# Companies That Support Linux: CoSoSys

CoSoSys develops data-loss prevention products for computers and mobile devices that access and store sensitive data. The company's Endpoint Protector 4 (http://www.endpointprotector.com/products/endpoint_protector) features device control to manage Windows, Mac OS X, and Linux machines.

Recently, CoSoSys joined The Linux Foundation and released a private beta version of Data Loss Prevention for Linux, which is available upon request for Ubuntu, openSUSE, CentOS, and Red Hat. The company is also investigating the possibility of expanding its technology to help manage wearable devices.
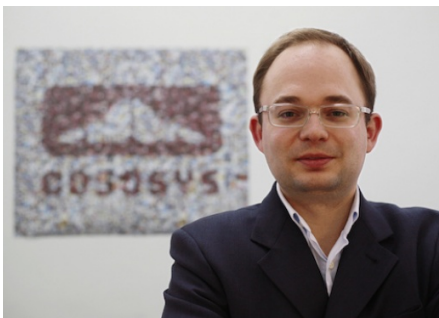
Roman Foeckl, founder and CEO of CoSoSys

To find out more, we spoke with Roman Foeckl, founder and CEO of CoSoSys (http://www.endpointprotector.com/), who explains how and why the company uses Linux and talks about trends that are shaping the industry.

What does CoSoSys do?

CoSoSys specializes in Data Loss Prevention (DLP) for Windows, Mac OS X and Linux, Mobile Device Management (MDM), and Mobile Application Management for iOS and Android, and applications for portable storage device encryption and enhancement. The application portfolio includes functions, such as device control, content filtering, mobile device security, file tracing and shadowing, password security, data synchronization and network security. Our flagship product, Endpoint Protector 4, was named Data Loss Prevention solution of the Year in the 2014 and 2015 Computing Security Awards, and it is certified with Common Criteria EAL2.

How and why do you use Linux and open source?

Endpoint Protector, our DLP and MDM solution, is based on Linux. Our server console runs on the operating system, which allows us to customize the solution as much as we want and to deliver our software as a virtual machine (VM). We chose Linux because it is extremely versatile and secure, which are essential characteristics for any data security product.

The ability to deliver our software as a VM is one of our main differentiators. By combining this with open source solutions, we are able to make more frequent releases

of our product to address constantly evolving security threats.

Why did you join The Linux Foundation?

For us, it was a natural next step since we support Linux with our DLP software, and our solutions are Linux-based. We feel passionately about supporting the Linux community because it shares a lot of our same values, especially with its emphasis on, and reputation for, being secure. In the new open source world, it is incredibly important to give back and support the technologies that so many of today's most influential products are built on.

What interesting or innovative trends in your industry are you witnessing and what role do Linux and open source play in them?

The Internet of Things (IoT) is one of the top innovative trends that is shaping DLP and MDM, and changing data security as we know it.

Interconnected devices, systems, and other items collecting and exchanging data are enhancing the world we live in. Homes, cars, offices, and even cities, are becoming smarter and adapting to and anticipating our needs. While this is enhancing our lives and sparking a new wave of innovation, it also comes with increased risk. These technologies use and store a huge amount of behavioral and other personal data. In light of IoT evolution – the number of Internet-connected devices is expected to reach 50 billion by 2020 – new threats to data security are starting to emerge. DDoS attacks, hijacking or backdoors could pose serious problems for healthcare, banking, and other highly sensitive industries. Therefore, information security vendors have already started to contemplate the development of solutions to secure IoT.

Open source solutions and Linux play an essential part in IoT and in keeping it secure. To date, they are considered the most viable options to allow the development of operating systems that support IoT devices. Open source software allows vendors of diverse infrastructure to adapt it according to the specific use of an IoT device -- for example, a heart monitor that connects to a doctor's smartphone through an app or a smart heating system that starts automatically right before you arrive home from work.

How is your company participating in that innovation?

We are investigating the possibility of managing wearable devices with our MDM solution to provide IT departments a solution to control them, just as they control iOS and Android mobile devices. Wearables are currently very popular, and they continue to make their way into enterprise environments. They are the closest thing to what IoT represents now, so we are determined to take a closer look at how they need to be secured by the IT departments.

How has participating in the Linux and open source communities changed your company?

Open source software is at the base of the creation of Endpoint Protector. Open source solutions and communities, like Linux, provide developers with a rich set of resources that are attainable, making their development easier and in turn speeding up the pace of innovation. Without Linux, and other open source solutions, creating Endpoint Protector would have been much more costly and challenging, and may not have even made it to market.

Is there anything else important or upcoming that you'd like to share?

While Linux is one of the most secure operating systems, users and developers alike need to keep in mind that it, or any technology, is by no means impenetrable. Human error and insider threats are some of the top causes for data losses and data thefts, which can and do still occur even in a highly secure environment. Confidential data can end up in the wrong hands if users upload it or copy it to unauthorized cloud apps and services, or send it to recipients who cannot be trusted.

To address these kinds of scenarios, we recently launched Content-Aware Data Loss Prevention for Linux (http://www.endpointprotector.com/solutions/data-loss-prevention-DLP-for-Linux). The solution provides detailed content inspection before it is uploaded or copied to online applications and blocks the content, in case it is flagged as sensitive, ensuring sensitive data doesn't end up in the wrong hands.

Roman Foeckl is the founder and CEO of CoSoSys (http://www.endpointprotector.com/), and co-founder of Onyx Beacon (http://www.onyxbeacon.com/). Roman's vision is to offer a Data Loss Prevention solution that is easy to use and implement, and covers all popular platforms -- from Mac OS to Windows to Linux. He believes organizations of all sizes should be able to protect their data against accidental loss or intentional theft. He's been a regular contributor to the IT Security community, with articles featured in various outlets, including VentureBeat, SC Magazine, CSO, and many others.