NETWORKWORLD Reprint

THE CONNECTED ENTERPRISE = OCTOBER 17, 2016

Check Point SandBlast takes endpoint protection to another level

Credit: Thinkstock

BY DAVID STROM, NETWORK WORLD

Check Point has long been known as a firewall company but it is reaching beyond its roots with a new series of protective technologies under its SandBlast line.

SandBlast has been around for several years, but received several significant updates over the past year to make it a truly effective endpoint protection product that can handle a wide variety of zero-day exploits across your entire enterprise.

The goal behind SandBlast is simply stated: you want to lock down as many entry points for malware as possible, and make your network less of a target for hackers to establish a beachhead and run these exploits.

SandBlast covers email-based attachments, phished emails, embedded links in documents, bad websites and malware already installed on your endpoints. This is very comprehensive, and why the product has merit.

Some of the SandBlast software comes from its acquisition of Hyperwise last year that has been integrated into the product line. Hyperwise developed a sandboxing system designed to stop malware infections before they execute.

SandBlast offers a dizzying array of protective technologies, configurations, integrations and security methods. The hardest part of this product is figuring out what specific configuration to cost-effectively deploy. Once that is accomplished, keeping it running on a daily basis is a no-brainer.

Underlying technologies

SandBlast introduces two new technologies to the Check Point line: Threat emulation and threat extraction. The two operate together to isolate potential exploits. Threat emulation (at least from Check Point) has been around for about a year: when it finds a potential vulnerable data file, such as an infected PDF or Word document with active content, it can block it from being transmitted and automatically kick off a sandbox emulator to detonate the file and see what it does. The sandbox can run a

variety of pre-set Windows OS configurations going back to XP, and by default is set to observe six minutes' worth of real time activity.

Emulation is another cat-and-mouse game that malware authors play with the security vendors. Newer malware versions deploy a variety of techniques to evade detection. For example, some malware is programmed to do nothing for a period of time so the six-minute inspection period might not see anything happening. Others will look for telltale signs that it is running inside a VM, such as registry keys, disk size or specific drivers. And some will also examine human interaction residues like cache files and mouse movements.

This is why the second technology is useful. Called threat extraction, this happens more quickly, within a few seconds of seeing a potential malware target. If the security modules detect active content that could pose a threat, it is removed and the remaining part of the file is transmitted to the user. If the user needs the embedded macros or the scripts, they can wait until the emulator has finished its analysis and will receive notification that the file has been checked out to be clean.

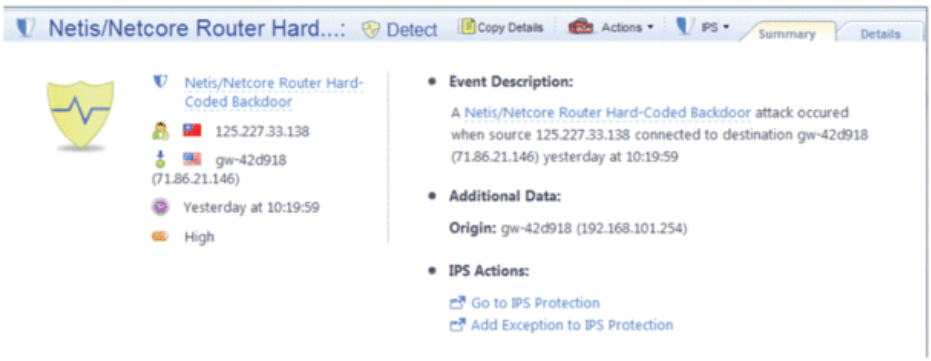
These operations cover not just file scanning but also careful CPU and OS process inspection. This is similar to what the newer endpoint protection products offer and shows how serious Check Point is with this product line.

How it works

During our tests, the product actually worked as intended. No matter what virus package we tried, SandBlast caught it, cleaned it, and stopped the exploit from propagating. Indeed, within minutes of setting up our server with a public IP address, we saw an attack blocked and then logged that was coming from China. It was trying to execute a known backdoor exploit on our server.

When we tried to download unknown virus samples, the unit also blocked them. Infected PDFs and Excel spreadsheets were cleansed as promised, but were still viewable within a few seconds of being received with the active content removed.

