

The Software Alliance logo consists of the text "The Software Alliance" in a white sans-serif font, centered within a white square. This square is surrounded by a blue border that forms a larger square shape with inward-pointing corners.

The  
Software  
Alliance

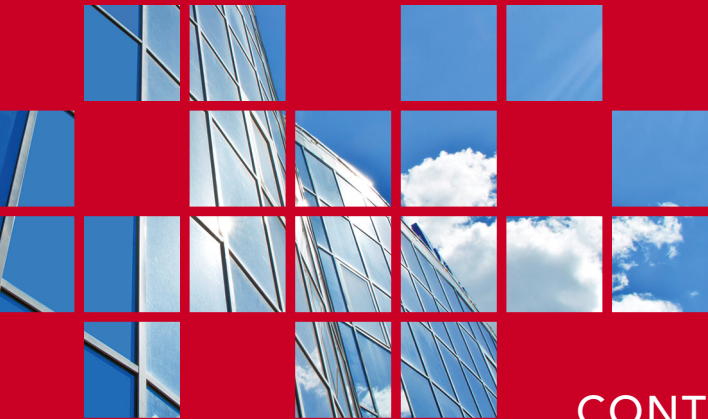
The BSA logo features the letters "BSA" in a bold, white, sans-serif font, centered within a white square. This square is surrounded by a blue border that forms a larger square shape with inward-pointing corners.

**BSA**

# Seizing Opportunity Through License Compliance

**BSA GLOBAL SOFTWARE SURVEY**  
MAY 2016





## CONTENTS

Key Trends and Findings.....	1
A Strong Correlation: Malware and Unlicensed Software .....	4
Global Trends .....	5
Rates and Commercial Values of Unlicensed PC Software Installations .....	6
Effective SAM Needed as Part of Cloud Computing .....	9
Methodology .....	10
Better Protection for Your Organization From Cyber Risks .....	14
About BSA   The Software Alliance .....	16



# Key Trends and Findings

Software provides the essential launchpad for creativity across numerous industries and human endeavors. Through transformational innovations such as apps and cloud computing, software supplies the mechanism through which innovative thinkers are delivering sweeping benefits that touch billions of lives each day.

An important corollary associated with the growth and ubiquity of software is that cybersecurity is a top concern for businesses and organizations around the globe — and for good reason:

- 430 million new pieces of malware were discovered in 2015, up 36 percent from 2014.<sup>1</sup>
- Organizations experience some form of malware attack every seven minutes.<sup>2</sup>
- In 2015 more than half a billion personal information records were stolen or lost through data breaches.<sup>3</sup>

The harm that organizations face from such cyberattacks is hard to overstate. In fact, the research firm IDC estimates that the global cost from cyberattacks exceeded \$400 billion in 2015.

In addition to the potentially enormous financial impact of cyberattacks, enterprises can suffer damage to their reputation and declining customer confidence. Even just one successful cyberattack “can do serious harm to a company’s reputation and credibility,” says the *2016 Symantec Internet Security Threat Report*.

A necessary first step in addressing cybersecurity is to look inward. Enterprises first need to understand what has been deployed in their own networks. And they need to ensure that the software running in their networks is legitimate and fully licensed. That’s critical, because the link between the use of illegitimate or otherwise unlicensed software and encountering malware is extremely strong (see *A Strong Correlation: Malware and Unlicensed* on page 4). Simply put, if organizations can work to ensure the legitimacy of software they are using, they can significantly mitigate cyber risks.

<sup>1</sup> *2016 Symantec Internet Security Threat Report*, Volume 21, p. 5, available at <https://www.symantec.com/security-center/threat-report>.

<sup>2</sup> *Fighting Cybercrime with Actionable Insights*, IBM Corporation, 2014, available at <http://www.slideshare.net/IBMBDA/infographic-fighting-cybercrime-with-actionable-insights>.

<sup>3</sup> *2016 Symantec Internet Security Threat Report*, Volume 21, p. 54, available at <https://www.symantec.com/security-center/threat-report>.

## DANGEROUS PRACTICES PERSIST, DESPITE AWARENESS OF RISKS

This year's Global Software Survey, which canvassed consumers, IT managers, and enterprise PC users, paints a picture of a global community well aware of the cybersecurity dangers posed by unlicensed software. It also shows that enterprises continue to use it at an alarming rate.

Around the world, CIOs recognized that avoiding security threats associated with unlicensed software is a critical reason for ensuring the software running in their networks is legitimate and fully licensed. And across every region in the world, those same CIOs also said their highest concern was loss of data associated with such a security incident.

Importantly, it's not only CIOs who recognized the risk. In the broader survey of consumers and workers, 60 percent cited the security risk associated with unlicensed software as a critical reason to use legitimate, fully licensed software at work. And they, too, were highly concerned about loss of data. But, surprisingly, these well-placed concerns did not stop dangerous practices.

It is critically important for a company to be aware of what software is on the company network. Yet there is a significant awareness gap concerning the extent of unapproved and unknown software that employees are installing. CIOs estimate that 15 percent of their employees load software on their work PCs, but in reality nearly double that percentage of employees say they are doing so.

