™

Trend Micro Cloud One™

Security Services Platform for Cloud Builders

Platform:

- Single-sign-on
- Common user and cloud account enrollment
- One place for visibility
- Common procurement & billing
- Common support & documentation
- Expandable platform



Cloud-native, SaaS-based platform with the most extensive set of cloud security services

Trend Micro Cloud One™

Security Services Platform for Cloud Builders

Security for serverless functions, APIs, and applications

File scanning for cloud storage services

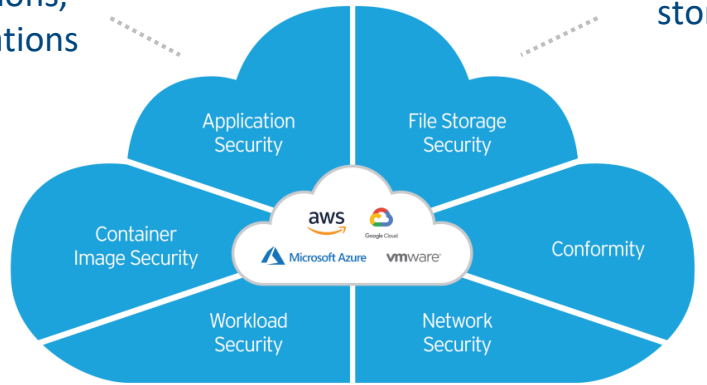


Image scanning in build pipeline

Assurance cloud infrastructure is configured securely

Runtime container and workload security

Network layer IPS to secure entire VPCs

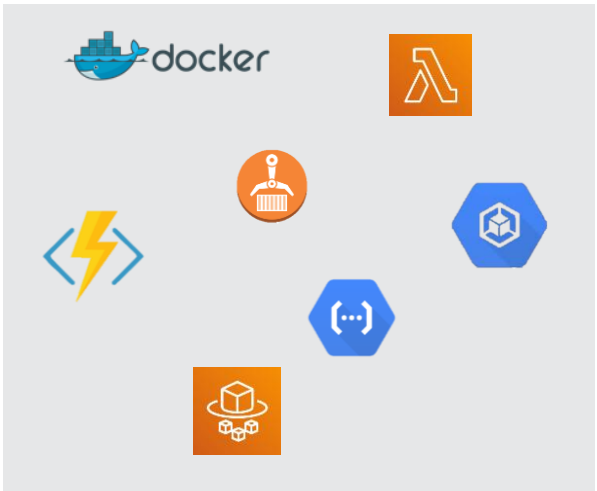
TREND MICRO | TippingPoint

TREND MICRO

Flexible to Give Your Builders Choice

Hybrid, Multi-cloud & Multi-service

70+ cloud services supported



Any Vintage of Application

from monolithic to containers to serverless

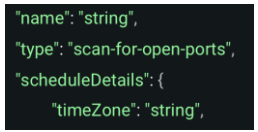
Broad Platform Support

Thousands of supported kernels with rapid updates

Automated to Help You Scale with Speed

Security-as-code lets DevOps teams build security into their build pipeline and release continuously & frequently
RESTful APIs: change policy, check status, automate reporting

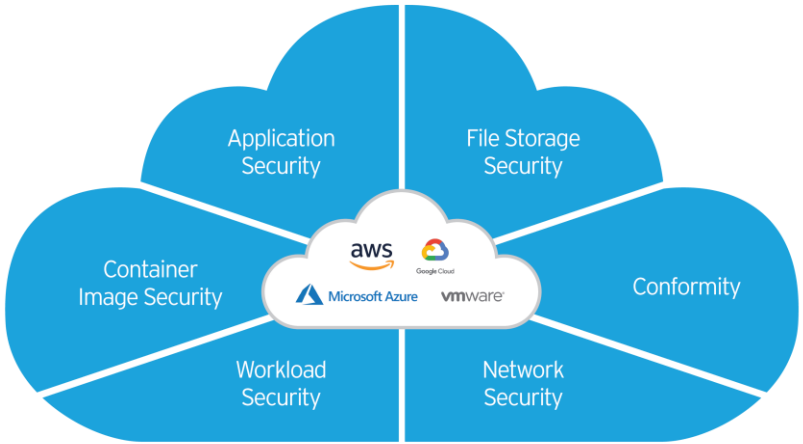
Built in automation: ex. automated deployment and discovery, auto-scaling, event-driven tasks



Quick-start templates to get your teams up and running quickly: Cloud Formation, ARM Templates, VMware.
Automation Center: sample code & scripts

Assuring cloud infrastructure is deployed securely and complies with regulatory standards: 600+ cloud best practices, NIST, HIPAA, PCI, GDPR etc.