To get started with SandBlast you will need some hardware that is on premises, inspecting your network traffic. It comes as a software blade that can be added to one of the existing Check Point hardware appliances. If you already run a Check Point firewall or IPS Security Gateway, this is probably the easiest decision, and the fastest way to implement this protective feature. Not all gateways can run this blade, with some of the very lower-end boxes not



Evidence of an attempted attack from a Chinese IP source.

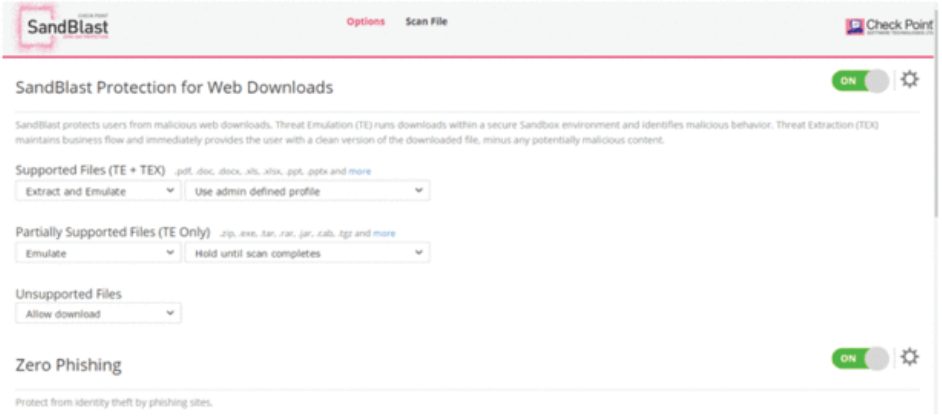
currently supported. This is because of the CPU-intensive nature of the detection schemes. You'll also need to be running firmware v77.30 or later to be able to add the SandBlast blades.

You don't need to be an existing Check Point firewall user, however. You can also purchase one of the second-generation Check Point SandBlast emulation appliances that have been out for about a year that can work with other firewall vendors. These take a piece of malware and stand up a VM to see what happens.

If you have a large network with lots of users and servers, this is probably the preferred path. Emulation takes a lot of CPU and disk, and these need to be done on a separate box. This box can sit at various points on your network. Their location depends on how many firewalls are enabled with the threat prevention software.

You don't need to purchase the emulation appliance if you have the Check Point firewall or other perimeter appliance: you can also deploy SandBlast in the cloud. SandBlast can augment Check Point's existing ThreatCloud service. This is used for reputation management and supports other security services such as intrusion-prevention systems, antivirus and anti-bot protections. If you have a hybrid cloud environment, you will need both the on-premises appliance and the cloud connection to scan everything.

Once you have your hardware and/or cloud servers, the next step is deploying SandBlast endpoint agent software. This comes in two possible configurations. One way is a browser plug-in for Chrome browsers, with IE support coming shortly and others coming later. Any Chrome browser (including Chromebooks but not Android devices) is supported. This is a way to protect your web-based transactions broadly across your enterprise. Setting up the plug-in is dirt simple, and there are a number of options as shown in the screen shot above to configure how the protection features of the plug-in are implemented.



SandBlast plug-in configuration settings for Chrome browsers.

The other way is to deploy agents on Windows 7 and above and Server 2008 R2 and above desktops. If you already use Check Point Endpoint Protection, this is a simple process of adding the SandBlast software to these agents. This includes both forensics and emulation features. The agent contains a superset of protections of what is available from the browser plug-in.

There is one other item, which is how SandBlast works with your enterprise email stream. If you are already using Microsoft Office 365, you can connect to the mail server and it will screen your mail traffic accordingly.

Included in the SandBlast family is a series of APIs that can be used by third party vendors to kick off the emulation and examination processes. For example, Bit9 uses this interface and sends files to the emulator for further analysis.

Once all this gear is installed, you set up security policies just as you would for any other Check Point product. Actually, there is just one rule (see screen shot below) that needs to be added to enable the SandBlast inspection routines. By default, it blocks any "high-risk" applications from running across your network. This includes file-sharing sites such as Dropbox. Making an exception to this to allow access is quickly accomplished with a few mouse clicks.

There are other configuration settings for SandBlast that are more specific to how the threat extractions happen, which particular file types are selected for examination, what information is presented to the user when a file fails the security checks, and whether you want malicious files converted to benign PDFs. That is all done on the screens shown below.

