Leaders in Threat Protection Services
Securing over $2.0 Trillion in Assets

- Founded 2001
- 450 Clients with Extensive IP in Heavily Regulated Industries
- 99.6% Customer Loyalty

Typical Customer Attributes
- 50-25,000 employees
- 1–20 global offices
- 1-25 sensors/customer
- $250M to $160B AuM

- High value assets
- High Risk Sensitivity
- Min. in-house skills
You Will Be Hacked.
Looking for a New Category

INCUMBENT CATEGORY

MSSP

Threat Management

Device Management

INSTABILITYITY & JOCKEYING

Security model is broken

Value dissonance: spend vs. secure

Opportunity to nudge industry in our direction

EMERGENT TERMINOLOGY

CONVERGENCE

Analyst Definitions

New Market Entrants

Incumbent Vendor Repositioning

CMaaS/CTP

CONVERGENT POSITIONING

Follow Us @eSentire
Copyright © eSentire 2014
Gartner Cross-silo Architecture

MSSP
Managed Security Services

CMaaS
Continuous Monitoring

C-ATP
Active Threat Protection

Security model is broken

Value dissonance: spend vs. secure

Analyst Definitions

Follow Us @eSentire
Copyright © eSentire 2014

4 November 2014
2014 Gartner discovers a new security approach called continuous advanced threat protection.
The Risks to Enterprise

**THREAT ACTORS**
- Hacktivists/Activists
- Terrorists
- Nation state-sponsored
- Organized Criminals
- Smash-&-Grab Criminals
- Insiders

**TARGETS**
- Intellectual property (IP)
- Website Brand Damage
- Mergers and acquisition (M&A) insider information
- Credentials to bank accounts
- Industry-sensitive documents and information

**ATTACKS**
- Socially engineered emails/calls
- Phishing scams (emails with infected links)
- Infected media
- Stolen mobile devices
Over the past 12 months, the SOC has identified:
- 100% increase in Spear Phishing attacks
- 10% increase in DriveByDownload attacks
- 20% increase in focused Scans/Brute Force attacks
Attacks Often Remain Undetected

78% Initial Intrusions Rates as LOW Difficulty

66% Took MONTHS or More to Discover

69% Discovered by EXTERNAL Parties

40% Used Some Form of MALWARE
Security Technology Spend Doubled in 10 Years

Gartner

$60B
2012

$67B
2013

$86B
2016

$46 Billion Globally in 2013

$0 $5 $10 $15 $20 $25 $30 $35 $40 $45 $50


4 November 2014

Follow Us @eSentire
Copyright © eSentire 2014

Slide 10
Traditional Security Approaches

PERIMETER DEFENSE

ASSETS & DATA
Traditional Security Approaches

- Malware Detection
- User ID and Password
- Data
- Router
- Firewall

Follow Us @eSentire
Copyright © eSentire 2014
Traditional Security Approaches

- Data
- Host Virtualization
- IDS
- Router
- Firewall
- PKI
- Malware Detection
- User ID and Password
- VPN
Hard Tokens
Containerization
Virtualization
VPN
PKI
Malware Detection
User ID and Password

Data
SW & HW Certificates
IPS
Packet Inspection
SSL
Host Virtualization
IDS
Router
Firewall
Gartner Security Findings

Signatures are dead is misguided hyperbole

Detection and Response > Blocking and Prevention

Incident Response is the wrong mindset

Protection is integrated service NOT siloed offerings

Monitoring and Analytics are at the core of all next-generation Security platforms
## Legacy Security Is No Match for Targeted Attacks

### INDISCRIMINATE
Malware | SPAM | DoS

### TACTICAL
Compliance-based | Reactionary

<table>
<thead>
<tr>
<th>PHILOSOPHY</th>
<th>Perimeter (multiple, dislocated)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOCUS</td>
<td>Protect all systems</td>
</tr>
<tr>
<td>DETECTION</td>
<td>Signature-based technology</td>
</tr>
<tr>
<td>AWARENESS</td>
<td>Headline news</td>
</tr>
<tr>
<td>RESPONSE</td>
<td>Shut down/wipe compromised systems</td>
</tr>
</tbody>
</table>

*Architecture attributed to IBM*
Legacy Security
Is No Match for Targeted Attacks

