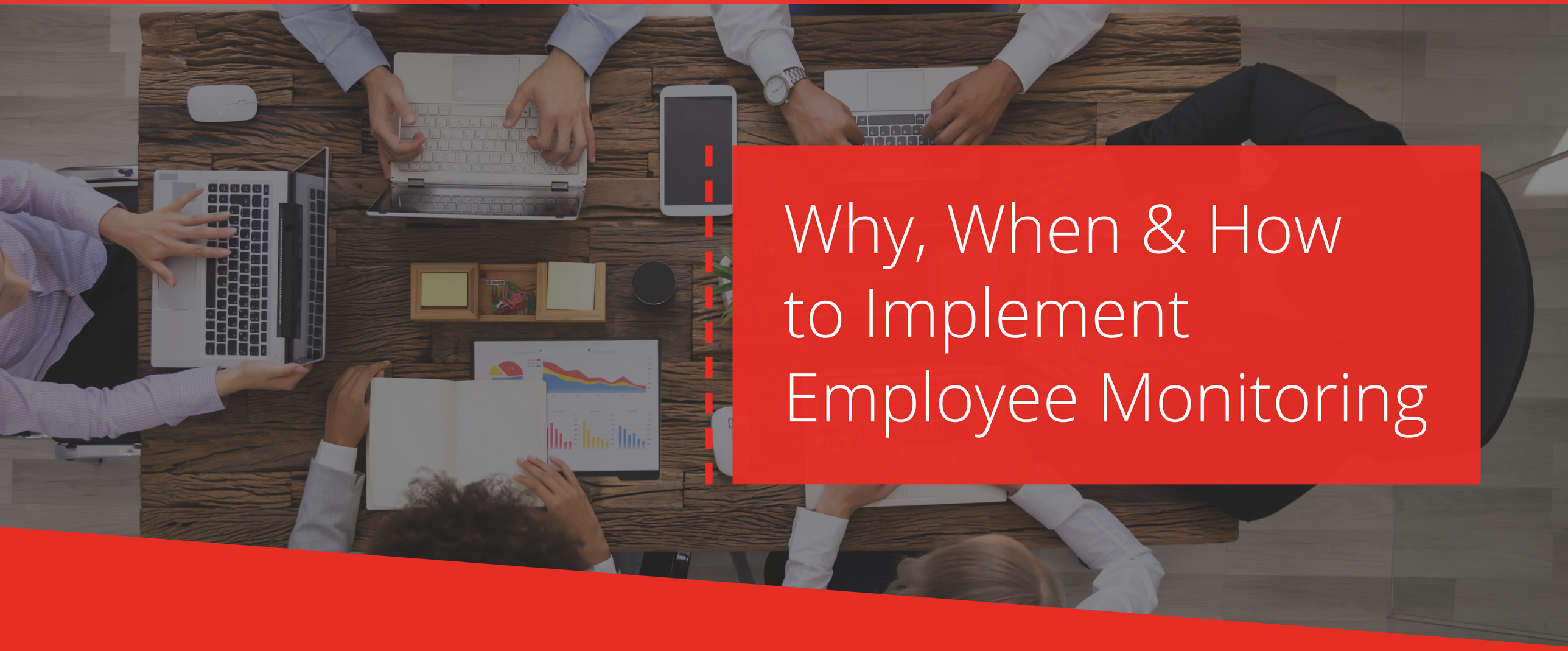
EMPLOYEE MONITORING

A common-sense guide for implementing endpoint security

Interfocus
A KYOCERA GROUP COMPANY



Why, When & How to Implement Employee Monitoring

Why Engage in Employee Monitoring?

> "No man is an island, entire of itself; every man is a piece of the continent, a part of the main.
>
> **– JOHN DONNE**

In today's interconnected business environment, the words of poet John Donne take on new meaning as both businesses and individuals grapple with how to simultaneously remain open within a connected world and also protect their assets, identity and reputation from outside attacks. This has become incredibly important in the business world, as employees rely more and more on connectivity to perform their work.

As the number of devices connected to corporate networks continues to grow as users become mobile and remote, the amount of sensitive data also continues to grow as business processes become more digitized and automated.

Each network touchpoint creates a potential entry point into your company's systems, your confidential and proprietary data, and your clients' or vendors' networks. With that in mind, understanding how, when and where your employees are using their devices and data is an important metric in protecting your business and—ultimately—your reputation. Knowing this information will also help you set policies and guidelines that can help you ensure that everyone is on the same page when it comes to data security and avoiding risky behaviors and activities. You will also gain insight into where efficiencies could be maximized and resources could be deployed in other ways.

Employee monitoring

is about peace of mind.