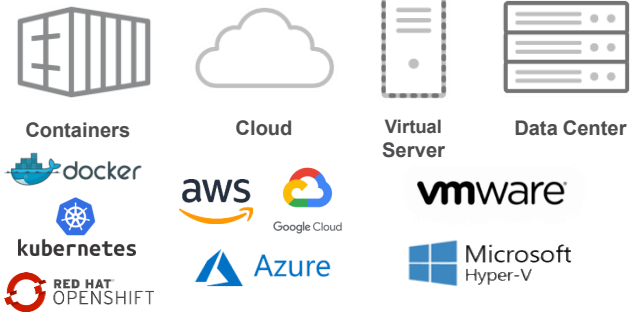
All-in-One to Minimize Complexity



- You can’t secure what you can’t see - visibility and control for your entire infrastructure
- Delivers tool and vendor consolidation
- Common user and cloud account enrollment
- Buy how you want: subscription and consumption options
- Buy where you want: AWS and Azure Marketplaces, preferred channel partner

Cloud One - Workload Security (VM Based)

Environments

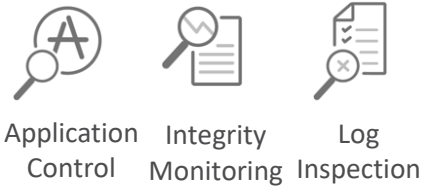


Platforms

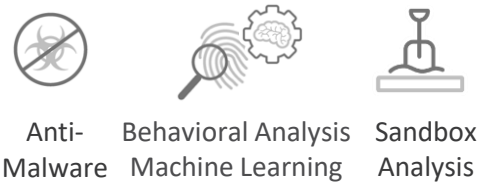
API & Integrations

Network Security

System Security

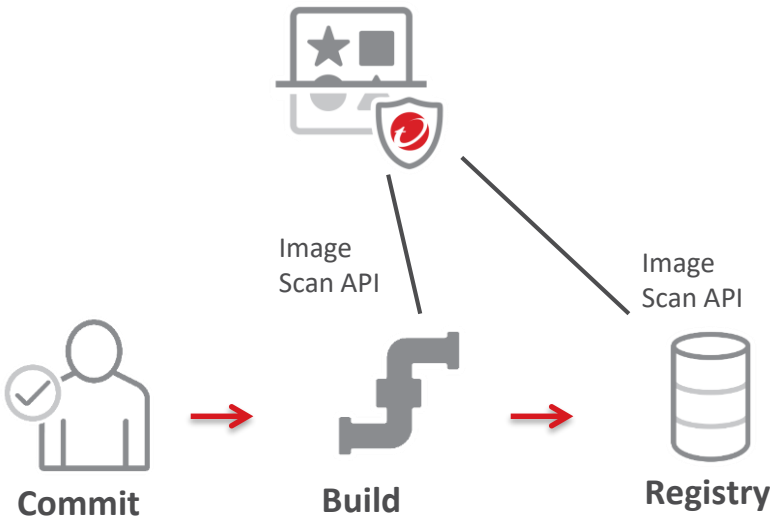


Malware Prevention



Runtime workload security for cloud workloads, containers & servers

Cloud One – Container Image Security (Container Based)



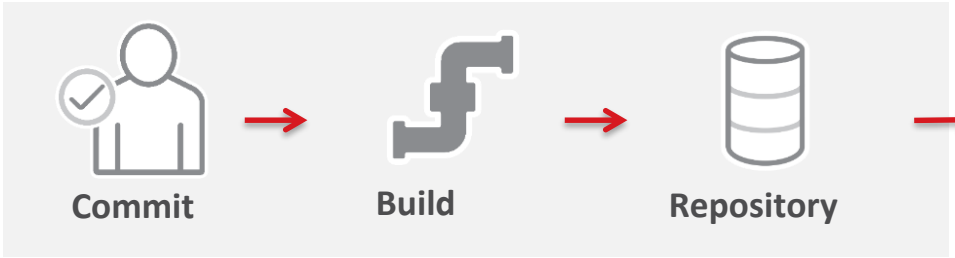
- Scans container images in the development pipeline
  - Vulnerabilities
  - Malware
  - Secrets & IOCs
  - Compliance (CIS, PCI, HIPAA)
- Build pipeline scan for earliest detection
- Registry scanning for recurring & latest threat intelligence
- Pipeline toolset integration via APIs

Software build pipeline image scanning

Container Security Enhancements

Cloud One – Container Image Scanning

Cloud One – Workload Security



Addition of Snyk open-source vulnerability rules NEW!

