



Combatting Advanced Targeted Attacks: **PROTECT**

Part I of the Combatting Advanced Targeted Attacks Blueprint Trilogy

Security Connected Reference Architecture Technology Blueprint

Intel® Security recommends a three-pronged approach for disrupting advanced targeted attacks, starting with enhanced protection, described in this guide. The goal of this Protect stage is two-part: to stop the most pervasive attack vectors while disrupting never-before-seen techniques and payloads, and to derive insights that can strengthen countermeasures and inform investigators of unfolding activities. To see the rest of the story, read the companion Detect and Correct blueprints.

Raising the Bar on Prevention

The Situation

The majority of individual security technologies are quite effective at addressing the problems that they were designed to solve. Yet seldom does a day go by without a new hack making the news. It is an ongoing battle. On one side, you have highly skilled, organized, and motivated attackers with the dedication and ingenuity to launch unlimited variations of sophisticated targeted attacks. They succeed if only one gets through. To defeat them, overwhelmed security teams with limited time and budget typically have controls that are designed to block generic and opportunistic threats, not the refined and adaptive control systems necessary to combat the zero-day malware, social engineering, and other tactics used in stealthy targeted attacks. If you play defense, you may feel that your job is impossible. The odds seem heavily stacked against you, but you have to find a way to block those attacks and keep the bad guys out of your environment.

Driving Concerns

Keeping these ultra-focused opponents out means overcoming multiple hurdles. Because of the diversity of these challenges, there is no single silver bullet or miracle technology to block such attacks. Each requirement necessitates a precise set of functionality, plus integration that crosses boundaries to eliminate coverage gaps that aid the attacker. Let's take a look at why protecting against targeted attacks is so hard.

- **Designed to evade.** Advanced targeted attacks are specifically designed to evade being recognized and blocked by traditional countermeasures. Well-funded, persistent, and motivated attackers take the time to understand your defenses—and their weaknesses—to specially craft an attack that can make its way around your organization's specific controls.
- **High level of sophistication.** These efforts combine multiple techniques, such as zero-day malware, exploits like SQL injection or remote code execution, and social engineering in one single attack. Amongst those techniques, the delivery methods of choice, such as watering holes take advantage of end users as the weakest link, to get them to install zero-day malware on their systems.
- **Zero-day malware.** This is probably one of the most efficient tools in the attacker's arsenal and a dilemma for security teams. How can the security team ensure that a new and unknown file is safe for the user to run, or be sure that the file needs to be blocked without generating false positives?
- **Limited countermeasure intelligence.** Most attacks weave through existing layers of defenses before compromising their target. The mechanisms to block those attacks are in place, but the countermeasures lack the intelligence required to identify and act upon the attack. Obtaining the necessary intelligence is critical to enable defenses to do their job.
- **Disconnected security.** One product might block one salvo or phase of an attack, but if the attack uses other vectors, your defenses might still miss it. So, even if you have the ability to block an attack, siloed and disjointed security solutions make it impossible for you to distribute that intelligence in a timely fashion to your entire environment for protection against that attack. This model also hinders aggregation of threat and event intelligence into a coherent and actionable assessment of attack activity.

Solution Description

Advanced targeted attacks have shown that they are capable of bypassing standard defenses. This means that no standalone security technology can prevent all attacks. This is why Intel Security proposes a radically different approach: the coordinated use of traditional and advanced protection technologies to disrupt and block advanced targeted attacks. This comprehensive approach is achieved by building a security framework capable of generating its own intelligence and of distributing it within seconds across the entire security ecosystem. The resulting protection ecosystem can not only block and disrupt advanced targeted attacks, but also grows more intelligent and stronger as it blocks those attacks.

