NETWORKWORLD Reprint

THE CONNECTED ENTERPRISE ≡ MARCH 06, 2017

Review: vArmour flips security on its head

Instead of focusing on the bad guys, vArmour identifies good processes and locks them down.

BY JOHN BREEDEN II, NETWORK WORLD

Almost every cybersecurity program these days does some sort of scanning, sandboxing or traffic examination to look for anomalies that might indicate the presence of malware. We've even reviewed dedicated threat-hunting tools that ferret out malware that's already active inside a network.

However, what if there were a different way to approach security? Instead of searching for behaviors that might indicate a threat, what if you could define everything that is allowed within a network? If every process, application and workflow needed to conduct business could be defined, then by default everything outside of those definitions could be flagged as illegal. At the very least, critical programs could be identified and all interactions with them could be tightly defined and monitored. It's a different way of looking at security, called segmentation.

One of the advantages of segmentation is that if properly deployed, it can almost reestablish a perimeter type of defensive footing, which has all but evaporated from traditional networks and never really existed in the cloud.

The vArmour suite that we reviewed is designed to allow segmentation to happen in any environment, including massive data centers and in the cloud. It is able to do this without deploying agents and works regardless of the hardware deployed. We tested vArmour in a cloud and virtualized environment to see how this evolving form of security worked, how well it could lock down applications and workflows against tampering and malware, and the level of difficulty involved in setting up and maintaining segmentation over time.

Putting on the vArmour

VArmour is deployed as a virtual appliance within the data path and as a virtual switch which is able to separate workloads at network Layer 2 for control of multiple micro-segments. No changes or disruptions in network traffic happen as a result of the deployments.

Pricing starts at $5,000 for an annual subscription per hypervisor, and being software based, the whole thing is easily scalable to data centers with up to 50T of throughput or 100 million concurrent connections. Our test network did not get anywhere close to that, but the processes and centralized policy interface program, called the Director, was exactly the same for our moderately sized testbed.

When first deploying vArmour, the program was set to Learning Mode. This was not unlike the way that many traditional security programs operate, where the software monitors and logs all traffic to get a better idea of normal network activities.

It takes a fair amount of work to determine all legitimate network activities, and it's unlikely that network administrators will know every single thing going on within their network, and everything that needs to happen within their network, in order to conduct business. This learning process helps to collect that data so sound blanket policies can be created.

This early learning process is especially important because vArmour is designed for very granular, and thus more accurate, control over network processes. For example, you would not use the software to whitelist protocols or entire virtual LANs. Instead, you would allow the use of a certain protocol as part of a specific workflow using specific applications.

So, an authorized user might be able to use FTP as part of the interface between a web application and a database, but not able to use the same protocol to extract files from a different server that is not part of their authorized activities.

This allows for true segmentation and micro-segmentation where very specific uses of programs and tools are authorized. Ideally, this would mean that even if a user had their credentials compromised, the activities of the attacker using the stolen identity would be severely limited. Any attempt to do anything outside of an authorized activity would be immediately flagged and possibly blocked depending on the set policies.

Setting up policies to define all authorized activities can be a lot of work, especially on very large and complex networks. The vArmour software does a good job of helping out with its learning mode, and the ability to take set policies and apply them to other segmented areas. But you will still likely run into instances where individual users are doing legitimate things that are outside of the norm.

For that, vArmour allows administrators to create blanket policies that apply, if nothing else does. This could be as simple as blocking any activity that falls outside of a defined and authorized process, allowing the activity but flagging it for scrutiny, or even sending suspicious traffic to a honeypot.

Called a deception point, vArmour allows for traffic that is unauthorized to be sent to a honeypot, in addition to simply logging the activity. The honeypot can be as detailed or as sparse as a user wants, or even look like a copy of the network populated with fake data. It can be part of a threat intelligence or a traditional defense program where collected users and IP addresses are blocked from the regular network if they get sent there. Or it can just be a holding area to give admins time to examine suspect activity.

If a unique activity is being conducted by an authorized user for a legitimate reason, then a policy can easily be added to remedy the situation and allow them back into the real network. The deception point is completely optional, but a powerful tool nonetheless.

For our testbed, the initial setup process took about an hour, though the program was in learning mode for a week or so beforehand. Larger networks or ones where many users are all doing their own thing, meaning less blanket policies could be applied, could take significantly longer. You might even need to deploy vArmour to only deal with segmented areas within the network and then use other more traditional security programs to police the rest of the non-segmented areas.

