ENDPOINT SECURITY – A MARKETPLACE OF SILVER BULLETS?

Fernando Montenegro
Senior Industry Analyst, Information Security
451 Research
@fsmontenegro
DISCLAIMER
Why are we here?

Help you become a better informed consumer.

---

Top Security Pain Points
Information Security Respondents

Q1. What are your organization’s top information security pain points? Please select up to three.

- User Behavior: 34.1%
- Staffing Information Security: 21.0%
- Lack of Budget: 20.4%
- Security Awareness Training (Ineffectiveness or Difficulty): 19.0%


Percent of Sample
n = 495
Methodology

451 Voice of the Enterprise

60,000+ members

- Quarterly insights:
  - Budgets & Insights
  - Workloads & Projects
  - Organizational Dynamics
  - Vendor Evaluations

Briefings, Inquiries, Research

- 100s of hours
  - Enterprise IT
  - Service Providers
  - Security vendors
  - Finance professionals
  - Qualitative research
  - Independent
Poll:

- How many endpoint vendors here at RSA?
- How many endpoint vendors in the market overall?
Economics in 60 seconds

- Information Asymmetry & Insufficiency
- Signaling and Screening
- Market for Silver Bullets
- Herding & “best practices”

<table>
<thead>
<tr>
<th>Seller Has Information</th>
<th>Buyer Has Information</th>
<th>Buyer Lacks Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seller Lacks Information</td>
<td>Limes (Insurance)</td>
<td>Silver Bullets (Security)</td>
</tr>
<tr>
<td>Seller Has Information</td>
<td>Perfect Market</td>
<td>Lemons (Used Cars)</td>
</tr>
</tbody>
</table>

“All models are wrong, but some are useful”

George Box

Endpoint definition

- Software deployed to laptop/notebook/desktop
  - Windows, MacOS, Linux
- Areas of interest
  - Malware and exploits
  - Executable content
  - System-level components/telemetry
- Servers are adjacent
- Mobile is adjacent... for now

Exclusions:
- Data Leakage/Loss Prevention
- Vulnerability Management
- Endpoint Authentication
- Proxy Agents
- ...
- Containers
Market Demand & Supply

451 VotE

<table>
<thead>
<tr>
<th>Category</th>
<th>Percent of Sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Govt/Educ</td>
<td>13.3%</td>
</tr>
<tr>
<td>10,000+ employees</td>
<td>18.8%</td>
</tr>
<tr>
<td>1,000-9,999 employees</td>
<td>18.4%</td>
</tr>
<tr>
<td>250-999 employees</td>
<td>11.6%</td>
</tr>
<tr>
<td>1-249 employees</td>
<td>38.0%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>38.0%</strong></td>
</tr>
</tbody>
</table>

n = 474

Traditional Enterprise: Symantec, Trend Micro, McAfee, Sophos, Kaspersky

SMB/Small-Medium Enterprise: Bitdefender, Avast, Malwarebytes, ESET, Panda, Comodo, ...

Recent entrants: Tanium, FireEye, Carbon Black, Cylance, Crowdstrike, Cybereason, Endgame, SentinelOne, ...

Focused offerings: Bromium, Avecto, Barkly, Guidance, Lastline, Minerva Labs, Ericom, Absolute, ...

Other enterprise: Cisco, Palo Alto, Check Point, Fortinet, RSA, Microsoft, IBM, Webroot, ...

≈ 120
Q: On a scale of 1 to 5, where 1 is ‘Very Ineffective’ and 5 is ‘Very Effective’, how would you rate your current suite of endpoint security tools against the following use cases?
451 Research Endpoint Market Map
Q20. How many endpoint security solutions are currently employed by your enterprise?

RSA 2018 Endpoint Vendors

- **Diamond**: ~65 vendors
- **Platinum**: ~65 vendors
- **Gold**: ~65 vendors
- **Silver**: ~12% of vendors
- **Bronze**: ~0% of vendors
- **Exhibitors**: ~0% of vendors
- **Early Stage...**: ~0% of vendors

Total vendors: ~65 vendors

**Endpoint Vendors (%)**
ENDPOINT SECURITY TECHNOLOGY
Danger! ML != Automation

Pipelines

Different models per use case

Where is it used
  — Static Analysis
  — Behavioral
  — User Interfaces (NLP)

