Endpoint

Created: October 2016

Problems	Solution Feature	Customer Benefits	Differentiation
Protection from advanced and emerging threats	**Block malware before it executes *and* stop live threats that exhibit malicious behavior** - Real Protect (RP) static and dynamic behavioral analysis	• **Defeat more zero-day malware,** including difficult-to detect objects, such as ransomware, by analyzing attributes pre-execution and dynamic behavior to confirm as malicious. • **Fast and proactive protection:** Machine-learning automatically updates threat models used for behavioral analysis. • **Signature-less classification** is performed in the cloud and therefore maintains a small client footprint while providing near real-time detection. • **Reduce the effort required to adapt** defenses using automated machine-learning classification and a connected security infrastructure. • **No manual intervention required:** Automatically unmask, analyze and remediate threats using integrated defenses that trigger responses and adapt to stay ahead of emerging threats	• **Stops more threats** than signature or static-only protection by combining pre-execution feature extraction and dynamic behavioral analysis • **Reduces resources needed** for security through integration and automation within the holistic threat defense. • **More effective against difficult-to-detect malware** by allowing it to show the "bad" behaviors, analyze them real-time, and then automatically terminating and remediating the threat. • **Maximum efficiency and efficacy** - Machine learning that uses both supervised training, for drift avoidance, and automated clustering for updating threat models. The only solution that combines static and dynamic behavioral Machine Learning into an integrated solution. • **Updates all connected security components** – Automatically updates the TIE reputation score so that additional network protection is immediate
	Prevent greyware from making known malicious changes to endpoints – Dynamic Application Containment (DAC)	• **Patient zero protection:** Immediately limits known malicious changes to the endpoint. More effective against difficult-to-detect malware since it actually takes action at the endpoint instead of a VM. • **Limits exposure:** Detects and contains suspicious greyware to stop "infection" before malware infects the endpoint. Delivers increased detection speed and provides protection for endpoints both on and off the network. • **Maintains business continuity:** It uses access control rules to monitor, contain, or release specific behaviors while preserving the end-user experience.	• **Immediate containment** with the ability to maintain endpoint productivity while conducting further analysis • **Does not require cloud access** or a physical or virtual appliance to track and contain malicious behavior when endpoints are both on and offline. • **Lightweight** with minimal system impact without the overhead of a heavy virtual sandbox or appliance. • **Reduces time from encounter to containment and protection** while minimizing time-consuming manual intervention.
	Dynamic, integrated framework and automation - Threat Intelligence Exchange (TIE) & Data Exchange Layer (DXL)	• **Dynamic reputations neutralize emerging threats:** All TIE-connected components learn collectively from the insights of a single encounter, and use synthesized threat intelligence, to convict emerging threats in milliseconds. • **Self-Updating with Lower TCO**: Advanced integration and automation fortifies protection and simplifies processes. • **Instant Actions:** A common architecture enables immediate action on threats, policy updates, detection and security updates. • **Unites disparate technology solutions, across multiple vendors** enabling instant sharing of contextual insights to deliver immediate threat protection.	• **Synthesizes local, global and 3rd party intelligence** on the fly and make comprehensive reputation-based convictions. • **Collectively learns** from a single encounter to neutralize emerging threats as a holistic system. • As **the most comprehensive reputation system in the industry**, Intel Security's Global Threat Intelligence (GTI) network uniquely provides ability to scan the full spectrum of new 'and emerging threats in real-time. • **DXL's open messaging framework enables instant sharing** of contextual insights to deliver immediate threat protection and share patient-zero insight with all other endpoints to prevent infections from spreading. • **Integration and shared intelligence** across the entire threat defense lifecycle to enable faster response and the ability to immediately update protection.

