The Blended IPS: Leveraging Snort and Optimizing Malware Security

An overture to the open source security community.
The Blended IPS: Leveraging Snort and Optimizing Malware Security
An overture to the open source security community.

Table of Contents

Snort and Open Source Signatures ................................................................. 3
The Challenges of Open Source ................................................................. 4
The Blended IPS: Choose Your IPS Carefully .................................................. 4
  We hold these IPS essentials to be self-evident. ........................................... 4
  McAfee Network Security Platform: The optimum IPS for blended malware security. ........ 5
Importing Snort Signatures onto the McAfee Network Security Platform ..................... 5
Finding New Types of Attacks ........................................................................ 7
  Static code analysis: Uncovering latent threats. ............................................. 7
  Endpoint intelligence: Network visibility of compromised hosts. ....................... 8
Optimize Security Investigations with Transparency .......................................... 9
  Transparency in IPS signature logic and alert details. .................................... 9
  Advanced detection: JavaScript emulation and code execution maps. ................. 10
Limiting Information Overload ....................................................................... 12
  Limiting false positives. ............................................................................... 12
  Providing actionable data. ........................................................................... 12
Blocking Traffic .............................................................................................. 13
  High blocking efficiency out-of-the-box. ....................................................... 13
  Flexible blocking options. ......................................................................... 14
Conclusion ...................................................................................................... 15
The purpose of this paper is to present the satisfied Snort user and open source security proponent with a modestly controversial proposal. We will argue that the most effective way to add advanced malware detection and automated threat blocking to an existing Snort-based intrusion prevention system (IPS) is through a blended IPS deployment that combines the strengths of Snort and the leading commercial IPS: McAfee® Network Security Platform.

Our presumption in making such a claim is prompted by two factors:

- The growing volume of stealthy, targeted zero-day attacks that are successfully bypassing signature-based defenses.
- A sense that some widely held opinions on the relative merits of open source and commercial security software may not fully reflect recent developments on the commercial side.

In fact, McAfee—part of Intel® Security—and the McAfee Network Security Platform now offers the expert security analyst far greater visibility into the triggering events of an attack alert, greater ability to import and customize existing signatures, a far wider portfolio of signature-less detection technologies, and a level of integration between detection and prevention facilities that greatly reduces both analyst workloads and time-to-protection from newly identified threats.

In the end, whether or not our colleagues in the open source community find these arguments persuasive, we hope the discussion will prove interesting and informative.

Snort and Open Source Signatures

For the benefit of non-users who may be reading along, Snort is a free, open source network intrusion detection and prevention system that performs real-time traffic analysis and packet logging on IP networks. Developed by Martin Roesch and initially released in 1998, Snort has evolved into a mature, feature-rich solution that currently claims more than 4 million downloads and nearly 400,000 registered users, making it the world’s most widely deployed technology for network traffic visibility and security. The software is supported by a global community of users and contributing developers, and has become a valuable tool for security organizations looking to share security data and signature protections.

Snort performs protocol analysis, content searching and matching, and can detect a wide range of attacks and probes including buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and more. It uses a flexible rules language to describe traffic and its open source rules can be read in their entirety. This transparency allows users to make informed decisions about the significance of an alert based on detailed visibility into the events and logic that triggered its creation. Direct access to granular attack information is one of the attributes that has most endeared Snort to its dedicated users.
The Challenges of Open Source

Full disclosure is not without its drawbacks, though, starting with a tendency toward labor-intensive administration and the potential to inflict alert fatigue and information overload. With a default preference to deliver more information rather than less, Snort tends to be noisy until an initial installation signature set has been carefully tuned to a specific environment and the priorities of its security team. It is not uncommon for Snort to issue tens of thousands of alerts daily on a busy enterprise network, which can easily lead to exhaustion and paralysis. It's worth keeping in mind that the attacks that eventually caused so much damage at Target were detected by security analysts close to the initial penetration point, but their warnings were disregarded in the volume of peak season security events.

There is also an element of vulnerability associated with the open nature of Snort signatures and the community process through which new threats are evaluated and signatures developed. Both the signatures and the public processes are open to anyone with $30 for a Snort subscription, including malware developers. With a complete view of signatures and detection rules, an attacker can easily understand a defense's signature-based inspection logic.

