CurrentWare

Employee Monitoring

Best practices for balancing productivity, security and privacy

Executive Summary

Employee monitoring is no longer exclusively a top-down initiative. 92% of workers are open to being monitored by their employers, but **only if it used to provide benefits for their personal performance and well being.**[1]

In today's privacy-conscious world employers need to monitor employees in a way that is **transparent, minimally invasive, and respectful of employee privacy.** They need to carefully balance the demands of organizational productivity, employee privacy, and regulatory compliance requirements surrounding the storage, use, and protection of their employee's data.

If you want to join the 94% of organizations that use employee monitoring to gain actionable workforce insights you need to set yourself up for success by **adopting a privacy-first employee monitoring strategy**.[2]

This white paper outlines the benefits of monitoring employee computer usage and provides actionable tips for creating an employee monitoring strategy that respects employee privacy, protects sensitive data, and provides tangible insights you can use to manage your workforce.

---

[1] *"More Responsible Use of Workforce Data Required to Strengthen Employee Trust and Unlock Growth, According to Accenture Report" 21 Jan. 2019, https://newsroom.accenture.com/news/more-responsible-use-of-workforce-data-required-to-strengthen-employee-trust-and-unlock-growth-according-to-accenture-report.htm. Accessed 4 Sep. 2020.*

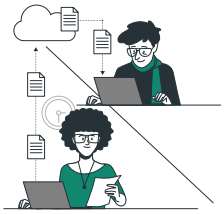
[2] *"Insider Threat 2018 Report – Crowd Research Partners." https://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf. Accessed 4 Sep. 2020.*

CHAPTER 1

Trends Impacting the Modern Workforce

The world has changed drastically since the early days of employee monitoring. Direct oversight is no longer practical. Organizations need to adapt their methods to accommodate these trends.

Trend #1
The Rise of Remote Workers



There has been a demand for remote work well before COVID-19 forced businesses to adopt it on a global scale. The 2019 State of Remote Work report by Owl Labs found that nearly two-thirds of U.S. workers work remotely at least some of the time. Greater than 50% of the on-site workers surveyed want to work remotely in the future.[3]

Recent findings confirm that COVID-19 is going to have a lasting impact on the future of work. **74% of CFOs surveyed by Gartner in March of 2020 plan to convert part of their workforce to permanent remote positions.**[4] Employee demand for flexible work arrangements is also high, with 76% of employees surveyed by Global Workplace Analytics in 2020 wanting to continue working from home.[5]

The 2018 Insider Threat Report from Cybersecurity Insiders found that 94% of organizations deploy some method of monitoring their users.[6] Employers need to be mindful of how their monitoring practices are perceived by employees that are working from the privacy of their homes.

---

[3] *"2019 State of Remote Work Report – Owl Labs." https://resources.owllabs.com/state-of-remote-work/2018. Accessed 1 Sep. 2020.*

[4] *"Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently" 3 Apr. 2020, https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2. Accessed 3 Sep. 2020.*

[5] *"Work From Home Experience Survey Results – Global Workplace Analytics" https://globalworkplaceanalytics.com/global-work-from-home-experience-survey. Accessed 1 Sep. 2020*

[6] *"Insider Threat 2018 Report – Crowd Research Partners." https://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf. Accessed 3 Sep. 2020.*

Trend #2

The Data Privacy Revolution

Consumers are becoming more aware of how their privacy is being affected in our modern world. Social media networks, search engines, and nearly every major website have built core business processes around the collection, analysis, and monetization of consumer data.

Privacy advocates want greater control over their data. They want a say in how their data is being collected, used, and stored. This demand has contributed to data privacy legislation such as Europe's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Employees want to know how their computer usage data is being collected, protected, and used. A successful employee monitoring initiative needs to work with employees to address these uncertainties.

Trend #3

Rapid Workforce Digitalization

The internet has positioned itself as the cornerstone technology that enables modern businesses. Unfortunately, misuse of the internet by employees can also lead to severe consequences. Internet abuse creates opportunities for harassment, reduced productivity, and cybersecurity threats.

Computer monitoring software serves as a critical tool for deterring undesirable behaviors in the workplace. A 2019 study published by the National Center for Biotechnology Information found that awareness of security measures such as monitoring computer activities increased compliance with policies designed to protect electronic medical records.[7]

Businesses that don't monitor employees take on significant risks. A lack of visibility into workplace technology usage provides bad actors with the opportunity to abuse their privileges undetected.

