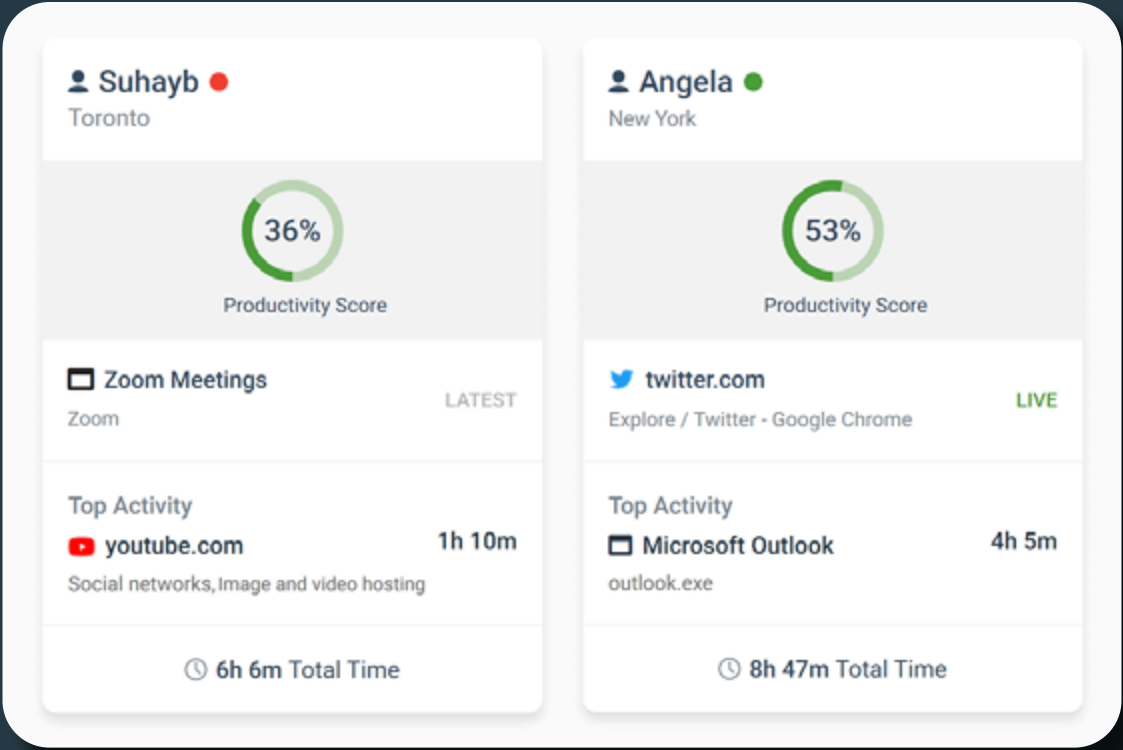




Boost Productivity, Ensure Compliance & Safeguard Data



The Critical Role of User Activity Monitoring & Endpoint Restriction



81% of companies that deployed monitoring tools saw an **increase in productivity** ¹



A failed software compliance audit can cost as much as **\$500k in fines** per violation ²



83% of IT pros reported that employees stored company data on **unsanctioned cloud services** ³

Cybersecurity & Compliance

The global average cost of a data breach in 2023 was USD \$4.45M, which was a **15% increase over the previous** three years. ⁴

Prevent & Detect Data Theft

63% of employees in a Code 42 report have stated that they **brought data from their previous employer to their current employer.** ⁵

Monitor & Control the Flow of Data

Gartner predicts that by 2027, 75% of employees will have used tools without getting approval from IT. ⁶ 83% of IT professionals reported that employees **stored company data on unsanctioned cloud services**—Putting that data at significant risk of theft, leakage, and loss. ³

Software Asset Management

Maximize the ROI of software investments by reducing expenses, restricting access to sensitive applications, and ensuring new tools are adopted.

Combat Software Wastage

In 2023, nearly half of all software/SaaS went unused by employees, **resulting in wastage of nearly \$537M/year.** ⁸ With real-world insights into the usage of costly tools such as Salesforce (Up to \$6k/user/year) and Qlik Analytics (\$32,400/yr <=10 full users), you can dramatically decrease wastage by consolidating unused or redundant tools.