Open source code can also be analyzed for clues to vulnerabilities, especially by comparing a patched version to a previous release. Locating and understanding a patch can provide strong evidence of the prior vulnerability, which can then be exploited in unpatched systems. Within the closed source security industry, software vendors are commonly allowed the opportunity to patch a vulnerability before publicly announcing it. This ensures that a patch is available as soon as the vulnerability is acknowledged. In the open source community, conversely, vulnerabilities are often announced as part of the patch development process. This was the case with the recent OpenSSL Heartbleed vulnerability, which caused major problems for organizations scrambling to patch the problem immediately.

But Snort’s greatest limitation may lie in its primary dependence on signatures to detect intrusions. New, targeted, stealthy attacks may traverse the network without interference until effective signatures are developed and distributed. As formidable as may be the response capabilities of the global Snort community, there remains an unavoidable gap between the appearance of a new threat and the time when Snort can effectively block that threat on a network. Within that gap Snort’s protective capabilities are limited by its lack of signature-less detection.

The Blended IPS: Choose Your IPS Carefully

Given Snort’s established popularity in signature-based detection, its huge installed base, and the vast amount of user expertise in existing security teams, what is the best roadmap strategy for an organization seeking to move beyond attack detection to proactive intrusion prevention with advanced malware capabilities? Is there a way to build on an existing investment in Snort while reducing exposure to the software’s weaknesses? Is there a development path that better serves operational efficiency? To answer these questions we must begin be defining our expectations of a successful IPS installation.

We hold these IPS essentials to be self-evident.

In today’s threat environment, an IPS solution must do several things very well to justify its acquisition and operating costs, particularly when the IT environment hosts a successful Snort deployment.

- **Build on existing expertise and processes.** If there is existing Snort expertise in the organization with heavily used investigative workflows, the IPS should integrate with, support, and strengthen these efforts.
Find ALL malicious activity. Signature-based detection is an essential IPS capability, but also insufficient on its own. The system must also be able to find and stop the growing volume of attacks for which no signature is available. And since individual signature-less detection methods are inevitably less reliable than high-probability pattern matching, an IPS solution should layer multiple techniques to maximize effectiveness.

Reduce information overload. An IPS should be designed to limit the number of false positive alerts so that IT staffs spend more time examining actionable events and less time excavating alert logs. It should provide advanced workflows to expedite attack assessment, without reducing direct analyst access to granular event detail.

Excel at investigating malicious activity. An IPS should provide deep transparency into the events and logic surrounding every alert, so that all attacks can be quickly investigated and thoroughly understood. It should support flexible integration of new information types and sources as they become available, allowing security teams to adapt and respond to evolving threats.

Reduce time to threat blocking. Finally, while an IPS should alert on all attacks, it should also provide an extensible range of configurable options for rapidly blocking newly detected threats with a minimum of manual intervention by the security team, and a minimum of tuning to optimize accuracy and performance.

McAfee Network Security Platform: The optimum IPS for blended malware security.
We believe that there is, at this time, only one IPS solution that fully meets all these requirements, and that it comes from the commercial side of the security software marketplace: McAfee Network Security Platform. Together with the suite of McAfee products that extend and enhance its already formidable malware detection and blocking capabilities, McAfee Network Security Platform offers the most powerful development path for security teams seeking to extend the capabilities of an existing Snort deployment, increase their ability to quickly find and block previously unknown attacks, and dramatically reduce the administrative workloads associated with sensor tuning and maintenance.

Let’s look at how McAfee Network Security Platform fulfills each of the requirements listed above.

Importing Snort Signatures onto the McAfee Network Security Platform
Leveraging the value of an existing Snort installation starts with the ability to utilize its signature set in a new IPS solution. McAfee was one of the first vendors to provide Snort signature import in 2009. McAfee Network Security Platform supports both Snort and McAfee signature bases, allowing the security team to create an overlapping blend of signature methodologies that raises the level of detection effectiveness while eliminating the delay and administrative overhead associated with recreating existing signatures.
Snort signatures can be imported into McAfee Network Security Platform through the User-Defined Signatures (UDS) Editor found in the software. The UDS Editor is a powerful tool that enables the creation and customization of new signatures and the import or export of existing ones.

Note that when importing Snort signatures, both the .rule and the snort.conf files are needed, as the McAfee Network Security Platform will reference the configuration file for proper Snort environment variables. The import process also provides a de-duplication feature which automatically notifies the user when a Snort signature is imported for a vulnerability for which a McAfee signature already exists. This helps streamline the import process by focusing on specialized or important Snort signatures that may be unique to the security environment.
Finding New Types of Attacks

Signature-based inspection is an essential function for any IPS solution, but signatures alone are insufficient to identify previously unknown zero-day attacks. A robust signature-based inspection engine serves to quickly and efficiently eliminate the large volume of known threats, and vulnerability-based signatures focused on protocol behavior have shown some success in stopping certain unknown attacks, but today’s stealthy malware is adept at bypassing signature-based defenses.