Moreover, the Global Software Survey found:

- Although trends have improved marginally, 39 percent of software installed on PCs around the world in 2015 was not properly licensed, representing only a modest decrease from 43 percent in BSA's previous global study in 2013.
- Even in certain critical industries, where much tighter control of the digital environment would be expected, unlicensed use was surprisingly high. The survey found the worldwide rate is 25 percent — a full one in four — for the banking, insurance, and securities industries.
- Some 49 percent of CIOs identified security threats from malware as a major threat posed by unlicensed software.

## THE SOLUTION: MANAGING SOFTWARE ASSETS, EMPLOYEE EDUCATION

Not only are enterprises incurring unnecessary risk by failing to manage their software assets closely, they're also missing out on cost savings. The potential efficiency gains associated with careful management of software assets can be significant.

**Studies have shown that properly managing software can lead to real cost savings — as much as 25 percent — by driving out hidden inefficiencies from over-licensing applications or harboring unused software.**

The combination of mitigating significant risk and realizing substantial savings provides organizations a major opportunity to positively affect their business operations and bottom line.

Fortunately, there is an established discipline for doing so — software asset management (SAM) (see the four-step action plan on page 15).

*Properly managing software can lead to real cost savings — as much as 25 percent — by driving out hidden inefficiencies from over-licensing applications or harboring unused software.*



Organizations that effectively deploy SAM have an inventory of what's in their network; have policies and practices for purchasing, deploying, updating, and retiring software; and have aligned their software needs to their software practices. Effective SAM is baked into the business in the same way any other sound control policy would be.

Yet policies and practices alone are not enough. Even best-in-class policies fail if employees are not educated about the policies and their importance, as the survey emphasizes.

By proactively combining effective SAM with increased employee education, companies are able to seize the opportunity to make themselves safer, more cost-effective, and more efficient.

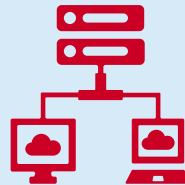
### UNLICENSED SOFTWARE: THE REALITIES



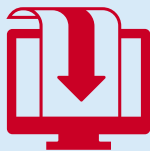
Cyberattacks cost businesses more than \$400 billion in 2015.



A strong connection exists between cyberattacks and the use of illegitimate or unlicensed software (see A Strong Correlation: Malware and Unlicensed Software on page 4).



Too many CIOs are not controlling their networks and, in fact, underestimate significantly how much unauthorized software has been deployed.



Twenty-six percent of employees admitted installing outside software on work computers, and of those 84 percent acknowledged installing two or more unauthorized programs.



Despite the growing use of mobile devices, 70 percent of enterprises reported having only an informal policy or none at all concerning connecting personal mobile devices at work.

## A STRONG CORRELATION: MALWARE AND UNLICENSED SOFTWARE

Malware is a huge problem for organizations — and one of the main culprits is unlicensed software.

An analysis done as part of BSA's new Global Software Survey finds that the higher the rate of unlicensed PC software, the higher the likelihood that users will experience potentially debilitating malware.

The findings are the result of a regression analysis, a statistical process for estimating the relationships among variables. Here, they showed a very strong positive correlation between malware and unlicensed software.

Specifically, the correlation coefficient is 0.78, where 1.0 is a perfect correlation. By comparison, the correlation between education and income level is 0.77, and the correlation between a nation's adherence to the rule of law and its level of IT sophistication is 0.79. The closer the coefficient is to 1.0, the stronger the relationship

between the two variables under study, and the more likely that the value of one will be able to predict the value of the other.

These results confirm an earlier 2015 study by IDC, which also found that unlicensed software use "is a strong predictor of malware encounters" and that "there is empirical evidence of causation."

This link between unlicensed software and cyber risk is one that CIOs should sit up and pay close attention to, as the security environment is increasingly threatening and damaging.

Cybersecurity threats are growing, as evidenced by the findings of Symantec in its most recent *Internet Security Threat Report*:

- More than 1 million new threats were created each day in 2015.
- There was a 35 percent growth in ransomware attacks in 2015.
- Sixty-five percent of all targeted attacks in 2015 struck small- and medium-sized organizations. These organizations have fewer resources and many haven't adopted best practices.

And these attacks are expensive. A successful cyberattack on average costs an organization \$11 million, according to industry estimates. In the aggregate, IDC estimates that organizations spent more than \$400 billion last year alone responding to the fallout from cyberattacks.

Well beyond the financial cost, and perhaps even more destructive and debilitating, is damage to reputation. In an industry poll conducted by IBM last year, 61 percent of organizations stated that data theft and cybercrime are the greatest threats to their reputation.

The findings highlight that a significant hidden cost associated with using unlicensed software is the possibility of unwittingly opening up an organization to cyber risk in doing so. The findings also argue for instituting first lines of defense: ensuring that no illegitimate or unlicensed software is acquired by anyone, and that software is regularly updated and security patches are installed as soon as they are received. Failure to do so can cause serious problems.

*An analysis done as part of BSA's new Global Software Survey finds that the higher the rate of unlicensed PC software, the higher the likelihood that users will experience potentially debilitating malware.*



# Global Trends

Cybersecurity has become a top concern for companies and other organizations around the world. These and other factors — including increased awareness of the importance of proper SAM, and years of education and enforcement — contributed to a modest decrease in unlicensed software use in more than a decade, from 43 percent to 39 percent.

