XGen™ Security for an Evolving IT and Threat Landscape

Eva Chen
CEO and Co-Founder
February, 2017
Requires Several Aspects of a Security System

**Security Management**
- Real-time view of events and incidents
- Event analytics
- Incident management
- Audit and reporting

**Threat Defense**
- Adapting to evolving hacker behavior and techniques
- Balance between detection and false positives

**Policy Enforcement**
- Network traffic and rule enforcement
- Set and forget
- “Block” or “Pass”
Strategy: Purpose-Built Solutions Per Segment

Consumer  
Small Business  
Enterprise  
Very Large Enterprise
Challenge: Rapid Change

- Shifts in IT Infrastructure
- Changes in User Behavior
- Emergence of new Threats
Result: Huge Increase in Threat Volume/Variety

Business Email Compromise attacks on the rise; average payout is large at US $140k

Sources: Trend Micro Research, and “The Next Tier”, Trend Micro Threat Predictions for 2017
65% had zero-day or unknown malware
90% had active Command and Control in their networks
80% had network attacks or exploits

Source: Trend Micro Live proof of concepts with 263 organizations, 2016
A War Between Defenders and Attackers

Water shapes its course according to the nature of the ground over which it flows; the soldier works out his victory in relation to the foe whom he is facing.

Therefore, just as water retains no constant shape, so in warfare there are no constant conditions.

- Sun Tzu, The Art of War
Formula for Success Must be ‘Cross-generational’

\[ x = I + U - T \]

Anticipate shifts in IT Infrastructure

Embrace changes in User Behavior

Adapt protection for new Threats
Anticipated Key Shifts Well with Number of Firsts!

- LAN Server Security
- MSN Hotmail Protection
- Integrated Virtualization Security
- Cloud Computing Security
- Network Defense
- Leading Consumer Anti-Virus
- Gateway Security
- Smart Protection Network
- Advanced Threat Detection


Novel Check Point VMware Amazon web services Microsoft Azure
Continuous Innovation of Threat Defense Techniques

- Anti-malware
- Anti-spyware
- Personal Firewall
- Host-based IPS & Firewall
- Encryption & DLP
- Web/File Reputation
- Integrity Monitoring
- White-listing
- Variant Protection
- Behavior Analysis
- Exploit Prevention
- Census Check
- Sandbox Analysis
- App Control
- Investigation & Forensics (EDR)
- Network IPS
- DDoS Protection
- DGA Defense
- High-Fidelity Machine Learning
- Ransomware Remediation
- Encryption & DLP
- Integrity Monitoring
- White-listing
- Variant Protection
- Behavioral Analysis
- Exploit Prevention
- Census Check
- Sandbox Analysis
- App Control
- Investigation & Forensics (EDR)
- Network IPS
- DDoS Protection
- DGA Defense
- High-Fidelity Machine Learning
- Ransomware Remediation
Fueled by Market-leading Threat Intelligence: Now Including World’s Best Zero-day Vulnerability Research

- 450+ vulnerabilities 1H 2016
- Average of 57 days zero-day filter coverage before public disclosure

DVLabs
Delivering the best protection against the full range of KNOWN and UNKNOWN threats
SMART
Maximizes protection
OPTIMIZED

Minimizes IT impact
CONNECTED

Speeds time to protect, detect and respond
SMART: Unique Blend to Protect Endpoints

- Web & File Reputation
- Exploit Prevention
- Application Control
- Variant Protection

Safe files allowed

Malicious files blocked

Legend:
- Known Good Data
- Known Bad Data
- Unknown Data
- Noise Cancellation

NEW!

Pre-execution Machine Learning
Behavioral Analysis
Runtime Machine Learning

SMART: Unique Blend to Protect Endpoints
2,300+ new customers in 2016

1,200+ new customers in 2016

15k+ new customers in 2016

1. Includes both new Deep Discovery and TippingPoint customers
2. Does not include Worry-Free or CloudEdge customers
MARKET SHARE LEADER
in corporate server security for the 7th straight year!

Gartner Magic Quadrant for Endpoint Protection Platforms
January 2017

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 construed 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.

Gartner Magic Quadrant for Intrusion Detection and Prevention Systems
January, 2017

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 http://www.trendmicro.com/us/business/cyber-security/gartner-idps-report/

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 construed 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.

RECOMMENDED
Breach Detection System
3 YEARS IN A ROW

99.8% Detection Rate

TippingPoint
RECOMMENDED
Next-Generation IPS

99.5% Security Effectiveness
Consumer Business: Priorities for Growth

- Strengthen our support services to grow and retain consumer base; premium services with big data intelligence
  - Although PCs are in decline, there are still 20M PC units shipping monthly!

- Capture NEW opportunities like securing consumer IoT
What is Next?
More Points of Protection Needed

I
- Evolved cloud computing (e.g. containers)
- IoT

U
- Privacy concerns
- Adoption of IoT
- Even more mobile

T
- Ransomware continues
- Cyber-propoganda
- IoT hijacking
Trend Micro IoT Initiatives Gaining Speed

- **2012**: SafeLock lockdown solution released
- **2014**: Deep Discovery network detection
- **2015**: ASUS partnership for home routers
- **2015**: TUTK ThroughTek partnership
- **2015**: vCPE on NFV showcase w/ NXP
- **2016**: Launch of solution for IoT / IoV
- **2016**: Microsoft Partnership & SDK release
- **2012-2015-2016**: Partnership & SDK release

---

**NFV DPI showcase with ADLINK intel**

**Mirai DDOS attack**
Trend Micro IoT Security Deployment Cases

Public Cloud
- Deep Security SaaS (AWS, Azure)
- Home Security Box
- Secure SDK
- Secure SDK

Private Cloud
- Deep Security on-premises
- TippingPoint Cloud Edge
- Secure SDK

Hybrid Cloud
- Deep Security
- Edge Security With NFV/SDN
- Secure SDK
Protecting Customers Now and In the Future!

\[ x = I + U - T \]

**Anticipate**
shifts in IT Infrastructure

**Embrace**
changes in User Behavior

**Adapt**
protection for new Threats