Cyber-security fortresses built on quicksand

Vincent Smyth, Flexera Software

The recent spate of cyber-security breaches, such as those suffered by Sony, Office and Anthem/BlueCross Blue Shield, underscores just how vulnerable enterprises are to malware and hacker attacks. CEOs at organisations of all sizes are well aware of the risks and are taking unprecedented interest in the measures that their IT and security teams are putting into place to fend off potentially catastrophic intrusions into their systems by hackers and other malicious actors.

Towards this end, organisations are building security fortresses that incorporate people, processes and technology to defend against cyber-security threats. While these fortresses are extremely sophisticated at keeping one step ahead of the threats – it may come as a surprise that they are often being built on quicksand.

Security foundations

Security standards and requirements frameworks have been developed by myriad organisations over the years to address risks to enterprise systems and their critical data. The SANS Institute is one of the largest sources for information security training and security certification in the world. In 2008, SANS Institute led a consortium of US and international agencies and security experts to create a prioritised list of security controls that would have the greatest impact in improving organisations’ risk posture against real-world threats.

The first of the prioritised Critical Security Controls identified by SANS focuses on the organisation’s ability to actively manage (inventory, track and correct) all hardware devices on the network so that only authorised devices are given access. According to SANS, this control is critical because attackers are continuously scanning the address space of target organisations, waiting for unprotected systems to be attached to the network. They’re also looking for devices that come and go off the network (such as laptops), that can become software is found and prevented from installing or execution. This is critical because, according to SANS, attackers continuously scan and target organisations looking for vulnerable versions of software that can be remotely exploited. For instance, if an employee using a vulnerable browser is directed to an untrustworthy website, attackers can compromise the employee’s machine by installing backdoor programmes and bots giving the attacker long-term control of the system.

The second of the 20 SANS Critical Security Controls focuses on inventory of authorised and unauthorised software. According to Vincent Smyth, Flexera Software, unlicensed software use is a strong predictor of malware encounters. Each dot represents an individual country’s rate of unlicensed software use and predicted rate of malware encounters. The pattern shows a statistically strong predictive value. Source: BSA/The Software Alliance.
complete software inventories cannot find systems running vulnerable or malicious software to mitigate problems or root out attackers.

An organisation’s ability to effectively inventory its IT assets to identify authorised versus unauthorised hardware and software serves, in effect, as the foundation for the other cyber-security defences. This is so because without this foundation, attackers can and will continually find new vulnerable machines and software as soon as existing, known vulnerabilities have been secured and fortified by the organisation.

This was also the conclusion of a recent BSA/IDC report, ‘Unlicensed Software and Cyber-security Threats’. According to that report, the more unlicensed software running on an organisation’s network, the greater the malware risk. The report concludes that the data’s obvious implication is that lowering the incidence of unlicensed software will lower cyber-security risk.

Lack of inventory

The ease with which unlicensed or unauthorised software can find its way onto company systems is staggering. Most employees can proactively go to the Internet and download software they may need to do their jobs – and often do so instead of putting in requests to their IT departments and waiting for reviews and approvals. Indeed, many employees also install non-work related applications onto their devices, such as music or video applications, that can have questionable provenance.

It may seem obvious that the ability to inventory hardware and software is critical to building a strong cyber-security foundation. And it may seem like a foregone conclusion that most organisations would already have these inventory capabilities in place simply as a matter of sound IT asset management principles. Therefore it may come as a surprise that, in fact, most organisations do not have adequate software inventory capabilities in place – threatening the foundation upon which they are building their cyber-security defences.

According to a Flexera Software ‘2013-14 Key Trends in Software Pricing & Licensing Report’, prepared jointly with IDC, only 36% of the report’s survey respondents said that they use automated commercial software to manage their software estates. The majority of respondents reported using a patchwork of methods – or doing nothing at all. For instance, 25% of respondents said they were managing software licenses using manual methods, such as spreadsheets, while 9% are using home grown systems. Some 18% are using tracking tools provided by their vendors, and 7% are simply not tracking their software licenses at all.

The challenges

Given the lack of broad-based software license management capabilities being implemented, it begs the question: Why is inventorying IT assets such a complex and difficult task? There are actually many reasons.

For instance, with respect to desktop applications, different data sources on a device can be used to identify software applications. None of them provide enough data by themselves – they all must be considered to accurately inventory local installations. These data sources can include:
• Software Packaging data: The add/remove programs (aka ‘Programs and Features’) entries found on Windows devices, RPM (RedHat Package Manager) on Linux, etc. On Windows devices, packaging data provides a very accurate list of software applications installed on the computer. In some instances, additional data may be required to clearly identify the software applications, such as finding the edition installed.

• File data: Executable, dll, ini, jar manifest files, etc, on the hard drive. On the Windows platform, the file header sometimes provides information such as the publisher, the version and the name of the application. The size, name, checksum or content of a file can also be used to identify an application.

• Registry information on Windows devices: For instance, the operating system description, version and edition can be found in the Windows registry.

