EINPRESSWIRE

Counting the cost of unlicensed software use

With software piracy on the increase, it is not only vendors who are losing out, as the implications for users are significant too

The danger of malware infiltration from unlicensed software

LOS ANGELES , CALIFORNIA, UNITED STATES, August 25, 2021 /EINPresswire.com/ -- The latest analysis into over a billion usage events that software anti-piracy, license compliance, and cybersecurity experts, [Cylynt](), have recorded, revealed an increase of more than 44% in the instances of software piracy in the previous 12 months. This represents increased revenue recovery opportunities for Cylynt customers to the value of almost a quarter of a billion dollars, a near 100% increase year on year. The value of piracy cases increased due to employees working from home illegally downloading software rather than purchasing it through their companies.

> It takes an average of 243 days for an organization to detect an unlicensed software package and with the high possibility of malware infection - this can be a catastrophic period to be ‘in the dark’.”
>
> *Graham Kill*

This has made a lot of companies sit up and take notice, and Cylynt reports that it is not only the software vendors that are being significantly impacted – by loss of revenue that is rightly theirs, as well the potential for reputational damage - it also seriously affects those who have the unlicensed products in use.

With 34% of illegally downloaded software containing malware, employees who illegally download software are often unknowingly subjecting their companies to hacking and ransomware demands. 74% of malware was undetectable via signature-based tools according to WatchGuard, the chances of becoming infected through illegal software downloads has reached an all-time high.

The Cylynt platform is trusted by some of the world's leading software companies for enhanced business intelligence and globally is protecting around $50 billion of software assets and Cylynt's latest data highlights the wide-ranging risks that companies face with unlicensed software. This may be inadvertent use where licenses have been exceeded by an organization, so that the additional use is not then included in the latest patches and upgrades. These patches include all-important improvements and fixing security vulnerabilities as well as general operating upgrades. The unlicensed use can also include software that has been added by individuals to help them in their roles, but it is not part of the company's approved business software. The increase in individuals working remotely has given opportunity for this to rise.

"We help protect the licensed software products of some of the leading companies around the world, ensuring they have Zero Dark Usage [of their software] and they keep the returns they've justly earnt," commented Graham Kill, Executive Chairman and CEO of Cylynt Group. "For the users of those ISVs' software, we also ensure that only properly licensed software is on their networks, meaning that they too have Zero Dark Usage of risky software on their networks and are compliant so as not to expose themselves to cybersecurity risks through pirate software."

"Our data reveals that companies all too often have no knowledge that an employee is making use of unlicensed software until it is far too late. It takes an average of 243 days for an organization to detect an unlicensed software package and with the high possibility of malware infection from unlicensed software and piracy, this can be a catastrophic period to be 'in the dark'."

Software piracy is often accompanied by malware attacks and the Global Software Survey reports that a malware attack from unlicensed software can take up to 50 days for a company to resolve and costs an average of US$2.4million.

As well as the danger of malware infiltration and its associated financial expense, possibility of data loss and downtime, Cylynt also reveals and illuminates other associated risks that companies face from having unlicensed software on their network. These include data privacy issues and information leaks, with the related brand damage and penalties that accompany such breaches. There is also risk to reputation and credibility, which may be very public through media or with shareholders. Financial penalties will incur with any overuse, as back payments may be sought as well as putting all legitimate licensing in place. Contract negotiating or renewal terms may no longer be looked on as favorably as for those with a clean sheet. In some countries, criminal charges may also apply and those with responsibility, such as company directors, could face a prison sentence if successfully prosecuted.

"Some users of pirated software might think that this only affects the big software vendors and believe that it doesn't cause harm as the companies can absorb the financial loss of revenue, but this can't be further from the reality," Graham Kill concludes. "The implications go far and wide across all organizations and permeate even further into the economy, without prevention the cost of unlicensed software use will continue to grow."

More information on Cylynt’s analysis can be found here.

About Cylynt
Cylynt provides SaaS based anti-piracy, license compliance and software monetization technology for the world’s leading software companies. Cylynt’s data-driven approach to software utilization enables technology companies to derive more value while protecting their IP and clients are currently realizing an ROI of 9:1. Cylynt helps clients make informed business decisions, correct licensing problems, and protect customers from unfair competition. With a solution for every budget, Cylynt’s innovative technologies organize, analyze, and interpret telemetry data into meaningful market insights and quality lead generation.

To find out more: www.cylynt.com
For all media enquiries c.pennington@cylynt.com

Caroline Pennington
Cylynt
email us here
Visit us on social media:
Twitter
LinkedIn