Deep Security/Intrusion Defense Firewall - IDS/IPS

Coverage Statistics and Comparison

Trend Micro, Incorporated

A technical brief summarizing vulnerability coverage provided by Deep Security and Intrusion Defense Firewall. The document also outlines a comparison with a leading network IDS/IPS vendor.

Version 1.2
May 2014

Deep Security/Intrusion Defense Firewall - IDS/IPS Coverage Statistics and Comparison

1. Purpose of this note

Deep Security's IDS/IPS module is one of the key protection modules of the product. IDS/IPS uses Deep Packet Inspection to provide protection against the exploitation of network vulnerabilities. It protects critical servers and endpoints against known and unknown vulnerabilities. This document helps a decision maker understand the value provided by Deep Security and its coverage against vulnerabilities in the software platforms and applications that it protects.

This document also helps in understanding and comparing Deep Security/IDF coverage against a standard network IDS/IPS product. This helps understand IDS/IPS products coverage in the industry, in general, and provides a fair comparison with Deep Security. This comparison has been done against a leading *network* IDS/IPS vendor in the market with a large market share.

2. Background Information.

Since Deep Security's IDS/IPS module focuses on network vulnerabilities, the data represented is only for network-based threats. Also, the comparison has been done against network a IDS/IPS product with respect to network vulnerabilities.
The following points must be noted to understand the rationale behind the comparison:

- Since it's a comparison of network vulnerabilities, local vulnerabilities are not considered.
- A network IPS can theoretically protect any platform so they cover a lot of software platforms and applications which don't apply to the product category that Deep Security belongs to e.g. Platforms like Apple, Netware
- This is a comparison in terms of coverage and not about product features.

3. Deep Security/IDF Coverage Statistics

Deep Security Vulnerability Research Labs provides regular updates every 2 weeks scheduled on second and fourth Tuesdays of the month. Deep Security Rule updates are also shipped out-of-band for 0-days and any critical threats that need to be addressed sooner than the scheduled update. The updates address latest vulnerabilities targeting servers and end points.

Here's a high level view of protection provided by Deep Security in the years 2012 and 2013.

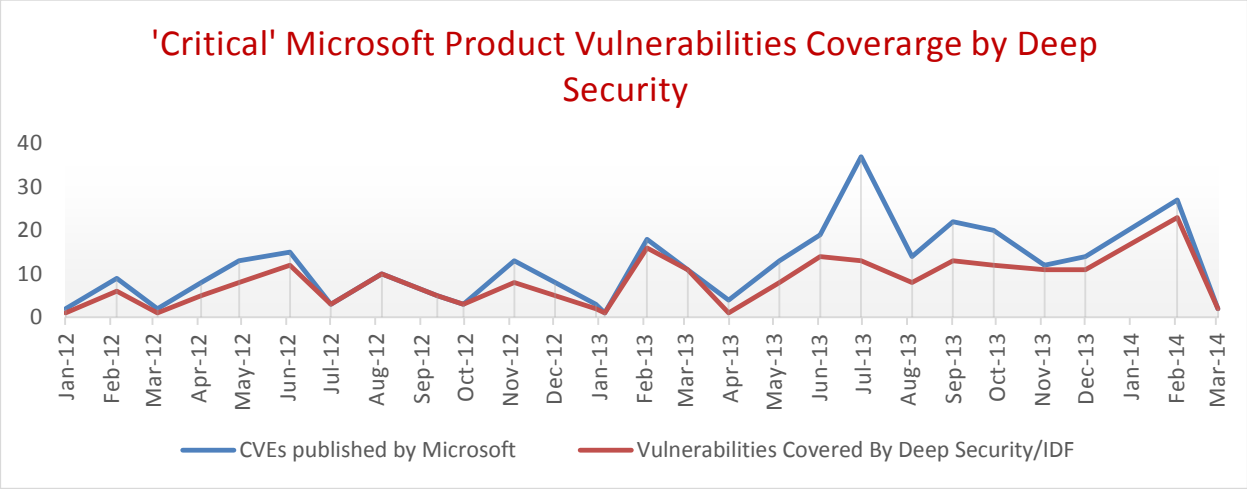
	2012	2013
New Rules shipped	318	477
Updated Rules	288	449
Zero-days addressed	11	12
Rules for Server Applications/Platforms	93	180
Rules for Desktop applications	222	296

To date, Deep Security provides protection for about 900 specific vulnerabilities in Microsoft products.

