kaspersky BRING ON THE FUTURE

Improving remote worker productivity with Kaspersky Endpoint Security Cloud

Reduced productivity and time-wasting have been a concern for many years. In 2017, businesses were warned that employees were wasting up to 7.5 hours every week (one working day!) scrolling through social media at work. Other distractions include surfing the web, online shopping and checking personal email, adding up to a significant potential loss of productivity. One study quoted in Inc magazine suggests that the average employee spends just 2 hours and 53 minutes engaged in productive activity.

These concerns have only intensified as the pandemic forced businesses to increase adoption of remote working. Small business owners are anxious that productivity may drop even further once employees are away from the culture and conventions of the office. For many managers this loss of direct oversight is deeply concerning.

End the uncertainty

Before damaging the delicate bond of trust between employer and employee, you need to be sure of your facts. You must know where time is being wasted and by whom. Only then will you be able to take appropriate action. And this is where Kaspersky Endpoint Security Cloud can assist.

As well as detecting malware incursions, Kaspersky Endpoint Security Cloud offers a range of monitoring tools that allow you to see how systems are being used. From the central control panel you can access a Monitoring report that shows which apps are being used on the Windows devices connected to your network.

Broken into four sections – email, file sharing, social media and miscellaneous – you can see exactly which websites, apps and services are being accessed by your employees using their work devices. You can then drill down for more details, such as who is visiting personal email accounts or scrolling through Facebook the most.

From these statistics, you can accurately estimate how much company time is being wasted – and by whom Kaspersky Endpoint Security Cloud also assigns a risk rating to each of these services. This allows you to see not only how working time is being spent, but also the level of security threat these activities present.

Take action if required

With the ability to see the top five services being used – including non-work services – you can then formalize a strategy for dealing with the issue. The IT team finally has an accurate understanding of how corporate resources are being used and the new risks being posed by remote workers.

That understanding can then be applied to developing practical solutions. Where bad habits have been identified, the team can plan and deliver end-user training to raise awareness and promote better IT hygiene and online safety. Take cloud storage for instance. When you discover users are reliant on 'free' services, use the opportunity to remind employees they should be using the official, company approved alternative because of its enhanced safety and security. The same is true for video conferencing, social networking and public email services, all of which have officially approved versions.

The IT team can also liaise with the HR department to query resource usage and develop a strategy that aligns IT policy with employment goals. You can jointly develop plans that improve employee satisfaction and protect the business, blocking services and applications that are identified as problematic or risky.

With a single mouse click you can lock out specific services for a single user. Or you can just as easily create and apply a rule for all users that blocks access to problematic websites and applications. So if you discover there is a particular site that is widely abused, like Facebook or Gmail, you can ban it instantly.

Is this contentious? Not really. Blocking access to online content inside the office is actually quite common. One smaller survey found that 39% of employers block social media sites on the company network, 30% restrict access to entertainment sites, 27% don't allow visits to online shopping sites and 23% bar employees from checking sports websites. It is not unreasonable to apply similar restrictions when using company-owned IT equipment during work hours – even for users working remotely.

Deeper insights, greater control

With its automated usage reporting and analysis, Kaspersky Endpoint Security Cloud allows you to better understand your company IT. Designed to be simple and intuitive, you can very quickly see what is and is not working, and make plans accordingly.

These benefits are not restricted to remote endpoints either. Kaspersky Endpoint Security Cloud can be used to manage your entire IT estate – including systems based inside the office. Which means that the same reporting and access controls can be applied without requiring additional tools or investment. You can use the internal reports to make important strategic decisions about how to boost productivity, both inside and out of the office.

To learn more about Kaspersky Endpoint Security Cloud, and how it will help your business better manage security and productivity for your distributed workforce, please contact us to arrange your free trial.

Find out more about Kaspersky Endpoint Security Cloud

Kaspersky
Endpoint Security
Cloud

Cyberthreats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise
Threat Intelligence Portal: opentip.kaspersky.com
Interactive Portfolio Tool: kaspersky.com/int_portfolio

www.kaspersky.com

© 2022 AO Kaspersky Lab.
Registered trademarks and service marks are the property of their respective owners.

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Know more at kaspersky.com/about/transparency

Proven.
Transparent.
Independent.