At the same time, there is growing concern about cybersecurity threats, as well as increased awareness of the relationship between an organization's vulnerability to these threats and its use of unlicensed software. In this year's survey, for instance, 60 percent of consumers and workers identified security threats from malware as among the top reasons not to use unlicensed software.

Accompanying the global decline in the use of unlicensed software was a corresponding drop (4 percent in constant-dollar terms) in the commercial value of unlicensed software, to \$52.2 billion.

Yet despite these positive developments, for 72 of the 116 markets covered in the study, more than half of the total PC software deployed in 2015 was unlicensed; in 37 markets, 75 percent or more was unlicensed. There is still much more to be done.

## REGIONAL HIGHLIGHTS

Every region's rate of unlicensed software fell in 2015, but some dropped more than others.

In general, regional rates were driven by the larger countries, such as China in the Asia Pacific region and Brazil in Latin America.

This sometimes had paradoxical effects: while China dropped by 4 percent, Asia Pacific as a whole dropped only 1 percent to 61 percent. This is because China's increased share of the PC market in the region pulled the overall average upward, because China's overall unlicensed rate is still higher than the region as a whole.

The reverse happened in Latin America, where Brazil's three-point drop and Mexico's two-point drop were enough to bring the regional average

*Sixty percent of consumers and workers identified security threats from malware as among the top reasons not to use unlicensed software.*

(continued on page 8)

## RATES AND COMMERCIAL VALUES OF UNLICENSED PC SOFTWARE INSTALLATIONS

	RATES UNLICENSED SOFTWARE INSTALLATION				COMMERCIAL VALUE OF UNLICENSED SOFTWARE (\$M)			
	2015	2013	2011	2009	2015	2013	2011	2009
<b>ASIA PACIFIC</b>								
Australia	20%	21%	23%	25%	\$579	\$743	\$763	\$550
Bangladesh	86%	87%	90%	91%	\$236	\$197	\$147	\$127
Brunei	66%	66%	67%	67%	\$19	\$13	\$25	\$14
China	70%	74%	77%	79%	\$8,657	\$8,767	\$8,902	\$7,583
Hong Kong	41%	43%	43%	47%	\$320	\$316	\$232	\$218
India	58%	60%	63%	65%	\$2,684	\$2,911	\$2,930	\$2,003
Indonesia	84%	84%	86%	86%	\$1,145	\$1,463	\$1,467	\$886
Japan	18%	19%	21%	21%	\$994	\$1,349	\$1,875	\$1,838
Malaysia	53%	54%	55%	58%	\$456	\$616	\$657	\$453
New Zealand	18%	20%	22%	22%	\$66	\$78	\$99	\$63
Pakistan	84%	85%	86%	84%	\$276	\$344	\$278	\$166
Philippines	67%	69%	70%	69%	\$431	\$444	\$338	\$217
Singapore	30%	32%	33%	35%	\$290	\$344	\$255	\$197
South Korea	35%	38%	40%	41%	\$657	\$712	\$815	\$575
Sri Lanka	79%	83%	84%	89%	\$163	\$187	\$86	\$77
Taiwan	36%	38%	37%	38%	\$264	\$305	\$293	\$227
Thailand	69%	71%	72%	75%	\$738	\$869	\$852	\$694
Vietnam	78%	81%	81%	85%	\$598	\$620	\$395	\$353
Other AP	87%	91%	91%	90%	\$491	\$763	\$589	\$303
<b>TOTAL AP</b>	<b>61%</b>	<b>62%</b>	<b>60%</b>	<b>59%</b>	<b>\$19,064</b>	<b>\$21,041</b>	<b>\$20,998</b>	<b>\$16,544</b>
<b>CENTRAL AND EASTERN EUROPE</b>								
Albania	73%	75%	75%	75%	\$10	\$10	\$6	\$8
Armenia	86%	86%	88%	90%	\$18	\$26	\$26	\$14
Azerbaijan	84%	85%	87%	88%	\$90	\$103	\$67	\$52
Belarus	85%	86%	87%	87%	\$76	\$173	\$87	\$55
Bosnia	63%	65%	66%	66%	\$24	\$21	\$15	\$14
Bulgaria	60%	63%	64%	67%	\$78	\$101	\$102	\$115
Croatia	51%	52%	53%	54%	\$49	\$64	\$74	\$71
Czech Republic	33%	34%	35%	37%	\$150	\$182	\$214	\$174
Estonia	42%	47%	48%	50%	\$16	\$20	\$25	\$19
FYROM	64%	65%	66%	67%	\$15	\$19	\$22	\$15
Georgia	84%	90%	91%	95%	\$25	\$40	\$52	\$54
Hungary	38%	39%	41%	41%	\$107	\$127	\$143	\$113
Kazakhstan	73%	74%	76%	78%	\$89	\$136	\$123	\$74
Latvia	49%	53%	54%	56%	\$23	\$29	\$32	\$24
Lithuania	51%	53%	54%	54%	\$37	\$47	\$44	\$31
Moldova	86%	90%	90%	91%	\$36	\$57	\$45	\$28
Montenegro	76%	78%	79%	81%	\$6	\$7	\$7	\$11
Poland	48%	51%	53%	54%	\$447	\$563	\$618	\$506
Romania	60%	62%	63%	65%	\$161	\$208	\$207	\$183
Russia	64%	62%	63%	67%	\$1,341	\$2,658	\$3,227	\$2,613
Serbia	67%	69%	72%	74%	\$54	\$70	\$104	\$67
Slovakia	36%	37%	40%	43%	\$55	\$67	\$68	\$65
Slovenia	43%	45%	46%	46%	\$30	\$41	\$51	\$39
Ukraine	82%	83%	84%	85%	\$129	\$444	\$647	\$272
Rest of CEE	87%	89%	90%	88%	\$70	\$105	\$127	\$56
<b>TOTAL CEE</b>	<b>58%</b>	<b>61%</b>	<b>62%</b>	<b>64%</b>	<b>\$3,136</b>	<b>\$5,318</b>	<b>\$6,133</b>	<b>\$4,673</b>
<b>LATIN AMERICA</b>								
Argentina	69%	69%	69%	71%	\$554	\$950	\$657	\$645
Bolivia	79%	79%	79%	80%	\$98	\$95	\$59	\$40
Brazil	47%	50%	53%	56%	\$1,770	\$2,851	\$2,848	\$2,254
Chile	57%	59%	61%	64%	\$296	\$378	\$382	\$315
Colombia	50%	52%	53%	55%	\$281	\$396	\$295	\$244
Costa Rica	59%	59%	58%	59%	\$90	\$98	\$62	\$33
Dominican Republic	76%	75%	76%	77%	\$84	\$73	\$93	\$66
Ecuador	68%	68%	68%	67%	\$137	\$130	\$92	\$65
El Salvador	81%	80%	80%	80%	\$63	\$72	\$58	\$46
Guatemala	79%	79%	79%	80%	\$169	\$167	\$116	\$74
Honduras	75%	74%	73%	74%	\$36	\$38	\$24	\$17
Mexico	52%	54%	57%	60%	\$980	\$1,211	\$1,249	\$1,056
Nicaragua	82%	82%	79%	79%	\$23	\$23	\$9	\$5
Panama	72%	72%	72%	73%	\$117	\$120	\$74	\$42
Paraguay	84%	84%	83%	82%	\$89	\$115	\$73	\$29
Peru	63%	65%	67%	70%	\$210	\$249	\$209	\$124
Uruguay	68%	68%	68%	68%	\$57	\$74	\$85	\$40
Venezuela	88%	88%	88%	87%	\$402	\$1,030	\$668	\$685
Other LA	83%	84%	84%	83%	\$331	\$352	\$406	\$430
<b>TOTAL LA</b>	<b>55%</b>	<b>59%</b>	<b>61%</b>	<b>63%</b>	<b>\$5,787</b>	<b>\$8,422</b>	<b>\$7,459</b>	<b>\$6,210</b>



