Information Security Decisions

TechTarget

What's Supposed to Happen at the Endpoint Now?

Karen Scarfone
Principal Consultant
Scarfone Cybersecurity

events.techtarget.com

The State of Endpoint Protection

- Half of Information Security magazine's enterprise readers don't think the signature scanning approach works well anymore
  - Only 49% of malware was detected by antivirus software in 2012 (https://symantecevents.verite.com/29201/)
  - One in five readers thinks they won't be committed to static signature malware detection in five years
- 76% of intrusions involve "weak or stolen credentials"
  - Verizon's 2013 Data Breach Investigations Report (http://www.verizonenterprise.com/DBIR/2013/)
- Average U.S. data breach cost in 2012: $5.4 million
  - https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf
- Over 90% of surveyed organizations allow BYOD to some extent
  - http://www.ponemon.org/local/upload/file/2013 State of Endpoint Security WP_FINAL4.pdf

What Does This Mean for Endpoint Security?

- Conventional wisdom has become outdated
  - Antivirus, firewall are no longer enough
- Increased threats against mobile devices
  - Increased capabilities
  - Increased use
  - Increased target value
  - Increased attack vectors/vulnerabilities
- Time to reevaluate endpoint security controls

Agenda

- Endpoint protection software
- Additional endpoint-based security controls
- Network-based controls for endpoint security
- Conclusions

Endpoint Protection Software

- Antivirus software
- Application whitelisting
- Device control
- Endpoint data loss prevention (DLP)
- Enterprise mobile device management (MDM) *
- Host-based firewall
- Host-based intrusion detection/prevention system (IDPS)
- Storage encryption
- Vulnerability assessment

* MDM capabilities significantly overlap those of endpoint protection software

Endpoint Protection Software Vendors

- Arkoon Network Security
- Beyond Trust
- CheckPoint Software
- Eset
- F-Secure
- GFI Software
- IBM
- Kaspersky Lab
- LANDesk
- Lumension Security
- McAfee
- Panda Security
- Sophos
- Symantec
- Trend Micro

Antivirus Software

- Same capability that's been available for many years
- Best suited to detecting known instances of malware
- Still an important component of endpoint security
  - Detects 49% of malware (2012)
- Not nearly as effective as it used to be
  - Today's malware threats are highly customized and targeted
  - Often using social engineering instead of software vulnerability exploitation
- Primarily signature-based
  - Can't develop signatures for identifying the novel and unknown

Application Whitelisting

- Limits which applications may be installed and/or executed on an endpoint
- Only useful for environments that are able to tightly restrict what applications are to be used while still providing the necessary services to their users
- Can prevent the execution of known and unknown malware, as well as attack tools and other malicious software
- Can also prevent use of applications with known vulnerabilities that could be exploited to access sensitive data or otherwise gain unauthorized access to the endpoint

Device Control

- Sometimes referred to as port control
- Software that prevents unauthorized endpoint use of mobile devices and removable media
  - USB drives, CDs/DVDs, etc.
- Can prohibit all use of certain classes of mobile devices and/or removable media
- Can more granularly limit what types of data may be stored on them, often working closely in conjunction with endpoint DLP technology
- Can prevent the spread of malware, as well as preventing the sprawl of sensitive data to locations other than its origin

Endpoint Data Loss Prevention (DLP)

- One of the newest components of endpoint protection solutions
- Intended to stop inadvertent and intentional breaches of sensitive data
  - Social Security numbers and credit card numbers
  - Proprietary intellectual property
- Monitors an endpoint's storage to identify sensitive data
- Monitors an endpoint's use to identify actions involving sensitive data
  - Copying and pasting from a customer database to an email
- Can be run in a monitor-only mode or in an enforcement mode that stops attempted policy violations from succeeding

Enterprise Mobile Device Management (MDM)

- Geared toward controlling and protecting mobile devices
  - Primarily smartphones and tablets
  - Also laptops in some cases
- Traditionally provides some of the other security capabilities that endpoint protection software does, including endpoint DLP, device control, and storage encryption
- A suite of security controls to protect the sensitive data on an endpoint
- Establishes a secure sandbox for an organization's applications and data to be housed within
  - Helps to isolate them from other threats and vulnerabilities on the endpoint

Host-Based Firewall

- Also known as personal firewalls
- Been around almost as long as antivirus software
- Have lost effectiveness over the years as threats have changed
- Most of today's threats are at the application layer or the "human layer," not the network layer
- Still provides valuable protection to endpoints—by blocking unwanted connection attempts
- Doesn't stop the vast majority of threats against endpoints