- Protect your business
- Have all your employees work toward the same positive goal
- Ingrain compliance into your work processes and employee mindset

Employee Monitoring Tools & Metrics

What You Need to Know

Employee monitoring tools deliver numerous metrics and insights that you can use to drive your business forward: employee working hours, productivity rates, time spent accessing the internet, which business systems they use the most, and so much more. It can be overwhelming to think through what data you need and how to use it. As you think through what data to review and how to assess it, make sure that any data you review helps in:

Knowing what is happening as it happens.

Having the real-time information on activity can help prevent breaches, minimize exposure in attacks and understand where your IT team needs to deploy its resources.

Understanding your monitoring options.

There are numerous software solutions on the market, and it can be difficult to measure which is actually beneficial to your work. Seeing how employees use software can help reduce unnecessary expenditure and help you get your employees the right tools to do their jobs.

Investigating issues after they occur.

In a perfect world, you would never have anything to investigate. The reality is, though, that even if an attack doesn't occur, someone, somewhere will engage in risky activity that could open you up to attacks in the future. The ability to investigate will enable you to better educate your employees, understand where future risks might occur and keep your processes up-to-date in dealing with security-related matters.

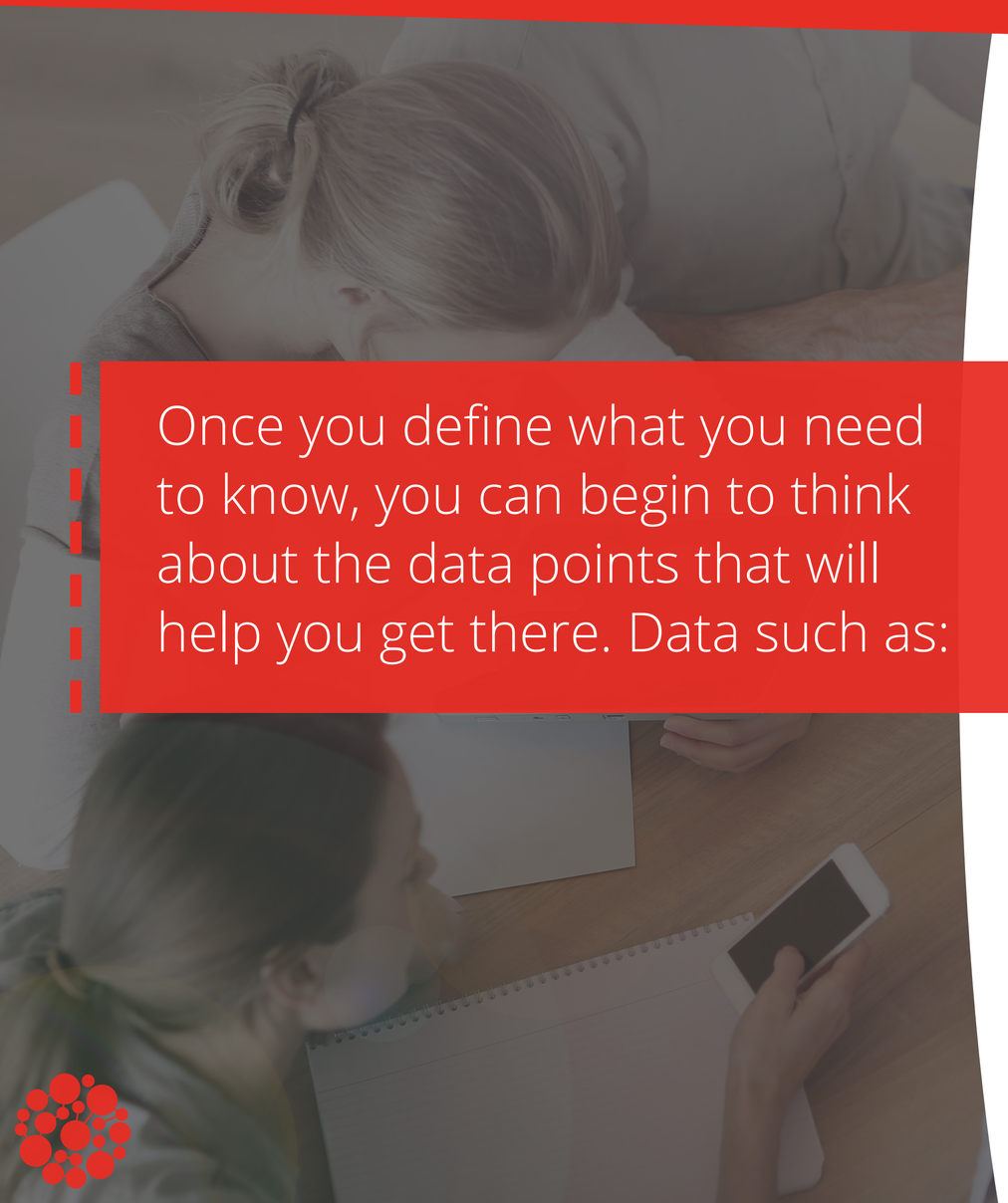
Educating your employees in real time.