---

[7] *Kuo, K., Talley, P. C., & Cheng, T. (2019). Deterrence approach on the compliance with electronic medical records privacy policy: The moderating role of computer monitoring. BMCA Medical Informatics and Decision Making, 19(1). doi:10.1186/s12911-019-0957-y*

CHAPTER 2

Why Employee Monitoring Is Important

Employee monitoring software is a critical tool for meeting the needs of modern businesses.

1. Monitoring Detects Employee Disengagement
2. Monitoring Helps to Reduce Software Expenses
3. Monitoring Provides Valuable Workforce Insights
4. Monitoring Protects Businesses From Shadow IT
5. Monitoring is a Crucial Data Loss Prevention Tool
6. Monitoring Reduces Legal Liability & Protects Staff

1. It Detects Employee Disengagement

Actively disengaged employees cost the U.S. up to **$605 billion each year** in lost productivity.[8]
By monitoring employees an organization can discover early warning signs of disengagement such as excessive unproductive web browsing.

An important caveat is that not all non-work web activity is a definitive sign of disengagement. Personal browsing has even been found to have a positive impact on productivity **so long as internet browsing did not consume more than 12% of work time.**[9]

For the optimal balance between autonomy and productivity employee monitoring software can be used to confirm if personal browsing is within reasonable limits.

---

[8] *"State of the American Workplace report – Gallup." https://www.gallup.com/workplace/238085/state-american-workplace-report-2017.aspx . Accessed 3 Sep. 2020.*

[9] *Coker, B. L. (2011). Freedom to surf: The positive effects of workplace Internet leisure browsing. New Technology, Work and Employment, 26(3), 238-247. doi:10.1111/j.1468-005x.2011.00272.x*

2. It Drastically Reduces Software Expenses

Underutilized software costs businesses in the US and UK an estimated **$34 billion per year.**[10]

Employee monitoring detects redundant or underutilized software that can be decommissioned or consolidated. Businesses that track utilization rates will improve their capital efficiency and protect against application sprawl.

---

[10] *"Software Usage and Waste Report 2016 – 1E Resources." https://www.1e.com/resources/report/software-usage-waste-report-2016/ . Accessed 3 Sep. 2020.*

3. It Provides Valuable Workforce Insights

Historical employee monitoring data is critical for identifying workforce trends.

- We have departments with consistently high utilization rates. Are they overworked? Is there an opportunity to grow the company in this area?
- Are employees making use of the new software we recently implemented? If not, do employees need more training?
- How engaged are our employees? Do they spend the majority of their time on-task?

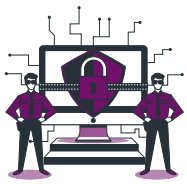
Business intelligence tools such as Tableau or BigQuery provide further insights by combining raw computer activity data with other metrics that are relevant to the organization.

4. It Protects Businesses From Shadow IT

Gartner predicted that by 2020 a third of successful attacks on enterprises would be shadow IT exploits.[11]

Shadow IT refers to any system, solution, or software that's used without approval from the IT department. This lack of oversight is a unique threat to an organization's cybersecurity.

Software usage data allows security teams to detect the use of shadow IT in the organization. Once detected they can be officially adopted, blocked from use, or substituted with viable alternatives.



5. It's a Crucial Data Loss Prevention Tool

58% of data loss events in healthcare involve insiders, making insider threats the single greatest data security threat for the industry.[12]

Organizations that collect, process, and/or store sensitive data are responsible for the security and integrity of that data.

With the average total cost of a data breach being an estimated **$3.86 million** organizations rely on employee monitoring to detect and deter high-risk behavior.[13]

Data theft is not unique to entry-level employees and management either. A 2018 report by data loss prevention company Code42 found that **72% of CEOs admit they've taken valuable intellectual property (IP) from a former employer.**[14]

Monitoring activity on data egress points such as USB storage devices and file sharing websites is crucial for detecting and preventing data theft.

