Trend Micro
Experienced, Innovative, Market Leader

14. September, 2020
A world safe for exchanging digital information

• Cybersecurity focused for 30+ years
• Profitable since going public in 1998, with over $1.5B in sales (FY2019)
• 500,000+ commercial customers
• 6700+ people passionate about security across 65+ countries

Eva Chen, CEO and Co-founder of Trend Micro
Continuous Industry Firsts

- Gateway scanning of SMTP, HTTP, FTP
- Optimized security for VMware®
- Optimized security for Microsoft® Azure™ workloads
- Cloud workload protection platform with integrated container security
- Specialized IPS for OT
- Broadest cloud security platform as a service

- LAN security for Microsoft & Novell
- Specialized security data center servers
- Optimized security for Microsoft® Azure™ workloads
- IoT Reputation Service
- AI-based writing-style DNA analysis for email fraud
- XDR with endpoint, email, servers, & network combined

Overview

Managed XDR

One Console
One Alert Schema
Fewer, higher fidelity, actionable alerts
Guided investigation

Correlation
Artificial Intelligence, Big Data Analytics
Detection rules by our Security

Network Defense
Hybrid Cloud Security
Visibility & Investigation
User Protection
Today's challenges!
Infrastructure change...
Generation Conflict?
Example 1
Cloud Migration

- Ransomware
- Unpatched OS
- Communication with C&C Server
Example 2
Cloud Native Applications

Vulnerabilities in open source code & the code you write

3rd party App Vulnerability

SQL Injection

File Storage

Malicious File

File Upload

Development

Commit

Code Repository

Build

Build Automation

Push
Example 3
Cloud Operational Excellence (CCoE)

- Cross-account access to repository
- Open storage on internet
- Serverless
- Container Services
- Orchestration
- Workloads
- Monitoring
- Encryption
- Keys not rotated frequently enough

Misconfigured Cloud Formation templates

Development

Commit

Source Code Repository

Build

Build Automation

Push

Developers
Trend Micro Cloud One™
The Perfect Storm for Cloud Security

Exploding set of cloud infrastructure services

DevOps increasing velocity of application delivery

Multiple teams making infrastructure & security decisions

More demanding compliance requirements

Too many security tools

New vectors for breaches

More demanding compliance

© 2020 Trend Micro Inc.
Strategic Priorities for Cloud Builders

Cloud Native Applications
- Deliver fast, iterate often
- Infrastructural as-code
- Leverage: code reuse, open-source and public code repositories
- Containers
- Serverless

Cloud Workloads
- Physical
- Virtual
- Cloud

Cloud Storage

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

Cloud Operational Excellence
- Repeatable & consistent
- Infrastructure and cost optimization
- Multi-cloud
- Cloud Center of Excellence (CCoE)

Cloud Migration
- Transition, not a cut-over
- Hybrid cloud is the norm
- Physical, Virtual, Cloud
Trend Micro Cloud One™

Security Services Platform for Cloud Builders

Cloud Native Applications

- DevOps
- Cloud Workloads
- Containers
- Cloud Storage
- Serverless

Cloud Operational Excellence

- Assurance
- Governance
- Risk & Compliance

Cloud Migration

- Physical
- Virtual
- Cloud
Trend Micro Cloud One™

Security Services Platform for Cloud Builders

Platform:
- Single-sign-on
- Common user and cloud account enrollment
- Common procurement & billing
- Common support & documentation
- Expandable platform

File scanning for cloud storage services

Assurance cloud infrastructure is configured securely

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

(Formerly Deep Security as a Service)
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
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 Migration

OPERATIONAL CHALLENGES

- Hybrid & multi-cloud
- Central visibility
- Performance
- Windows relevance
- Evolving existing security processes

- Ransomware
- Unpatched OS
- Communication with C&C Server
Cloud One – Workload Security

**Environments**
- Containers
- Cloud
- Virtual Server
- Data Center

**Platforms**
- Windows
- Linux

**API & Integrations**
- Ansible
- Chef
- Puppet
- ServiceNow
- Splunk

- Unified protection & incident response
  - Vulnerabilities (IDS/IPS) & lateral movement, Firewall
  - Integrity Monitoring, application control & log inspection
  - Malware & ransomware (w/ behavioral & machine learning)
- Automated deployment, APIs and integrations
- Accelerate compliance
- Broad platform & environment support

Runtime workload security for cloud workloads, containers & servers
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
Cloud Native Applications

Vulnerable Container Images

Container Registry

Vulnerabilities in open source code &

3rd party App Vulnerability

OPERATIONAL CHALLENGES

- Security slowing devops down
- Automation in CI/CD pipeline
- Too many tools
- Heavy use of Linux

Developers

Code Repository

Build Automation

SQL Injection

File Storage

File Upload

Serverless

Containers

Workloads

File Storage

Vulnerable Container Images

3rd party App Vulnerability
Cloud One – Container Security

- 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
Cloud One – Application Security

- 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

- 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 uploaded & APIs for custom actions

Advanced-malware scanning for cloud-based storage services
Cloud Operational Excellence (CCoE)

OPERATIONAL CHALLENGES

- Rapid growth in new cloud services
- Learning curve for proper configuration
- Many teams using cloud services
- Lack of visibility
- Proving compliance

MISCONFIGURED CLOUD FORMATION TEMPLATES

- Cross-account access to repository
- Serverless
- File Storage
- Open storage on internet
- Keys not rotated frequently enough

- Container Services
- Orchestration
- Monitoring
- Encryption

WORKLOADS

- Development
- Encryption
- Cross-account access to repository
- Open storage on internet

- Keys not rotated frequently enough

- Development
- Encryption
- Cross-account access to repository
- Open storage on internet

- Keys not rotated frequently enough
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
Hybrid Cloud Security Offerings

Trend Micro Cloud One
Cloud native, Saas-based platform

Deep Security as a Service

Deep Security Software

Workload Security
Container Image Security
File Storage Security

Deep Security Smart Check
Deep Security Smart Check
Deep Security Smart Check
Trend Micro deployment shifts over time—from on-premises to SaaS-based solutions. Created with real data by artist Stefanie Posavec.
Appendix
Market Leader in Vulnerability Disclosure

Zero Day Initiative

• 3500+ independent vulnerability researchers
• Discovered over half the vulnerabilities in 2018

Source: IHS Markit, 2018 Public Vulnerability Market
Trend Micro has been named a leader with highest score in current offering and strategy categories in The Forrester Wave™: Cloud Workload Security, Q4 2019

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.

Source: The Forrester Wave™: Cloud Workload Security, Q4 2019 by Andras Cser with Merritt Maxim, Matthew Flug, and Peggy Dostie
Trend Micro’s assessment shows that we deliver the most cloud security controls and criteria.


GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved. 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 designations. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.
#1 market share for Hybrid Cloud Workload Security with 35.5%

FREE! Phishing Awareness Service

Send users a realistic phishing campaign

Analyze the results

Raise user awareness with training

https://phishinsight.trendmicro.com
Cyber Risk Index
Find out how prepared you are for cyber attacks

FREE Cyber Risk Awareness Tool
Assess your organization’s cyber preparedness, experience, and future outlook

http://www.trendmicro.com/cyberrisk
Cybersecurity Assessment Service

Free security assessment service that scans Microsoft® Office 365® inboxes and endpoints to gauge the overall security posture

A simple way for a security professional to:
• Check their Office 365 inboxes for undiscovered email threats
• Check key endpoints for undiscovered threats
• Review a final report in PDF form and share with stakeholders outlining any threats existing in their environments

https://assessment.xdr.trendmicro.com