To Secure Your Endpoints, You Better Take Steps!
Executive Summary
The days of relying on traditional antivirus protection to secure the jagged perimeter of endpoint devices are over. So what lies beyond? Today's endpoint security architecture requires a layered approach built on four key components. This study provides an overview of the greater endpoint security landscape, details four key areas that must be addressed, and provides predictions and recommendations for enterprises seeking to create, augment or replace their existing endpoint security stack.

Report Scope
This report provides a general overview of the often confusing landscape of endpoint security. It also dives deeper into four key use cases, the solutions in each and the features found to be most relevant by Trace3 customers. These use cases are:
- Endpoint Protection Platforms
- Endpoint Threat Detection & Response
- Threat Isolation
- Exploit Technique Mitigation

The solutions presented in this report are not intended to be an exhaustive treatment of each use case. Solutions selection was based on customer adoption, feature set richness and market presence. Analysis of these use cases and solutions are the basis for the predictions and recommendations provided.

It is important to note that this report does not detail mobile security solutions other than as they are covered by the four primary use cases. Mobile security will be dealt with in a future report looking at trends across the mobility space.

Did You Know...
- Ransomware is on pace to be a $1 billion a year crime this year - FBI
- 10 is the average number of evasion techniques used per malware sample
- 97% of malware is unique to a specific endpoint, rendering signature-based security virtually useless
- 600% increase in attachment-based malware attacks from 2014 to 2015
- $38.5 billion is the estimated financial damage caused by MyDoom, now considered to be the most expensive and fastest-spreading virus ever
- 600,000 Facebook accounts are compromised daily
The endpoint security landscape is ever-changing in both complexity and scope as solutions mature and attacks adapt accordingly. At present there are at least sixteen primary use cases that compose the endpoint security landscape:
- Endpoint Protection Platforms - deliver antivirus, anti-spyware, personal firewall, application control, behavioral blocking and other styles of host intrusion prevention capabilities in an integrated platform
- Endpoint Detection & Response – focuses on detecting and investigating suspicious activities on hosts and endpoints
- Threat Isolation - creates virtual instances of entire endpoints, select applications, browsers, or email to isolate malicious operations from the actual endpoint
- Exploit Technique Mitigation - enforces in-memory protection to guard against attack methods that take advantage of system and software vulnerabilities
- Data Loss Prevention - detects and prevents potential data breaches and exfiltration by monitoring, detecting and blocking sensitive data while in-use, in-motion and at-rest
- Data Encryption - changes data into an unreadable state by using algorithms or ciphers, rendering it useless to anyone without the encryption key
- Sandboxing - executes untested or untrusted programs, possibly from untrusted third parties, without risking harm to the host machine
- Patch Management - acquires, tests, and installs multiple patches across all administered endpoints
- Deception - uses deceit and/or feints to thwart an attacker's cognitive processes, automation tools, breach progression or delays the attack's activities
- Intrusion Detection Systems - monitors a network or system for malicious activity or policy violations and reports incidents to security staff or systems
- Intrusion Prevention Systems - a preemptive approach to network security used to identify potential threats and initiate a response
- Remote Application Access - securely connects a remote user to an in-house application, by using a secure connection channel (e.g., virtual private network)
- Threat Intelligence - aggregates, correlates, and analyzes threat data from multiple sources in real-time to support defensive actions
- Threat Forensics – identifies root cause of a security breach by providing access to the raw details of the attack, the business context, its impact and associated risks
- User Behavior Analytics – as it applies to endpoint security, UBA uses endpoint agents to set behavioral baselines from which anomalies and potential threats are detected and reported

Because the distinctions between these various use cases often blur and overlap, this report has selected four key use cases to focus on. These four use cases span both the prevention and detection spaces of endpoint security and provide a solid foundation upon which the remaining use cases can be layered.
Gartner defines an Endpoint Protection Platform (EPP) as "a solution that converges endpoint device security functionality into a single product that delivers antivirus, anti-spyware, personal firewall, application control and other styles of host intrusion prevention (for example, behavioral blocking) capabilities into a single and cohesive solution."

More advanced EPP solutions integrate with vulnerability, patch and configuration management capabilities to provide more proactive protection. Beyond just fighting malware, modern EPP products now typically include data protection features, such as disk and file encryption, data loss prevention, and device control. The majority of the EPP market is focused on PC-type endpoints; however, these solutions increasingly encompass management and tracking of other mobile devices, such as tablets and smartphones.