Security Connected Reference Architecture

Technology Blueprint

There are three main steps in building this coordinated framework. First, you need to deploy your countermeasures where they matter. Most companies already have a lot of the necessary solutions in place, but they may not be taking full advantage of the latest features or be fully activated. Since attacks keep evolving, it makes sense to look at our recommendations for step #1 and review what you already have. If you are in good shape, you can move to #2 and #3, which look at intelligence and orchestration, respectively.

- 1. Deploy your countermeasures where they matter.** To refine your control technology to perform the front-line blocking of sophisticated attacks, align your defense to the specific steps an attack would follow. In the case of an advanced targeted attack, it means taking care of the following.

On the network:

- Block reconnaissance from attackers with IPS.
- Prevent malware from reaching its target by:
 - Analyzing network traffic, including looking for advanced evasions, weaponized malware obfuscated inside PDFs, and other documents.
 - Scanning websites for dangerous pages and malware.

On the endpoint:

- Prevent the execution of malware:
 - Whitelisting to block execution of unapproved files or applications.
 - Endpoint protection such as antivirus or host IPS that blocks malicious activities based on signatures, rules, and heuristics.
 - Advanced threat protection module able to immediately protect against zero-day malware based on local intelligence and risk.

- 2. Arm your countermeasures with the best intelligence.** Once you have your protection countermeasures in place, they need to know what to block. Using a broad array of engines allows you to effectively balance the need for both protection and performance. This pragmatic approach means resisting the temptation to exclusively invest in only the most advanced technologies, and instead, looking to get more value out of your existing technologies. When used as standalone technologies, solutions such as signature-based detection allow you to weed out the low-hanging fruit so you can focus on the hard stuff. They offer precise detection, cut out noise, and reduce the load imposed on advanced technologies.

But as we know, they are not enough against zero-day malware. That's why you need to supplement them with technologies capable of handling unknown malware. Those engines and relevant intelligence sources can be built in to the countermeasures described in step #1, or can be deployed as their own internal or external systems. Here is a list of engine types and intelligence sources to consider for arming your countermeasures:

Intelligence Source	Definition
Signatures and Blacklisting	Weed out the obvious fast. Usually built in to countermeasures.
Whitelisting	Allow the known good. Concept can be applied to URLs, IP addresses, files, or applications. Can be part of a countermeasure or be a standalone offering.
Global Intelligence or Reputation	What the rest of the world knows about that file, IP address, sender, or message. External source.
Local Intelligence	What your own security products or team members know about a file or other indicators. Internal source. Usually housed in an internal server.
Community-Based Intelligence	What people in the security industry or your contacts at other companies or in your specific vertical know. For example, intelligence gathered via incident response at other companies or intelligence collected from industry groups or government threat advisories.
Behavioral Analysis	Does this file behave like it's malicious? Built in to some countermeasures.
Dynamic Analysis	What happens if we let the file run completely? Usually a dedicated appliance, often called a sandbox.
Static Code Analysis	What is the exhaustive list of changes and activities and their ramifications that would occur on a system if it ran this file? Usually a dedicated appliance.

Table 1. Intelligence sources and their definitions.

Security Connected Reference Architecture Technology Blueprint

3. Connect your defenses to work together in real time. While good countermeasures and unparalleled intelligence will significantly block and disrupt advanced targeted attacks, the effectiveness of the protection can be raised even higher by enabling all the security solutions to share intelligence instantly, within your environment, so they are all able to immediately block emerging threats. For maximum efficiency, the solution needs to be able to:

- Share intelligence between all countermeasures.
- Share it in milliseconds.
- Capture events with context to identify emerging threats and attack events.
- Adjust policies and configurations to counteract the new threat.

Decision Elements

These factors could influence your architecture:

- Do you already have most of the countermeasures described in step #1 in place?
- Do you want to build on top of your existing defenses, or is there a renewal or upgrade that could facilitate change?
- Are you using multiple anti-malware vendors at different layers to make up for detection gaps?
- How many consoles do you currently use to manage all your security products?