---

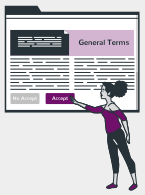
[11] *"Gartner's Top 10 Security Predictions 2016" 15 Jun. 2016, https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/. Accessed 3 Sep. 2020.*

[12] *"2020 Data Breach Investigations Report – Verizon" https://enterprise.verizon.com/resources/reports/dbir/. Accessed 3 Sep. 2020.*

[13] *"Cost of a Data Breach Study | IBM." https://www.ibm.com/security/data-breach. Accessed 3 Sep. 2020.*

[14] *"Survey Reveals 72 Percent of CEOs Admit to Taking IP, Ideas and Data with Them from a Former Employer" 24 Jul. 2018, https://www.code42.com/news-releases/ceos-admit-taking-data-from-former-employer/. Accessed 3 Sep. 2020.*

6. It Reduces Legal Liability & Protects Staff



Electronic monitoring software is rated as the most effective deterrent of inappropriate web use in large firms[15] Internet abuse in the workplace presents a significant risk if left unaddressed. Employees that visit hateful, pornographic, or otherwise harmful websites while at work create a hostile work environment for their coworkers.

Failure to monitor for and address this type of behavior undermines organizational performance and creates serious legal liabilities for employers.[16]

While internet use policies set standards for internet use in the workplace, without some form of electronic monitoring employers risk being unable to detect and deter egregious web browsing.

---

15 "Employee Internet Abuse: Risk Management Strategies And Their Effectiveness – NetAddiction." http://www.netaddiction.com/articles/eia_strategies.pdf. Accessed 3 Sep. 2020.

16 "Workplace e-mail and Internet use: employees and employers beware – Bureau of Labor Statistics." https://www.bls.gov/opub/mlr/2003/02/art3full.pdf. Accessed 8 Sep. 2020.

CHAPTER 3

How to Monitor Your Employees While Respecting Their Privacy

Organizations need to monitor their employees transparently, proportionately, fairly, and safely. Monitoring in this way protects employees and ensures that monitoring is positively perceived.

Be Transparent About Employee Activity Monitoring

Employees that are not aware that they are being monitored, why they are being monitored, and how they are being monitored are less likely to find employee monitoring acceptable.[17]

Fortunately 84% of employers surveyed by the American Management Association follow the best practice of notifying their employees that they monitor and review computer activity.[18]

Covertly monitoring employees leads to higher employee turnover and increased levels of stress.[19] This creates perceptions that their employer is spying on them and unfairly scrutinizing their every move.

An effective employee monitoring strategy empowers employees. They need to know that it's being implemented for tangible benefits rather than stemming from a lack of trust in their ability to self-manage.

Starting with transparency at the forefront gives employees an opportunity to find out whether or not their employer's data collection is **fair, minimally invasive, and beneficial for them.**

> **"Employers must not use tech to control and micromanage their staff. Monitoring toilet breaks, tracking, and snooping on staff outside working hours creates fear and distrust. And it undermines morale."**
>
> – Frances O'Grady, General Secretary of the British Trades Union Congress [20]

Best Practices For Improving Transparency

- Allow employees to access their own data. This gives them the autonomy to monitor their own productivity, which has been shown to improve performance. [21]
- Disclose the scope of employee monitoring during onboarding and within employee handbooks/policies.
- Ensure that employees understand how data is being collected, what data is being collected, and how it will be used.
- Involve a representative sample of employees during the planning process.

Determine the Required Scope of Monitoring

Creating a privacy-first employee monitoring program requires significant forethought.

It needs to have a clearly understood purpose and an implementation that is minimally invasive for the intended outcomes. Part of this process is **determining the organization's goals and the metrics they need to achieve those goals.**

Organizations that are subject to GDPR use a **Data Protection Impact Assessment (DPIA)** to evaluate their proposed solution against the potential impacts it may have on employee privacy.[22]

A DPIA demonstrates the employer's commitment to the GDPR principle of *proportionality*, which stipulates that the solutions used to further the legitimate interests of a data controller (employer) **must not exceed the potential impacts on the data subject (employee).**

Even if your organization is not legally required to use a DPIA it will serve as an important baseline when planning your privacy-first employee monitoring program.