Host-Based Intrusion Detection

- Functionality provided can vary greatly among implementations
  - Some analyze attempts to execute code on the endpoint
  - Some analyze the endpoint's incoming and outgoing network traffic
  - Some monitor the endpoint's filesystem
  - Some analyze the endpoint's logs
  - Most do combinations of two or more of these techniques
- Primary benefit of using host-based IDPS is to detect unknown threats based on their suspicious or unusual behavior

Storage Encryption

- Most commonly implemented form of storage encryption for endpoint protection software is full disk encryption (FDE)
- FDE fully encrypts the endpoint's storage media so that the data stored on it cannot be recovered when the endpoint is in an unauthenticated state (e.g., has been powered off)
  - Protects against a data breach should the device be lost or stolen
- Some endpoint protection software also provides forms of storage encryption other than FDE
  - File or disk encryption
  - Active when a host is booted
  - Only allow access to the sensitive data within them after proper authentication has been provided

Vulnerability Assessment

- Exact nature varies among endpoint protection solutions
- Fundamental idea is that it detects known vulnerabilities in the endpoint
  - Primarily its operating system and common applications (web browser, email client, etc.)
- Types of vulnerabilities it can detect may include missing patches, outdated software, and misconfigured security settings
- Has no capability to stop threats
- Can notify users and system administrators of security problems so that they can be addressed before exploitation occurs

Benefits of Endpoint Protection Software

- More effective and efficient prevention and detection
  - Less overhead, especially in parsing communications, files, etc.
  - Collaboration among security controls
  - Event correlation—identifying malicious events that no single security control can recognize on its own
- Eases deployment of new security technologies
- Reduces costs
  - Software licensing and supporting infrastructure
  - Single interface/management capability

Criticisms of Today's Endpoint Protection Software

- Replaces existing investments in point solutions
  - "Best in breed" solutions
- Offer newer, more advanced capabilities that organizations might not be ready for
- Few, if any, solutions that are fully integrated, fully capable
- Resource intensive
- Some capabilities missing
  - Patch management
  - Configuration management
  - Application-specific security controls

The Future of Enterprise Protection Software

- “53% of organizations in a recent Gartner survey already use a single vendor for several of these functions, or are actively consolidating products”
  - Gartner’s Magic Quadrant for Endpoint Protection Platforms
- Some functionality being built into OSs
- Increased capabilities
- Merging of endpoint protection software and MDM capabilities

Additional Endpoint Security Controls

- Patch management
- Configuration management
- Application-specific
  - Antispam
  - Web filtering
  - etc.

Benefits of Additional Endpoint Security Controls

- Patch and configuration management (vulnerability management)
  - Identify and correct known vulnerabilities to prevent their exploitation
  - Provide prevention capabilities not supported by endpoint protection software
  - Operational
- Application-specific
  - Applications have become a popular attack vector
  - Identify and stop known threats to prevent breaches
  - Provide detection capabilities not supported by endpoint protection software
- Reside within the endpoint, travel with it

Criticisms of Additional Endpoint Security Controls

- Stovepiped, not integrated

The Future of Additional Endpoint Security Controls

- Patch and configuration management likely to stay separate
  - Operational nature
  - Broader than just security
- Application-specific controls likely to be integrated into endpoint protection software
  - Some products already doing this
  - History of integrating point solutions

Network-Based Controls for Endpoint Security

- Network access control (NAC)
- Network-based firewalls
- Network-based intrusion detection
- Network-based vulnerability assessment
- Network-based DLP
- Network-based app-specific controls
  - Email, web security gateways

Benefits of Network-Based Controls

- Centralized management (configure once)
- NAC and other controls protect endpoints with security deficiencies (especially if their endpoint protection is lacking, e.g., BYOD technology)
- Take workload off endpoints

Criticisms of Network-Based Controls

- Do not protect mobile clients unless all mobile traffic is forced back through the organization's networks
- Lack of correlation between controls
- Lack of environment-specific knowledge (role of each host, etc.)
- Not as effective as host-based counterparts in some cases

The Future of Network-Based Controls

- Continued consolidation from the network down to the endpoint itself
- Future of NAC
- Shift toward anomaly-based detection methods

Conclusions

- Endpoint protection software is already the primary approach to providing prevention and detection capabilities for endpoints
- Security features provided by endpoint protection software continue to increase in breadth and depth
- The importance of network-based controls for endpoints (desktops, laptops, mobile devices) is declining

Thank You! Questions?

Karen Scarfone

karen@scarfonecybersecurity.com

http://www.linkedin.com/in/karenscarfone