mimecast

Protecting Data While Maintaining Privacy: A Guide for Security Teams

Three Steps to Protecting Sensitive Data and Respecting Employee Trust and Privacy

Navigating the Data Privacy Conundrum

On the heels of shifting to a post-pandemic hybrid work culture follows another gowning trend — employee monitoring.

A survey conducted by ExpressVPN revealed that 78% of companies report using employee monitoring software to track employee performance and online activity, while another report showed that businesses demand for employee monitoring software is 51% higher on average at the start of 2023 compared to 2019.

The motivation behind this new trend is partly because companies want to ensure that employees remain productive, and because data security is an emerging concern; a 2020 Ponemon Institute survey reports that 47% of companies rely on employee monitoring and surveillance tools to prevent insider-driven data loss.

Indeed, insider threats have been growing. The 2023 Data Exposure Report shows that there's been a 32% average increase in the number of insider-driven data exposure, loss, leak and theft events that companies estimate they experience a month. This translates to an average of 300 events per company per year—a deeply concerning figure for security leaders worldwide.

However, today, this 'Big Brother' approach comes with a new set of problems and complexities:

Tightening Data Privacy Regulations

New regulations like the EU GDPR and the CCPA in the U.S. are putting strict requirements on how employers can monitor and use employee data.

Ineffective Approach to Minimizing Insider Threats

Using employee monitoring software may give the illusion of improved security, but it's not an effective way to minimize insider threats. Invasive surveillance tools tend to lead to false positives, irrelevant data collection and a culture of fear rather than one of collaboration and trust. Additionally, these tools do not address the root causes of insider-driven data loss, such as lack of employee training and holistic data protection programs.

'Big Brother' Methods Create a Culture of Distrust

Invasive surveillance tools make employees feel that their privacy rights are being violated, leading to resentment and a lack of trust toward their employer. This culture of distrust causes employees to feel less inclined to report incidents or raise concerns, creating new security gaps.

Security & Privacy: A complicated relationship

The changing landscape of data privacy regulations, growing employee resistance to invasive surveillance methods, and the emergence of new methods of working and collaborating have rendered the traditional 'Big Brother' approach less effective for curbing insider threats.

Today, businesses are under tremendous pressure to protect their intellectual property, assets, trade secrets, and data from intentional and unintentional leaks. Figures from the 2023 Data Exposure Report show that 76% of CISOs expect data loss from insider events to increase in the next 12 months. With insider-driven data leaks costing companies $16 million per incident on average, data security has never been a bigger concern.

Nevertheless, with the rise of new data privacy regulations and increasing employee awareness, businesses also have an obligation to provide a safe and fair workplace for their workers, particularly one that safeguards their privacy rights.

The question is, how can companies implement insider threat management programs and monitoring tools that secure sensitive data while still respecting employee privacy?

Employee Monitoring vs. Data Protection: What's the Difference?

To better understand the balance between employee monitoring and data protection, it's essential to differentiate between traditional and modern monitoring tools.

Traditional employee monitoring tools, such as user and entity behavior analytics (UEBA), are designed to monitor employees' day-to-day activities within the organization. They monitor all activity, regardless of whether it's risky. These tools allow employers to track employee personal details, locations, and behaviors, such as browsing habits and productivity.

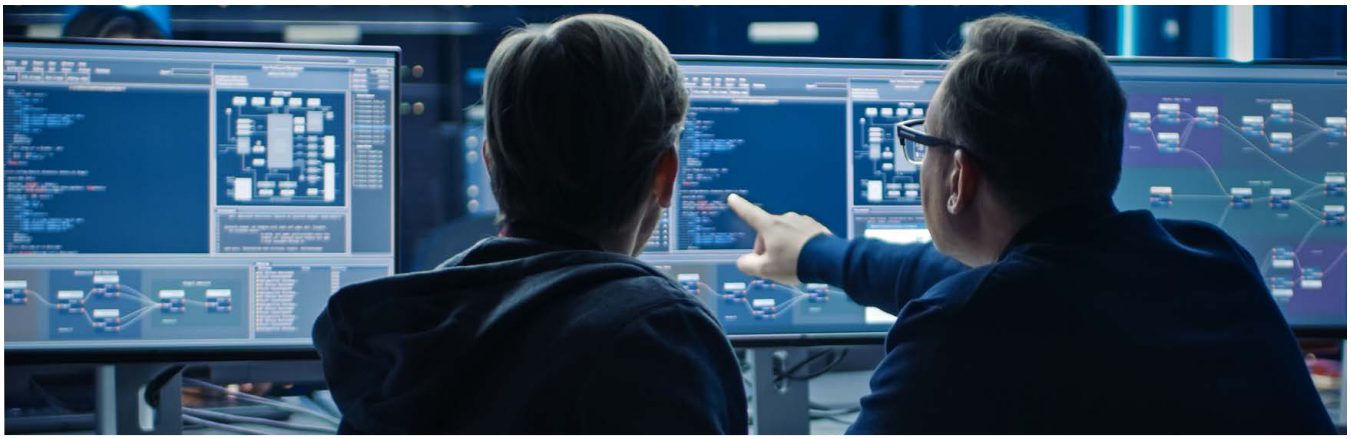
While these UEBA and other monitoring tools can help identify potential insider threats, they also raise concerns about violating employee privacy and fostering mistrust between employers and employees. Such mistrust leads to friction and a lack of cooperation which gives rise to new security gaps and insider threats.