	Endpoint Security (ENS) Module-to-module communication– across all modules	• **Communication between threat** defenses allows linkage of seemingly disconnected events. Module-to-module communication in ENS allows detection of targeted attacks that other point product vendors would miss. • **Proactive web protection** ensures safe web browsing with web protection and filtering for endpoints. • **Integrated firewall** blocks hostile network attacks and offers the ease of centralized management.	• **Stay ahead of threats** with ENS connecting disparate security components into a collaborative system where threat defenses can talk to, learn from and inform one another of emerging threats. • **Near Real-Time Communication** between threat defenses enables the sharing of events so IT can take action against potentially dangerous applications, downloads, websites, and files as suspicious behaviors are observed.
	True Dynamic Whitelisting - Application Control	• **Eliminate labor-intensive list management or signature updates:** Immediately thwart zero-day advanced threats without list management or signature updates. • **Dynamic whitelisting trust model reduces costs:** by eliminating expensive manual support requirements. • **Provides file & application reputation:** Leverages reputation sources from McAfee Global Threat Intelligence and Threat Intelligence Exchange.	• **True dynamic whitelisting** that is easy to configure and use is a clear differentiator for Intel Security. • **Dynamic whitelisting requires lower operational overhead** when compared to legacy whitelisting techniques. Other vendors have higher operational overhead as a result of their manual management effort.
	Stops Web malware before it reaches endpoint - McAfee Client Proxy Agent built into ENS 10	• **Endpoints protected regardless of whether they are located on or off-network**, endpoints are fully protected with the most up-to-date reputation convictions (all web traffic routed to McAfee Web Gateway (MWG), cloud or on-premises) • **Reduce resources required for remediation** by stopping zero-day malware from the internet before it reaches an endpoint.	• **Behavioral emulation (Gateway Anti-Malware engine)** delivers #1 zero-day malware detection rate in a Web Gateway • **Unique ability to stop zero-day malware from ever reach the endpoint** (stops in-line with traffic flow preventing delivery to endpoint) as few other vendors (only Blue Coat, and only for files, not JavaScript or HTML like MWG) • **Deployment flexibility** as no other Web Gateway vendor (Blue Coat, Cisco, Websense, Zscaler) allows customers to utilize both on-premises and cloud-based web gateways with the same policy for both, managed by one single console.

Sales Play Accreditation Battlecard

Problems	Solution Feature	Customer Benefits	Differentiation
It takes too long to detect compromises, discover the unknown, and recover	**Simplified management** - ePO	• **Automated responses** (triggers, search and respond) to rapidly mitigate threats using ePO. • **Reduced administrative burden:** Easier to adapt defenses using automated classifications and a connected security infrastructure. • **Single console** provides greater security visibility and direct drill down capability to explore and instantly manage events. • **Actionable reporting and event handling** with an automated response system to streamline event management and common tasks. • **Drag-and-drop dashboards** provide increased real-time visibility across the entire ecosystem.	• **Centralized management and action via single console** (McAfee ePO) is a clear Intel Security differentiator, delivering a single pane of glass. • **Symantec customers need five separate consoles and five separate databases** to achieve central management for complete endpoint solution. • **Open platform** software development kits (SDKs) facilitate rapid adoption of future security innovations. • Deployment of additional emerging vendors (Cylance, Bit9, etc.) requires additional management consoles and endpoint agents
	Prioritized threat visibility with context and the ability to take immediate action – Active Response	• **Consolidated threat context:** A dashboard that combines enterprise-wide reputations, behavior score, alternate names, etc... • **Prioritized threats and workflow:** Surface high-priority threats and all infected hosts to immediately investigate, take action and update protection. • **Simplify investigations:** Flexible investigation and response tools remove uncertainty and provide deeper insights. • **Quickly adapt defenses against future attacks:** Triggers can be set to recognize critical event or state changes and generate alerts or reactions to hunt and kill threats. • **Save precious time** by seeing and remediating today's threats and then set trigger actions for the threats of tomorrow with one step	• **Single-Click remediation** at a single endpoint or across all endpoints and then easily move to updating protection across the organization. • **Collectors look beyond program executable** (PE) or running files into code and objects that may be lying dormant, or may even have been deleted in an attempt to cover the attacker's tracks • **Highly customizable**, users can search across traditional data silos and black holes to easily find precisely the combination of details that matches the indicator, such as file name launched on date by user. • **Pre-configured to act** on search results and can accommodate custom actions prescribed by the user to meet a specific objective • **Automatic intelligence updates:** Dynamic behavior scoring aggregates associated events and automatically adjusts the behavior score.
Point products operate in silos and only offer isolated threat intelligence	**High detection rates for secure Web Gateway** - Web Gateway	• **Highest detection rates for malware in a secure web gateway**. AV-TEST results show 95% detection of 0-day malware, attributable to the Gateway Anti Malware (GAM) engine. • **Flexibility** to add sandboxing/ static code analysis either during a web request or out of band.	• Blue Coat detected 74% of 0-day malware in the same test • Websense detected 58% of 0-day malware in the same test. • Zscaler has never been tested for 0-day malware detection (red flag!) Cisco detected only 25% of 0-day malware in the same test
	Open Messaging Framework for sharing contextual insights - Data Exchange Layer (DXL)	• **Unites disparate technology solutions, across multiple vendors** enabling instant sharing of contextual insights via TIE to deliver immediate threat protection.	• **No other vender has open messaging framework that enables instant sharing of contextual insights** to deliver immediate threat protection.
	Tight Integration with Advanced Threat Defense and Endpoint to enable instant information sharing and action – Advanced Threat Defense (ATD)	• **Reduced time from encounter to containment and protection** when threat intelligence is instantly shared with endpoint thus minimizing time-consuming manual intervention. • **Streamlined workflows** enable efficient alert management through a single interface.	• **Extensive integration with endpoint and to the network edge** to enable security components to work as a collaborative single entity to enhance security.