Most commonly, employee awareness and education about avoiding risky behavior happens infrequently, as part of an annual compliance process, or after an incident occurs. Annual compliance education can be ineffective because it is perfunctory and taken out of context from employees actually doing their jobs. Education after an incident suffers from the obvious shortcoming that it comes too late. Educating in real time mitigates the possibility that risky behavior continues unknowingly.

Knowing what you need to know is important to create a structured, transparent process to monitor employee activity, but it also gives you a solid base to begin communicating the "what" and "why" to your employees as you implement monitoring tools.

Interfocus
A KYOCERA GROUP COMPANY
Interfocus.us | Info@Interfocus.us

What Does Employee Monitoring Look Like?



Once you define what you need to know, you can begin to think about the data points that will help you get there. Data such as:

Website Access

You should know who is accessing what sites and when. This will help you mitigate the risk of intrusion and consistently enforce web policies.

Remote Workforce

Employees have more flexibility than ever before on how, when and where to get work done. This is great for work-life balance, but can be a headache for IT staff. Helping to easily control and monitor how your remote workforce connects to your network is a key piece of managing cyber risk.

File Activity

Maintaining and understanding file activity can help ensure that rogue data isn't allowed access to your network.

Email Monitoring

Email can be a main entry point into your business networks, making email monitoring a key part of any employee monitoring solution.

USB Monitoring

It can be difficult to manage and secure memory devices, but ignoring them can create IT nightmares. Any monitoring solution needs to include real-time management of external devices.

Print Usage

Looking at print usage can give you visibility into operational violations, helping to make your network secure and to educate employees about keeping their activities compliant with company policies.

Implementing Employee Monitoring *on Your Team*

Implementing employee monitoring tools in your business can be fraught with tension. Your employees may feel that monitoring tools come from a “Big Brother”— like place of distrust, which could lead to higher stress, decreased productivity, and higher turnover rates. Exactly the opposite of what you intended in the first place!

When considering how employee monitoring software will help your business, you need to understand, formulate and communicate your goals in a way that all participants—everyone on your team—will understand and accept.

You should plan and discuss the following topics as your create you communications plan.

TOPIC ONE

How will this make us more secure?

Increasingly, companies must have controls and procedures in place to ensure that the right people have access to the right information at the right time. Employee monitoring software tracks the interactions between users, devices and information and ensures that your policies are understood and enforced at all times. This is not always about the employee, but also about the software use. Communicate that to your employees, along with the importance of security. Not everyone knows just how pervasive online attacks and security breaches can be—especially if their functional area is outside of the IT space. Creating an education campaign about security can help employees see monitoring as a partnership between everyone in the company to help ensure the safety of every device and all data.

Interfocus
A KYOCERA GROUP COMPANY
Interfocus.us | Info@Interfocus.us

TOPIC TWO

How will this make us more efficient?

Efficiency insights from employee monitoring tools include knowing which applications are used the most, what are the most heavily used data and information sources, and what are the most productive times of the work day. These data points can be useful to the employer, but can also help employees understand how to work more efficiently so they can avoid long work days and can maintain work-life balance.

Before having this employee discussion, define what activity will be recorded as well as how and when the aggregate metrics will be reviewed and acted upon. Employee monitoring can be fear-inducing because of the unknown consequences, giving rise to concerns such as:

How will this affect my review?

Am I expected to never take a break?

Will this put me in competition with my coworkers?

These are valid questions that you need to address with your employees before implementing these tools. Transparency is key. Having an understanding of why efficiency is important and how it will be measured will help negate a pervasive fear among your employees that can zap productivity and result in turnover.

TOPIC THREE

How will this help us comply with reporting and other regulatory requirements?

We are the stewards of our customers' private information as well as our company's proprietary data, and there are growing requirements to report on suspected incidents in rapid fashion. It is important to not only comply with current regulations but also prepare for future ones. The logs and audit trails maintained by employee monitoring software are critical inputs to identify where breaches may have occurred.

Selecting an Employee Monitoring Solution

Employee monitoring solutions are often geared toward large enterprises. Other solutions, like LanScope Cat, offer smaller entities the same monitoring capabilities, but come pre-configured and automated to help smaller teams manage risk and cyber attacks in an efficient manner. With all of the available options, you need to make sure you consider:

Your budget.