McAfee takes a layered approach to traffic inspection that supplements signature-based methods with comprehensive signature-less inspection. McAfee Network Security Platform stacks up to seven different signature-less inspection engines on top of signature-based inspection that utilizes McAfee and Snort signatures, including dual application of both signatures for a single vulnerability, if desired. The result is the industry’s most flexible and rigorous threat-detection process.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Architecture</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee Network Security Platform inspection</td>
<td>Signature</td>
<td>Native McAfee architecture. Vulnerability and exploit based inspection for protocol analysis and content matching.</td>
</tr>
<tr>
<td>Snort inspection</td>
<td>Signature</td>
<td>Open source architecture. Vulnerability and exploit based inspection for protocol analysis and content matching.</td>
</tr>
<tr>
<td>McAfee Advanced Threat Defense</td>
<td>Signature-less</td>
<td>Full sandbox in virtual environments catches stealthiest of malware with dynamic and static code analysis.</td>
</tr>
<tr>
<td>Real-time emulation</td>
<td>Signature-less</td>
<td>In-line browser and JavaScript emulation with behavioral and structural heuristic malware detection.</td>
</tr>
<tr>
<td>Deep file analysis</td>
<td>Signature-less</td>
<td>In-line emulation for JavaScript in PDF files.</td>
</tr>
<tr>
<td>Endpoint intelligence</td>
<td>Signature-less</td>
<td>Endpoint process visibility on IPS. Identify and stop malicious processes on endpoints establishing network connections.</td>
</tr>
<tr>
<td>Advanced botnet</td>
<td>Signature-less</td>
<td>Intelligent correlation of activity across IPS that signify botnet infestations.</td>
</tr>
<tr>
<td>McAfee Network Threat Behavior Analysis</td>
<td>Signature-less</td>
<td>Intelligent correlation of activity across the network (IPS, switches/routers) that isolate and amplify malicious activity.</td>
</tr>
<tr>
<td>McAfee Global Threat Intelligence</td>
<td>Signature-less</td>
<td>Real-time, reputation-based content blocking.</td>
</tr>
</tbody>
</table>

Here are two examples of how signature-less McAfee inspection technologies help security teams find new types of unknown attacks, the ones that signatures are most likely to miss.

Static code analysis: Uncovering latent threats.

This innovative technology is part of the tiered inspection sequence applied by McAfee Advanced Threat Defense, the malware sandbox component of McAfee Network Security Platform. Static code analysis provides an essential complement to dynamic analysis—the sole inspection technique in most sandboxes—because it reveals the latent behavior of application code that fails to execute in the sandbox. Often this code has been packed, making it difficult to access the source code or predict runtime behavior. Packing programs like Themida and Armadillo are typically used by software manufacturers to prevent others from reverse-engineering their product. These programs have been widely adopted by malware writers to hide their code from sandboxes and security analysts, and unpacking their obfuscated output can be extremely labor intensive.

The static code analysis in McAfee Advanced Threat Defense unpacks obfuscated malware quickly and automatically, providing readable source code in just seconds. It works so well, many malware research organizations buy and use the product for that feature alone.
With the source code in hand, McAfee Advanced Threat Defense can identify malware by its code footprint analysis as well as by its behavior in the sandbox. Figure 3 shows a standard McAfee Advanced Threat Defense analysis report detailing how much of the code ran in the sandbox, and how much of the full source (not just the run code) is similar to other types of known malware. In this example the family classification score identifies 71% of the analyzed malware code as similar to previously seen malicious malware code.

Figure 3. Analysis from McAfee Advanced Threat Defense showing the combined results of dynamic analysis and static code analysis.

**Endpoint intelligence: Network visibility of compromised hosts.**

Another innovative detection method pinpoints successful penetrations using connection context provided by the host systems themselves. Endpoint intelligence addresses a problem common to many large organizations: Isolation of critical security information in the operational data silos of various IT teams. Often the network security team doesn’t get the one piece of data that might trigger an important alarm because it resides in the endpoint team’s management system.

Endpoint intelligence is facilitated by a small plug-in on the McAfee endpoint agent that captures and transmits network connection metadata. This allows anomalies on the endpoint to be identified as malicious at the network level by the McAfee Network Security Platform.