In contrast, modern data protection tools focus on protecting data rather than monitoring employees' personal behavior. These tools take a metadata-driven approach to insider threat detection and response. By focusing on data movement to untrusted locations, these tools offer an approach that respects privacy rights while still enabling organizations to protect their sensitive information.

While monitoring and surveillance can be valuable for edge cases of insider threat, modern data protection tools offer a more balanced and effective approach that minimizes potential violations of employee privacy and promotes a culture of transparency and collaboration, while tailoring mitigation responses to the offender and offense.

Traditional "Big Brother" Tools vs Modern Data Protection Tools

ASPECT	TRADITIONAL INVASIVE TOOLS (e.g. UEBA)	MODERN MONITORING AND DATA PROTECTION TOOLS (e.g. INCYDR)
Methodology	Focus on monitoring employee activities and behavior, including keystrokes, website visitations, and email attachments, often without employee knowledge or consent.	Focus on monitoring data exfiltration events and alerting organizations when data moves beyond their trust boundaries without monitoring employees' personal details or everyday behaviors.
Privacy Concerns	High risk of violating employee privacy rights and creating a culture of distrust, leading to decreased morale and productivity.	Secures data by tracking all data movement to untrusted locations and providing user education to mitigate security gaps due to human error.
Effectiveness	Limited ability to prevent insider risks and detect data exfiltration events due to false positives and difficulty identifying genuine threats.	Provides a comprehensive view of data exfiltration events, including file activity and user activity, allowing for proactive risk analysis and response.
Compliance	UEBA tools may conflict with data privacy regulations such as GDPR and CCPA, leading to legal and financial risks.	Ensures compliance with data protection regulations and frameworks while maintaining adherence to privacy regulations, mitigating legal and financial risks.
Employee Trust	High risk of decreasing employee trust leads to reduced employee morale and productivity.	Bite-sized cyber security education that's both proactive and situational works to prevent data breaches from happening in the first place by teaching employees what to look out for and encouraging secure practices, enhancing employee trust and building a culture of security.



The Three Es of Creating a Culture of Security: Expertise, Enforcement, and Education

While modern monitoring and data protection tools are essential in enforcing data protection, they are just one part of the larger solution to creating a culture of security and collaboration.

Businesses must also include the other two critical Es—'Expertise' and 'Education'.

Enforcement

Treating everyone like a threat creates rogue employees. Focus on where data is going, how it's getting there, who's moving it, so that you can understand risk severity and respond accordingly.

Expertise

The right partners help to know where to start and understand the rapidly converging data protection space. That expertise can guide clear communication with employees about what data is monitored, why it's being monitored, and how that data is used.

Education

Many data security incidents happen in the normal course of doing business, so a security-allied workforce is your best protection. Tailor response to the offender and the offense, using micro-trainings to guide and correct.

These three Es – Expertise, Enforcement, and Education – are all critical to gaining employee buy-in and setting the foundation for building a robust insider threat management program.

Adhering to these principles helps organizations create a culture of security and collaboration that protects the organization and empowers employees to be part of the solution.

However, implementing the principles of the three Es requires a clear plan of action that respects employee privacy while protecting company data.

3 Steps to Building a Successful Insider Threat Program Without Violating Employee Privacy

Below are three steps to building a successful insider threat program that minimizes privacy risks and maximizes effectiveness.

Focus on monitoring the right things

If it sounds obvious, it bears repeating because too many companies get this step wrong: Make sure your insider threat program is focused on monitoring the right things — not looking in the wrong direction or trying to look in every direction.

Here are considerations to help you hone the focus of your insider threat program:

Monitor exfiltration points and identify threats non-invasively

Too many files contain IP, and there are too many places it can go. Monitor all exfiltration methods (combined endpoint & cloud agent) for any suspicious activity. When an event happens, distinguish real threats from risky event with context-driven indicators, and then validate by seeing actual file contents.

Identify trusted locations and collaborative methods

Policy-based security tools and programs are usually error-prone and difficult to manage; there are just too many possible activity combinations to effectively determine what's risky and what isn't. Instead, identify trusted locations and collaborative methods, and set your tools to only flag activity outside these trust boundaries. That way, you cut the noise and only alert your security team for truly suspicious activity.

Focus on the data – not the people.

Because it's people who pose a risk, many companies' security programs focus on their people — using employee monitoring tools like user and entity behavior analytics (UEBA). Due to its intensive employee monitoring, this approach has implications for employee privacy and culture — and it's simply the wrong focus. It's the data you're responsible for protecting. It's the data you should be watching. For example, you don't need to see everything your employees are doing on their web browsers — you just need to see web browser activity that touches your protected data.

Build a program focused on seeing what matters most

When it comes to cybersecurity, businesses are often stumped at how to reduce noise. Attempting to monitor every behavior and potential risk can quickly be overwhelming, leading to alert fatigue and strained resources.

