Endpoint security myths and why they persist

In this interview, Roman Foeckl, CEO of CoSoSys, illustrates the most prominent endpoint security myths and explains why they persist. Furthermore, he talks about the hurdles with protecting endpoint clients in the enterprise and offers advice on what organizations can do in order to stay ahead of the threats.

What are today's most prominent endpoint security myths? Why do they still persist?

Endpoint security is a widely used term that means different things to different people. To make things worse, the term and its meaning has changed over the last 5 years or so. It has evolved from anti-virus/anti-malware solutions, to firewall, device control and intrusion detection. Endpoint security software differs in its definition also from one vendor to another, so one can expect to find data loss prevention capabilities included as well. No wonder that several myths emerged among IT security decision makers when it comes to endpoint security. The use of the term is furthermore evolving since what an endpoint is changes as well and it now includes also tablets and smartphones besides desktops, laptops and thin clients.

Myth 1: Endpoint security equals Data Loss Prevention

As vendors of Content Aware Data Loss Prevention (DLP), Device Control and Mobile Device Management (MDM), we see very often people’s confusion when it comes to endpoint security and Data Loss Prevention, even from IT Admins that all have a slightly different take on the terms endpoint security and Data Loss Prevention. For example, if endpoint security software includes Device Control functionalities, an instant connection to Data Loss Prevention is made.

The error lies in the fact that DLP is focused on internal threats, while anti malware solutions are directed to external threats. Besides that, the Device Control solution integrated or bundled with anti-virus, is limited to a small number of options that can be applied and devices that can be monitored. What about the other exit points? If a user tries to leak a sensitive file through E-mail to a not trusted recipient, how is the data loss prevented with the endpoint security software? In most cases the internal threat is not addressed with an endpoint security solution at all, besides the fact that a malware infection can be stopped. An intentional data breach is not detected simply because traditional endpoint security solutions do not focus on the inside threat.

Myth 2: Macs are a special category of endpoints that don’t require protection

I think probably the biggest myth of all in endpoint security is that a Mac is safer than a Windows PC. This has been somehow true for most of the recent past since Macs have been out of the scope from attackers and not widely used by companies until recently. This has changed and this mindset has to change. Macs just need as much attention to be protected as do PCs from an IT Security point of view, with Anti-Malware measures against outside and insider threats to prevent data losses. Facts show that Macs can be defeated (e.g. Flashback Trojan). When it comes to Device Control and DLP functions, the situation is similar, as many IT Managers consider that a small number of Macs in the company represent a minority, so there is no danger of data breach. They couldn’t be more wrong. It is enough for one employee to copy a highly confidential file on a thumb drive and leak it to the competition or simply lose it. Any type of endpoint needs the same amount of attention be it a Mac, a PC or a mobile device.

Myth 3: Endpoint security is THE security solution and nothing else is needed

The data security strategy resumes to Endpoint Security for many businesses. Reasons like small budgets, lack of knowledge, overlooking of threats that do not come through traditional ways, over-reliance in employees determine managers to maintain the status quo.

The truth is things change and we understand change is difficult most of the times. But there is no other way in a field like IT security. People and IT Security need to adapt to the context and seek to address the diversity of threats that put the company information in danger.

Surprisingly, insiders' threats represent in more than 50% of cases the cause for a data breach. Either a stolen USB stick, external HDD, or a frustrated employee who decides to get revenge by publishing sensitive data or selling it or just an honest mistake are the events related to insiders' threats. These can be prevented by using Content-Aware Data Loss Prevention, Device Control and Encryption Solutions.

Businesses must build their data protection strategy on layers, starting with user identity and access management, server security, network security, cloud and mobile security, DLP, etc. depending on the organization infrastructure. Sticking just to endpoint security is as dangerous as wearing just a helmet on a motorcycle (which offers the minimum level of safety).

What are the most significant hurdles with protecting endpoint clients in the enterprise?

The first and biggest problem is the fact that most of IT staff, like all of us, is reluctant to read documentation. They are too busy to do that and they prefer to have assistance directly from the vendor. I guess it is perfectly justifiable in the pressure of today's lack of time when every new task needs to be completed "yesterday".

Secondly, highly restrictive policies cause drop-off productivity. Users are annoyed by to many notifications and approvals that they have to make and many times their work is interrupted. Resource consumption is a third hurdle that users report to IT admins. There are many endpoint security solutions that require a lot of resources and slow down workstations and daily tasks implicitly.

Another headache is caused by deployment. There are always some endpoints that somehow are omitted, either from the AD, because of compatibility issues, or other technical or organizational aspects.

At times it seems we're fighting a losing battle with endpoint security. What can organizations do in order to stay ahead of the threats?

Even though most of the threats that are addressed by endpoint security software are external, the human factor is equally important because even the strongest anti-virus or firewall cannot stop users to click on a link or download a file that can contain malware. Same goes for Device Control solutions that cannot solely work against data leakage threats, since users are an important component of the implementation. Organizations should assign more resources for users' training and education. An educated user is the safest user. Data security should be as popular as team buildings or product training. Data security contributes indirectly to business continuity and profitability, so it should be treated as such.

What are the essential attributes of a robust endpoint protection solution?

For IT administrators that are in charge of deployment and management, essentially implementing and running IT Security solutions it is vital to have an Endpoint Protection solution that meets the following criteria: covering as many types of endpoints as possible, meaning essentially many Operating Systems (Windows, Macs, iOS and Android) and device types. Ease of installation and management, helpful documentation and support, granularity to allow different levels of authorization and create policies according to the organizational units, intuitive interface and detailed reports represent the essential attributes of a robust Endpoint Security solution.

Ease of use to administer the Endpoint Protection Solution is a primary factor. Having to spend most of your time learning how to deploy and to work with the software, when you are responsible for the solution to actually implement and deploy it is a big negative. The best is to have a fast way to deploy the solution through either virtual- or hardware-appliances or as a cloud based platform for the management components. This way admins can focus on the important parts like composing policies that are enforcing security, but leave users work productively.

If we think about users, there are several requirements that need to be fulfilled. Intrusion should be reduced to minimum so they can do their job. Notifications should be informative and educational and why not, funny. Resource consumption must be also diminished to minimum to avoid workstations' slowdown and keep a good user experience intact.