

Perimeter, Host and Endpoint Security – Finding the Right Mix

One of the oldest assumptions about security is that security is never enough and you can never do too much to protect yourself. The need for security is not new and humans have had such issues since they have been around. If you are protecting a physical location from external attacks, you fortify the exteriors first. But then you further fortify and protect the most important assets with further security. For example, most likely you will want to protect the armory with a special cage and a number of guards. But it is unlikely that you will put a guard at every door, or make every door an armored one for that matter. This for two reasons: first, the cost, and second the fact that too much security can actually get in the way of your daily operations. There is indeed a point when you reach too much security.

It appears that in military terms we have discovered, by trial and error over the centuries, what the right mix of perimeter, host and endpoint security is. IT Security is not that different. Inside your perimeter you are protecting your assets. In IT terms your most valuable asset is your data. But you also need to protect your workstations and servers, to a certain extent, because this in turn protects your data.

The solution to this is obviously a mix, to be addressed at different levels, one of which, often overlooked, is the architecture of your network and the permissions to move around the network. We discuss the issues of security thinking of firewalls and anti viruses, and forget that simply adjusting the architecture of a network and properly segregating functions over different segments can increase the strength of a network and its resilience to attacks.

To focus on the perimeter, because that is where Network Box plays its role, we certainly would like to see companies abandon the traditional monitored passive intrusion detection systems, and moving (finally) to the active intrusion prevention, which requires little monitoring and reacts on its own to attacks. An alert and report system is still useful to know what is happening. But the Internet moves way too rapidly for a human to be able to proactively protect a network by simple monitoring. The system needs to be resilient to attacks, with a proper combination of firewall to lock up what is not needed, and IDP to watch over what needs to be open.

A UTM appliance is by far the best solution, simply because the features and functions that can be achieved by integrating all the parts in one box, cannot be achieved by putting together a number of systems and try to make them cooperate with each other. Even so, any security system is only as good as the last time it was updated. The Network Boxes are updated from the SOC via proprietary PUSH technology, to keep them always up to date, thus reducing the risk of attack by the latest virus or through the latest discovered vulnerability.

Pierluigi Stella CTO



Pierluigi Stella is CTO of Network Box USA, Inc. Pierluigi worked for 15 years at IBM, accumulating international

experience primarily in the oil and manufacturing sectors. With a sterling track record of successfully accomplished projects, an extensive technical know-how, and six years as head of both the technical as well as customer service divisions of Network Box USA, Pierluigi has been helping financial institutions and health care providers develop their security policies, and has accumulated extensive experience and knowledge of security issues. He is one of the founders of Network Box USA. Pierluigi graduated magna cum laudae with a Masters in Electrical Engineering and has received numerous industry recognitions for notable career achievements including two Excellence Awards for innovative design.

Contact Info

www.networkboxusa.com