CSO

BUSINESS RISK LEADERSHIP

July 13, 2017 www.csoonline.com

TODAY'S TOP STORIES

SandBlast Mobile simplifies mobile security

Check Point's SandBlast Mobile fits in between mobile device managers and security event log analyzers, and actually makes it easier to manage the overall security footprint of your entire mobile device fleet.

By David Strom

Credit: IDGNS

Many of us would rather give up one of our limbs than stop using our mobile phones or tablets. But as we become more addicted to mobiles, it means more opportunities to be infected by malware and other exploits. And if our phones are infected, chances are attackers can use them as a gateway to our corporate networks.

Mobile threats are on the rise, due to a perfect storm of circumstances. Mobile devices have traditionally been less protected than desktops, and the amount of malware in app stores is increasing. Some apps that claim to protect users are really infection vectors, known as 'FakeAV'. Millions of users have downloaded these apps, quickly turning BYOD into BYOT -- Bring Your Own Trouble.

In addition, reading emails on your phone means you have less time and less screen real estate to scrutinize their content, making it more likely you will open a phished attachment, click on a malicious link, or bring up a document that contains malware.

Finally, poorly constructed apps that are susceptible to man-in-the-middle attacks allow hackers to intercept data as it passes from a device to a server. Last February, security researcher Will Strafach identified dozens of IOS apps vulnerable to these kinds of attacks.

As a result of these threats, traditional AV vendors such as Avast, Symantec, and others have produced mobile versions of their endpoint apps. And a new category of startups -- like Lookout Security, NowSecure, and Skycure -- have begun to provide defense in depth for mobiles. Another player in this space is Check Point Software, which has rebranded its Mobile Threat Protection product as SandBlast Mobile (SBM).

This is a completely different product from the SandBlast product I reviewed last year. Check Point acquired the technology behind SBM two years ago when it bought Lacoon, another Israeli security vendor. I looked at SBM in June for this review.

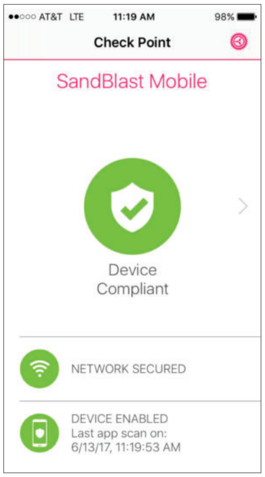
Easy Install

SBM fits in between mobile device managers (MDMs) and security event log analyzers, and actually makes it easier to manage the overall security footprint of your entire mobile device fleet. You will still need an MDM product to really implement things such as application whitelisting, segregating work apps and data from personal ones, tracking a stolen phone, controlling network access, and other tasks that aren't necessarily security-related. One of the nice things about SBM is that it works well with several MDMs, including Airwatch, MobileIron, Maas360, Blackberry Enterprise Server, and Good Technology.

SBM comes with two critical parts: a smartphone app, either for Android (running at least v4.03) or iOS (running at least v8), and a web-based console that connects to various cloud components, including Check Point's ThreatCloud malware investigation service. ThreatCloud collects malware and exploits from more than 100,000 nodes sitting on networks around the globe; it currently contains more than 11 million samples.

This is probably the simplest Check Point product that I have ever used because you can get it as a complete software-as-a-service tool that requires no hardware. (If you would rather have your data remain on-premises, Check Point sells a separate hardware appliance that will satisfy this requirement.)

The hardest part will be



●●○○○ AT&T LTE 11:19 AM 98%

Check Point

SandBlast Mobile

Device Compliant

NETWORK SECURED

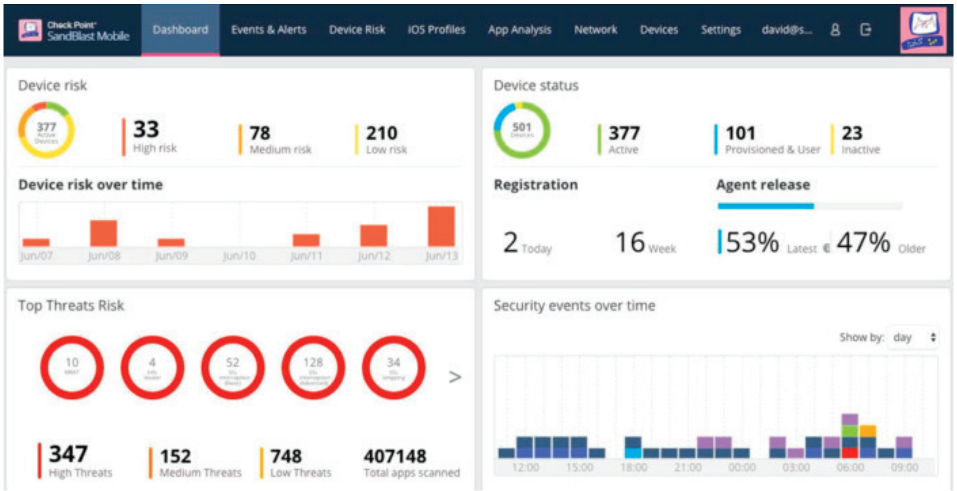
DEVICE ENABLED
Last app scan on:
6/13/17, 11:19:53 AM

David Strom/Check Point

SBM's phone status screen is simple and doesn't have many controls.

setting up integration with your MDM and log analyzers, as well as activating your end users. You can activate SBM either manually or automatically by installing it via an MDM. The manual method sends out a link to download the app via email or SMS notification.