Technologies Used in Our Solution

Working with an array of Intel Security and third-party countermeasures that enable step #1, the McAfee® Threat Intelligence Exchange and the McAfee Advanced Threat Defense support step #2 and step #3, providing the pillars of a solution for preventing advanced targeted attacks from compromising your environment. The most powerful advantage of the solution is that the components work in real time with your entire environment to immediately block zero-day malware. Both Threat Intelligence Exchange and Advanced Threat Defense are designed to augment your existing protections through open interfaces and factory-tested integrations. This allows you to benefit from your existing investment while also raising the bar of advanced threat protection.

Offering local assessment of malware reputation, McAfee Threat Intelligence Exchange works with McAfee Endpoint Protection to block new and risky files from executing on the endpoints. When it can't assess the file, Threat Intelligence Exchange will leverage Advanced Threat Defense to determine if a file is malicious. Intel Security network and content products can leverage Advanced Threat Defense as well, submitting samples to find out if a file is malicious. If Advanced Threat Defense determines the file is indeed malicious, the countermeasure that found it will block it. At the same time, the solution will tell the Threat Intelligence Exchange server about the malicious file and it will immediately inform all of the other products, and those products will begin blocking, too. Therefore, the combination of Threat Intelligence Exchange and Advanced Threat Defense allows you to get more value out of your existing environment without having to completely replace existing infrastructure with the latest and shiniest technology.