**INDISCRIMINATE**
Malware | SPAM | DoS

**TARGETED**
Advanced | Persistent | Organized | Motivated

**Threats are evolving from nuisance to targeted attacks**

<table>
<thead>
<tr>
<th>PHILOSOPHY</th>
<th>TACTICAL</th>
<th>STRATEGIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perimeter (multiple, dislocated)</td>
<td>Compliance-based</td>
<td>Assume constant compromise</td>
</tr>
<tr>
<td>Protect all systems</td>
<td>Reactionary</td>
<td>Prioritize high-risk assets</td>
</tr>
<tr>
<td>Signature-based technology</td>
<td></td>
<td>Behavioural-based technology &amp; methods</td>
</tr>
<tr>
<td>Headline news</td>
<td></td>
<td>Consume real-time threat feeds</td>
</tr>
<tr>
<td>Shut down/wipe compromised systems</td>
<td></td>
<td>Quarantine, gather and preserve forensics</td>
</tr>
</tbody>
</table>

*Architecture attributed to IBM*
Gartner C-ATP Architecture

PREDICT
- PROACTIVE EXPOSURE ASSESSMENT
- PREDICT ATTACKS
- BASELINE SYSTEMS
- REMEDIATE/MAKE CHANGES
- DESIGN/MODEL CHANGE
- INVESTIGATE/FORENSICS

PREVENT
- HARDEN AND ISOLATE SYSTEMS
- DIVERT ATTACKERS
- PREVENT INCIDENTS
- DETECT INCIDENTS
- CONFIRM AND PRIORITIZE
- CONTAIN INCIDENTS

RESPOND

CONTINUOUS MONITORING & ANALYTICS

Follow Us @eSentire
Copyright © eSentire 2014
Gartner C-ATP Full Lifecycle Protection

**Predict**
- Proactive Exposure Assessment
- Predict Attacks
- Baseline Systems
- RemEDIATE/MAKE CHANGES
- Design/Model Change
- Investigate/Forensics

**Prevent**
- Harden and Isolate Systems
- Divert Attackers
- Prevent Incidents
- Detect Incidents
- Confirm and Prioritize
- Contain Incidents

**Respond**
- Continuous Monitoring & Analytics

**Detect**
- Detect Incidents
- Confirm and Prioritize
- Contain Incidents
Gartner Five Styles of Defense

- **TIME**
  - REAL-TIME/NEAR REAL-TIME
  - POST COMPROMISE

- **WHERE TO LOOK**
  - NETWORK
  - PAYLOAD
  - ENDPOINT

- **DETECTION**
  - STYLE 01 Network Traffic Analysis
  - STYLE 03 Payload Analysis

- **RESPONSE**
  - STYLE 02 Network Forensics
  - STYLE 04 Endpoint Behavior Analysis
  - STYLE 05 Endpoint Forensics
Continuous Monitoring at All Layers

NETWORK

APPLICATION FRONT END

APPLICATION BACK END

ENDPOINT

INFORMATION

PEOPLE
### Paradigm Shift in Security

<table>
<thead>
<tr>
<th>OLD MINDSET</th>
<th>NEW REALITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIGNATURES</td>
<td>ALGORITHMS</td>
</tr>
<tr>
<td>POINT SOLUTIONS</td>
<td>PLATFORMS - CORRELATE</td>
</tr>
<tr>
<td>FIXED PERIMETERS</td>
<td>ADAPTIVE PERIMETERS</td>
</tr>
<tr>
<td>OWNERSHIP = TRUST</td>
<td>REPUTATION SERVICES</td>
</tr>
<tr>
<td>SECURITY APPLIANCES</td>
<td>SECURITY SOFTWARE</td>
</tr>
<tr>
<td>SOLUTION SILOS</td>
<td>ADAPTIVE SYSTEMS</td>
</tr>
<tr>
<td>SECURITY APPLIANCES</td>
<td></td>
</tr>
<tr>
<td>MANUAL POLICY CONFIG</td>
<td>AUTOMATION</td>
</tr>
<tr>
<td>BLOCK/PREVENT</td>
<td>DETECT/RESPOND</td>
</tr>
<tr>
<td>INCIDENT RESPONSE</td>
<td>CONTINUOUS RESPONSE</td>
</tr>
<tr>
<td>PROTECT NETWORK/DEVICES</td>
<td>PROTECT INFORMATION</td>
</tr>
</tbody>
</table>