SEIZING OPPORTUNITY THROUGH LICENSE COMPLIANCE: BSA GLOBAL SOFTWARE SURVEY

	RATES UNLICENSED SOFTWARE INSTALLATION				COMMERCIAL VALUE OF UNLICENSED SOFTWARE (\$M)			
	2015	2013	2011	2009	2015	2013	2011	2009
<b>MIDDLE EAST AND AFRICA</b>								
Algeria	83%	85%	84%	84%	\$84	\$102	\$83	\$55
Bahrain	54%	53%	54%	54%	\$34	\$27	\$23	\$21
Botswana	79%	79%	80%	79%	\$23	\$20	\$16	\$11
Cameroon	82%	82%	83%	83%	\$21	\$9	\$9	\$7
Egypt	61%	62%	61%	59%	\$157	\$198	\$172	\$146
Iraq	85%	86%	86%	85%	\$120	\$116	\$172	\$129
Israel	29%	30%	31%	33%	\$161	\$177	\$192	\$148
Ivory Coast	80%	80%	81%	79%	\$22	\$24	\$16	\$14
Jordan	56%	57%	58%	57%	\$34	\$35	\$31	\$26
Kenya	76%	78%	78%	79%	\$113	\$128	\$85	\$66
Kuwait	58%	58%	59%	60%	\$94	\$97	\$72	\$62
Lebanon	70%	71%	71%	72%	\$65	\$65	\$52	\$46
Libya	90%	89%	90%	88%	\$65	\$50	\$60	\$25
Mauritius	54%	55%	57%	56%	\$7	\$7	\$7	\$4
Morocco	65%	66%	66%	66%	\$57	\$69	\$91	\$64
Nigeria	80%	81%	82%	83%	\$232	\$287	\$251	\$156
Oman	60%	60%	61%	63%	\$59	\$65	\$36	\$39
Qatar	48%	49%	50%	51%	\$72	\$77	\$62	\$50
Reunion	39%	39%	40%	40%	\$2	\$1	\$1	\$1
Saudi Arabia	49%	50%	51%	51%	\$412	\$421	\$449	\$304
Senegal	75%	77%	78%	78%	\$12	\$9	\$9	\$5
South Africa	33%	34%	35%	35%	\$274	\$385	\$564	\$324
Tunisia	74%	75%	74%	72%	\$49	\$66	\$51	\$44
Turkey	58%	60%	62%	63%	\$291	\$504	\$526	\$415
UAE	34%	36%	37%	36%	\$226	\$230	\$208	\$155
Yemen	87%	87%	89%	90%	\$11	\$9	\$15	\$10
Zambia	81%	81%	82%	82%	\$4	\$3	\$3	\$2
Zimbabwe	90%	91%	92%	92%	\$7	\$4	\$4	\$4
Other Africa	84%	85%	86%	86%	\$419	\$484	\$363	\$260
Other ME	84%	85%	87%	88%	\$569	\$640	\$536	\$294
<b>TOTAL MEA</b>	<b>57%</b>	<b>59%</b>	<b>58%</b>	<b>59%</b>	<b>\$3,696</b>	<b>\$4,309</b>	<b>\$4,159</b>	<b>\$2,887</b>
<b>NORTH AMERICA</b>								
Canada	24%	25%	27%	29%	\$893	\$1,089	\$1,141	\$943
Puerto Rico	41%	42%	42%	46%	\$28	\$27	\$44	\$46
United States	17%	18%	19%	20%	\$9,095	\$9,737	\$9,773	\$8,390
<b>TOTAL NA</b>	<b>17%</b>	<b>19%</b>	<b>19%</b>	<b>21%</b>	<b>\$10,016</b>	<b>\$10,853</b>	<b>\$10,958</b>	<b>\$9,379</b>