Security Connected Reference Architecture Technology Blueprint

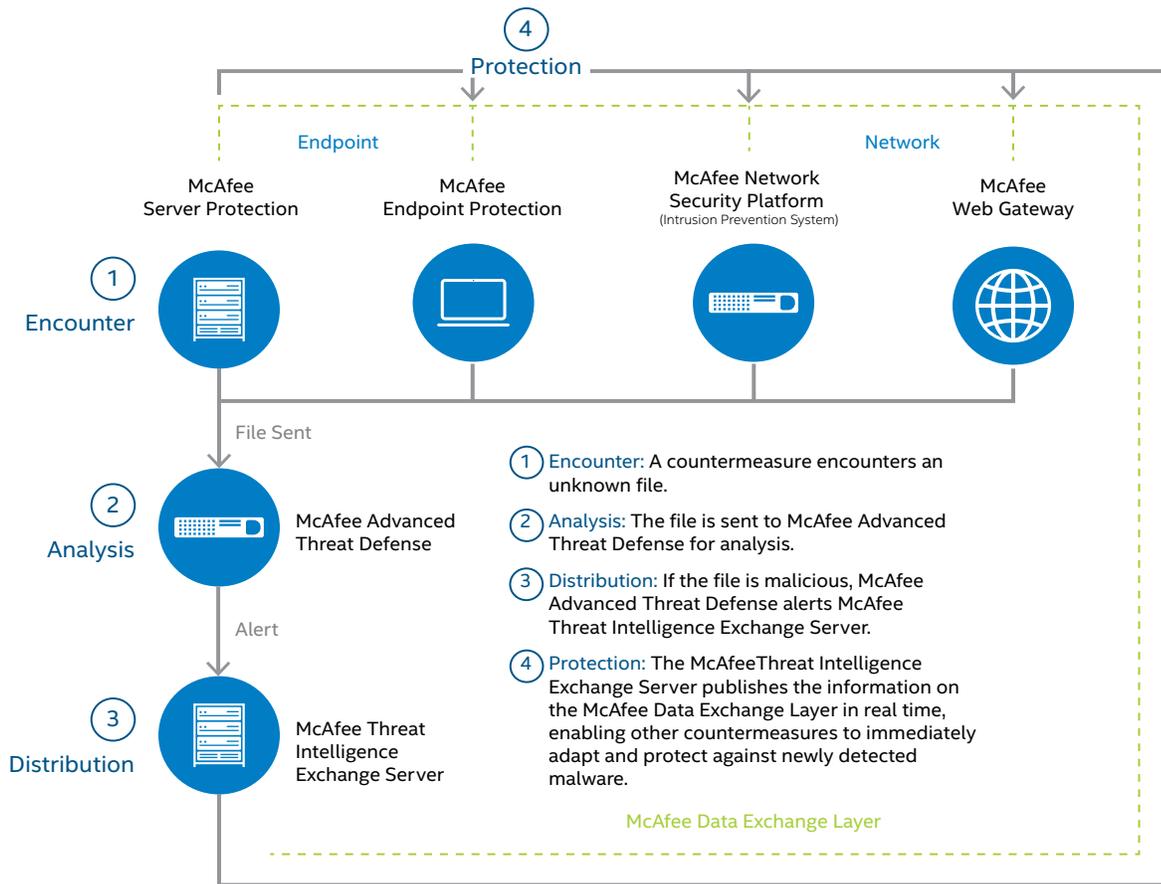


Figure 1. Technologies used in the Intel Security solution.

1. Deploy your layered countermeasures where they matter.

▪ Network:

– McAfee Web Gateway blocks web-borne attacks prevalent in advanced targeted attacks, including watering holes.

Since almost everyone surfs the Internet, attackers often use compromised web servers to deliver malware or compromise unsuspecting visitors' browsers. McAfee Web Gateway is designed to specifically analyze requested websites and Internet downloads for potential threats, preventing advanced targeted attacks from compromising your environment via your user's usage of the Internet. McAfee Web Gateway takes advantage of the powerful Gateway Anti-Malware engine to identify unknown malware (see step #2 for details about the Gateway Anti-Malware engine). Using extensive content inspection, reputation analysis, and site categorization, plus file filtering techniques, McAfee Web Gateway can be used to block undesirable sites or content. And finally, it performs SSL scanning, examining the contents of encrypted web traffic for hidden malware.

– McAfee Intrusion Prevention System (part of McAfee Network Security Platform) foils network-based attacks and lateral movement.

Not all attacks originate from the outside. By keeping an eye on the activity inside your own network, the McAfee Network Security Platform protects you against potential internal attacks. It combines file reputation from McAfee Global Threat Intelligence, deep-file analysis with JavaScript inspection, and signature-less advanced malware analysis to detect and block zero-day threats, custom malware, and other stealthy attacks travelling inside your network. The Network Security Platform malware protection abilities also take advantage of the Gateway Anti-Malware engine (described in step #2).