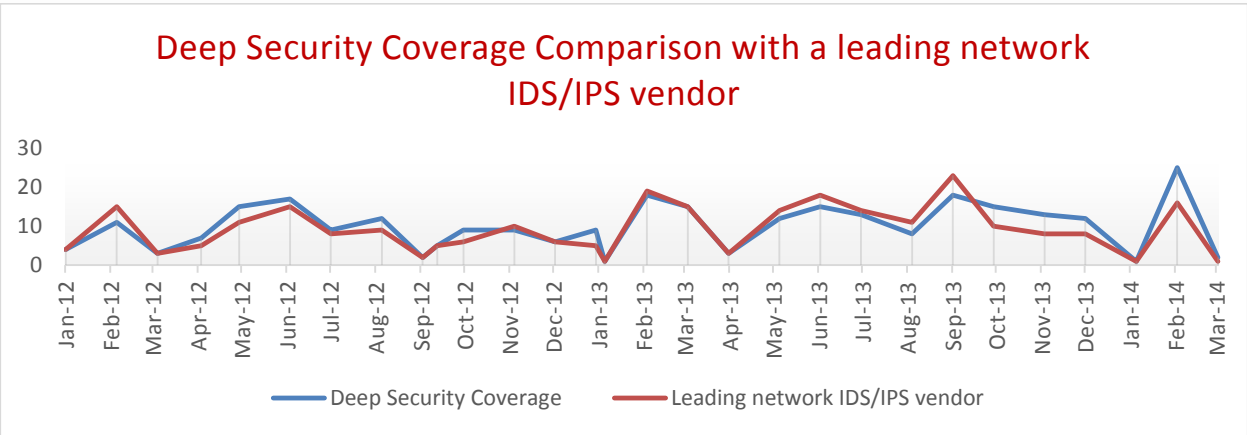
4. A closer look at Microsoft coverage

In 2012 and 2013 Deep Security's Intrusion Prevention module provided protection for 289 Microsoft product's vulnerabilities. There were a total of 548 vulnerabilities published by Microsoft in the entire year.

Although this overall coverage is approximately 50% the graph below outlines how many 'critical' Microsoft vulnerabilities were addressed by Deep Security over the 2012 and 2013 two year period. The rating is based on Microsoft's classification of its vulnerabilities as outlined in its advisories. These vulnerabilities almost always have information from Microsoft provided to Trend Micro as part of the Microsoft Active Protections Program (MAPP). Overall for the years 2012 and 2013, the cumulative coverage of critical vulnerabilities is 69%.



To understand how the comparable network IDS/IPS did protecting these vulnerabilities, here's a comparison of the vendor with Trend Micro Deep Security. This comparison is for 'Critical' Microsoft Product Vulnerabilities.