But if you are new to Check Point or haven't used their products lately, you will have a learning curve to get up to speed. SandBlast comes with a suite of attack visibility tools like SmartView Tracker, SmartLog and SmartEvent. These tools aid in forensics and help see what the malware detected by the sandbox would have done, had it been allowed to run.

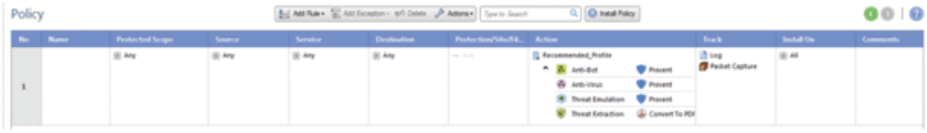
Depending on their focus, these reports will either be completely understood at first glance or look like Greek, and that goes to the biggest challenge of using the product. Because SandBlast bridges the worlds of desktop, enterprise, and infrastructure security, different personnel will have different reactions, different turf battles, and different experiences with it. In addition to these consoles, you can always go to the command line to investigate what is going on with your box.

Some of the reports and threat information displayed are just one step removed from log files that can take a while to parse and become actionable information. For example, if you have both the browser plug-in and the Windows agent running on the same PC, you will generate two security events for a typical phishing session: once as the webpage passes through the browser and another as the agent captures the information. This could be confusing or require coordination if you decide to deploy both plug-in and agent on your endpoints.

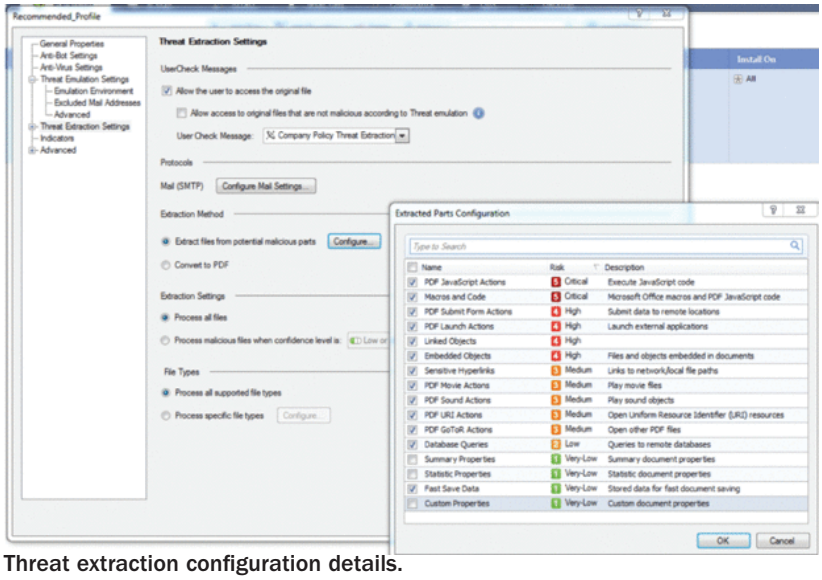
Other reports are more management-friendly and have HTML links to drill down further into specifics, as the analysis summary report shown on the next page.

SandBlast takes a cue from many of the advanced endpoint protection products we reviewed earlier this year in showing kill chains and residues deposited in great detail, along with timelines showing how quickly an infection can spread.

For example, while the malware is running inside an emulated VM, the protection software watches and automatically takes its own screen shots periodically to show you what happens with the malware as it does something bad or unexpected. These screen shots become part of the forensic report that is produced and archived for later examination. You can vary the default values for maximum file size to be examined (15 MB) and the time period to watch its behavior in the security policies.



This is the single policy rule needed to enable the SandBlast services.



Threat extraction configuration details.

Reports and consoles

SandBlast has a plethora of management consoles and reporting systems that can be used by a variety of IT workers. These are the standard Check Point consoles and if your staff is already familiar with how to navigate these screens there is little to add or to learn in terms of workflow when a security event happens.