Security Connected Reference Architecture Technology Blueprint

- **Endpoint:**
 - **McAfee Endpoint Protection protects your endpoint against attacks.** McAfee Endpoint Protection real-time scanning ensures that all of your systems, on-premises and on-the-go, are constantly protected against known malware, even those hidden in compressed files. In addition, it guards against buffer-overflow exploits that target vulnerabilities in Microsoft applications, a common technique used by advanced targeted attacks to gain a foothold before downloading heavy-duty malware.
 - **McAfee Threat Intelligence Exchange Endpoint module blocks unknown malware from running across your environment.** Threat Intelligence Exchange offers an additional layer of defense against zero-day malware. Expanding on traditional antivirus signature and heuristic protection provided by endpoint suites, Threat Intelligence Exchange examines files and allows or blocks execution based on the local endpoint context (file, process, and environmental attributes—for example: does the file execute from the recycle bin? Or is it signed with a revoked certificate?) and the current available collective threat intelligence (organizational prevalence, age, reputation, and more). McAfee Threat Intelligence Exchange boosts traditional endpoint protection against zero-day malware with deeper inspection of unknown files, to prevent unknown malicious files from executing on the endpoints.
 - **McAfee Application Control protects your servers from unwanted programs.** Application Control allows only authorized applications to install and run on your systems. You control who, how, when, and what changes to mitigate malicious modifications. Its dynamic whitelisting feature helps prevent execution of unauthorized malware, including zero-day malware. Since it has a small footprint, it is not resource-intensive and offers an ideal protection for legacy systems with limited resources.
- 2. Arm your countermeasures with the best intelligence.** Now that you have strong anti-zero-day countermeasures in place, you need to provide them with the intelligence to identify and block attacks. Below is a list of the different inspection technologies and intelligence sources used in our products to uncover the presence of malware.
 - **Signatures block known malware.** Signatures are fast, efficient, and precise. When a signature is triggered, you can be confident the file or behavior is known bad. Signatures are used to block viruses, worms, spyware, bots, Trojans, and blended attacks. Our products use a comprehensive knowledgebase created and maintained by McAfee Labs, which currently includes close to 150 million signatures.
 - **Gateway Anti-Malware engine for real-time behavioral emulations.** The Gateway Anti-Malware engine uses multiple emulation capabilities to block zero-day threats that are meant to compromise your environment when users surf the Internet. It starts by dissecting the page into its various components, and then analyzes each component in detail. Finally, it emulates the target environment to evaluate the behavior of the payload. If it is doing anything suspicious, like trying to unpack an encrypted set of code, it will block the content. Some of its most advanced engines include the emulation of both the scripting language that might contain malicious code, and also the browser's functions that might be exploited. The Gateway Anti-Malware engine also includes an Acrobat Reader JavaScript emulator capable of detecting unknown malware embedded in PDF files.
 - **McAfee Global Threat Intelligence (McAfee GTI) unleashes cloud-based intelligence.** McAfee GTI is a real-time, cloud-based intelligence service that provides file, URL, sender, and IP address reputation. It can be queried to check the reputation of a file that has never been seen before and for which no malware signature exists, allowing you to block malware based on a reputation rather than a signature. When a piece of malware does not have a signature, countermeasures can automatically lookup its reputation by querying the McAfee GTI reputation service. Reputation is based on the collective intelligence of millions of sensors deployed worldwide, including at customer sites, 400 McAfee Lab's researchers, and an arsenal of automated tools.
 - **Community-based intelligence learns from what others are seeing.** There are times when you will gather intelligence from your community. That community can be your professional network, industry groups, or security advisories. The Intel Security solutions allow you to import that intelligence into each solution so you can benefit from external sources of intelligence right away. For example, if you learn about new malware through a security advisory issued by a group that is specific to your industry, you can import those bad files' hash and certificates into the McAfee Threat Intelligence Exchange for immediate protection. In addition, you can remarkably augment the technologies and intelligence available to your security solutions by deploying complementary sources of intelligence within your environment. Intel Security offers two additional products that are designed specifically to strengthen the utility and relevance of threat intelligence through deeper analytics and data sharing.