I tested the SaaS version on a variety of Android and iOS phones, including my own iPhone 7. I tried both manual install methods as well as using the Airwatch MDM to automatically install SBM through one of its policies. Once downloaded, it is just a few clicks to install, even on iOS devices where extra confirmation dialogs are required.



David Strom/Check Point

Check Point SBM's main dashboard gives you the 30,000-foot view of all your mobile devices.

SBM scans in depth

SBM runs four different protective scans on your mobile devices The first type of scan is the analysis of known threats and malware signatures – which is what typical phone-based AV tools do.

Sandblast also adds three additional scans:

- Dynamic sandbox emulation for Android only, which runs apps in a virtual environment to test for any suspicious behaviors.
- Advanced code flow analysis. This looks for evasive maneuvers or code samples, which are sent to human evaluators to prevent false positives.
- Reputation management and threat intelligence. This looks for who owns the certificates and whether an app is genuine.

These additional scans are why SBM is considered more defense in depth: It goes beyond looking for signatures and dives deeper into the malware's actual behavior.

SBM's web-based Dashboard displays a view of your entire mobile population. It is organized for large collections of thousands of devices, where an administrator can search and quickly find issues and threats.

The Dashboard has separate menus for events and alerts, for showing devices at risk (where you would do any forensics), a list of apps that it has found on every phone across your network (scored by risk and installed base), network connections at risk (reverse proxies, SSL hacks, and MITM attacks), and a collection of settings screens. You can drill down from the Dashboard via hot links to specific categories, for example, if you want to find out where all the high-vulnerability devices are located. The screens automatically update every minute; unfortunately, you can't change the frequency of updates.

If you want better login control for your admins, SBM currently only supports Google Authenticator for MFA access. Check Point is working on a SAML connector for later this year.

While the Dashboard is chock full of configuration choices, Check Point has already made most of them for you. This makes getting started quicker: other tools require more customization to be useful out of the box. Apps are assigned various risk levels by default, and non-malicious apps' risk levels can be changed by an administrator. You can quickly focus on which apps are causing the most pain and work on eliminating them from your network.

One of the advantages with SBM is a very granular user roles selection, ranging from super users who have rights to everything, to basic security managers who have minimal rights, with six categories in between. Another nice feature: You can change user access levels immediately without having to log out.

SBM in Action

Using both Android and iOS handsets I ran through a series of infection scenarios, including launching several man-in-the-middle attacks, ran malware apps that seem legit but are designed as information stealers, and downloaded phishing scams from OpenPhish. I also tested SBM against Stagefright, an Android exploit that grants an attacker root access. Finally, I tried downloading random infections found on Virus Total; those that were genuine malware were immediately flagged. (VirusTotal does have numerous entries that aren't actual malware.)

SBM found all of our intentional infections quickly and displayed notifications on the phone and management dashboard within a few seconds.

However, there are a few drawbacks to SBM. First, it doesn't remediate any problems with the phone -- IT managers or end users have to take the appropriate action. But there is one exception: If SBM detects that your phone is now part of a man-in-the-middle attack, it will recommend moving you to a special VPN maintained by Check Point. My phone got such an alert and immediately moved me to this VPN. Once my phone was placed on this VPN, I had a problem using the Sandblast VPN with the Uber app; car locations didn't show up on the map, making it useless. Check Point is aware of this and working on a fix.

Another drawback with using the VPN is that it is somewhat power-hungry, depleting my battery from a full charge in about 10 hours.

Finally, the MDM integration with Sandblast brings up an important point. If your organization is big enough, chances are you will have separate staff to handle the MDM and security activities. This could create a turf battle over who controls SBM activities. It will require some cross-training on both the MDM and SBM management consoles so your staff understands how to install SBM and how to handle its security alerts and mitigations. While this isn't a technical problem -- the integration is satisfactory -- it could be a major political stumbling block in using SBM, or really any mobile protection tool.

Overall, SBM offers solid mobile protection for your end users, and is very affordable, starting at $5 per month per protected device. It is certainly worth the expense, given the cost of cleaning up after an infection.

SandBlast Mobile

https://www.checkpoint.com/products/sandblast-mobile

Pricing: Either $5 per device per month, or $10 per user per month for up to three devices. If you want to isolate your private data from Check Point's cloud management tool, you will need additional hardware to run SBM on-premises. ■

David Strom — Contributing Writer

Check Point®
SOFTWARE TECHNOLOGIES LTD

www.checkpoint.com/mobilesecurity