User-Based Licensing for Endpoint Protection and BYOD

Five reasons why you should license by employee, not devices

Contents

Brought to you compliments of

WEBROOT®

Can Smarter Licensing Improve Security?

IT managers and security professionals don't spend much time thinking about software licensing. But sometimes a smarter licensing plan can simplify IT administration, reduce costs and improve security. A perfect example is a new model for endpoint and mobile device protection that licenses software by employee, rather than by device.

In this paper, we will look at:

- Why per-device licensing of endpoint protection is becoming increasingly dysfunctional.
- How adopting user-based licensing benefits administration, budgeting, productivity and security.
- The advantages of Webroot's new SecureAnywhere Business User Protection licensing.

Why Per-Device Licensing No Longer Makes Sense

The prevalent model for endpoint and mobile device protection is out of step with reality.

Most antivirus and endpoint protection products for PCs, laptops and servers are licensed by "endpoint" or "node." The same licensing model has been extended to security products for mobile devices.

Pricing by device made sense when the average worker had one desktop PC or laptop connected to the Internet and server environments were not constantly changing due to virtualization. But that has changed today:

- The average knowledge worker had 2.8 network-connected devices in 2012, and will have 3.3 by 2014.[1]
- "Devices" now come in many flavors, including desktop PCs, laptops, notebook and tablet computers, smartphones, virtual desktops running on servers, and physical and virtual server environments.
- Employees are bringing their own smartphones into the company environment, thanks to bring-your-own-device, or BYOD, initiatives. Some staff members often use personal laptops, as well.
- The churn rate of devices is increasing: Americans replace their smartphones every 22 months, compared with three years or more to upgrade corporate PCs.[2]
- Companies are increasingly using virtual desktops, making it harder to count devices — especially since virtual environments are constantly being moved across multiple servers.
- Most organizations have multiple servers connected to the Internet that contain confidential data, including Web, application and database servers.

This complex environment makes it extremely difficult for companies to comply with their per-device license agreements, and equally difficult to project costs into the future for budgeting.

It also undermines security because employees and their managers are severely tempted to cut corners and "forget" to deploy security software to new devices — particularly if they are employee-owned.

But a few innovative vendors have introduced an alternative licensing model for endpoint and mobile security where companies simply need to know the number of employees, and each employee can protect multiple devices. Here's a look at five reasons why your company should consider user-based licensing:

Keeping Tabs

To comply with device-based licensing, organizations must track:

- More devices
- More types of devices
- Employee-owned devices
- More rapidly replaced devices
- Virtual devices that disappear and reappear on different servers
- Servers that store confidential data

Reason No. 1: Less Administrative Burden

It has always been an administrative burden to count copies of software on devices in order to comply with license agreements. Someone needs to keep track of devices that are issued,

[1] "BYOD and Virtualization, Top 10 Insights from Cisco IBSG Horizons Study," Cisco, 2012.

[2] "International Comparisons: The Handset Replacement Cycle," Recon Analytics, June 23, 2011.

recovered, transferred, upgraded, lost, stolen and replaced. BYOD policies and the proliferation of devices have made that job far harder.

This tracking activity is repetitive and boring, and adds no value to the organization. It also leaves administrators with the nagging (and usually accurate) suspicion that they are either violating licensing agreements by undercounting devices or wasting money paying for software on devices no longer in use.

With a user licensing model, administrators simply track the number of employees using the software.

Reason No. 2: Simpler Budgeting

Accurate budgeting can be impossible when the number of devices within the organization fluctuates and when different types of systems — PCs, laptops, mobile devices, virtual desktops, and Web and database servers — have different license costs, with different quantity-discount schedules.

The uncertainty is even greater for organizations that allow employee-owned devices whose numbers are not under the control of the manager or anyone else with budget responsibility. In this situation, social trends and fads can have unexpected effects in device usage during the course of a budget cycle.

It is far easier to project costs when the only variable is the number of employees.

Reason No. 3: Less Impact on Productivity

Do employees need to requisition software for their laptops and smartphones? Do they need to notify someone when they switch software to a new device or transfer a computer to another person? Does a manager need to approve these steps? If so, there is a purchasing or accounting process that involves employees, managers and possibly purchasing and accounting personnel.