Remote Worker Productivity

Flexible work options are key to attract and retain talent—But you need to be prepared to **address the productivity challenges that come with it**

Why Are Monitoring Tools So Popular?

79% monitor to better understand how staff spend their time, 65% want to confirm staff work a full day, and 50% want to prevent personal use of company equipment. ⁷

Are Employees Stealing Time at Work?

Some employees may exploit the visibility challenges of remote and hybrid work to misrepresent their efforts. Examples of time theft detected by monitoring software include **absences from workstations** (60%) and **working a second job** (52%). ¹

CurrentWare's Capabilities & Benefits



Cybersecurity & Compliance

Address controls required by cybersecurity frameworks. Track and restrict the flow of data through egress points such as USB flash drives and cloud storage services. Prevent users from accessing high-risk websites.



HR Investigations

CurrentWare is the digital witness you need to gather proof of misconduct. Ensure a safe workplace with insights that support the HR investigation process. Enforce policies by preventing access to undesirable resources.



Data Loss Prevention

CurrentWare's endpoint DLP features protect sensitive customer data, trade secrets, and PII against data breaches to insider threats. Block file transfers, control removable media usage, and get alerts of user activity.



Insider Threats

Protect sensitive data against negligent and malicious insiders with CurrentWare's insider threat detection and prevention tools. Capture evidence of high-risk activity such as attempts to use unauthorized storage devices.



Employee Productivity

Make informed decisions with granular insights into unproductive web browsing, app use, idle time, and absenteeism. Take screenshots and get alerted to excessive distractions that may require intervention.



Internet Management

Prevent misuse of the internet with advance awareness and control over web browsing. Block sites based on category, URL, or domain. Apply unique internet access policies to groups of users or computers.

Why Choose CurrentWare?



Simplicity

We prioritize ease-of-use to simplify deployment and management of our software solutions



Hospitality

We support you every step of the way—whether you're on your free trial or actively using CurrentWare



Affordability

We provide our solutions at an advantageous price to keep security accessible to everyone



Longevity

Since 2003 we've ensured the security & productivity of law firms, government entities, and more

Key Features



Data Loss Prevention

Device Control

Ensure only authorized removable media devices are able to be used. Set Full Access, Read Only, or No Access permissions for storage devices. Prevent the use of other devices including HID, Bluetooth, and Network Share drives.

Restrict File Transfers

Prevent files from being transferred to portable storage devices based on filename, extension, or removable device type.

Temporary Device Restriction Override

Generate a time-limited, device-specific, and single-use code that provides a user with full access permissions to their peripheral devices.

DLP Reports & Alerts

Monitor transfers of files to cloud storage services, removable media devices, and more. Get alerts of high-risk file transfers. Audit removable device usage for anomalous activity.

Offsite Protection

Client software ensures DLP policies are enforced off-network, even without internet access



Web Filtering & App Blocking

Internet Access Control

Block sites based on URL, domain, or content category. Includes 100+ URL categories to easily prevent users from accessing social media, porn, virus-infected websites, and more!

Application Blacklisting

Prevent the launching of unauthorized programs such as software that contains sensitive information, cloud storage services, or games.

Block Downloads/Uploads of Files

Stop users from downloading or uploading files from the internet, software apps, and more!

Endpoint Port Filter

Reduce the attack surface of endpoints by blocking unused TCP/UDP ports

Custom Block Message

Display a message or redirect to another page when a website is blocked. Users can optionally request access to the blocked site.

Offsite Protection

Client software ensures security policies are enforced off-network, even without internet access

Key Features



BrowseReporter

User Activity Monitoring

Track Computer Usage

Get insights into technology use to make data-informed productivity, security, and technology management decisions. Track web browsing, application usage, bandwidth consumption, and more!

Automated User Activity Alerts & Reports

Automate the generation of user activity reports on a set schedule or when specific activities occur such as excessive idle time or visits to inappropriate websites

Screenshot Monitoring

Take automatic screenshots at a set interval or based on activity. Remotely view desktops in real-time to take ad-hoc screenshots.