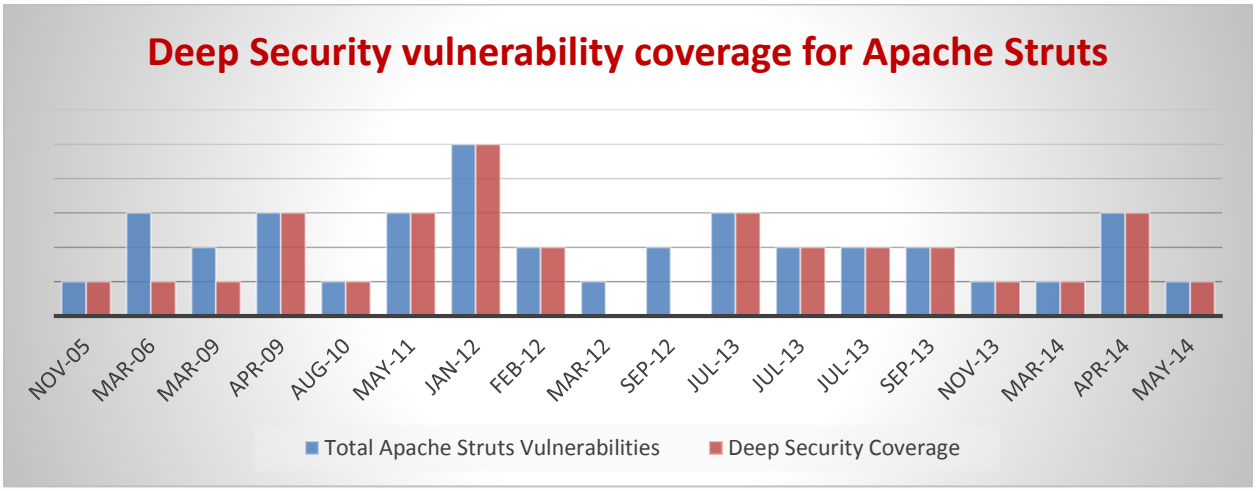


5. Non-Microsoft Products

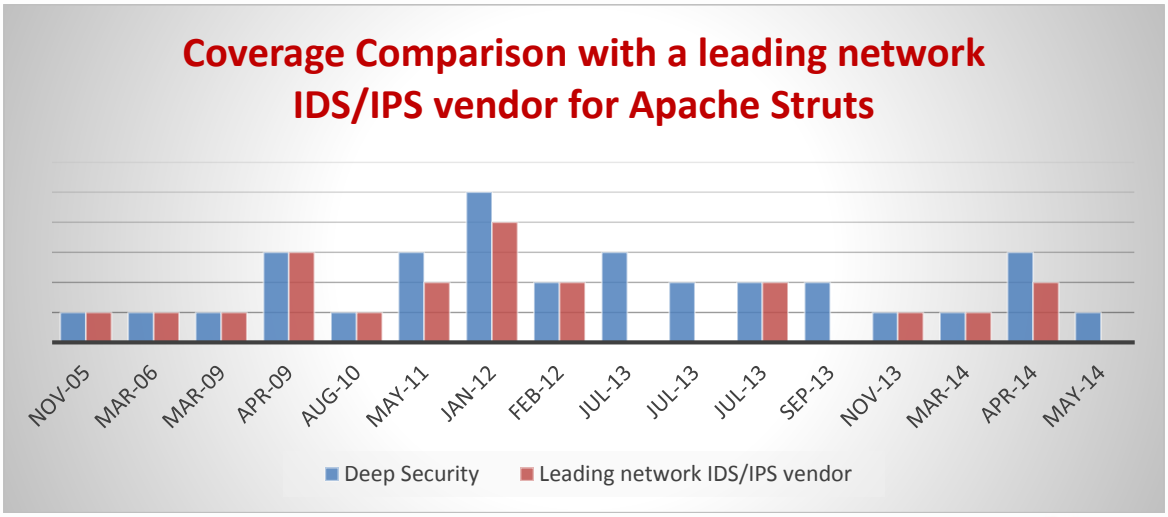
Here's another example of coverage provided by Deep Security for an open source application platform – Apache Struts.

Web Applications are the most internet facing software applications and they can be highly vulnerable. Media talks about specific application vulnerabilities e.g. Adobe, Java etc. when they are used in attacks. However, the attacks on Web Applications still top the chart. SQL Injection, Cross Site Scripting, Web Shell, Command Injections still rule the list as they are the ones which have resulted in the largest data thefts.
The top Common web servers and applications that were exploited in 2013 were Apache Struts, PHP, Wordpress, Joomla etc.

Here's how Apache Struts vulnerabilities coverage looked like.



The following is a comparison on how Deep Security's coverage compares against the network IDS/IPS vendor for Apache Struts



6. Summary

The data presented in this paper summarizes that Deep Security provides effective protection against network vulnerabilities to protect your critical infrastructure including both - servers and desktops.

Also, given the fact that technologically, Deep Security and IDF work quite similar to a network IDS/IPS product the protection coverage for vulnerabilities is similar to a leading network IDS/IPS vendor. There are minor differences because of vulnerability information sourcing, research results etc.

The data clearly shows that Deep Security protects a server or desktop with IDS/IPS protection capabilities comparable to a network IDS/IPS.