---

[17] *Tomczak, D. L., Lanzo, L. A., & Aguinis, H. (2018). Evidence-based recommendations for employee performance monitoring. Business Horizons, 61(2), 251-259. doi:10.1016/j.bushor.2017.11.006*

[18] *"The Latest on Workplace Monitoring and Surveillance – The American Management Association." 8 Apr. 2019, https://www.amanet.org/articles/the-latest-on-workplace-monitoring-and-surveillance/. Accessed 28 Aug. 2020.*

[19] *Tomczak, D. L., Lanzo, L. A., & Aguinis, H. (2018). Evidence-based recommendations for employee performance monitoring. Business Horizons, 61(2), 251-259. doi:10.1016/j.bushor.2017.11.006*

[20] *"Barclays Probed by U.K. Privacy Agency for Snooping on Staff" 10 Aug. 2020, https://www.bloomberg.com/news/articles/2020-08-10/barclays-probed-by-u-k-privacy-regulator-for-snooping-on-staff. Accessed 4 Sep. 2020.*

[21] *Stanton, J. M. (2000). Reactions to Employee Performance Monitoring: Framework, Review, and Research Directions. Human Performance, 13(1), 85-113.A doi:10.1207/s15327043hup1301_4*

Best Practices for Reducing Privacy Impacts

- **Do not track more than necessary.** Only collect, store, and use the types of data that are adequate and relevant for the stated purposes. Overly invasive monitoring methods such as capturing individual keystrokes and webcam feeds are highly likely to infringe on employee privacy rights unless there is a legitimate business need that cannot be adequately met through less invasive methods.
- **Only use monitoring for the stated purpose.** Lack of predictability leads to increased perceptions of invasiveness among employees. By using employee monitoring data for its stated purpose employers improve their employee's trust that the system is being used fairly and responsibly.[24]
- **Do not monitor personal devices.** Employees have a reasonable expectation of privacy on their personal devices, even if they use them for work purposes. Employee monitoring solutions that limit data collection to work hours can reduce privacy impacts, though the potential to capture personal computer activity may remain a concern.
- **Limit data accessibility & retention.** Computer usage data may be sensitive. Restricting access to monitoring data to a "need to know" basis limits opportunities for misuse. Employers may also be required to store data for a predetermined period as part of their industry compliance standards. Periodically culling data that is no longer relevant reduces the employer's liability by reducing the amount of data that would be leaked following a data breach.

> **"If organisations wish to monitor their employees, they should be clear about its purpose and that it brings real benefits. Organisations also need to make employees aware of the nature, extent and reasons for any monitoring"**
>
> – Spokesman from the UK's Information Commissioner's Office[23]

Use Monitoring Data Fairly

The perceived privacy impacts of an employee monitoring solution are significantly impacted by how the data is used.

Employee monitoring is best received when the collected data is **used for learning and developmental purposes.**[25]

By using monitoring data for the employee's benefit, employers greatly increase the likelihood that the proposed solution will be perceived as fair.

Best Practices For Using Monitoring Data

- **Avoid singling out individual employees.** Singling out individual employees creates perceptions of unfairness that lead to decreased job satisfaction.[26] Employers can improve the acceptance of their monitoring program by monitoring across their organization and referencing aggregated data for insights rather than addressing the usage of specific employees. Addressing the monitoring data of individuals should be reserved for instances of high risk and clearly objectionable behaviors such as accessing pornography or engaging in illegal activities.
- **Monitor employees equally.** To avoid perceptions of discrimination, employees in similar roles should be monitored and assessed equally. This can be extended further by including managers in the monitoring ecosystem.
- **Do not use computer activity data as the sole indicator of performance.** Even if the majority of an employee's role involves the use of the computer it is normal for a productive employee to have periods of time where they are temporarily inactive on their workstations as they can be engaged in other job-adjacent tasks.
- **Understand the limitations of employee monitoring.** Computer usage data does not always provide full context for the activities captured. Seemingly unproductive or unacceptable usage behaviors may have greater relevance to the organization than can be readily determined through the exclusive use of computer monitoring.
- **Do not make significant decisions solely based on employee monitoring data.** Decisions that have a significant effect on employees such as promotions, job retention, and salary negotiations should not be made solely using employee monitoring data. These types of decisions require human intervention and external factors to ensure that the evaluation is fair, accurate, and adequate.

Protect Employee Monitoring Data From Misuse

Employee monitoring data can be highly sensitive depending on its nature.

Organizations need to ensure that security measures are in place to **prevent their employee's data from being misused or leaked to unauthorized parties.**

3 ways to prevent unauthorized access

1. **Password protection.** Password protecting the consoles and dashboards used to access employee monitoring data limits the potential for unauthorized access.
2. **Operator permissions.** Limit the amount of data available to authorized users according to the needs of their role. For example, managers can be provided access to their department's data without granting them access to departments that they do not manage.
3. **Administrative safeguards.** Limit the number of people with direct access to employee monitoring data. This can be accomplished by establishing a process for requesting data access on an as-needed basis.