Although there are many products on the market today that tout their EPP qualifications, a great number of solutions do not present all capabilities especially platform features such as personal firewalls, URL filtering, application control, full disk encryption and endpoint data lost prevention. Incumbents in this space (e.g., Symantec, McAfee, Kaspersky, Trend Micro) present the full featured platforms but often vary on how they implement methods of protection. For example, signature-based detection approaches is a common architecture on many incumbent solutions, however newer players are relying on advanced algorithms, machine learning and behavior analytics. Another area in which solutions differ is in the attacks they detect and prevent and the platforms that they protect (e.g., OS platforms, mobile support, extranet assets).

The key features in evaluating and selecting EPP solutions are:
- Anti-Malware – Protection against attacks caused by malicious software
- Non-Malware – Protection against attacks from non-malware based threats such as stolen credentials, scripts, etc.
- Advance Persistent Threat – Protection against slow, undetected attacks aimed at stealing data without detection often with access gained through stolen credentials from a successful spear-phishing attack
- DLP – Endpoint Data Loss Prevention
- Encryption – Endpoint disk encryption to prevent exfiltration of useful information even if there is a successful breach
- HIPS – Host Intrusion Prevention System is installed on an individual endpoint and monitors for suspicious activity
- Forensics – The ability to perform targeted investigations on endpoints in the event of a breach
- Legacy Threat Intel – Signature-based methods of detecting threats such as antivirus or anti-malware software
- Advanced Threat Intel - Aggregation and application of security data such as new threats, behavior analysis, malware, hostile addresses, etc.

It is important to note that, EPP solutions are often augmented with Application Control solutions especially in embedded systems like dedicated servers, ATMs, Point-of-Sales devices, Healthcare devices etc. For this study, however, application control will not be explored and is left to a future report.

EPP solutions have recently received some bad press prompting many customers to investigate alternatives. However, it is important to keep in mind that many emerging technologies (e.g., EDR) do not provide a full replacement of EPP functionality. It is a more reasoned approach to view EPP as a key layer in your endpoint security strategy allowing it to identify and protect against the obvious malicious attacks so that your next layer of defense can focus on more complex threat techniques.
Endpoint Detection & Response

EDR technologies monitor endpoint activities and aid in the detection, containment, investigation and remediation of malicious behavior. EDR solutions detect suspicious events, such as execution events, registry events, file events and network events but also check for patch compliance and threat scoring and containment. Because EDR solutions do not interrupt running processes, they are used for monitoring and response only and not for automated intervention. EDR solutions are a detection and response solution and therefore should be considered as one layer of a larger protection solution along preventative technologies such as EPP solutions.

EDR solutions feature four primary capabilities: Detect security incidents, contain the incidents at the endpoint, investigate security incidents and remediate endpoints to a preinfection state. At the time of this study, vendor implementation of these four capabilities vary greatly (see accompanying feature comparison matrix). EDR solutions are far from handsfree and do require a considerable amount of security expertise. As such, organizations with a strong security operations center (SOC) are the primary candidate for EDR solutions while smaller shops may consider an outsourced EDR service deployment.

EDR Solutions should be evaluated for the following features:
- Managed Hunting – Aggressive tracking and reporting cyber-adversaries
- Real-Time Agent Scoring – Score live activity on the agent to determine malware-like behavior
- Centralized Data – Real-time centralized data collection to collect pertinent endpoint data immediately, usually on a limited scope
- Real-Time Search – Real-time search data across many live endpoint agents to determine current conditions
- Incident Containment – Limit or control network connectivity of endpoints being investigated to deny attacker access
- Events Feeds to SIEM – Send events (e.g., syslog, CEF) to a SIEM or other log management tool
- Built-in Sandboxing – Check discovered executables and/or document files for malicious signs by running or opening them inside a isolated sandbox

It is important to note that, EDR platforms are tightly focused on the detection of, and response to, sophisticated malware attacks but lack prevention or threat intelligence capabilities. Therefore, EDR forms only one layer of an overall endpoint security stack. While today's EDR solutions are not viewed as a replacement for an EPP solution, the two solutions often complement each other in organizations that can manage the interaction, integration and operations of the two solution platforms.
Threat Isolation (also known as Endpoint Containment) removes the burden of distinguishing between malicious and legitimate content or executables. Considered a prevention layer, threat isolation solutions create a protective barrier between the user, the endpoint and open internet by creating an isolated virtual instance of the entire endpoint or specific applications and performing all operations within this virtual cocoon transparently to the user. If any malicious code is encountered its effects are applied only to the virtual instance which is destroyed when the user logs out.