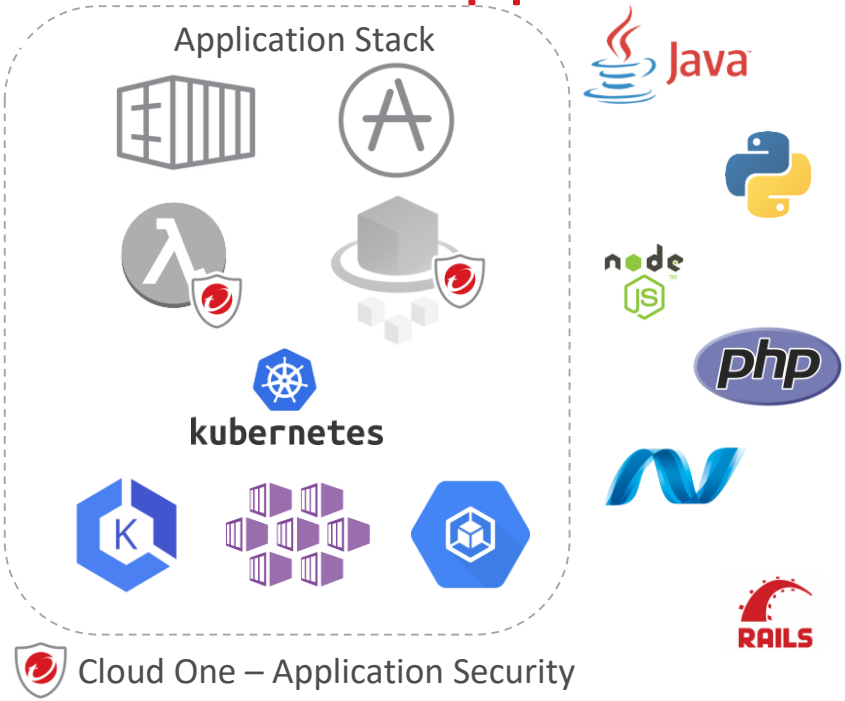
Admission Control NEW!

Compliance Validation NEW!

Security agent (deploys as a NEW!

Full lifecycle, full stack container security

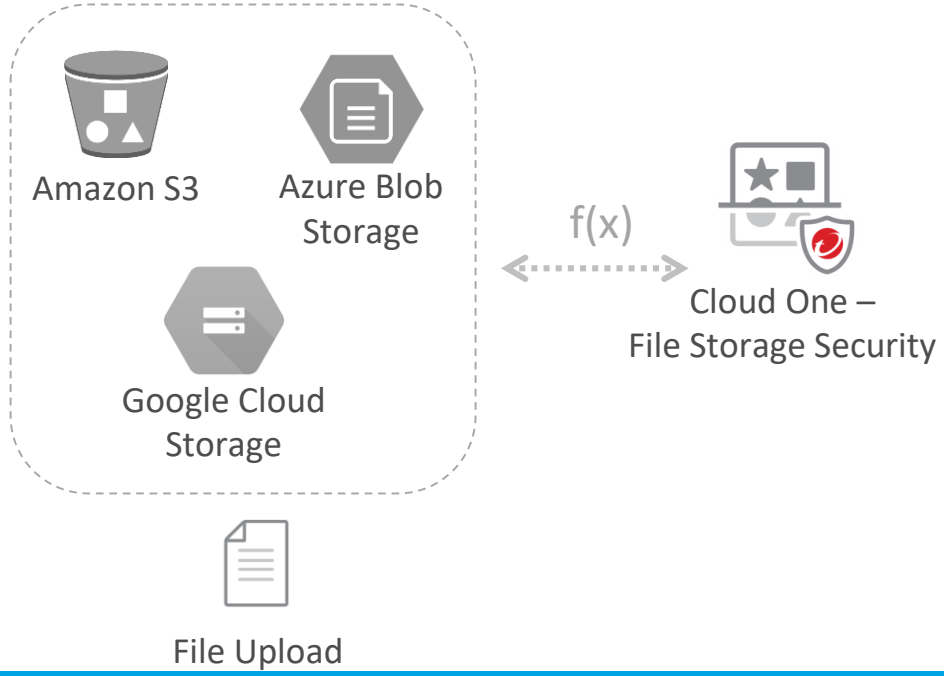
Cloud One – Application Security (Serverless)



- Protects against exploitation of vulnerabilities & data exfiltration
  - SQL injections
  - Remote command execution
  - Illegal file access, malicious payloads & URL redirects
- Minimal impact on performance and development streams – implement with 2 lines of code
- Visibility down to the line of code
- Broad platform support

Security for serverless functions, APIs, and web applications

Cloud One – File Storage Security (Cloud Storage)