---

[22] *"Data Protection Impact Assessment (DPIA) – GDPR.eu." https://gdpr.eu/data-protection-impact-assessment-template/. Accessed 4 Sep. 2020.*

[23] *"Should you be monitoring your staff with AI? – Raconteur." 14 May. 2019, https://www.raconteur.net/technology/ai-business-2019/ai-workplace-surveillance. Accessed 4 Sep.*

[24] *Stanton, J. M. (2000). Reactions to Employee Performance Monitoring: Framework, Review, and Research Directions. Human Performance, 13(1), 85-113. doi:10.1207/s15327043hup1301_4*

[25] *Tomczak, D. L., Lanzo, L. A., & Aguinis, H. (2018). Evidence-based recommendations for employee performance monitoring. Business Horizons, 61(2), 251-259. doi:10.1016/j.bushor.2017.11.006*

[26] *Tomczak, Lanzo, & Aguinis, H. Evidence-based recommendations for employee performance monitoring. 61(2), 251-259. doi:10.1016/j.bushor.2017.11.006*

CHAPTER 4:

Case Studies

The success of employee monitoring relies heavily on how it is executed. This section will compare and contrast two unique employee monitoring use cases with drastically different implementations.

Employee Monitoring Done Right – Shady Maple Follows Best Practices

Afraid to Use the Bathroom – Barclays' Lack of Transparency Backfires

Shady Maple Follows Best Practices

Shady Maple is a farm market and fresh produce distributor based in Eastern Pennsylvania, USA. They use employee monitoring and web filtering software to manage employee productivity and enforce the acceptable use of technology in the workplace.

Problem

During a period of rapid expansion Shady Maple realized that they needed to adapt their productivity management methods to scale with them.

Excessive unproductive web browsing and file downloads were hogging the available bandwidth and distracting their employees.

Without centralized access to web activity data they had no way to address this misuse of company resources.

Solution

Employee monitoring reports from BrowseReporter gave Shady Maple the exact insights they needed to address the misuse of technology in the workplace.

They could readily identify the websites that were responsible for excessive bandwidth consumption, address inappropriate web activity in the workplace, and **provide employees with an opportunity to self-manage their non-work web browsing.**

BrowseControl's category web filtering feature provided Shady Maple with a quick and convenient solution for proactively blocking websites that were known to contain pornography and other unsuitable content for their workplace.

Results

- **Improved bandwidth availability.** Bandwidth usage reports provided an opportunity to coach employees on Shady Maple's internet use policies and block frequently abused websites that were unproductive and bandwidth-intensive. Employees were delighted by the increased productivity caused by improved network speeds.
- **A safer workplace.** Shady Maple protected their network and their employees from unsafe and inappropriate websites. Continuous monitoring and web filtering became an integral part of their operations, allowing them to detect and block high-risk web activity.
- **Greater employee engagement.** Direct access to web activity reports empowered Shady Maple's employees to manage their productivity. With a scalable way to manage internet abuse without sacrificing autonomy Shady Maple noticed immediate improvements in productivity.
- **Data-informed management.** Employee monitoring reports gave Shady Maple's Human Resources department the ability to present tangible evidence of disinclination to employees who had been underperforming.

---

[27] *"Case Study: Shady Maple Farm Market – CurrentWare." https://www.currentware.com/whitepapers/CaseStudy-Shady-Maple-Farm-Market.pdf. Accessed 4 Sep. 2020.*

[28] *"Barclays Probed by U.K. Privacy Agency for Snooping on Staff" 10 Aug. 2020, https://www.bloomberg.com/news/articles/2020-08-10/barclays-probed-by-u-k-privacy-regulator-for-snooping-on-staff. Accessed 4 Sep. 2020.*

[29] *"UK ICO Opens Probe Into Barclays for Employee Surveillance" 24 Aug. 2020, https://www.cpomagazine.com/data-privacy/uk-ico-opens-probe-into-barclays-for-employee-surveillance/. Accessed 4 Sep. 2020.*

[30] *"Barclays scraps Big Brother-style spyware on staff computers" 20 Feb. 2020, https://www.cityam.com/breaking-barclays-scraps-spyware-on-staff-computers/. Accessed 1 Sep. 2020.*

Barclays' Lack of Transparency Backfires

Barclays is a bank based in the UK. As they process data of European citizens they are expected to be compliant with GDPR's data processing requirements.

