NETWORKWORLD Reprint

THE CONNECTED ENTERPRISE ≡OCTOBER 31, 2016

Beat the bad guys at their own game with SafeBreach's simulated cyberattacks

SafeBreach takes vulnerability assessment to the next level with continuous monitoring, simulations and wargames

BY JOEL BREEDEN II, NETWORK WORLD

The best way to get experience with most jobs or tasks is to do them. It's difficult to learn how to drive a car without getting behind the wheel. Soldiers need to face the enemy in order to gain combat experience. And IT administrators have to experience and mitigate attacks to learn how to best defend their networks.

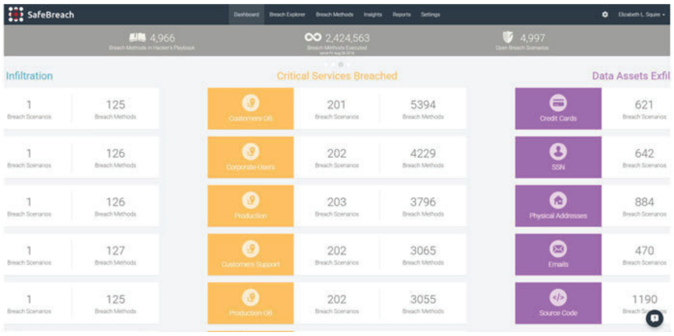
The problem with these scenarios is that they involve a degree of risk. It's not all that helpful to learn how to counter a cyberattack if the first one you experience puts your company out of business.

That's where the SafeBreach continuous security validation platform comes in. Deployed as a service, through the cloud or internally, it can show cybersecurity teams exactly where the network vulnerabilities are and how to plug those holes. It can even run wargames so that IT teams can learn the best ways to respond to attacks on their actual networks.

We reviewed SafeBreach with a test network of thousands of virtual clients. There were data servers and clients, with systems configured for business groups like customer service and accounting.

Deploying SafeBreach is extremely fast. It works within cloud-based services like Amazon, and on physical systems and hardware. It can even be deployed in a hybrid configuration, with the actual software installed as an appliance, or as software running on a host machine inside a network.

Once the core program is installed, you need to deploy agents on every system within the network. The agents don't need any special permissions and work with Windows, Mac and Linux clients and servers, both physical and virtual, and also in the cloud. For the most part, the agents only need to know that the box or virtual box exists, where it exists, and basic information about it. They act as a target for the attacks that will later be simulated.



The main dashboard shows all the different scenarios that can be safely run by SafeBreach to simulate attacks against a protected network.

Long live the new and improved AV

One thing we discovered during our setup process is that when deploying agents, users should place one machine sitting alone outside of all corporate firewalls. Placing an agent on that outside box will allow SafeBreach to use it to simulate the rest of the world. Specifically, the outside box can become an attack vector in the pending simulations, which is important since most real-world attacks are going to be coming from the outside.

Once SafeBreach knows your network topography, you need to tell it where sensitive information resides. This is done in the Settings tab of the main console. While the system will already know the type of systems and the IP addresses, you still need to define everything else. You can tell SafeBreach, for example, where credit cards, Social Security numbers, physical addresses, e-mails or proprietary information is stored. You will need to populate that data by hand, but it does not take very long thanks to a good graphical interface that SafeBreach generates showing your network topography. The total setup time was less than an hour for a fairly large test network.

It's worth noting that while the SafeBreach program can be advantageous for IT managers at all skill levels, it should probably be set up by higher-level professionals. At the very least, those doing the setup should know where all sensitive data resides, so the map can be accurately drawn. The program does not do any scanning or logging of files on the servers or clients themselves.

So if you want to run accurate simulations, you need to make sure that information about where data resides is completely accurate. Also, if the location of data moves, say if a new server is brought online, that information needs to be updated, so there will need to be some maintenance of SafeBreach over time to ensure that both the network topography and the location of data is kept up to date.

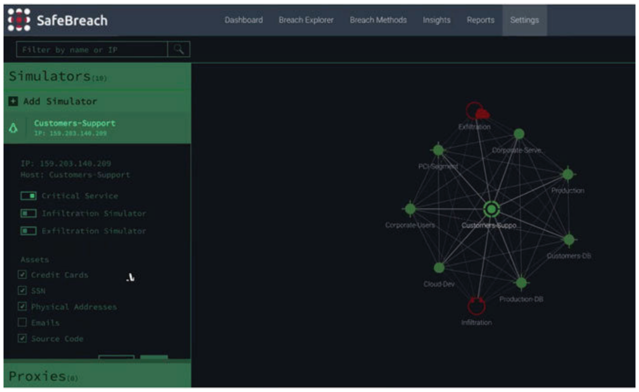
Once up and running, most of the SafeBreach interface will be through the main dashboard, which can look quite scary for cybersecurity teams. For example, right from the start on our test network we saw a nightmare scenario where there were more than 200 critical service breaches, over 600 incidents of credit card data being extracted from the network and over 1,000 incidents of foreign source codes being added to network servers. In actuality, these were just potential breach paths, but it should be more than enough to wake most defenders up to the reality that few networks are completely safe.