Throwing down the gauntlet

Once vArmour is configured, most of the administrator interactions are going to be through the Director part of the program. Upon loading, the main screen shows various high-level snapshots about what is going on within the protected network. It breaks this down into a very granular level so that individual bytes, packets and events can all be studied.

In many ways, this is not too different from most traditional security programs. You can see things like the number of unique inbound sources coming into a network and where the outgoing traffic is heading. You can also see how much traffic is being regulated by policies, and what is being caught by the catchall policy that you hopefully setup in the first phase to deal with anything outside of your norm.

The Director has a simple menu running down the left side that allows for the creation of policies and an alert that triggers whenever something is sent over to the deception point and the possible honeypot, if you also set one up.

Most likely, administrators are going to want to deal with deception point alerts first. Either an exploit has been caught trying to do something outside of an authorized policy, or some authorized user is attempting to do some valid process and is getting blocked. Either way, the situation is easy enough to remedy.

At the top of the main interface are two buttons, Monitor and Configure. The idea is that you start in the monitor tab where you can perform investigations about anomalies attempting to act outside of your authorized segmentations. Then you click over to Configure where you can take action. Perhaps you need to authorize that user and his unique process, or perhaps you need to capture IP and other relevant data about an attack that was trying to act outside of vArmour policy so that it can be blocked at the SIEM for the entire network.

The interesting, and comforting, thing for most cybersecurity analysts when dealing with alerts is that for the most part, there is no need to rush. Unlike a traditional security system where an alert may indicate an ongoing attack that needs to be quickly mitigated, with vArmour, as long as you have catchall policies in place, the segmented network and its data are in no danger.

Just because someone is trying to use FTP to extract data does not mean that they are being successful. If they are not using that protocol as part of an authorized workflow, then they are not getting anything and could even be wasting their time in the network honeypot. The biggest danger is probably an annoyed user trying to do something legitimate and having to wait for an authorizing process to be set by the administrator before they can continue.

The program does a good job of showing what every user is attempting to do within the network. You get information about the source and destination IP of traffic, the exact application being used, the category of the application, the amount of traffic being transferred and the frequency of those occurrences. This data could be used for almost anything from traditional SIEM security policy setting to threat intelligence to insider threat detection.

Should something require a new policy, all we had to do was click over to the configure tab and set it. We could also authorize new workflows in the same way, or create a micro segmentation around a critical application. The only slight negative about creating segmentations on the fly is that users might experience a connection issue to that resource for a few seconds while the new segmentation policy is being put in place or modified.

The vArmour console even ranks applications by risk, much like a traditional security program. Risky applications like those using censured protocols, insecure or older versions of applications and those apps which have been associated with lateral spread or data exfiltration bubble up to the top there.

We were about to jump in and deal with one critical alert, when we remembered that because of the way vArmour was configured, that app wasn't getting anywhere except perhaps over to the honeypot. We confirmed that the cloud was safe, and could configure a specific policy to deal with the risky program if it was somehow authorized for use.

Protected by Armour

On the one hand, defining every authorized workflow and application, and the specific contexts where they can be used, can be a lengthy process that involves a lot of work, despite the fact that vArmour helps to smooth it out as much as possible.

However, doing that work on the frontend will save a lot of trouble once vArmour is fully activated. Assuming your catchall policies are properly configured, nothing bad could happen within any segmented part of the network protected by those policies. Alerts can still pop up, but you don't have to drop everything to deal with them before your critical data is compromised – they are already being dealt with by the policies you previously configured.

The only other way that you could probably create that level of segmentation would be by deploying lots of next generation firewalls, but anyone who has done that probably knows the pain of multiple devices all needing to be patched and monitored.

Plus, in the case of cloud computing, you are basically adding hardware elements to a software cloud, for another potential headache. Besides, most firewalls don't allow the very granular control that vArmour offers. Plus, it puts everything into a central management console with almost infinite scalability, for traditional networks or inside the cloud.

Even outside of industries where segmentation is becoming a regulatory requirement, flipping the way security is dealt with from a constant scanning for malware where APTs still manage to slip through, to one of authorizing valid uses and simply excluding everything else makes a lot of sense. True segmentation was difficult to do without a centralized management structure like vArmour. But it's possible now, and from our testing, works very well to protect the most important parts of any network or cloud.