Threat Isolation is a new approach to endpoint protection based on the assumption that all endpoints will eventually be penetrated despite other protection layers. Solutions in this space create a virtual instance in which to isolate these bad actors thereby limiting the impact of any malicious operations. Within this virtual instance the user is granted unrestricted access and if harmful executables are encountered, installed or run they are isolated to the contained environment never touching the actual endpoint. When the user exits the session, the environment and its malicious content are automatically discarded and the user presented with a new clean instance upon the next launch.

If done correctly, isolation is accomplished transparent to the end user both in terms of performance and user experience. This approach proves especially valuable to endpoints locked into older (unpatchable) OS versions or legacy applications with known vulnerabilities. Because the virtual instances of the endpoint or applications are temporal, threat isolation is very effective against evasion techniques, zero-day attacks and advanced persistence threats. However, since threat isolations solutions are relatively new and still maturing it is recommended that they be deployed as an adjunct to an EPP layer.

Today's treat isolation solutions come in two primary flavors:
- OS Isolation - A virtual instance of the entire endpoint is created on logon and torn down when the user logs off. This approach does have some performance impacts but does protect the entire endpoint instead of select applications. This approach is most commonly used in ultra-secure environments such as military, classified projects and special access operations.
- Programmatic Isolation - Since the vast majority of malicious attacks target only a handful of programs, this approach only creates virtual instances for select applications such as email, web browsers, select applications or document handling applications (e.g., PDF viewer). This is a much lighter weight approach than OS Isolation making it less impactful on performance and user experience but without full protection of the endpoint. Programmatic isolation is very quick and easy to implement and transparent to the end user.
Exploit Technique Mitigation

Exploit Technique Mitigation solutions prevent malicious software from exploiting flaws in hardware, system resources, operating system and software flaws such as guarding against memory overflow attacks. Today’s attackers rely on a small number of exploit techniques, such as Return Oriented Programming, because the development of new techniques is arduous and time consuming. As such, solutions that protect against commonly used exploitation methods can be very effective in thwarting attacks.

Tools such as Palo Alto Traps, Endgame and Malwarebytes present a cadre of techniques to stop exploitation of memory corruption, logic flaws and malicious code execution. Microsoft provides EMET as a part of the Windows operating system to protect against memory/corruption types of attacks. Ensilo offers a unique mitigation approach in which they prevent any exfiltration or communication between malicious code on the endpoint and the attacker’s base system thereby rendering most common exploits inert.

These solutions typically present a combination of the following features:
- Memory Corruption Prevention – Exploit that manipulates the operating system’s normal memory management mechanisms
- Logic Flaw Prevention – Exploits that manipulate the operating system’s normal processes and execute the target application
- Malicious Code Execution Prevention – Prevents the recognized exploit technique from progressing
- Data Exfiltration Prevention - Prevents unauthorized transfer of data executed maliciously

As with the other security solutions, it’s important to keep in mind, that not all Exploit Technique Mitigation solutions cover all exploit possibilities and not all malware requires an exploit. Nonetheless, Exploit Technique Mitigation solutions typically have low management overhead and minimal user impact making them one of the easiest to implement and most protective layers of a comprehensive protection plan.
Trace3's Take

Predictions

1. Endpoint Security solution providers compete in a very crowded and highly-funded market space. Incumbents, such as Symantec and McAfee, have the daunting task of not only fending off attackers but also keeping up with emerging solutions who are, conversely, aiming to grow their solution into larger platform like offerings. Over the next two years, we expect to see an increase in platform offerings either through merger and acquisition or through in-house development efforts to expand into adjacent security markets.

2. As exploits continue to become more advanced, countermeasures become more automated and orchestrated. While this trend to automation is allowing more to be done with less operational labor, endpoint security will not reach a "hands off" level of maturity in the foreseeable future.