How we tested

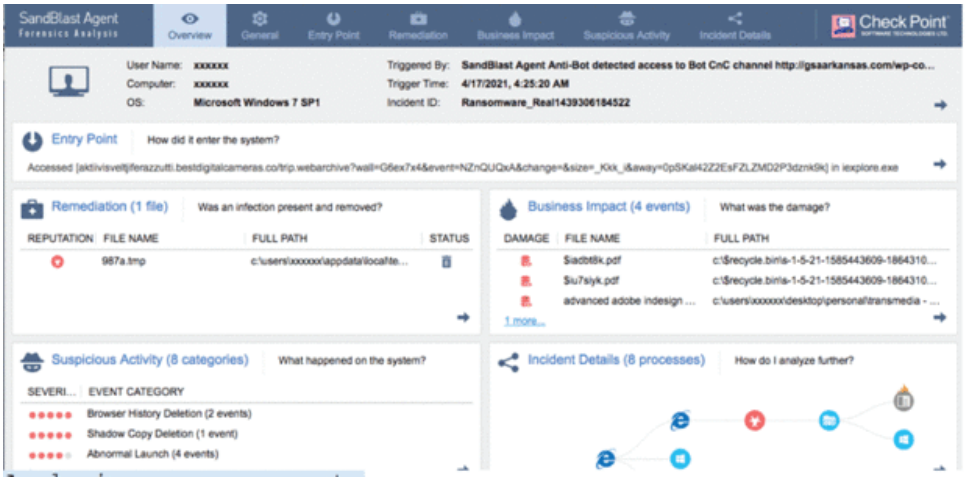
We tested SandBlast at the offices of one of their value-added resellers, Enterprise Consulting Group (ECG) outside of St. Louis. (There are about 20 other VARs that have been qualified by the company to support the product around the US.) We used a Security Gateway 15600 model and connected it to several Windows 7 and 10 clients and a Kali Linux box as a source of threats. We downloaded, or tried to download, a series of malware, both already known and several new threats that had just been posted to VirusTotal, OpenPhish.com and other similar sites. We examined the reports and alerts produced by the SandBlast products and compared it with what other endpoint protection products we've seen, along with setting up protective policies and changing the product's security parameters.

Pricing

You might suspect with a product with so many moving parts that pricing is complex. It took us over an hour to study the various online pricing pages and further discussions with company representatives before we could comprehend what we would pay for our configuration, let alone understand the cost range of other models. There are three basic components to the overall price: endpoint agents, appliance/cloud servers, and management software.

If you purchase any of the software agents, they start at $18 per user per year for the cloud-based protection and go to $55 per user per year for everything included. This latter price includes using the browser plug-ins, which if purchased separately are $15 per user per year.

The cheapest Security Gateway model that supports a usable SandBlast installation –



Analysis summary report.

such as with dual power supplies and a 10GB NIC -- is the 5600. This starts at $34,400. We tested the 15600 model that starts at a base price of $79,000, but you will end up spending at least $100,000 by the time you supply multiple NICs and other high-performance options such as support for multiple VMs to segment your network. The second and subsequent years renewal are $15,500 for the smaller appliance and $30,500 for the larger one that we tested. If you go the route of buying one of the SandBlast appliances, the smallest one called the TE100X starts at $27,000. This price is based on processing 100,000 files per month and is recommended to support 1,000 users: if you need more capacity, you will want a larger-sized and higher-priced appliance.

On top of these prices, if you are buying multiple appliances that you intend to distribute around your global domain, you will also need to add a Smart-1 enterprise manager. This is what Check Point sells to handle policy creation and management for its entire security line. That can add several thousand dollars to the final price tag.

Add all of this gear up, and you are very quickly into the six-figure space pretty quickly if you have hundreds or thousands of endpoints.

Conclusion

Despite the high price tag, Check Point has spent some time figuring out how to do endpoint and zero-day protection effectively and with the right collection of gear. It won't be cheap, especially if you are a small enterprise. To see what Check Point can find on your network, they offer a free security checkup service, start with this URL here. And you may need the services of one of their VARs to help figure out your most optimal configuration and to get started. But for an effective means to protect against unknown exploits, SandBlast is worth its cost.

Check Point®
SOFTWARE TECHNOLOGIES LTD

WORLDWIDE HEADQUARTERS
5 Ha'Solelim Street, Tel Aviv 67897, Israel
Tel: 972-3-753-4555 | Fax: 972-3-624-110
Email: info@checkpoint.com

U.S. HEADQUARTERS
959 Skyway Road, Suite 300, San Carlos, CA 94070, USA
Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233