<b>WESTERN EUROPE</b>								
Austria	21%	22%	23%	25%	\$131	\$173	\$226	\$212
Belgium	23%	24%	24%	25%	\$190	\$237	\$252	\$239
Cyprus	45%	47%	48%	48%	\$14	\$19	\$19	\$16
Denmark	22%	23%	24%	26%	\$176	\$224	\$222	\$203
Finland	24%	24%	25%	25%	\$171	\$208	\$210	\$175
France	34%	36%	37%	40%	\$2,101	\$2,685	\$2,754	\$2,544
Germany	22%	24%	26%	28%	\$1,720	\$2,158	\$2,265	\$2,023
Greece	63%	62%	61%	58%	\$189	\$220	\$343	\$248
Iceland	46%	48%	48%	49%	\$10	\$12	\$17	\$11
Ireland	32%	33%	34%	35%	\$87	\$107	\$144	\$125
Italy	45%	47%	48%	49%	\$1,341	\$1,747	\$1,945	\$1,733
Luxembourg	19%	20%	20%	21%	\$21	\$30	\$33	\$30
Malta	44%	44%	43%	45%	\$4	\$5	\$7	\$7
Netherlands	24%	25%	27%	28%	\$481	\$584	\$644	\$525
Norway	23%	25%	27%	29%	\$178	\$248	\$289	\$195
Portugal	39%	40%	40%	40%	\$145	\$180	\$245	\$221
Spain	44%	45%	44%	42%	\$913	\$1,044	\$1,216	\$1,014
Sweden	21%	23%	24%	25%	\$288	\$397	\$461	\$304
Switzerland	23%	24%	25%	25%	\$448	\$469	\$514	\$344
United Kingdom	22%	24%	26%	27%	\$1,935	\$2,019	\$1,943	\$1,581
<b>TOTAL WE</b>	<b>28%</b>	<b>29%</b>	<b>32%</b>	<b>34%</b>	<b>\$10,543</b>	<b>\$12,766</b>	<b>\$13,749</b>	<b>\$11,750</b>
<b>TOTAL WORLDWIDE</b>	<b>39%</b>	<b>43%</b>	<b>42%</b>	<b>43%</b>	<b>\$52,242</b>	<b>\$62,709</b>	<b>\$63,456</b>	<b>\$51,443</b>
European Union	29%	31%	33%	35%	\$11,060	\$13,486	\$14,433	\$12,469
BRIC Countries*	64%	67%	70%	71%	\$14,452	\$17,187	\$17,907	\$14,453

\*BRIC Countries are Brazil, Russia, India, and China.

down by 4 percent to 55 percent, because their average unlicensed rates were lower than the regional average.

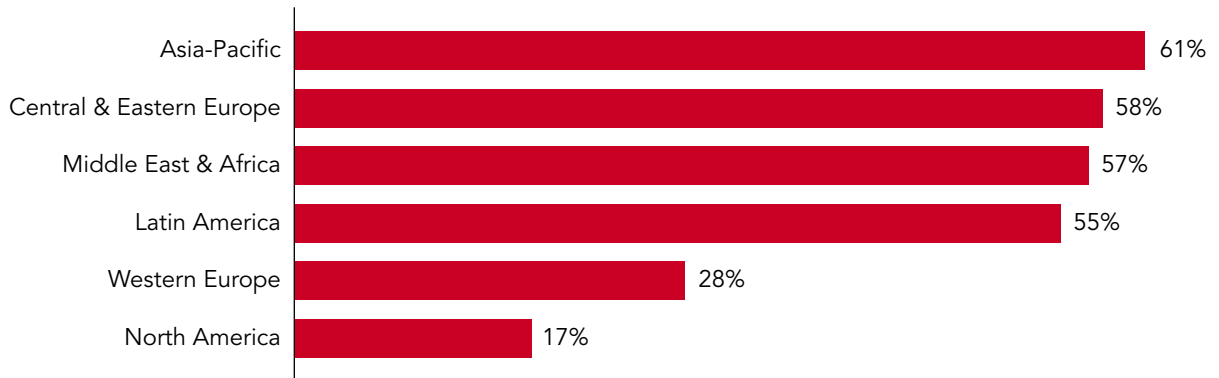
Perhaps the starkest change from 2013 was in Central and Eastern Europe, where Russia's unlicensed rate was up 2 percent, and the difference between the current dollar drop in commercial value from 2013 (50 percent) was radically different from the real drop (4 percent), due to the ruble's devaluation.