- Multi-cloud storage support for Amazon S3, Azure Blob, Google Cloud Storage Service
- Advanced anti-malware
  - File reputation
  - Variant protection
  - Machine Learning
- Automated to scan whenever new files are are uploaded & APIs for custom actions

Advanced-malware scanning for cloud-based storage services

Cloud One – Conformity

Auto-check

Continuously check for adherence to best-practices & compliance standards – from build-pipeline to runtime

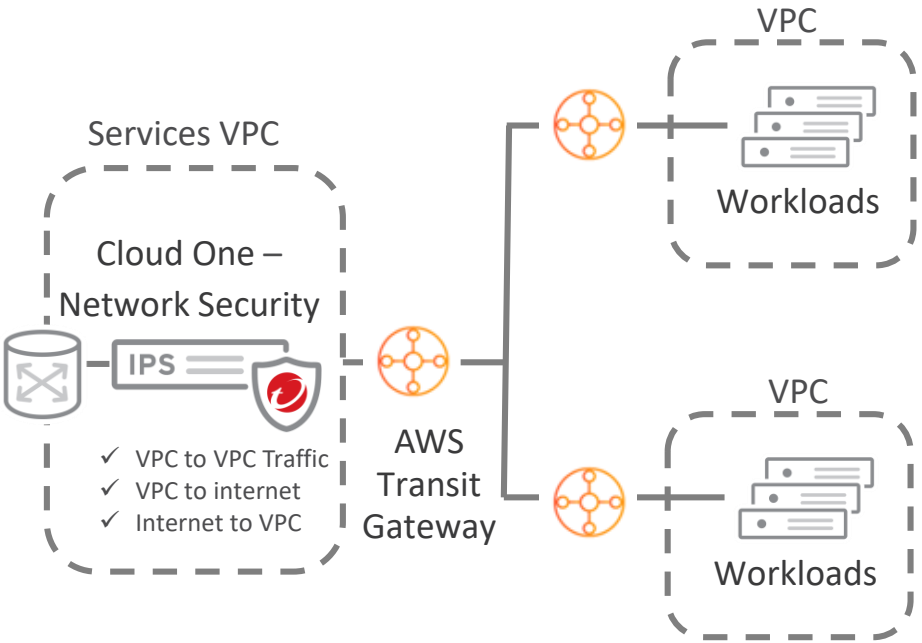
Auto-correct

Fix problems faster with self-healing and integration with devops workflows

- 70+ services supported across AWS & Azure
- Knowledge base of 600+ best practice rules for cloud configuration
- Built-in compliance for: AWS Well Architected Framework, PCI, HIPAA, NIST, GDPR, CIS
- Step-by-step remediation rules with 70+ controls with self-healing

Assurance cloud infrastructure is configured and deployed securely

Cloud One – Network Security



- Optimized and integrated to cloud network fabric for ingress and egress IPS inspection
- Virtual patching against vulnerabilities and active blocking of threats and C&C traffic
- Flexible options to deploy quickly and transparently inline without re-architecting
- Scales without deploying multiple instances for network-speed inspection up to 10 Gbps

Rapidly secure entire VPCs & cloud network segments

Security fueled by leading threat research

Cyber Threats | Vulnerabilities & Exploits | Targeted Attacks | 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

TREND MICRO™ | research

TREND MICRO

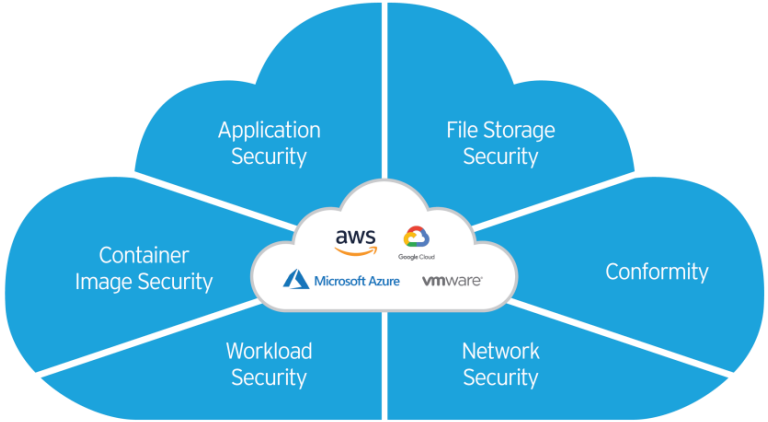
Trend Micro Cloud One™

Security Services Platform for Cloud Builders

Flexible.

Automated.

All-in-one.



Strategic Cloud Priorities

- Cloud migration
- Cloud-native application delivery
- Cloud operational excellence

Cloud Security Simplified


TREND MICRO
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.**