A lack of transparency surrounding their employee monitoring practices prompted an investigation in August of 2020 by the Information Commissioner's Office (ICO), the United Kingdom's privacy watchdog. [28-30]

> **"The stress this is causing is beyond belief. It shows an utter disregard for employee wellbeing. Employees are worried to step away from their desks, have full lunch breaks, take bathroom breaks or even get up for water as we are not aware of the repercussions this might have on our statistics."**
>
> – Barclays whistleblower via City A.M.

Problem

Barclays installed productivity monitoring software on their employee's workstations **without their knowledge, consultation, or informed consent.**

Employees unexpectedly began receiving automated warnings once they fell below a certain activity threshold. The time that employees normally spent away from their computers became a source of inactivity that the program used to determine who would receive the warnings.

Results

- Because Barclays **did not communicate their intentions** before implementing the solution, their employees were uncertain as to how their activity data would be used.
- Employees became increasingly concerned that time spent stepping away from their desks, having full lunch breaks, or taking bathroom breaks **would be used against them** in performance evaluations. Barclays wasn't wrong for wanting greater productivity from its workforce. Unfortunately their implementation **lacked the transparency necessary** to adequately communicate the goals and intentions of their solution.

  The combination of ambiguity and automated warnings caused their workforce analytics project **to be perceived as an oppressive top-down disciplinary tool.**

CHAPTER 5

Employee Monitoring Software Buyers Guide

The feature sets offered by employee computer monitoring software vendors are incredibly diverse. This overview covers the key features you will want to consider when evaluating your options.

Tracking Features

The employee monitoring software you choose needs to capture the metrics that matter to your organization. The following metrics provide valuable workforce data with minimal impacts on employee privacy.

- Internet usage tracking
- Application usage tracking
- Active, idle, and total time tracking
- USB activity monitoring
- Tracking for off-site and remote workers
- Tracking of users and devices
- Alerts & notifications

1. Internet Usage Tracking

Website tracking provides reports on the websites visited and bandwidth used by employees, departments, or individual devices. This data is often gathered into reports to address network latency, employee productivity, and inappropriate workplace internet usage. The best monitoring softwares can improve the utility of these reports by filtering out less relevant data such as URLs associated with content delivery networks (CDNs) and other web components that employees are not directly interacting with.

2. Application Usage Tracking

Application tracking logs the time that employees spend using computer software programs such as word processors, computer games, and web browsers. Tracking computer applications used by employees helps manage software licenses, identify excessive use of unproductive programs, and detect unauthorized software.

3. Active, Idle, and Total Time Tracking

The best employee monitoring solutions have the ability to accurately report how employees are spending their time. The ability to differentiate computer activities by active, idle, and total time helps improve the accuracy and utility of computer monitoring data.

- **Active Time** is the time spent directly interacting with a website or application
- **Idle Time** indicates that an application or website was open without being interacted with for a set period of time
- **Total Time** is the combination of active time and idle time

Solutions that can track **active time** and **idle time** separately are more accurate than solutions that only track **total time**. Solutions that only track total time will report a list of applications and websites that were open on the computer without properly contextualizing whether the employee was actually using them.

4. USB Activity Monitoring

Data can easily be stolen through removable media such as USB flash drives and external hard drives. USB activity monitoring is vital for preventing data breaches for organizations with sensitive data such as personally identifiable information (employee records, customer data, etc), intellectual property, and regulated data.

5. Tracking For Off-site & Remote Workers

Employers that manage a mix of traditional and non-traditional staff such as remote workers, transient workers, hybrid workers, contractors, and temporary workers need employee monitoring solutions that monitor employees no matter where they work.

Offline monitoring stores data locally until a connection with the database can be reestablished. This is particularly important for workers that travel as they may not have consistent internet access.

6. Tracking of Users & Devices

Device monitoring will track all activity on a specific device whereas **user monitoring** will track the individual user regardless of the device they use.

Device monitoring is often used by internet cafes, schools, and libraries to oversee the use of devices that regularly change users without necessarily requiring unique login credentials.