Sales Play Accreditation Battlecard

Objections	Intel Security Response
Customers feel they need to go to an emerging competitor (like Bit9+Carbon Black, FireEye / Mandiant) for innovation and advanced threat capabilities because Intel Security is just a traditional AV vendor	These emerging competitors do not have the additional protection (network, server, data protection, SIEM) that deliver the intelligent collaborative protection needed to combat today's advanced threats. Customers will have to deploy additional endpoint security (aka: antivirus, encryption, etc.) requiring additional management consoles from separate vendors. Cylance's solution has a track record of producing many false positives: https://www.av-test.org/en/antivirus/business-windows-client/windows-10/december-2015/cylance-protect-1.2-154676/ Cylance uses static analysis alone which limits the threats you can catch, because significant threats exist that are best caught with a behavioral method. There are a lot of threats that are very difficult if not impossible to catch with a 'static only' approach (example: malware misusing a "known clean application" by making it perform malicious behaviors) Real Protect has BOTH Static and Dynamic Behavioral analysis capabilities, is able to track malicious behaviors, analyze the dynamic behavior of malware and match against known malware behaviors using an automated learning algorithm. We not only have a much broader portfolio – it is integrated. We have multiple modules that are integrated to share information like web reputation, local reputation, information from multiple scanners, ePO, MAR integration, etc. Cylance will still require an additional purchase and perhaps continuing ongoing purchases to fill the gaps.
Vendors such as Crowdstrike, Cylance, Tanium, and Carbon Black+Bit9 are preaching that companies should no longer spend money on traditional endpoint AV (implying McAfee)	Endpoint AV remains a core requirement, for two reasons. First, it is preferred requirement by mainstream regulations such as PCI, and businesses need to have it for compliance. But perhaps more importantly, if you turn off AV, then you turn on a green light for actors to use AV-style tactics in their attacks. You shouldn't unplug AV, you need to supplement it by adding on more capabilities.
Competitors are communicating FUD regarding Intel divesting McAfee products e.g. recent EOL's	McAfee products and Intel Security continue to be an important part of Intel's strategy moving forward. Together, as one team we are driving innovation to the security industry by providing more dynamic protection for our customers. Our portfolio review and rationalization process helps ensure we are investing in the right areas to continually innovate and lead the market with the best solutions that address our customers' security needs. Divestiture decisions allow us to prioritize our resources and strategy on innovations that best address the ever changing threat landscape, such as advanced targeted attacks (ATAs).
I have been with Vendor <X> for many years, the cost and burden of migrating to a new vendor is too high.	Endpoint Security (ENS) leverages the integrated EASI installer to offer an accelerated and simplified deployment process. The Endpoint Migration Assistant walks users through the migration process. It will migrate all settings and configurations automatically, based on current settings and new product defaults, or users can select and configure them manually. The admin experience has been optimized .with a new client installer that decreases install time to around 90 minutes for ePO On-Premises and 15 minutes for ePO Cloud. The modular plug-and-play protection client allows products to be added with ease. Admins save time & stress with a one click install experience. Few mistakes can be made. Supporting WinWire: Barclay's - $8.6M Integrated Security Win Ends Bank's 10-Year Relationship with Symantec *https://sales.intelsecurity.com/us/employee/sales/confidential/winwires/ww-barclays-2016-jan.pdf*
We have a policy not to buy everything from one vendor.	This is logical thinking as if a vendor adds a little to its core technology simply to launch similar products in related spaces then a customer ends up using the same technology in multiple places, potentially with the same shortcomings. However fortunately, Intel Security does not use that model Firstly many core products were acquisitions of the best-of-breed vendor (e.g., ATD came from ValidEdge). Secondly extensive post acquisition development work is performed around integration to meaningfully integrate workflows
Carbon Black+Bit9 offer a complete EDR solution	Considered the EDR Market Leader, Carbon Black has strong hunting capabilities; however, they don't prioritize events very well, are very limited in remediation and the ability to automatically update protection – essential features when quickly responding and streamlining defenses. While the Confer acquisition makes for an interesting story, it still lacks meaningful integration, and requires a new client and manager that only add to the complexity of the Carbon Black solution. They also don't participate in 3rd party protection validation or VirusTotal. In short, the expense of complexity and deployment, setting up an adequate infrastructure, is well known to far exceed the initial purchase price. And those that opt for cloud data access find it expensive. In addition, deploying Carbon Black and Bit 9 still requires separate management consoles, which will add complexity and multiple contextual changes that might add additional burden to IT Security Staff. Moreover, most organizations will have additional needs for data protection or server security, why should customers deploy separate consoles from different vendors when they can have on from Intel Security?