While the short-term effect of this process on any one employee's productivity may be small, the cumulative impact over many employees can be very large indeed.

With user-based licensing, you can deploy security software to additional devices without wasting everyone's time on paperwork.

Reason No. 4: Complexity Can Damage Security

Complexity and bureaucratic processes can lead people to cut corners in ways that harm security. Sometimes, licensing issues can drive the company's security posture in bad ways.

If it is annoying or time-consuming to secure licenses for additional devices, some employees are going to circumvent the process by using personal devices for business purposes — without installing security software. This leaves the devices, and the company's data, vulnerable.

If department managers or IT administrators have exhausted their software budget, they may turn a blind eye toward, or even encourage, the same neglect.

With user-based licensing, there are no hurdles to obtaining security software for new devices, so employees and managers have no incentive to find workarounds.

Reason No. 5: User-based Licensing Can Save Money

Saving money on security software makes department heads and chief financial officers happy and leaves more funds are available for other IT projects.

User-based licensing reduces the chances of paying for software that is never used or is installed on systems that have been retired.

Also, user-based pricing will almost always result in lower overall costs when employees have more than one Internet-connected device (see the examples in the appendix).

The Advantages of Webroot SecureAnywhere Business User Protection Licensing

Webroot® has introduced a user-based licensing plan that demonstrates all of the advantages listed above.

The Webroot SecureAnywhere Business User Protection plan is based on a single per-user fee that covers up to four devices per employee, including desktop PCs, laptops, notebook and tablet computers, iOS and Android smartphones, and virtual desktops. Web servers, database servers, file servers and other servers can also be counted toward the total of protected devices, making it easy to protect the entire infrastructure that supports employees and the business.

Each device receives highly effective malware protection, and all types of protection are managed from a single, intuitive, web-based management console.

With Webroot SecureAnywhere Business User Protection:

- There is very little administrative burden, because administrators need to track only the number of employees, not the number and type of devices.
- Budgeting is easy, because costs can be projected based on headcount, a variable that is already included in everyone's budget assumptions.
- Employees and managers can protect data on new devices without wasting anyone's time on procurement activities.
- Employees won't be tempted to degrade security by using unprotected devices.
- Servers as well as PCs and mobile devices can be protected with the same product set and licensing plan.
- Organizations with any significant number of mobile devices can cut costs.

For more information on Webroot's user-based licensing, please visit www.webroot.com/userprotection

Return to top

Appendix — License Cost Savings Scenarios

How much money can be saved with a user-based licensing plan? The answer depends on the plan and the number of employees and devices. But the calculations below show the range of savings for three scenarios. In the first scenario, a company has 80 employees and every employee has a laptop, but only half of the employees have a mobile device. The second company has only 40 employees, but each one has a mobile device. The third has 120 employees, with 1.5 mobile devices per employee. It is assumed that every 10 users require one server that also needs to be protected.

These scenarios show savings for per-user licensing for groups even with relatively low mobile device ownership, and very large savings for organizations with typical mobile device use.

Employees	80	40	120
Per employee: Laptops / mobile devices / servers	1.0 / 0.5 / 0.1	1.0 / 1.0 / 0.1	1.0 / 1.5 / 0.1
Company total: Laptops / mobile devices / servers	80 / 40 / 8	40 / 40 / 4	120 / 180 / 12
Total laptops, mobile devices and servers	128	84	312
Per-Device License Model*			
License cost per system	$26.94	$28.13	$25.72
Total license cost	$3,448	$2,363	$8,025
Per-User License Model*			
License cost per user	$39.99	$39.99	$34.99
Total license cost	$3,199	$1,600	$4,199
Savings With Per-User Licensing			
	7%	**32%**	**48%**

* Assumptions: These calculations are in U.S. dollars based on U.S. pricing for one-year licenses, with standard quantity discounts. With per-device licensing, the servers require one endpoint protection license. With Webroot SecureAnywhere Business User Protection licensing, the servers can be counted as devices belonging to an employee and so do not require a separate license.