In a workplace setting where the employer wishes to understand the browsing habits of individual employees, **device-level insights may not provide sufficient details** as their employees may not have a designated workstation (in the case of hot desking) or they may share devices with their coworkers.

When selecting a provider, organizations should ensure that both device-level and user-level monitoring is available to provide them with the best flexibility for their needs.

7. Alerts & Notifications

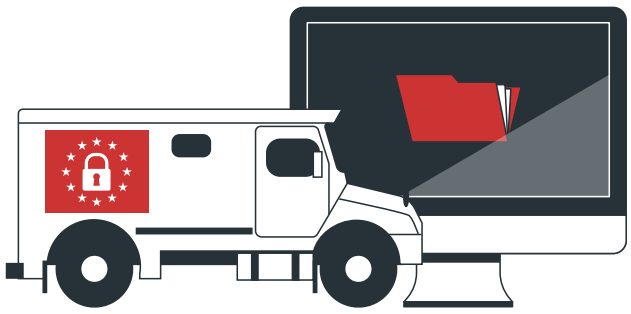
Alerts and notifications are a critical data loss prevention feature. They alert administrators to insider threats engaging in suspicious or risky behavior. These alerts can also notify human resources staff and managers when inappropriate computer usage is detected, such as visiting pornographic websites.

The exact mechanism for alerting will vary by the software provider. Alerts could be sent to a central console, an email address, via SMS to a cell phone, or to other security applications such as Security Information and Event Management (SIEM) dashboards.

Privacy Features

Reducing the impact on employee privacy requires control over what data is collected, how it's collected, and how it is stored. When evaluating vendors keep an eye out for these important features.

- Scheduled monitoring
- Custom data retention
- Automated monitoring notifications
- Access permissions & policy groupings



---

1. Scheduled Monitoring

Scheduled monitoring allows computer activity tracking to occur exclusively during designated time periods. This provides employees with the opportunity to privately browse the internet during periods where personal use is common such as breaks and after work. This also allows employers to collect representative data samples for general analysis rather than continuously monitoring.

2. Custom Data Retention

Organizations that have a legal requirement to monitor their employees often have data retention requirements that dictate how long data must be stored for before it can be safely deleted. Configurable data retention settings make auditing, eDiscovery, compliance, and data storage convenient and scalable for large-scale deployments. The ideal solution will allow the organization to choose between storing the data indefinitely and automatically purging data at set intervals to ensure that records are maintained for only as long as is relevant for the organization's needs.

3. Automated Monitoring Notifications

Occasional reminders to employees that they are being monitored complement existing transparency practices. To help automate this process look for employee monitoring solutions that can send employees periodic reminders through notifications.

4. Access Permissions & Policy Groupings

User grouping features such as Organizational Units (OUs) within Active Directory allow administrators to adjust bespoke monitoring settings based on the unique context of the specific user or device.

Bespoke settings ensure that the solution does not cause a bottleneck in productivity or collect more data than necessary. A solution that does not provide flexibility for configurations will cause less at-risk users to have the same policy restrictions as users that perform tasks with sensitive data such as personal health information (PHI).

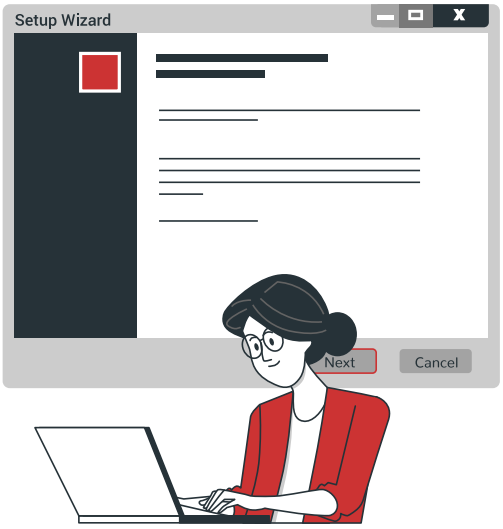
The ability to group users and devices based on location, department or role is crucial to limit the time investments and privacy impacts of the monitoring software. Best-in-class solutions allow for granular control of the product's features including who can run reports, who has access to a given group's data, and who will receive automated email reports based on the activity of the designated groups.

Deployment Options

Typical employee monitoring solutions require a proprietary software agent to be installed on employee computers. This agent must then connect to a server where the data will be stored.

Where your organization stores that data will be heavily dependent on industry requirements, contractual obligations, security & privacy considerations, and other organizational compliance mandates.