Security Connected Reference Architecture Technology Blueprint

- **McAfee Threat Intelligence Exchange provides local threat intelligence and real-time intelligence sharing.** The Threat Intelligence Exchange server (part of McAfee Threat Intelligence Exchange) is a dedicated server that acts as a repository for all of your threat intelligence. This includes the latest threat information from other countermeasures such as McAfee Advanced Threat Intelligence, our security information and event management (SIEM) solution, McAfee Intrusion Prevention System, and McAfee Global Threat Intelligence. In addition, you can query third-party sources (for example, VirusTotal) and other real-time and historical system-level and enterprise-level intelligence, such as indicator of compromise (IoC) data from forensic analysis. In addition, you can add in local file and certificate data to reflect attacks your experts have found, as well as specific organizational attributes such as in-house developed software. This means you can assemble, override, and tune intelligence source information to modify protection for your environment and organization.
- **McAfee Advanced Threat Defense reverse-engineers malware on the fly with static and dynamic analysis.** Advanced Threat Defense integration with other Intel Security devices and other vendors' products (through RESTful APIs) allows it to analyze new files trying to enter your environment, regardless of their entry point, from the network edge through the endpoint. McAfee Advanced Threat Defense uses multiple levels of static and dynamic techniques to analyze unknown files and nested payloads and determine if they are malicious. When a file is convicted, the software will leverage McAfee Threat Intelligence Exchange to share that information in real time with all security countermeasures, allowing them to immediately block the malicious file. Advanced Threat Defense can also publish IoC data to be used by other systems, including our SEIM solution, McAfee Enterprise Security Manager. Advanced Threat Defense performs a deep analysis of the payload forwarded by other security solutions, when they have not been able to successfully determine the nature of a file. Advanced Threat Defense used as a standalone solution will apply multiple types of inspection, from signatures and global threat intelligence through to the McAfee Gateway Anti-Malware engine (see next item). Where those inspections have already been performed by endpoint or network countermeasures, Advanced Threat Defense adds two complementary methods to analyze a file.
 - **Dynamic Code Analysis:** Advanced Threat Defense starts by running the file in a true sandbox that simulates the target platform—browser, operating system, and other attributes.
 - **Static Code Analysis:** Since not all malware code gets executed in the sandbox, especially if the code is programmed to detect a sandbox, McAfee Advanced Threat Defense then decompiles and examines the static code. It literally reverse-engineers the code to assess all attributes and instruction sets, and fully analyzes the source code without execution. Full static code analysis provides critical insight into input-dependent behaviors and delayed or hidden execution paths that often do not execute during dynamic analysis and are overlooked by less comprehensive sandbox solutions. This enables McAfee Advanced Threat Defense to detect virtually any kind of malware.

The integration of Advanced Threat Defense with other Intel Security solutions constitutes a powerful defense.

	Signatures	Global Reputation (McAfee GTI)	Local Reputation	Gateway Anti-Malware Engine	Static and Dynamic Code Analysis
McAfee Web Gateway	✓	✓		✓	
McAfee Intrusion Prevention System	✓	✓ (for HTTP and HTTPS traffic)		✓	
McAfee Endpoint Protection (McAfee VirusScan® Enterprise software)	✓	✓			
McAfee Advanced Threat Defense	✓	✓		✓	✓
McAfee Threat Intelligence Exchange		✓	✓		

Table 2. Summary of malware detection capabilities.

Security Connected Reference Architecture

Technology Blueprint

3. Connect your defenses to share intelligence in real time. Your countermeasures and intelligence sources might be scattered across your environment and the cloud. The Intel Security solution brings them together, in real time, with the McAfee Threat Intelligence Exchange. As soon as a countermeasure, analytics system, forensic specialist, or third-party source has identified a new threat, that new knowledge is shared immediately with all of the other countermeasures to allow them to block that threat immediately. This means that your environment will become smarter and will automatically adapt to emerging threats. This real-time collaboration between sources of threat intelligence countermeasures is what makes the Intel Security Connected approach so effective against advanced targeted attacks. McAfee Threat Intelligence Exchange connects all countermeasures to share new malware knowledge in real time. Threat Intelligence Exchange provides more than advanced threat detection on the endpoint. It also provides the infrastructure for real-time threat sharing between all of your countermeasures. The McAfee Threat Intelligence Exchange provides proactive sharing of threat intelligence via a communication layer called the Data Exchange Layer (DXL). McAfee Threat Intelligence Exchange, McAfee Web Gateway, McAfee Intrusion Prevention System, McAfee Advanced Threat Defense, and the endpoint protection are all connected with DXL, and integrated partner products are becoming available. If one of those solutions encounters an unknown file, Threat Intelligence Exchange will immediately share that information with all other security products so they can all instantly block that threat if they encounter it. The threat will be blocked at all levels of your defense system without the use of a malware signature. Through the cohesive Threat Intelligence Exchange framework, individual security products can act as a unified defense system. A key component of that framework, DXL allows all the security products—from Intel Security, its partners, and other vendors—to immediately share threat intelligence.