Other regional highlights from around the world:

- North America continues to have the lowest regional rate at 17 percent, although this constitutes a significant commercial value of \$10 billion.
- In Western Europe, the overall rate dropped 1 percent to 28 percent.
- In the Middle East and Africa, the overall rate fell two points to reach a total rate of 57 percent.

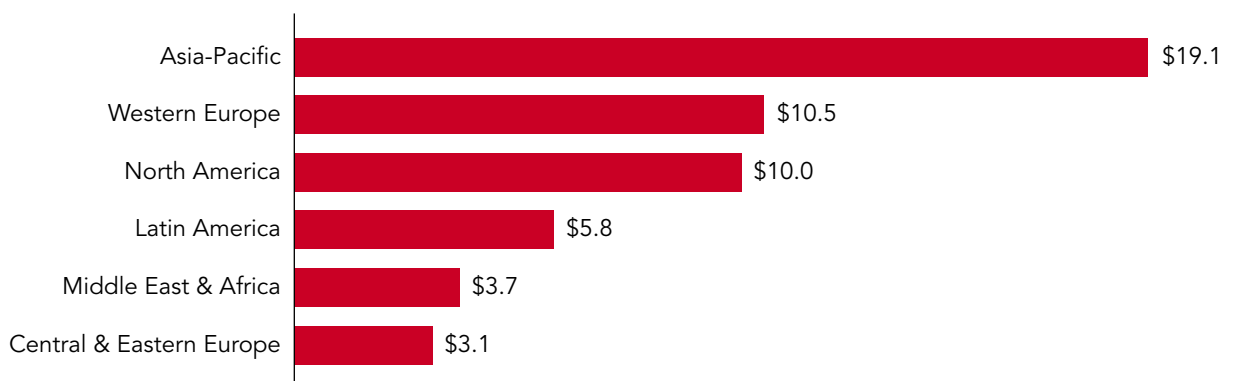
---

### Average Rate of Unlicensed Software Use



---

### Commercial Value of Unlicensed Software Use (in Billions)



## EFFECTIVE SAM NEEDED AS PART OF CLOUD COMPUTING

Cloud computing offers organizations the prospect of immense benefits. It allows anyone — a start-up, an individual consumer, a public-sector entity, or a small business — to access technology quickly, efficiently, and at scale. These services in return have opened the door to unprecedented connectivity, productivity, and competitiveness.

At the same time, the growing prominence of cloud computing highlights the need to maintain effective SAM systems, which manage the life cycle of software and cloud services within an organization. SAM is a best practice that can provide significant benefits.

Although cloud services are different than traditionally distributed software in important respects, the need to manage the life cycle of software is equally compelling in the cloud. An organization must know which cloud-based software it is entitled to, and the actual use of that software. Not taking full advantage of the use rights granted via cloud services can limit the amount of value an organization realizes. Using cloud computing without properly addressing SAM considerations can result in serious errors associated with cost and risk analysis.

Not knowing the extent of cloud services on a network may cause serious risks for organizations, such as using services not intended for commercial use, allowing services that expose sensitive internal data to external networks, and using services that originate from illegitimate cloud services providers.

A recent study by cloud security company SkyHigh Networks showed that the average large company has more than 1,100 cloud services in use across its network. This same study found that many organizations do not have a formal policy for approval of cloud services providers, or employees fail to follow the formal process when contracting with a cloud service provider. The lack of a formal process reinforces the importance of having SAM

programs in place that ensure the purchasing of cloud-based software only from reputable providers.

Credential sharing is another risk an organization that uses cloud services may face. Results from the new Global Software Survey indicate that credential sharing is widespread and on the rise.

The survey found 58 percent of users shared credentials for commercial cloud software services. Even more disconcerting, more than one in 10 users shared their credentials with people outside their organization. Among those who did share credentials with others, 72 percent indicated they did so occasionally or frequently.

Cloud services are typically subscription based, assigned to an individual user, and not to be shared with others. An effective software asset management system can monitor licensing provisions and the number of users accessing the cloud service.

At least part of the problem with credential sharing can be traced to insufficient education and lack of formal policies within organizations. The survey noted that 42 percent of respondents said their employers had only an informal policy regarding credential sharing or none at all.

Cloud computing offers unparalleled opportunities to democratize access to advanced technologies. SAM, as an essential facilitator within an organization, can ensure these new technologies are effectively incorporated while mitigating risks.

The push to mitigate risks at a time when cyber-related threats — and credential sharing — are on the rise globally is more than a best practice. It is the only practice.

*Many organizations do not have a formal policy for approval of cloud services providers, or employees fail to follow the formal process when contracting with a cloud service provider.*

# Methodology

The BSA Global Software Survey quantifies the volume and value of unlicensed software installed on PCs in a given year — in this case, 2015. To compile the report, BSA worked closely with IDC, one of the world’s leading independent research firms, to measure, understand, and evaluate licensed and unlicensed software use globally.

The study involves collecting 182 discrete data inputs and assessing PC and software trends in 116 markets.