Rather than focusing on every single action or worst-case scenario, combining comprehensive data visibility with contextual prioritization would be a more efficient approach. This would distill alerts for suspicious activity and allow security teams to tailor a response for the offender and the offense — from blocking unacceptable actions to correcting risky behaviors.

To help cut the noise, ensure that your insider threat program consist of tools that fill three different functions:

Logging and alerting

If you define sensitive systems as a focus, this is often a natural way to build out your program. Ensure that you capture suspicious activity that happens outside of your trust boundaries, so your security team gets only the alerts that matter. Capture all relevant logging activities (sometimes tricky with SaaS applications) and set up alerts for activities deemed riskier.

Special tools

You may decide there are additional tools you want to implement to monitor and manage your insider threat program. Depending on the technology implemented, you may get additional alerts, risk ranking, or integrated workflows to help guide your setup.

Defined processes

As much as we'd like to think technology can solve all of our problems, sometimes the best program starts with a manual process. This could include an onboarding or offboarding checklist, a periodic audit of privileged user activity and employee training

Build in flexibility

There is no one-size-fits-all formula for an insider threat program. The evolving nature of your organization and your employees' dynamic ways of working mean that no insider threat program is ever finished. The most effective programs build in flexibility and agility. This includes allowing for additional context, accounting for the potential of human error, and incorporating other stakeholders (legal, human resources, managers, etc.) into the program to ensure you address risk appropriately as it changes over time.

Communicate, communicate, communicate.

Finally, no matter how you decide to build out your program, transparency is a critical ingredient in ensuring efficacy from a data protection standpoint and trust from a company culture standpoint.

Make sure your employees understand:

What You're Monitoring

Be clear with employees about what information your program collects and monitors and how the data is being used. Proactive communication makes a huge difference in fighting the 'Big Brother' perception.

Why You're Doing It

Explain what your relevant data security and privacy regulations say — and how your insider threat program addresses regulatory compliance requirements. When employees don't understand the reason for monitoring, they become fearful or resentful and the culture of trust is damaged.

What You're Not Monitoring

Communicating what information you're not collecting is as important as ensuring employees understand what you are monitoring. Ultimately, staff should know that an insider threat program has nothing to do with tracking productivity or spying on online shopping. Moreover, employees should understand that your insider threat program isn't focused on them, but on the regulated and valuable data you need to protect. If their activity doesn't touch that data, they don't need to worry.

What They Can (and Can't) Do

Everyone will feel better about the program if they don't have to second-guess whether or not they are acting within protocol. Clear and well-communicated acceptable use policies are the answer. Are they permitted to use cloud storage services? If so, which ones? Can data be moved to USB devices and other local, removable storage devices? Can they share data on corporate collaborative platforms like Slack or Microsoft Teams? What's the policy for taking data home and/or keeping it in their notebooks? Finally, don't forget to consider contractors. A different standard is often applied to third-party users, and all involved need to understand that standard.

If you need a place to start, check out our **Acceptable Use Policy template**.

How Mimecast can Support your Efforts to Balance Data Protection & Employee Privacy

When it comes to building a successful Insider Threat Program, organizations face the challenge of striking a delicate balance between data protection and employee privacy.

Mimecast understands this challenge and offers comprehensive solutions encapsulating the three foundational E's — Expertise, Enforcement, and Education. Organizations can achieve robust security without violating employee privacy by leveraging Mimecast's data protection tools, including Incydr and Instructor.

Achieving the Balance

Mimecast Incydr offers an easy and effective way to protect your company's data from both malicious activity and mistakes, all while ensuring collaboration thrives and employee privacy is maintained. You can detect when data theft takes place across endpoints and cloud – on day 1, without policy setup by utilizing context such as where files came from, where they're going, who's moving them, and when. Incydr tailors your response to the offender and offense so you can correct mistakes, block unacceptable activity, and contain insider threats without employee surveillance. Gaining control over data won't create friction either; Incydr allies the business with security to protect your IP without disrupting collaboration or treating everyone like a threat.

Complementing Incydr is **Mimecast's Instructor solution**, which enhances employee training and education for risk response when mistakes happen. Instructor employs just-in-time micro training, correctly understanding that not every event is due to malicious intent. Instead of assuming wrongdoing, Instructor provides personalized training videos to correct user behavior and reinforce security best practices. This approach fosters a culture of trust and collaboration, where employees are empowered to make informed decisions and actively contribute to data protection efforts.

Conclusion

The complicated relationship between security and privacy requires a comprehensive approach that considers the three E's — Expertise, Enforcement, and Education. Mimecast's data protection solutions, including Incydr and Instructor, perfectly balance the need for robust security with respect for employee privacy. By monitoring data movement and providing in-time micro training, Mimecast ensures that sensitive data is protected while cultivating a culture of trust and collaboration.

In an age where data breaches and insider threats are ever-present, organizations can rely on Mimecast's solutions to navigate the data privacy conundrum. With Mimecast's data protection tools, organizations can build a successful Insider Threat Program that safeguards their valuable assets without compromising employee privacy.