- On premises
- Cloud-based
- Hybrid



1. On Premises

In an **on premises** solution the organization deploys the monitoring solution on their own infrastructure and manages their own data storage. The key advantage of an on premises deployment is that the organization has far greater control over how their data is stored, secured, and accessed.

The key disadvantages of an on-premises deployment is the upfront investment and knowledge required to setup and maintain local storage. Large-scale on-premises solutions require a greater investment up front for server space at the advantage of reducing costs over time when compared to ongoing subscriptions for cloud data storage. Small-to-medium organizations will often do well with simply using an existing computer to store employee monitoring data.

2. Cloud Based

In a **cloud based** solution the organization deploys the monitoring solution with data storage provided by the software vendor. The key advantages of a cloud-based deployment is convenience and reduced upfront costs. Rather than investing in the purchasing and maintenance of their own storage hardware the organization can opt to pay a monthly fee for data storage through their employee monitoring software vendor.

The key disadvantages of a cloud deployment is the lack of control over sensitive data and ongoing subscription costs. As data is sent to a third-party server for storage and processing, organizations with data security and privacy concerns may opt for an on-premise deployment for greater control.

Safety And Compliance Considerations For Cloud-based Storage:

- **Public vs Private Cloud Storage:** Is the data segregated from other users of the cloud storage provider or shared in a database?
- **Data Privacy:** How will they secure and handle the data? Is the data being mined in any way? Is the provider required to give government overseers access to the data?
- **Data Residency:** Which country is your data being stored in and how does that comply with the organization's data residency requirements?
- **Data Longevity:** How long is the data being stored for? Will the vendor retain copies of the data after the organization requests deletion?

3. Hybrid Deployment

In a **hybrid deployment** the organization combines on premise and cloud storage. They will typically use an on-premise solution to collect and process data locally and backup data to their existing cloud storage provider for data redundancy. They may also manage their own private cloud configuration through Amazon Web Services, Microsoft Azure Cloud, or Google Cloud rather than paying the employee monitoring software vendor to manage the deployment.

Pricing Structure

The investment required to implement employee monitoring software will vary based on the vendors pricing structure. Vendors will typically charge based on the number of licenses required, with discounts offered for larger volumes of licenses. The number of licenses required will be based on the number of users and endpoints in your organization.

- Perpetual licenses
- Subscription / software-as-a service (SaaS)
- Support & maintenance
- Feature add-ons

1. Perpetual Licenses

Perpetual licensing provides lifetime access with a single purchase which is typically priced per license. Perpetual licenses are typically linked to a specific version of the product with optional upgrades available for an additional purchase. The capital expenses of a perpetually licensed product require a greater initial investment with the benefit of long-term savings.

2. Subscription / Software-as-a-Service (SaaS)

Subscription pricing provides access to the software for an ongoing monthly or annual fee, which is typically priced per user. Subscription-based pricing is an operating expense that provides continuous access to product updates at the expense of ongoing payments.

3. Support & Maintenance

Perpetually licensed vendors may offer optional support and maintenance plans that include product upgrades and customer support. Subscription-based vendors typically include support and maintenance as part of their subscription fee, though some vendors may require upgrades to plans with increased costs to quality.

4. Feature Add-ons

Software vendors may offer enhanced features, plug-ins, and other assets for an added cost or subscription fee. These enhancements integrate with the base software to provide greater functionality. Examples include APIs to directly integrate the software's database to a business intelligence tool and ongoing updates to website categorization databases.

Conclusion

Employee monitoring software is a critical tool to ensure business continuity in our modern world. It covers visibility gaps caused by the rapidly expanding remote workforce, protects data from bad actors, and provides organizations with advanced insights into how their distributed workforce operates.

Balancing the needs of employee data privacy with organizational productivity and security is no small feat. To get the most out of these tools employers must monitor their employees in a way that is **transparent, fair, and respectful of employee privacy.**

By following the recommendations in this white paper employers can ensure their employee monitoring strategy empowers employees, boosts buy-in, and collects valuable workforce intelligence without invading the privacy of their employees.

About CurrentWare

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

CurrentWare's solutions are adopted by a wide array of government and private organizations including schools, hospitals, libraries, and for-profit businesses. CurrentWare customers improve their user productivity, data security, and business intelligence with advanced awareness and control over how technology is used in their organization.