Impact of the Solution

The Intel Security solution provides not only the key countermeasures, but the additional intelligence and connections to each other to benefit from that intelligence. This unique approach will help you defeat attacks that are designed to evade traditional security. Since all the components are connected, there will be tight protection. An attacker can try to be stealthy by getting in through different entry points and using different methods, but because it is connected, the entire Intel Security ecosystem will know about it and block it, helping to prevent compromise. The solution is also built around components that are designed to complement each other to block highly sophisticated attacks. Each countermeasure makes use of an array of protection engines and intelligence geared to check against multiple attack methods, making sure that even if the attacker uses multiple methods of delivery, at least one of our countermeasures will catch one of the delivery attempts. And it only needs to be caught once for the entire ecosystem to learn about it and immediately gain the ability to block the attack.

The inclusion of McAfee Advanced Threat Defense boosts the solution's efficiency. McAfee Advanced Threat Defense is your secret weapon against zero-day malware. It acts as your very own team of antivirus researchers, saving you critical time in determining whether a file is malicious and enabling your countermeasures to take the appropriate action on-the-fly, which makes all the difference between being protected and being compromised.

McAfee Advanced Threat Defense adds the final level to the layered and distributed sources of intelligence used by the Intel Security solution. The many sources of intelligence made available to your countermeasures ensure that they always use the latest and most complete sources of intelligence available to identify and act upon an attack, so you can be sure that no emerging attack will get through your defenses.

But the battle will be won by the speed at which that intelligence can be shared amongst all security defenses. By connecting your security products with the Threat Intelligence Exchange, the proposed solution allows you to share that intelligence in real time, raising the bar on prevention. It gets you as close as possible to proactively blocking targeted attacks. As a result, it allows you to weed out the obvious to allow your precious resources to focus on fewer, more critical incidents. It offers a sustainable, scalable, and continuous framework to handle advanced targeted attacks, and in doing so, it gives you more confidence in your ability to secure your environment. By gathering and sharing intelligence, your security infrastructure will get stronger after each encounter, increasing your ability to continually counter and disrupt the evolving landscape of targeted attacks.

Please read the [Detect](#) and [Correct](#) blueprints next to understand how this solution interacts with other components of an adaptive security architecture.

Security Connected Reference Architecture

Technology Blueprint

Q&A

How can I implement the Security Connected platform if I'm using some components from other vendors?

For customers with a multivendor set of countermeasures, there are APIs and integration options to allow them to get more value from these products as they move to the Security Connected platform. But the more Intel Security solutions you integrate, the faster you will experience a return on investment.

How hard is it to integrate those solutions together?

The solutions that have been designed to work together out of the box do not have any additional requirements to work together. In addition, integration has been significantly simplified through the McAfee DXL. The DXL uses an open-standard protocol to ensure communication between the components, thus reducing implementation and operational costs. For products that allow it, you can integrate them without additional cost or development.

Who else does this platform integrate with?

With the Security Connected platform, you have additional choices for integration. Through the McAfee Security Innovation Alliance, you can benefit from the most innovative security technologies not only from Intel Security but also from thousands of developers that can integrate with our extensible management platform. Today, more than 130 technology partners have joined the alliance. Their tools snap into the Security Connected framework. The Security Innovation Alliance enables you to leverage investments you've already made, bringing strategic tools together, and augmenting them where necessary.

In addition, the platform supports a range of open standards including STIX/TAXII, IoCs, and RESTful APIs. Our products support open standards wherever reasonable. The DXL framework, for instance, uses an open communication standard and any third party can integrate with DXL should they chose.

How should I get started if I'm currently using other solutions?

You can start by bridging what you have into the Security Connected framework. There are many ways to integrate your existing solutions to the framework. For example, new vendors join the Security Innovation Alliance frequently, and their offerings may already be pre-integrated and tested. But there are other ways as well. It would be best to ask your Intel Security sales team what the points of integration are for your specific products.