Sales Play Accreditation Battlecard

Crowdstrike Falcon Host looks to solve the "adversary" problem, not just malware problems. It's lightweight (<10MB) stealth agent, allows attack to execute and record data for forensic analysis.	Crowdstrike will let patient zero get infected and then cut the endpoint off from the network. They can't match McAfee Endpoint Threat Defense and Response's organization-wide visibility, deep insight, shared threat intelligence and a connected security ecosystem that can immediately adapt defenses against emerging threats. Crowdstrike doesn't provide a combination of static and dynamic behavioral analysis, immediate containment at patient zero, or the ability to hunt and respond across all endpoints, including customizable collectors and automatic responses.
Installing FireEye is a simple process because it's only a single device	While dropping in a single FireEye device for a POC seems simple, full deployment requires multiple appliances and third-party products. Separate appliances are required for different analysis on different protocols. The Advanced Threat Defense centralized deployment architecture covers multiple protocols and a larger volume of files (throughput) than FireEye, reducing the number of devices needed for broad coverage.
Any sandbox will work.	All sandboxes are not created equal. McAfee Advanced Threat Defense detects today's stealthy, zero-day malware with an innovative, layered approach. It combines dynamic analysis with in-depth static code analysis – the key to detecting highly camouflaged, evasive threats that may not execute in a virtual or sandbox environment.
All static analysis is the same	Static analysis is a generic term that refers to analysis without execution—that can include everything from a signature check to reverse engineering with full analysis of all instruction sets. The competition's static analysis is limited to basic analysis methods such as signature checks and file header examination. If malware is packed, most code analysis stops at the header. Advanced Threat Defense performs full static code analysis. To enable this level of analysis, ATD has the ability to unpack the code and disassemble it, essentially reverse engineering the malware to analyze all attributes and instruction sets to determine the intended behavior—and a huge advantage over the competition.
The FireEye/Mandiant combination seems to connect network detections with endpoint action	While the acquisition gives FireEye an endpoint presence, it does not provide protection and lacks the ability to be actionable beyond containment of the endpoint. The Mandiant agent is primarily used for endpoint forensics and incident response. It does not perform endpoint protection and cannot take actions on the endpoint
Some vendors suggest that I use free anti-virus as part of Microsoft or other tools and shift that budget to purchasing advanced protection capabilities.	Suggesting that companies should downgrade to "good enough" or free endpoint protection solutions (i.e. Microsoft SCEP), in order to apply that budget money to a different protection technology, is a false choice and represents a risky security strategy. Microsoft SCEP doesn't have integration with security solutions, which means customers lose the holistic security picture and centralized management provided by McAfee ePO. In addition, they lose the protection integration value provided by our integrated security platform. See study on True Cost of "Free" Endpoint Security or infographic into a cohesive security connected strategy.
Kaspersky has the best coverage of any vendor when it comes to securing a customer's environment.	Appropriate security for a customer's endpoint environment should be based on many advanced factors. Protection should include coverage for a broad set of platforms including mobile platforms, UNIX variants, and database security. Kaspersky has limited, if any, capabilities in many of these areas of advanced protection. Kaspersky also does not also have the TIE or DXL equivalent that connects endpoint security with other protections. Kaspersky is also focused primarily on the endpoint which is a problem for customers wanting to protect their entire enterprise.
Kaspersky's centralized management seems to have a lot of what Intel Security offers.	Creating granular policies and reports is a manual process and pre-built templates are lacking with Kaspersky. Application control and HIPS policies much be built from scratch as there are no preset rules or application lists. True centralized management through McAfee ePolicy Orchestrator (McAfee ePO) delivers single pane of glass visibility into the health of the security environment with a single console and database. Using a single console, Intel Security uniquely protects a variety of platforms with a powerful set of controls, such as traditional antivirus, HIPS, mobility, EDR (Active Response), application control, drive & native encryption, and third-party security solutions. Customizable dashboards and actionable workflows enable a quick view of security posture.
Microsoft security technologies, such as SCEP (formerly Forefront) and Bitlocker, are included in my Microsoft ELA (for free). Isn't that a cheaper route with good enough security?	Independent research shows that total-cost-of-ownership averages 58% higher for Microsoft than Intel Security as Microsoft requires, a minimum four to six consoles to manage endpoints compared to Intel Security's one console. See True Cost of "Free" Endpoint Security study or infographic Microsoft does not have an optimized solution for handling security in VM environments. Microsoft has a very bumpy history with AV certifications, failing many third party tests including multiple from AV-Test were they score lower than ISecG. Microsoft's primary focus is on malware that impacts the Microsoft environment, deprioritizing rare or targeted malware. McAfee ePO together with MNE (Management of Native Encryption) can also manage the native encryption (Bitlocker) allowing customers to manage their entire infrastructure from a single console.