• ISO tag files: The International Standardisation Organisation (ISO) 19770-2 is probably the best and most accurate way to identify a local software product on a device. It is supposed to provide the name, version and edition of the software product installed, as sold by the publisher. It may also contain the list of the software components and relationships between them. Only a few publishers such as CA, Adobe, Symantec, Flexera Software and Microsoft are using the ISO 19770-2 tag. It applies only to the latest releases of their products.

The raw data from these data sources needs to be filtered and processed to extract the commercial name of the products that require a license. This data represents up to 90% of all inventory data collected in many cases.

Maintaining accuracy

Many tools exist and are capable of performing inventory – the key issue is maintaining the accuracy of the inventory. New machines are installed and old ones retired every single day, and software products are installed, upgraded or removed on a regular basis. If an organisation has 10,000 desktops and laptops for instance, with an average lifetime of three years, 15 computers are retired and 15 are provisioned every working day, on average.

A process is needed to remove or disable computers in the configuration management tool when they are physically retired. The same applies to computers not reporting inventory for a long period of time, as they should be considered lost or stolen. In this case, the process must consider that users can be disconnected from the network for a long period of time – for instance, when they are on leave, travelling or working remotely from their home. Inventory is not performed on all devices at once, but typically on a rolling basis: the picture of the inventory is never 100% accurate on any one day; the challenge is to limit this area of uncertainty.

“When virtualisation technologies are used, these tools will likely fall short with regard to accurately reporting inventory or usage data in many scenarios”

If traditional desktop/laptop inventory can be resolved with inventory and configuration management tools, application and desktop virtualisation technologies may require a different approach. In most cases, virtualised applications leave evidence on a device that can be tracked along with their related usage data from an agent. For instance, this is possible with the latest releases of Microsoft App-V. An alternative solution is to directly query the virtualisation technology API and get either the relationship between virtualised applications and users, or the usage data, if available.

The biggest difficulty in a virtual desktop environment is to identify endpoint devices using the virtual machine. Again, for applications attached to a device-based licence metric, this information is needed. There are different techniques that can be used to get this data, but only a handful of tools are able to collect it. The last challenge is metering usage on applications running in the virtual desktop, some of which could be virtualised. In this case virtualised application usage data may need to be matched against the virtual desktop data to clearly identify the endpoint device. The usage monitoring tools for application virtualisation typically report usage against the virtual desktop itself rather than the endpoint device.

Desktop inventory cannot rely solely on traditional configuration management or dedicated inventory tools. When virtualisation technologies are used, these tools will likely fall short with regard to accurately reporting inventory or usage data in many scenarios. The solution is to use a combination of inventory tools and adapters to virtualisation and cloud technology frameworks to gather data and merge it in a single IT asset management repository for consumption by a software licence optimisation tool.

Datacentre environment

Beyond inventorying desktop software, the datacentre environment has the benefits of being smaller and more stable. However, software license management in this environment requires additional data – from hardware properties to relationships between hosts, virtual machines, partitions and clusters. Some complex server licence models require additional data. Software identification is also more challenging due to the heterogeneous nature of the datacentre and lack of standards.

Datacentre inventory is very different from the desktop world. Despite a smaller number of devices, it is a more complex and challenging environment due to the diversity of operating systems and technologies, the licensing metrics requiring additional data, and the emergence of hybrid (public-private) and private clouds. Different techniques must be used; a device-based inventory will likely fall short of accurately reporting inventory and usage data. As in the case of the desktop world, only a combination of tools will provide the data required for license management and software licence optimisation.
Conclusion

While most organisations have multiple sources of software and hardware inventory, they usually do not have a means to consolidate that data from across all their systems and environments to arrive at an accurate inventory that can provide high-level insight into what authorised versus unauthorised systems are running on the corporate network. And it is this lack of management-level insight that renders the very foundation of their cyber-security fortress vulnerable.

“The best strategy is to understand what data sources are available within the organisation and use them first. Then, deploy and use the additional features of an optimisation tool to arrive at an accurate and update inventory”

Tools are available that can provide this level of insight. Software licence optimisation solutions are already being deployed globally by organisations to help them ensure continual compliance with their software license agreements. These solutions are also being deployed to help ensure optimisation of software spend by helping organisations buy only what they need and use what they have.

Some of these software licence optimisation solutions can also help by providing a consolidated view of software and hardware inventory. By leveraging adapters to existing configuration management and inventory tools, access to virtualisation data via APIs, and additional inventory capabilities delivered by the optimisation tool, organisations should be in position to collect all of the necessary data. The best strategy is to understand what data sources are available within the organisation and use them first. Then, deploy and use the additional features of an optimisation tool to arrive at an accurate and update inventory.

About the author

Vincent Smyth is senior vice president EMEA at Flexera Software, responsible for driving revenue, market share and customer satisfaction in the independent software vendor, high-tech manufacturer and enterprise account domains. Prior to Flexera Software, he has held several sales management responsibilities for Business Objects, PTC and Computer Associates. He has extensive experience of doing business across Europe and the Middle East.

References