Measuring the scale and scope of illegal behavior like unlicensed software use clearly has its challenges. Although this study is considered to be one of the most sophisticated appraisals of global copyright infringement, BSA and its partners continually look for new ways to improve the data reliability. In 2011, in partnership with two prominent IT economic researchers, BSA made several modifications designed to refine the inputs and ensure the most accurate estimation of unlicensed software use possible.

## GLOBAL SURVEY OF SOFTWARE USERS

A key component of the BSA Global Software Survey is a global survey of more than 20,000 home and enterprise PC users, conducted by IDC in early 2016. The survey was conducted online or by phone in 32 markets that make up a globally representative sample of geographies, levels of IT sophistication, and geographic and cultural diversity. In addition, a parallel survey was carried out among 2,200 IT managers in 22 countries.

The surveys are used, in part, to determine the “software load” for each country — that is, a picture of the number of software programs installed per PC, including commercial, open-source, and mixed-source programs. Respondents are asked how many software packages, and what type, were installed on their PC in the previous year; what percentage were new or upgrades; whether they came with the computers or not; and whether they were installed on a new computer or one acquired prior to 2015. These questions are asked of both consumers and business users.

In addition, the surveys are used to assess key social attitudes and behaviors related to intellectual property, unlicensed software use, and other emerging technology issues. This insight provides fresh perspective each year on the dynamics underlying unlicensed software use around the world.

Survey countries are selected using a rotational strategy to maximize worldwide coverage year over year. Eleven priority markets are surveyed in concurrence with each study cycle and 52 countries are surveyed at least once every two to three cycles. The remaining countries are selected on an ad hoc basis. In any given study cycle, the



total survey population accounts for more than 85 percent of total software units deployed and around 90 percent of paid-for units, while ensuring that most markets are surveyed at least once every three study years.

## CALCULATING RATES OF UNLICENSED SOFTWARE INSTALLATION

Since 2003, BSA has worked with IDC, the leading provider of market statistics and forecasts to the IT industry, to determine rates of unlicensed software use and the commercial value of those unlicensed installations.

The basic method for coming up with the rate and commercial values in a country is as follows:

1. Determine how much PC software was deployed during the year by consumers and business users.
2. Determine how much was paid for or otherwise legally acquired during the year (such as through an open-source, free, or complementary license), again segmented by business and consumer usage.
3. Subtract one from the other to get the amount of unlicensed software. Once this amount is known, the unlicensed rate is computed as a percentage of total software installed.

$$\begin{array}{c}
 \text{Unlicensed Rate} \\
 = \\
 \text{Unlicensed Software Units/} \\
 \text{Total Software Units Installed} \\
 \\
 \text{\# PCs Getting Software} \\
 \times \\
 \text{Software Units per PC} \\
 = \\
 \text{Total Software Units Installed}
 \end{array}$$

To calculate the total number of software units installed — the denominator — IDC determines how many computers there are in a country and how many of those received software during the year. IDC tracks this information in quarterly research products called “PC Trackers” that cover 92 countries. The remaining few countries are researched annually for this study.

Once IDC has determined how many computers there are, both consumer PCs and business PCs, and using the software load data collected in the survey, it can determine the total software units installed — licensed and unlicensed — in each country.

To estimate the software load in countries not surveyed, IDC uses a cluster analysis technique to find like characteristics with countries with varying software loads and uses these characteristics to assign loads to countries not surveyed. IDC validates this by looking at correlations between the known software loads from surveyed countries and their scores on an emerging market measure published by the International Telecommunications Union, called the ICT Development Index, and dividing them into cohorts in order to compare them to unsurveyed countries.

To get the number of unlicensed software units — the numerator of the equation — IDC must determine the value of the legally acquired software market. IDC routinely publishes software market data from about 80 countries and studies roughly 20 more on a custom basis. For the few remaining countries, IDC conducts annual research for the purposes of this study. This research provides the value of the legally acquired software market. The value is broken down by consumer and business users.

To convert the software market value to number of units, IDC computes an average price per software unit for all of the consumer and business PC software in the country. This is done by developing a country-specific matrix of software prices — such as retail, volume-license, OEM, free, and open-source — across a matrix of products, including security, office automation, operating systems, and more.

IDC's pricing information comes from its pricing trackers and from local analysts' research. The weightings — OEM versus retail, consumer versus business — are taken from IDC surveys. IDC multiplies the two matrices to get a final, blended-average software unit price.

To arrive at the total number of legitimate software units, IDC applies this formula:

$$\begin{array}{c} \text{Software Market Value/} \\ \text{Average Software Unit Price} \\ = \\ \text{Legitimate Software Units} \end{array}$$

In 2011, IDC implemented several measures to validate its calculations of average software unit price. Analyst teams in 25 countries have provided additional information on software price by category and user (consumer or business) and estimates of acquisition type (e.g., retail, volume-license, free/open source) to serve as a cross-check against IDC's computed values. Rotating the countries for which information is collected each year allows IDC to recalibrate software prices periodically, and provides a more accurate estimate of legitimate software units from industry revenues.

Finally, subtracting the number of legitimate software units from the total software units reveals the number of unlicensed software units installed during the year.

$$\begin{array}{c} \text{Total Software Units Installed} \\ - \\ \text{Legitimate Software Units} \\ = \\ \text{Unlicensed Software Units} \end{array}$$

This process provides the underlying data for the basic rate equation.