3. Due to the increasing complexity of endpoint security solutions and the burgeoning number of endpoint security use cases (16 as of this writing) customers are clamoring for a more consolidated platform to focus their precious security analysts time on. However, although we do predict that some consolidation will be seen in the near future to address this, there will not be one holistic solution for endpoint security.

4. Microsoft is the target operating system for the vast majority of endpoint, and as such Trace3 expects the newer releases of Windows 10 to add substantial built-in prevention, detection and operational features. Look for big advances on this front.

5. A growing number of enterprises will adopt open-source or built-in OS features as their primary anti-malware solution (e.g., Avast, Malwarebytes, BitLocker, native MAC encryption) to free up budget currently being spent on traditional anti-virus solutions. This budget will be redirected to EDR, EPP or other emerging endpoint solutions.
Recommendations

1. Like everything else in security, protection in layers is the best approach to protect against malware. The best long-term endpoint security strategy will remain a layered approach centered on several key security platforms like EPP and EDR.

2. Although current market trends still focus heavily on malware protection, detection is becoming more important. Since there is no 100% effective prevention solution, detection products should be a key area of attention when beefing up a layered endpoint security stack.

3. Although patching and software updates are decidedly "unsexy", it is a mandatory step to ensure that this base level of protection is in place, up to date and automated before moving on to more advanced solutions. If patching and updating are limited by legacy application interoperability, your overall endpoint protection strategy should take this into account.

4. Consider your users when choosing endpoint solutions. Each technology demands some level of overhead which can impact operations, image management and user performance. Select endpoint solutions that best suit your users' usage profiles rather than which vendors have the best market presence.

5. Don't forget about the network. Ensure that your endpoint security solution stack is complementary with your network security architecture and policies and that operational integration between the two spheres of control is pre-coordinated.

6. When choosing endpoint solutions, look for complementary solutions that do not overlap so as to avoid software bloat and to minimize the number of endpoint agents needed.

7. Although many enterprises are seeking to replace their traditional AV solutions (e.g., Symantec, McAfee), however the EPP and EDR products on the market today do not yet cover all of the incumbent's features (e.g., DLP, encryption, white-listing). Also, many compliance audits require that there be some form of AV in place. As such, we recommend that a careful feature and policy study be done before replacing current traditional AV solutions in order to identify feature and policy gaps. This evaluation will determine if a cheaper, point solution for these gaps will suffice or if retaining the current AV solution is required.

8. Many customers are laser-focused on securing the endpoints under their control. However, it should be pointed out that, many security breaches are caused by endpoints outside the enterprise's control, such as devices owned by partners, suppliers, vendors, consultants and employee personal devices. These are also vulnerable attack surfaces that need to be evaluated when forming a robust endpoint security strategy.
To Secure Your Endpoints, You Better Take Steps!

A solution that converges endpoint device security functionality into a single product that delivers antivirus, anti-spyware, personal firewall, application control and other styles of host intrusion prevention (for example, behavioral blocking) capabilities into a single and cohesive solution.

## Exploit Technique Mitigation

### New Hotness: TRAPS by Palo Alto Networks, Malwarebytes

Solutions that prevent malicious software from exploiting flaws in hardware, system resources, operating system and software flaws such as guarding against memory overflow attacks.

## Endpoint Protection Platform

### New Hotness: Protect by Cylance, User Protection Solution by Trend Micro

A solution that converges endpoint device security functionality into a single product that delivers antivirus, anti-spyware, personal firewall, application control and other styles of host intrusion prevention (for example, behavioral blocking) capabilities into a single and cohesive solution.

## Endpoint Threat Detection & Response

### New Hotness: Falcon Platform by CrowdStrike, Tanium

EDR technologies monitor endpoint activities and aid in the detection, containment, investigation and remediation of malicious behavior.

## Exploit Technique Mitigation

### New Hotness: TRAPS by Palo Alto Networks, Malwarebytes

Solutions that prevent malicious software from exploiting flaws in hardware, system resources, operating system and software flaws such as guarding against memory overflow attacks.