Productivity Monitoring

Track web browsing, app usage, and idle time to detect time-wasting. Grade websites and apps as productive, unproductive, or neutral to gain insights into productivity trends.

Location Insights

Promote flexibility without sacrificing accountability with insights into how location flexibility affects employee engagement and productivity

Stealth Mode Option

BrowseReporter can run silently in the background or be configured to alert users. Enable optional privacy-enhancing features such as excluded users, automatic data deletion, scheduled monitoring, and limiting what is tracked to improve transparency and minimize data collection.



enPowerManager

Remote PC Power Management

Control PC Power States Remotely

Remotely control the power state of your computers. Boot, restart, hibernate, standby, and shutdown power commands available.

Logon/Logoff Tracking & PC Power History Reports

Generate reports with employee system login names and power events such as logon/logoff times. Combine with BrowseReporter's idle time tracking for advanced insights into activity levels.

Power Scheduler

Automate PC power events at a set schedule. Delay shutdowns to only occur after the PC has been idle for a set period of time

Configure Advanced Power Policies

Control power status of laptops when they are plugged in vs. running on batteries



Technical Details

Deployment Options

With CurrentWare, you're in complete control of how your data is stored, secured, and retained. **Your employees' data cannot be accessed by CurrentWare.**



On Premises

Install the management software on a standard Windows Pro computer, then deploy the client software to your users' computers



Remote Workers

Monitor your remote employees' computers by connecting their clients to the management software with simple port forwarding rules



Cloud & VDI

Enjoy the scalability and availability of the cloud by deploying the management software to a VM hosted by a cloud service provider

[Click Here to See CurrentWare System Requirements](#)

Customer Service & Technical Support

CurrentWare provides technical support throughout your entire experience. Our team will assist you with everything from deployment and upgrades to troubleshooting, ensuring you have the resources you need to succeed with our software.



Call Us Toll-Free

Help is just a call away! The CurrentWare sales, support, and operations team can be reached toll-free at [1-888-912-9619](tel:1-888-912-9619)



Start a Live Chat

Get connected instantly by [starting a live chat on our website](#).



Emails & Support Tickets

Sales@CurrentWare.com
Support@CurrentWare.com



Self-Serve Knowledge Base

Get 24/7 access to guides, video walkthroughs, and answers to frequently asked questions. Simply visit support.currentware.com!



CurrentWare's support team has been fantastic—I **highly recommend them!**

Every time I've needed help, they've gone above and beyond to get it resolved and addressed in a timely manner.

Kristen S.
Associate IT Director
The Coding Network





About CurrentWare

CurrentWare is a Canadian software company that provides a suite of workforce management and cybersecurity solutions with computer monitoring, web content filtering, data loss prevention, and remote power management capabilities.

CurrentWare's solutions are adopted by a wide array of government and private organizations including schools, hospitals, libraries, and for-profit businesses.

CurrentWare's customers improve their user productivity, data security, and business intelligence with advanced awareness and control over how technology is used in their organization.



1-888-912-9619



info@currentware.com



www.currentware.com



Sources

1. Digital.com. 60% of Employers Require Monitoring Software for WFH Workers. <https://digital.com/employee-monitoring-statistics/>
2. The Office of Legal Education - Prosecuting Computer Crimes, <https://www.justice.gov/criminal/file/442156/download>
3. G2. 21 Shadow IT Management Statistics You Need to Know. <https://track.g2.com/resources/shadow-it-statistics>
4. IBM Security® & Ponemon Institute. IBM Cost of a Data Breach Report 2023. <https://www.ibm.com/account/reg/us-en/signup?formid=urx-52258>
5. Code42. 2019 Data Exposure Report. <https://www.code42.com/resources/reports/2019-data-exposure>
6. Gartner. Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024. <https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024>
7. Owl Labs. State of Hybrid Work 2023. <https://owllabs.com/state-of-hybrid-work/2023>
8. Nexthink. How Much Does IT Waste on Unused Software Licenses? <https://nexthink.com/resource/unused-software-licenses>

Ready to Get Started?

Reach out to our team today to request a custom demo and set up a proof of concept trial in your organization

Book a Demo

Start Your Free Trial