## CALCULATING THE COMMERCIAL VALUE OF UNLICENSED SOFTWARE

The commercial value of unlicensed software provides another measure of the scale of unlicensed software use, and allows for important year-over-year comparisons of changes in the software landscape.

It is calculated using the same blend of prices by which IDC determines the average software unit price, including retail, volume license, OEM, free, open-source, consumer or business, etc. The average software unit price is lower than retail prices one would find in stores.

Having calculated the total units of software installed, as well as the number of legitimate and unlicensed software units installed and the average price per software unit, IDC is able to calculate the commercial value of unlicensed software.



## WHAT SOFTWARE IS INCLUDED

The BSA Global Software Survey calculates unlicensed installations of software that runs on PCs — including desktops, laptops, and ultra-portables, such as netbooks.

It includes operating systems, systems software such as databases and security packages, business applications, and consumer applications such as games, personal finance, and reference software. The study also takes into account the availability of legitimate, free software and open-source software, which is software licensed in a way that puts it into the public domain for common use. It is typically free but also can be used in commercial products.

It does NOT include software loaded onto tablets or smart phones. It also excludes software that runs on servers or mainframes and routine device drivers, as well as free downloadable utilities, such as screen savers, that would not displace paid-for software or normally be recognized by a user as a software program.

The study includes cloud computing services such as software-as-a-service (SaaS) and platform-as-a-service (PaaS) that could replace software that would otherwise be installed on personal computers. Software sold as part of legalization programs — such as a bulk sale for a government to distribute to schools — also is included in the study.

## THE IMPACT OF EXCHANGE RATES

Prior to 2009, dollar figures in the value tables were in current dollars from the year before. For example, the 2007 value of unlicensed software was published in 2006 dollars for easier year-on-year comparison. In 2009, BSA made a decision to publish value figures in the current dollars of the year being studied. Thus, 2009 values are in 2009 dollars, 2015 values in 2015 dollars, etc. We do not restate previous values in current dollars.

This is important when evaluating changes in the values over time. Some of the changes will be based on real market dynamics, some on exchange rate fluctuations from year to year.

For instance, 2013's commercial value of pirated software, if converted to USD at 2015 exchange rates rather than 2013 exchange rates, would be 13 percent lower than published.

# Better Protection for Your Organization From Cyber Risks

Although managing cyber risk is complex, there is a critical first step — understanding what is installed and running in your company's own network, and making sure your software is both legitimate and fully licensed.

Failure to take this threshold step can have serious consequences. A study by IDC found there is a

strong, positive correlation between the presence of unlicensed software and the likelihood of encountering malware.

Cybersecurity risks are such a serious concern that the 2013 expanded COSO Framework — the recognized global standard for internal controls — includes a recommendation that companies adopt internal

controls related to the legal use of technology, including software license compliance.

In addition, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) published a standard specifically on SAM.

SAM programs are essential. They are designed to help companies ensure they're properly managing their software in a way that ensures continuous compliance, minimizes exposure to risks, and maximizes the benefit companies derive from this critically important asset.

*A study by IDC found there is a strong, positive correlation between the presence of unlicensed software and the likelihood of encountering malware.*



## FOUR-STEP ACTION PLAN THAT YOU CAN APPLY TODAY



### STEP 1: Conduct an Assessment

Gather and maintain reliable and consistent data that you can use to assess whether you are properly licensed.

- Find out what software is running on your network.
- Understand whether that software should be there.
- Determine whether all software running in your network is legitimate and properly licensed.



### STEP 2: Align to Your Business Needs

Match your current and future business needs to the right licensing model.

- Look at new forms of licensing that may be more cost-effective, such as cloud subscriptions.
- Identify possible cost savings (for example, reuse licenses if allowed by the vendor).
- Make better use of maintenance clauses in your software license agreements to ensure you are getting appropriate value for the expenditure.



### STEP 3: Establish Policies and Procedures

Ensure that SAM plays a role in the IT life cycle in your business. For ISO-aligned SAM to be effective, the practices need to support the business's IT infrastructure and management needs to support the SAM process.

- Acquire software in a controlled manner with records to support the choice of platform on which the software will run and the procurement process.
- Deploy software in a controlled manner that also assists with the ongoing maintenance of the software deployed in the business.
- Remove software from retired hardware and properly redeploy any licenses within the business.
- Routinely install software patches and upgrades in a timely manner.



### STEP 4: Integrate Within the Business

Ensure that SAM is integrated and supports the entire business.

- Integrate SAM into all relevant life cycle activities within the business, not just IT life cycles.
- Improve on the data management processes built in Step 1.
- Ensure employees understand the proper use of software and the legal, financial, and reputational impact their software-related actions can have on the organization.

# About BSA | The Software Alliance

BSA | The Software Alliance ([www.bsa.org](http://www.bsa.org)) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life.

With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.







[www.bsa.org](http://www.bsa.org)

**BSA Worldwide Headquarters**

20 F Street, NW  
Suite 800  
Washington, DC 20001

T: +1.202.872.5500  
F: +1.202.872.5501

**BSA Asia-Pacific**

300 Beach Road  
#25-08 The Concourse  
Singapore 199555

T: +65.6292.2072  
F: +65.6292.6369

**BSA Europe, Middle East & Africa**

2 Queen Anne's Gate Buildings  
Dartmouth Street  
London, SW1H 9BP  
United Kingdom

T: +44.207.340.6080  
F: +44.207.340.6090