The core of the SafeBreach program is the Threat Intelligence Playbook, which is a constantly evolving and updated database of breach methods used by attackers. The current playbook at the time of our testing had almost 5,000 scenarios that attackers use to infiltrate networks. The team at SafeBreach uses Threat Intelligence feeds as well as its own research to keep that list constantly updated with the latest attack methods. Users can trigger simulated attacks against their network, and they will use the same techniques that the actual attacks follow. The only difference is that the simulated attacks are only going to reach out and touch the agents, not affect any part of the systems themselves.

But before you even run an attack scenario, it's probably a good idea to look at the information that SafeBreach can generate about network topography. For example, when we clicked on a server which we thought was deep inside the network that contained sensitive information, SafeBreach was able to show us that there were 137 paths from the outside, using our lone box placed out of the network as a starting point, to an intermediary system with no useful data. That critical link in the chain turned out to be a production database with nothing critical stored there. But from that step, should an attacker compromise that system, there were hundreds of paths that inched closer to the critical server, and 291 that went directly to it.

That told us two things about our current network security before we even ran a single scenario. First, that it was basically two hops from the outside to get to a protected data store, and second, that all of those attacks had to go through a single intermediary system that might have otherwise not generated any intense scrutiny. So one thing we might have wanted to concentrate on, had it been a real network, was locking down that chokepoint with powerful security and active monitoring.

Moving from passive browsing of the network into an actual breach scenario, we first threw the entire playbook at a scenario where credit card data would be stolen and smuggled out. We were not surprised to find hundreds of possible scenarios that might work. But fixing them all at once would take a long time. So instead, SafeBreach allowed us to whittle it down to the most likely scenarios and concentrate on them first. Filtering those results to just breach methods that would allow a script kiddie type of attack, which we thought the most likely, reduced the likely scenarios to just 24.



IP: 159.203.140.209
Host: Customers-Support

☑ Credit Cards
☑ SSN
☑ Physical Addresses
☐ Emails
☑ Source Code

The main dashboard shows all the different scenarios that can be safely run by SafeBreach to simulate attacks against a protected network.

We could then drill down into the specific attacks and found out that one of them relied on a specific remote access trojan that was able to slip through the network undetected, and which could have opened up a path to a command and control server. Massive data leaving the network would not have been detected in that scenario by our current network defenses. SafeBreach gave us the exact type of breach method, the malware that would be used and the path taken by attackers. From there we could generate a ticket with all of that information for IT to patch.

While SafeBreach can't actually fix the problems that it discovers, we have not seen any other program actively simulating an attack and finding specific vulnerabilities. Also, once teams report that the hole has been fixed, SafeBreach can be re-run to confirm that it is no longer a vulnerability. In one case, fixing a problem during our testing actually led to new ones. Although likely rare, SafeBreach can ensure that you are always moving your defenses in the right direction.

In addition to patching network holes, the program can be used to run wargames to help train IT teams. Setting up a scenario is fairly easy in the settings tab where we originally configured our network information for the main program. In our wargame, we used the setting of a contractor with VPN access into the protected network as our starting point. We set it so that the contractor was breached, and the attackers were using that trusted status to infiltrate the main network to steal confidential data.

IT teams could be alerted to the breach in the wargame and then work to analyze it and quickly plug the holes. Once they had taken corrective action, we could immediately check to see if what they did was successful. Working to win that scenario would not only help with morale, but would provide real-world experience that teams could tap into when a real incident occurred. Only there is no risk involved because it was just a simulation, although a very realistic one using the actual network.

It's interesting to note that because the agents deployed by SafeBreach don't need any special access, just a path back to the main program for reporting, we could have brought that breached contractor into the fold, perhaps stopping the scenario before it had a chance to even begin. Doing that would have allowed us to monitor their network for security problems, and given even better insight about the connections between the two organizations.

Pricing for the SafeBreach continuous security validation platform varies by organization, based on coverage and the number of simulators you need to run, so adding contractors might raise your costs. But with pricing starting at about $50,000, it's an incredibly good value to begin with, so there may be room for contractors within the budget.

In cybersecurity, people like to say that you don't know what you don't know. SafeBreach can uncover those unknowns, letting security teams discover exactly how big their potential problems are before they become actual issues. Kept constantly updated with the latest attack methods, SafeBreach can then ensure that potential vulnerabilities remain close to or at zero. After that, the wargaming type of training is just icing on the cake for this unique program that can probably fill an important knowledge gap in most organizations.

Breeden is an award-winning reviewer and public speaker with over 20 years of experience. He is currently the CEO of the Tech Writers Bureau, a group of influential journalists and writers who work in government and other circles. He can be reached at jbreeden@techwritersbureau.com.