Follow Us @eSentire
Copyright © eSentire 2014
Gartner Recommendations

- Spend less on prevention and more on detection and response
- Use Gartner’s 12 Critical Capabilities Framework
- Shift from Incident to Continuous Response
- Develop a SOC to provide continuous monitoring
- Continuous Monitoring at all layers
The Case for Active Threat Protection

TECHNOLOGY

» Ever changing threat landscape
» ‘Set and forget’ is a myth

PEOPLE

» Recruiting: scarce talent pool
» Retaining: highly competitive market

PROCESS

» Infrastructure, process dev/adherence
» Costly to build and maintain

Follow Us @eSentire
Copyright © eSentire 2014
A Final Thought...

Chief Security Officer

Follow Us @eSentire
Copyright © eSentire 2014
Gartner C-ATP | PREVENT

PREVENT
- HARDEN AND ISOLATE SYSTEMS
- DIVERT ATTACKERS
- PREVENT INCIDENTS

PREDICT
- PROACTIVE EXPOSURE ASSESSMENT
- PREDICT ATTACKS
- BASELINE SYSTEMS
- REMEDIATE/MAKE CHANGE
- DESIGN/MODEL CHANGE
- INVESTIGATE/FORENSICS RESPOND

PREDICT
- EXPOSURE ASSESSMENT
- ATTACKS
- BASELINE SYSTEMS
- REMEDIATE/MAKE CHANGE
- DESIGN/MODEL CHANGE
- INVESTIGATE/FORENSICS RESPOND

PREVENT
- HARDEN AND ISOLATE SYSTEMS
- DIVERT ATTACKERS
- PREVENT INCIDENTS

CONTINUOUS MONITORING & ANALYTICS
- DETECT INCIDENTS
- CONFIRM AND PRIORITIZE
- CONTAIN INCIDENTS
- DETECT

AUTOMATIC BLOCKS BASED ON IOCS
INBOUND PATIENT ZERO PROTECTION
SIGNATURE-BASED PREVENTION
DYNAMIC REPUTATION DEFENSE
MANAGED WHITELISTING

Follow Us @eSentire
Copyright © eSentire 2014
Gartner C-ATP | PREVENT

PREVENT
HARDEN AND ISOLATE SYSTEMS
DIVERT ATTACKERS
PREVENT INCIDENTS

PREDICT
PROACTIVE EXPOSURE ASSESSMENT
PREDICT ATTACKS
BASELINE SYSTEMS

REMEDIATE/MAKE CHANGE
DESIGN/MODEL CHANGE
INVESTIGATE/FORENSICS
RESPONSE

CONTINUOUS MONITORING
ANALYTICS

DETECT INCIDENTS
CONFIRM AND PRIORITIZE
CONTAIN INCIDENTS
DETECT

eSentire CAPABILITIES
SANDBOX/MALWARE DETONATION
BEHAVIOR-BASED DETECTION
ZERO-DAY EVENTS
IMMEDIATE AUTOMATIC & SOC-BASED CONTAINMENT AND REPORTING
BEHAVIOR-BASED SIGNATURE UPDATING

Follow Us @eSentire
Copyright © eSentire 2014
Gartner C-ATP | PREVENT

PREDICT
- PROACTIVE EXPOSURE ASSESSMENT
- PREDICT ATTACKS
- BASELINE SYSTEMS

REMEDIATE/MAKE CHANGES
- DESIGN/MODEL CHANGE
- INVESTIGATE/FORENSICS
- RESPOND

PREVENT
- HARDEN AND ISOLATE SYSTEMS
- DIVERT ATTACKERS
- PREVENT INCIDENTS

CONTINUOUS MONITORING & ANALYTICS
- DETECT INCIDENTS
- CONFIRM AND PRIORITIZE
- CONTAIN INCIDENTS

RESPOND
- DETECT

Follow Us @eSentire
Copyright © eSentire 2014
TRAP

Targeted

Retrospection

Analytics

Platform

Follow Us @eSentire
Copyright © eSentire 2014
Targeted Retrospection

MAX

MIN

INTRO

DISCOVERY

DISCLOSURE

PATCH AVAILABILITY

PATCH DEPLOYMENT

PATCH COMPLETION

NOW

DANGER ZONE

Follow Us @eSentire
Copyright © eSentire 2014