For every endpoint process that requires a network connection, a reputation check is issued. The reputation score, process identity, and other connection data received from the endpoint agent are shared with McAfee Network Security Platform. This enables insights into the origins and nature of network traffic flows that have never before been possible.

Consider the two views of user activity shown in Figure 4. From a network inspection perspective, the IPS sees a connection apparently associated with Oracle running on Carol's PC. But when this information is combined with endpoint data from Carol’s machine, we see that the process generating Oracle network traffic is actually Outlook.exe.
Figure 4. An example of endpoint intelligence. Although the IPS inspects normal Oracle traffic, when associated with endpoint information, security anomalies can be found.

This is an anomaly that should cause concern, and at this point the endpoint can be quarantined by McAfee Network Security Platform and investigated.

**Optimize Security Investigations with Transparency**

When it comes to investigating security incidents, nothing is more frustrating than not having all the information at your fingertips. Two things Snort users value most highly about the solution are its default tendency to surface event information in detail and the accessibility of its open source signature rules. This access is a distinct advantage for security administrators, especially in the pursuit of stealthy, evasive malware. The tendency of commercial security products to hold signature rules and alert detail within a proprietary black box has long been an obstacle to adoption by some security professionals, and McAfee has taken steps to make the signatures and alerting logic used by McAfee Network Security Platform more accessible and transparent.

**Transparency in IPS signature logic and alert details.**

McAfee has opened up its IPS signatures so administrators can immediately understand every alert in detail. Within the alert workflow, the attack descriptor provides compete detail about the signatures involved in the alert and the string matches that triggered them. Packet capture data can also be accessed through the Actions menu to expedite immediate investigation of the event.

Figure 5 shows an example of the alert detail that McAfee Network Security Platform now exposes.
Figure 5. The McAfee detailed alert display provides in-depth access to detection logic and easy access to packet logging details.

Advanced detection: JavaScript emulation and code execution maps.
McAfee Network Security Platform's signature-less inspection engines also provide access to compelling investigative content. For example, our in-line PDF emulation engine provides in-depth output on analysis results. That output—which is easily available within the flow of incident investigation—identifies the behavior of the analyzed file as well as the specific code that was determined to be malicious. This data can then be shared with various security teams to help easily understand and contain malware entering the network.
Figure 6. McAfee Network Security Platform’s in-line PDF emulation engine provides detailed forensics when malicious JavaScript is identified.

If this file had not been convicted by the PDF emulation engine, and had been sent on to McAfee Advanced Threat Defense for sandbox evaluation, static code analysis would have provided security researchers with a complete map of the code’s execution paths—both those that executed and were observed during dynamic analysis, and those latent paths that did not execute but might have given the proper endpoint environment variables.

Figure 7 shows both disassembly reports and malware execution paths as reported by McAfee Advanced Threat Defense. With this type of in-depth information easily available within the investigation workflow, malware analysis can be streamlined and organized in new and exciting ways, providing security teams with a solid basis for fast, accurate alert response.

Figure 7. McAfee Advanced Threat Defense’s malware execution map. Blue is code that ran in the sandbox during dynamic analysis. Red is code that did not run in the sandbox but was still analyzed through reverse engineering called static code analysis.
Limiting Information Overload
Nothing is more certain to alienate a security team from its new IPS installation than alert fatigue—the exhaustion that comes from trying to keep pace with a hyperactive network sensor. Compliance may dictate that all alerts be logged for the auditors, but that doesn't mean that each one must be escalated for administrative attention.

The real test of an IPS solution is twofold:
- How well are false positives understood and limited.
- How directly does the IPS provide the administrator with actionable data.

Let's see how McAfee Network Security Platform addresses these criteria.

Limiting false positives.
McAfee crafts signatures carefully and, before release, tests each one extensively to ensure the best possible balance of security and accuracy. For every signature in our database we provide a benign trigger probability graph. This is our assessment of the probability that an alert triggered by this signature will be a false positive, as well as the probable severity of a real attack.

Figure 8 shows an example. If the dot is up and to the right, you can block with confidence that false positives around this signature will be limited. A large percentage of the signatures in the default IPS policy have a low benign trigger probability. Having this type of information assigned to every alert helps teams get to blocking mode with less effort and provides tremendous value during the investigation phase.