How to test?
  — Ask process questions

“Typical” ML Pipeline: A tale of two worlds

Source: Netflix
Lifecycle

Prevention
- Avoid contact
- Reputation
- Content filtering
- Network integration
- App control
- Device control
- Cheap lookup
- File hashes

Protection
- Pre-execution checking
  - AI/ML
  - Network validation
  - Sandboxing
- Consider isolation
  - Virtualization
  - Remote execution

Detection
- Evidence of malicious behavior?
  - HIPS
  - App behavior...
- Targeted investigations
  - IoC
  - Timelines

Response
- Automated response
- Ad-hoc (remote) responses
- Rollback
- Remediation

Endpoint Detection and Response (EDR)
Technology - Prevention

- App control
  - Whitelisting, leverage cloud

- Device control

- Proxy/Gateway/Firewall integration
  - Reputation filtering

- Hash lookup
Technology - Protection

- “Funnel” mechanism
- Pre-execution ML
  - Static Analysis
- Reputation lookup
- Sandboxing
  - Local, Remote
- Autonomous operation
- Isolation
  - Virtualization
  - (Browser isolation)

Source: TrendMicro
Technology – Detection (\& Investigation)

- Detection automation
- Accelerated triage
- Ad-hoc search
- Static analysis
- Dynamic analysis (sandboxing)
- Threat intel integration
- Risk scoring

- Artifact reputation tracking
- Endpoint baseline definition and drift
- Application baseline definition and drift
- Heuristics filtering
- File-based metadata
- Full-disk inspection
- Routine vs incident data collection

Diagram:
- Endpoint
  - EDR + Local
- Enrichment
- Collection
- Analytics
- SOC, Reporting, Automation, ...
Technology - Response

- Automation!
- Rollback
- Remediation
- Quarantine
  - NAC, Firewall
  - Process Isolation
- Remote investigations
  - Remote console
- Data gathering
  - Forensics collection
- Deception
  - ‘Just in Time’ breadcrumbs
ENDPOINT TRENDS
Trends - Technology

Endpoint as “locus of control”

Base OS security improvements

Endpoint

Corp

Client

Home

Public

ISP

Source: ElectronicDesign
Trends – Customer and Product

Customer Trends
- “Assume breach” mentality
- Consolidation of use cases
- Quest for efficiency
  - Single agent
  - Cloud-based management
- Exploring new approaches, revisiting old ones
  - Browser Isolation, Deception, Micro-patching, Whitelisting

Product Trends
- Funnel approach
- “Kernels of truth”
  - Syscall behaviors
- ML/Artificial Intelligence widespread
- Security beyond work [HW]
Trends – Threat and Market

**Threat Trends**
- Ransomware
- Cryptominers
- Fileless attacks
- Worm-like delivery

**Market Trends**
- Widespread evolution
- EDR contested area
- More stringent testing
  - External testing
Trends - Testing

- External testing
- AMTSO
- VirusTotal
- MITRE ATT&CK
- Customer’s own testing
- HackerHurricane
- DerbyCon
- PinkTangent
- BlackHat
- (Engage VAR)
CONCLUSIONS
Conclusion

- Recognize noisy, inefficient market
- Break down technology
  - [Prevention], Protection, Detection, Response
- Recognize key trends
- Be a better consumer!
  - What do YOU need?

“Sunlight is the best disinfectant”

Justice Louis Brandeis

Apply What You Have Learned Today

- **Next week you should:**
  - Become familiar with MITRE’s ATT&CK Framework

- **In the first three months following this presentation you should:**
  - Ensure current endpoint is up to date (version and patches)
  - Identify threat profile of your organization
    - Collect information on what threats your organization actually sees

- **Within six months you should:**
  - Perform your own security testing of endpoint security solutions
References

- **Testing**
  - MITRE ATT&CK Framework - [https://attack.mitre.org/wiki/Main_Page](https://attack.mitre.org/wiki/Main_Page)
  - Hacker Hurricane – [https://www.youtube.com/watch?v=vBr3ur6bfQY](https://www.youtube.com/watch?v=vBr3ur6bfQY)

- **Market for Silver Bullets – Ian Grigg paper**

- **451 Alliance** - [https://www.451alliance.com/Apply.aspx](https://www.451alliance.com/Apply.aspx)
Q&A

@fsmontenenegro
Fernando.Montenegro@451research.com