Solution Brief

Protocol-Based IPS Architecture

Bringing common sense to threat detection

Today, every intrusion prevention system (IPS) claims to offer protocol inspection. Upon casual examination, this statement may be true. All security vendors provide basic analysis of popular protocols. But the fact is, the fundamental architectural design and inspection process of leading vendors' IPSs hasn't changed in more than a decade—with one key exception.

At Intel Security, our approach to protocol-based IPS inspection differs significantly from other security vendors. We use protocol inspection as the foundation of IPS solutions and build advanced intelligence on top of this architecture to provide superior protection and IPS performance. Numerous third-party security effectiveness and performance tests confirm this. To learn more about the role protocol inspection plays in efficient and effective advanced threat defense, read on.

Signature Terminology

- **Signature:** A fingerprint or collection of fingerprints used to identify a known attack.
- **Rule:** The actual syntax of a fingerprint.
- **String matching:** The process of matching a fingerprint to passing traffic.

Signatures, Signature-Less Engines, and Protocol Inspection

Intel Security uses three types of traffic inspection technologies within IPSs to detected malicious activity. Understanding each helps to clarify the role of protocol inspection.

Signature matching to stop known threats

Signature matching (or pattern matching) scans traffic of known attack signatures to detect attacks that have been previously identified and analyzed. This time-tested detection method is used by all IPSs, firewalls, and antivirus detection systems. Once security researchers confirm the identity of a malware attack and understand how it behaves, a signature is created and released, which must be applied to all security devices. The signature is then able to identify future instances of that same piece of malware, and block it. While efficient and powerful, the signature process still creates an inevitable vulnerability gap from the time researchers detect the malware, create the signature, and issue it for release.

Signature matching filters out variants of known attacks. However, this process is not effective for catching unknown threats, such as new attack methods and advanced evasion techniques. In addition, heavy use of signatures can result in high false-positive detection rates. Signature matching continues to have value in security solutions and still plays an important role. While most security vendors depend heavily on signatures as their primary line of defense, Intel Security considers them to be just one layer in a multilayered defense strategy.

intel Security

Signature-less engines

Signature-less inspection is an innovative approach for identifying and blocking unknown attacks. The driving tenet behind signature-less detection is the concept that the technology must find unknown threats by analyzing intent or understanding behavioral context.

Today, Intel Security leads the industry with multiple signature-less malware detection engines. These technologies identify and stop unknown malware attacks with high levels of accuracy and reliability by layering three separate analytical methodologies over a conventional signature-based defense:

- **Attack code analysis:** These technologies use lightweight emulation, sandboxing, and advanced static analysis to assess and predict the behavior of files and executables through direct examination or execution of the code.
- **Attack traffic analysis:** This inspection approach identifies malware attacks within the network through behavioral anomalies in the traffic flows they create. This technique correlates large volumes of network and endpoint events to extract faint threat signals from the background noise of normal network activity.
- **Attack reputation analysis:** This analysis approach adds external context and intelligence to local inspection and assessment.

Protocol inspection

When properly applied, protocol inspection can greatly reduce signature dependence and strengthen protection from unknown threats. As the first dedicated hardware IPS vendor, Intel Security (formerly McAfee) architected IPS appliances from the ground up, building on the foundation of protocol inspection.

How Protocol Inspection Works

Protocol engines parse out network traffic and prepare it for inspection. Each engine is based on industry-standard communication patterns for a given protocol. For example, one engine analyzes HTTP, one engine inspects FTP, one engine handles DNS, and so forth. The behavior and communications pattern of each protocol is well defined. As such, traffic behavior for each protocol type can be predicted and should look and perform a specific way. Conversely, abnormal behavior can also be identified and blocked.

This process can be defined as protocol anomaly detection. Protocol engines can detect abnormal behavior without relying on signature rules. If it's an anomaly, it's blocked, and no additional intelligence or processing is needed. Using this process, Intel Security solutions are able to discard traffic displaying anomalous behavior and focus processing resources on the remaining traffic, which is subjected to advanced signature-less inspection, signature inspection, and global reputation analysis.

As stated previously, most security vendors use some level of protocol detection. For example, all will have protocol engines for HTTP, FTP, and the most popular protocols. However, while most vendors inspect fewer than 20 protocols, researchers at Intel Security have created more than 200 protocol engines that are used by its solutions. In addition, by developing a dedicated hardware platform optimized for protocol anomaly detection, Intel Security's IPS solutions can deliver tremendous inspection accuracy and performance benefits. Since traffic is parsed and normalized first by the protocol engines, the signature check process requires very little additional performance overhead. The difference in performance impact between a single signature check and complete signature database is minimal.

Simple String Matching Doesn't Detect Zero-Day Exploits

Buffer overflows are a common exploit and shouldn't be able to outsmart an IPS. However, IPSs that rely primarily on rules and string matching lack the common sense to catch this basic technique when used as a zero-day exploit. Consider this example:

- A hacker submits a 400-character password in an attempt to overflow a memory buffer.
- Simple string matching won't detect this as an attack, even though basic common sense dictates that real users don't have 400-character passwords—and they don't submit regular text intermixed with binary characters either.
- Decoding the protocol will catch and block this type of anomalous behavior.

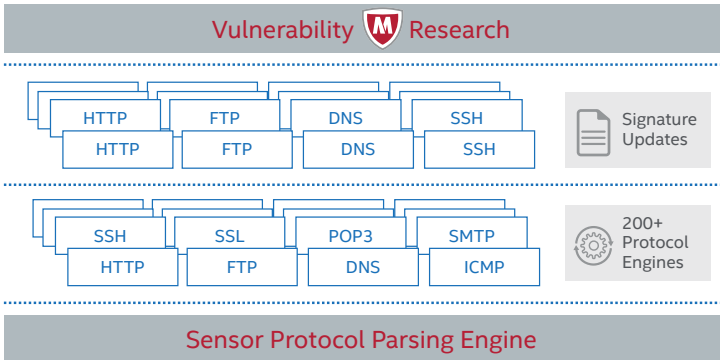

Figure 1. McAfee Network Security Platform's robust inspection architecture, with more than 200 protocol-parsing engines, helps offload the typical performance concerns when running a full signature database at scale.

Beyond Rules: A Common-Sense Approach

While the sophistication of attacks has dramatically increased in recent years, the architecture of security solutions for most vendors has not. Intel Security believes that IPSs must do much more than simply apply signature rules and forward packets. Detecting and stopping today's advanced threats requires behavioral analysis on all traffic flows. For more than a decade, Intel Security's IPSs have been architected to parse and decode the underlying protocol traffic entering the enterprise. The company has built upon this architectural foundation, adding proactive protection using advanced signature-less engines, global threat reputation analysis, and shared intelligence between other Security Connected devices.

To learn more about Intel Security IPS solutions, visit **www.mcafee.com/IPS**.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com