Providing actionable data.
McAfee provides six preconfigured workflows that help surface actionable data by correlating and ranking events contributed by all of McAfee Network Security Platform's advanced detection engines. Key workflows help security administrators investigate malware detections, active botnets, high-risk endpoints, network forensics, and endpoint executables. Figure 9 shows a typical display from the malware detection workflow. All relevant signature-less technologies are ranked according to threat score, and correlated events are easily available within this context for quick and easy understanding of relevant threat data. This gives administrators a running start, and helps drive the priority of incident investigations throughout the network and security teams.
Blocking Traffic
Once our signature set is tuned and McAfee Network Security Platform is up and running, our next priority—and ultimate goal—is to implement blocking mode. If we spend too much time tuning or tending alert logs, we’ll never get there. Once in blocking mode, of course, we want to be confident that the IPS can block as many attacks as possible.

Let’s look at how McAfee has addressed these challenges.

High blocking efficiency out-of-the-box.
McAfee Network Security Platform’s signature-based blocking is one of the highest in the industry as measured by NSS Labs. In its most recent Data Center IPS test, the McAfee solution blocked 99.6% of all attacks. Even more impressive was the lab’s test of un-tuned blocking rates, which measures the detection effectiveness of IPS tools running with default configuration settings and minimal tuning.

McAfee Network Security Platform delivered a 99.2% block rate out of the box, which was approximately the same as the best fully-tuned performance of the second-best IPS solution tested. With such strong default blocking performance very little effort and tuning are required of a security team in order to achieve expert blocking results.
Flexible blocking options.
Finally, McAfee Network Security Platform gives the security team multiple options to match content blocking to its own unique mix of business needs and risk sensitivity. For security teams that are concerned about interrupting network services with unintended blocking, McAfee provides two options which may be of interest.

- **Simulation blocking.** In this optional blocking mode, McAfee Network Security Platform generates alerts based on an applied policy, but allows the suspect traffic to pass. This allows a sanity check on the behavior of a policy or signature set of signatures.

- **Endpoint blocking.** When McAfee Network Security Platform is paired with the endpoint intelligence agent, compromised or malicious endpoints can be quarantined and prevented from establishing network connections. This offers quick, easy blocking at the endpoint level versus network-wide.

<table>
<thead>
<tr>
<th>Blocking Strategy</th>
<th>McAfee Network Security Platform Method</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>By application</td>
<td>Application control</td>
<td>Application control allows blocking of specific apps (Dropbox, BitTorrent, facebook, and games).</td>
</tr>
</tbody>
</table>
| By policy profiles      | Predefined policies                     | There are four defaults policies provided by McAfee:  
  - Default Inline IPS. Standard blocking policy.  
  - Default IDS. Standard non-blocking policy.  
  - All-Inclusive without audit. Based on defaults policy above, adds low-level alerts.  
  - All-Inclusive with audit. Based default policies above, adds low and informational alerts. |
| By traffic type         | Signature rule sets                     | Rule sets are a collection of signatures designed for a specific traffic type including web servers, mail servers, DMZ, UNIX family, and Windows family.  
  - Rule set signatures can feed a custom policy, which can then be applied to an interface or sensor. |
| By network segment      | Sub interfaces or VIDS                  | Network segments can be divided by VLANs or CIDR blocks.  
  - Individual network segments can be inspected by different inspection policies.  
  - For example, on the same sensor interface, engineering network segment can get a lighter inspection policy than the accounting network segment. |
| By endpoint             | Endpoint intelligence and quarantine     | Endpoint visibility on network IPS allows for misbehaving endpoints to be quarantined.  
  - Compromised endpoints will not be able to exfiltrate data and no network connection is available. |
| Test blocking           | Simulation blocking                     | New policies or signatures can be applied while in simulated blocking.  
  - Alerts will trigger and behave as if were blocking, but be truncated with “simulated” in alert viewer.  
  - A sanity check for policies and signatures without actually blocking. |
Conclusion
McAfee Network Security Platform is a commercial IPS solution that merits the consideration of any IT organization seeking to strengthen its advanced malware security, reduce its network security management workload, and leverage its investment in an existing Snort open source signatures. Version 8.1 allows fast, convenient import and re-use of existing Snort signatures. It packs the industry’s most complete quiver of signature-based and signature-less detection methods, provides industry-leading malware blocking performance with minimal tuning or customization, and slashes time-to-protection from new attacks.

McAfee Network Security Platform puts the security team in control of IPS sensitivity, with the ability to limit false positives and relieve alert fatigue. But when quick response is required it delivers actionable, detailed information to guide investigation and expedite remediation.

The philosophical divide between open source and commercial security has deep roots and long history, but the goals of both sides are the same. We at McAfee respectfully offer McAfee Network Security Platform as a bridge that may be useful to all.

1. NSS Labs, Data Center IPS Comparative Analysis, 2014