Sales Play Accreditation Battlecard

Symantec also claims to have central management and reporting. Isn't that as good as ePO?	Symantec Protection Center is limited to AV and web security and is only a landing page for their other consoles. Customers must still deploy and manage endpoint products with multiple consoles and databases. With Symantec, keeping an eye on your infrastructure is a nightmare – with so many consoles, viewing your security status in a single console is impossible. Gartner 2016 MQ Caution: "Symantec's security product portfolio is not integrated at a meaningful level, and requires five distinct consoles to manage the complete endpoint solution set."
It takes four Intel Security products to equal Symantec Endpoint Protection.	Intel Security endpoint protection solutions deliver comprehensive protection in a single, integrated, and centrally-managed solution. Intel Security offers consolidated manageability and greater security while reducing the operational cost of endpoint security. Symantec certainly cannot match the breadth of what Intel Security can deliver and does not have advanced functionality like TIE or MAR.
Symantec provides application control that is as good as Intel Security's offering.	Symantec's application control and whitelisting are very difficult to configure and require labor intensive activities, such as manual entry of registry components for applications that the admin wants to manage. Intel Security leverages reputation sources from McAfee Global Threat Intelligence and Threat Intelligence Exchange to provide reputation of files and applications within the enterprise and does not require manual support.
Intel Security is more expensive than other solutions.	Intel Security's approach across the various tiers of organizational sizes provides more complete capability at the same or lower initial cost, not to mention the ongoing operational cost is significantly lower as well. A single centralized console environment means a lower total cost of ownership via management of entire endpoint infrastructure and many third-party applications through a single console. Customers looking to purchase advanced threat prevention and EDR capabilities will spend more by purchasing and managing from separate vendors. Only Intel Security has these capabilities packaged into a single solution.
I've heard that Intel Security is very hard to deploy and configure.	Endpoint Security 10 has a single installer for all its components make it easy to install Also, Intel Security utilizes EASI (Endpoint Advanced Suite Installer) allowing someone to deploy and configure ALL endpoint products in 20 minutes using our best practice configurations ready-to-go. Competitors can take hours to deploy all endpoint components and still require someone to manually perform configuration/tuning for common options.