Trustwave blocks Web-borne malware - guaranteed, or your money back

Analyst: Adrian Sanabria

16 Jul, 2014

Today, Trustwave makes a bold announcement – a zero malware guarantee. The anti-malware market has no lack of bold marketing, but most are based on comparisons with competitors. It is one thing to say product A is better at preventing malware than product B, and quite another to *guarantee that malware will be stopped*.

The 451 Take

Although a guarantee to 'detect and stop 100% of malware propagated over the Web' initially made us cringe, we now see this as a win/win situation for both the customer and Trustwave. The company is obviously confident in the product, and the cost of paying for failures seems to be small compared with the opportunity to further improve the product when those failures occur. Besides, a failure means an opportunity to advertise SpiderLabs' incident response services. Still, in an age where we're told that breaches and compromise are inevitable, the anti-malware industry could use some guarantees.

Context

Trustwave has been busy rounding out its offering with a total of 14 tech acquisitions since 2006. An additional two were primarily services-related acquisitions. Application security testing vendor Cenzic was acquired earlier this year, shortly after the acquisition of the confusingly named database security vendor Application Security Inc in November 2013. However, it hasn't just been turning around and selling this technology as managed services. The company has focused on developing a centralized back-end and user-facing portal to tie everything together.

Long associated with its PCI consulting practice and payment card-related managed security service provider (MSSP) services, Trustwave has been working to break free of that mold. Its SpiderLabs research and services division, for example, has built a reputation for solid original security research. Trustwave's product offerings go far beyond what is required by PCI as well. In fact, it is one of few MSSPs that can deliver a wide range of fully owned, in-house-developed products rather than a white-labeled or 'bring your own' model.

Trustwave filed for an IPO in 2011, but due to stock market uncertainty, postponed later in 2011 and finally withdrew in May of this year. The company didn't seem to be hurting for cash because it spent hundreds of millions in no fewer than four acquisitions between the IPO filing and retraction.

Products

The product attached to the guarantee is Trustwave's Secure Web Gateway (SWG). With surveys and studies showing that the bulk of malware focused on the Web as an attack vector, Trustwave has chosen to apply the guarantee specifically to this fully managed gateway service. The guarantee allows customers to make claims up to once a quarter. A SpiderLabs forensic team investigates, and if the malware is determined to have been missed by the SWG, the customer receives a free month taken off the subscription and doesn't pay for the forensic investigation.

We see the guarantee as a win for both the customer and Trustwave. Trustwave is showing a great deal of confidence in the product, which is likely to inspire confidence in the customer as well. If it fails, the customer doesn't pay for the service or the investigation. Trustwave wins in that it's already set positive expectations should the product fail, and has an opportunity to demonstrate and advertise its forensic services. The results of the investigation can then be used to improve the efficacy of the product.

In addition to the zero malware guarantee, this announcement also debuts a new SWG dashboard, allowing customers to drill down into each individual Web transaction (yes, every individual GET and POST) and alert. Accompanying the front end is a new big data back end to handle storage and analytics for the huge influx of data this service will produce.

Technology

The SWG is available as a fully managed on-premises appliance, or licensed software/appliance available in virtual or physical form, with a pre-built EC2 version of the virtual appliance also available. A multi-tenant cloud-based version of the proxy is on the roadmap, which will have Trustwave competing from a technical perspective with non-MSSP offerings like that of Zscaler and

Sophos. To be clear, only the physical on-premises appliance is currently available as a managed service. The virtual versions, whether on-premises or in the cloud, are available only as unmanaged services. In addition, the zero malware guarantee applies only to the managed version.

At the heart of Trustwave's anti-malware offerings is its Global Threat Database, which consumes data from its own customers as well as third-party feeds, SpiderLabs and data from consulting services (e.g., incident response, penetration testing). An open API allows Trustwave products like SWG to consume this data, and also allows the company to customize the data and sell it as a variety of threat intelligence feeds.

To back up the zero malware guarantee, Trustwave combines its threat intelligence data with a varied and layered approach to keep threats from getting through. In real time, the SWG scans for threats using static, dynamic and behavioral code analysis. As part of testing behavior, the SWG runs code in a headless browser running in a sandbox on the appliance. Although short of running the code in a full OS sandbox, the compromise is necessary to keep the service real time. Real-time blocking is an important aspect of the service because Trustwave contrasts this approach with the 'someone's got to be patient zero' approach of most network-based anti-malware sandboxes. In this product category, due to the time necessary to let executables run to determine malicious intent, real-time protection isn't possible. A virtual patching approach also allows the SWG to protect against known Web/browser-related vulnerabilities. In addition to all these approaches, commodified signature and heuristic techniques are used as well. If it is already known to be bad, this is (computationally) a low-cost method to stop threats.

Architecturally, the SWG is a traditional forward proxy that is deployed on-premises as a physical or virtual appliance. If placed in a DMZ, off-premises laptops, tablets and smartphones can be funneled through the proxy, although we've spoken to enterprises with mixed results (mostly performance issues) with that approach. Trustwave deploys, installs, configures and maintains the appliance throughout its life. Although the TrustKeeper portal allows the customer to view all events and alerts, Trustwave's SOC will monitor for notable events and notify customers of issues as well. An EC2 version of the appliance is available for cloudy deployments.

Competition

The only other similar anti-malware guarantee we've seen is with Symantec's Norton Small Business security software suite, which is an endpoint anti-virus suite aimed at a different market. If an infection is found or suspected, Norton offers to remove it for free, and to refund the cost of the software if it can't.

On the smaller scale, we see Trustwave's SWG and zero malware guarantee competing with not only other Web gateways from the likes of Blue Coat, Websense and Sophos, but also cloud-based gateways from the likes of Zscaler.

On the larger scale, Trustwave is competing with the general anti-malware budget. We've yet to see any enterprises bold enough to remove anti-malware from the endpoint, so a secure Web gateway is always a complementary control to be purchased with whatever budget is left over after traditional anti-virus is paid for. We believe that it will be necessary in the long run for vendors to aim to supersede or replace traditional anti-malware products. This is partially because security budgets are finite, but mostly because we believe next-generation offerings will be capable of replacing traditional anti-virus in the near future. If this occurs, and the endpoint of the future is capable of adequately defending itself, network-based anti-malware offerings could become obsolete.

The fact that Trustwave's product is fully managed hasn't escaped us. The competition in that market is considerably smaller, with Trustwave's primary advantage and differentiator being its broad set of integrated offerings and the TrustKeeper portal that ties it all together. Symantec, IBM, HP, Verizon, Dell SecureWorks, Alert Logic and AT&T are all competitors, although most don't appear to have offerings as tightly integrated or as comprehensive and only a few of them own and develop near 100% of what they offer.

SWOT Analysis

Strengths

The campaign itself is a strength for Trustwave. Especially in the anti-malware space, we'd love to see products solid enough and companies bold enough to make similar guarantees. If it proves itself, this campaign could put Trustwave in the anti-malware spotlight in a very good way.

Weaknesses

The product addresses only a single attack vector. If we've learned anything about determined attackers, it's that they don't just stop when they fail – when they try again, you can be sure they'll choose a weaker point to attack.

Opportunities

If this campaign is successful, we hope to see Trustwave extend the approach and guarantee to products that cover other vectors and attack surfaces as well.

Threats

If some next-generation anti-malware products are as effective and comprehensive as they claim, network-based approaches could become redundant in just a few years.