### Featured Use Cases

<table>
<thead>
<tr>
<th>Exploit Technique Mitigation</th>
<th>Endpoint Protection Platform</th>
<th>Endpoint Detection &amp; Response</th>
<th>Threat Isolation</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://www.ensilo.com">Ensilo</a></td>
<td><a href="https://www.symantec.com">Symantec</a></td>
<td><a href="https://www.crowdstrike.com">CrowdStrike</a></td>
<td><a href="https://www.menlosecurity.com">Menlo Security</a></td>
</tr>
<tr>
<td><a href="https://www.microsoft.com">Microsoft</a></td>
<td><a href="https://www.kaspersky.com">Kaspersky</a></td>
<td><a href="https://www.fireeye.com">FireEye</a></td>
<td><a href="https://www.bromium.com">Bromium</a></td>
</tr>
<tr>
<td><a href="https://www.endgame.com">Endgame</a></td>
<td><a href="https://www.cylance.com">Cylance</a></td>
<td><a href="https://www.coutertack.com">CounterTack</a></td>
<td><a href="https://www.invincea.com">invincea</a></td>
</tr>
<tr>
<td><a href="https://www.paloalto.net">palosanto</a></td>
<td><a href="https://www.mcafee.com">McAfee</a></td>
<td><a href="https://www.tanium.com">Tanium</a></td>
<td><a href="https://www.fireglass.com">fireglass</a></td>
</tr>
<tr>
<td><a href="https://www.sophos.com">Sophos</a></td>
<td><a href="https://www.trendmicro.com">Trend Micro</a></td>
<td><a href="https://www.cisco.com">Cisco</a></td>
<td><a href="https://www.weblife.com">weblife</a></td>
</tr>
<tr>
<td><a href="https://www.sentinelone.com">SentinelOne</a></td>
<td><a href="https://www.carbonblack.com">Carbon Black</a></td>
<td><a href="https://www.cybereason.com">cybereason</a></td>
<td><a href="https://www.spikesoninc.com">spikes</a></td>
</tr>
<tr>
<td><a href="https://www.webroot.com">WEBROOT</a></td>
<td><a href="https://www.guidance-software.com">guidance software</a></td>
<td><a href="https://www.passages.com">Passages</a></td>
<td></td>
</tr>
</tbody>
</table>

© 2016 Trace3, Inc. All Rights Reserved
**Threat Isolation**

*New Hotness: MS Isolation Platform by Menlo Security, Threat Isolation Platform by FireGlass*

Isolating applications, browsers, and email from users devices in order to fully execute web content whether it is good or bad. This separates malicious content from endpoints.

---

**Other Materials (available upon request)**

*Endpoint Security Feature Comparison Matrices*

PowerPoint Presentation with Endpoint Security Feature Comparison Matrices on the four key STEPS use cases.

---

**Sources**

2. Gartner – Comparing Endpoint Technologies for Malware Protection – Mario deBoer – 2016
7. CNN Money - Cyber-Extortion Losses Skyrocket, says FBI - April 15, 2016
### Endpoint Detection & Response

#### EDR Feature Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>CrowdStrike</th>
<th>Tanium</th>
<th>Carbon Black</th>
<th>Cisco</th>
<th>CounterTack</th>
<th>FireEye</th>
<th>Cybereason</th>
<th>Guidance MKE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed Hunting</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Real-Time Agent Scoring</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Centralized Data</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Real-Time Search</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Incident Containment</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Events Feeds to SIEM</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Built-in Sandboxing</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
</tbody>
</table>

### Threat Isolation

#### Threat Isolation Feature Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>Bromium</th>
<th>invincea</th>
<th>fireglass</th>
<th>Menlo Security</th>
<th>weblife</th>
<th>SPIKES</th>
<th>Passages</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Isolation</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Email Isolation</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Browser Isolation</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Application Isolation</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Document Isolation</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
</tbody>
</table>
# Exploit Technique Mitigation Comparison

<table>
<thead>
<tr>
<th>Exploit Technique</th>
<th>360</th>
<th>Palo Alto</th>
<th>ENDGAME</th>
<th>Malwarebytes</th>
<th>Microsoft</th>
<th>ENSILO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Corruption Prevention</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NA</td>
</tr>
<tr>
<td>Logic Flaw Prevention</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NA</td>
</tr>
<tr>
<td>Malicious Code Execution</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>NA</td>
</tr>
<tr>
<td>Data Exfiltration Prevention</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
</tbody>
</table>

(end of report)