Employee monitoring is important, but it also needs to fit within your financial resources. Effective employee monitoring tools don't have to break the bank. Instead, they need to provide you the right value that will help your particular entity and workforce.

Your current resources.

Do you have an IT team of one? Or do you have an entire team that can be devoted to implementation and monitoring? How you've structured and deployed your current IT resources will help you understand what type of solution will best fit into your current setup. What you want to avoid is structuring your resources around the product. Instead, the product should enhance the capabilities of your current human resources.

Your immediate needs.

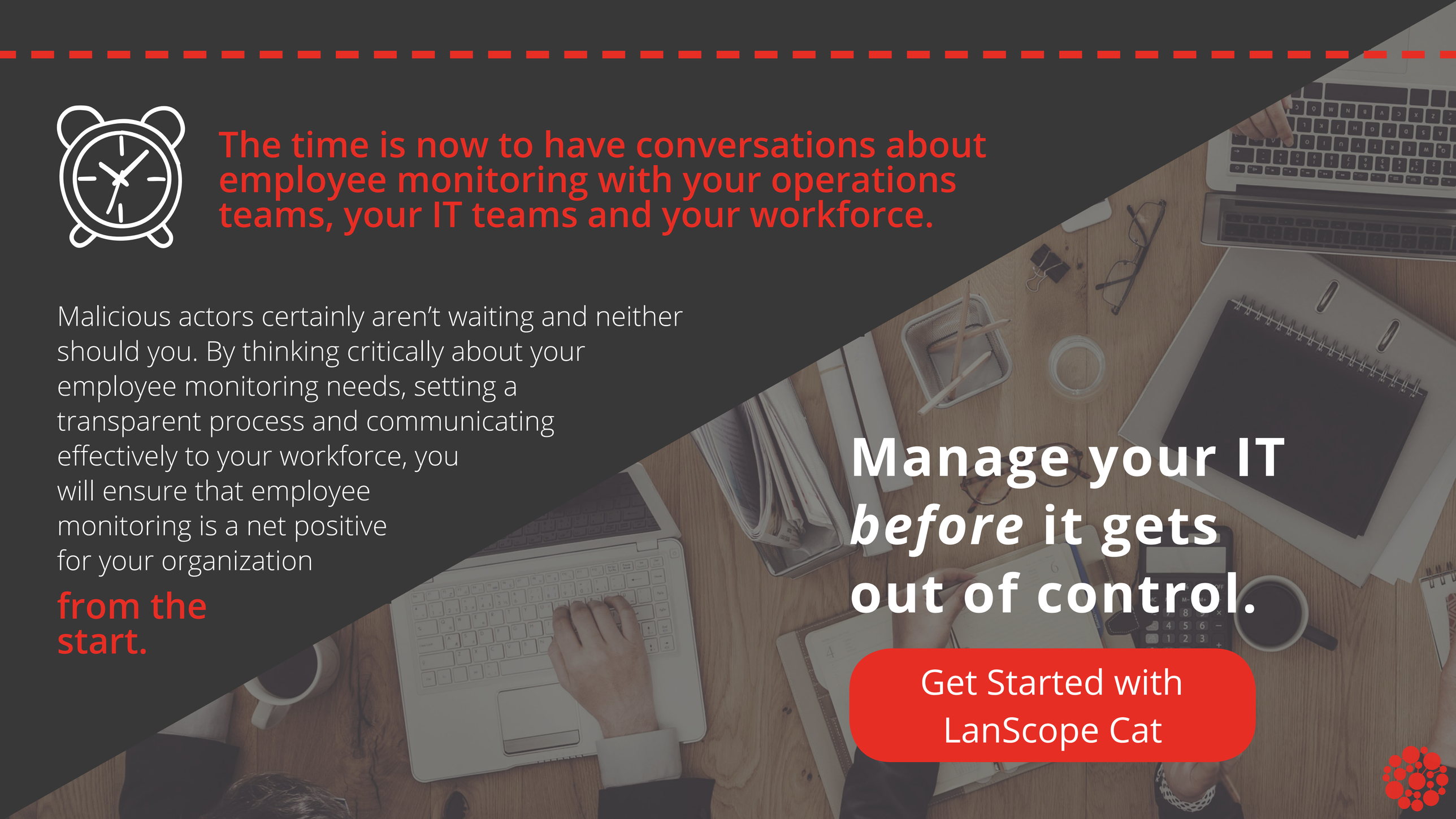
Do you have the ability to wait through longer implementation cycles? Or do you need something more immediate to begin protecting your data and your employees? You might also need a solution to pull double duty for you. For example, combining endpoint management with malware protection gives you a full-service solution, saving procurement time and money. Finding the right solution will often require balancing different needs and realities. Be honest with what you need—not what you THINK you should need.

Interfocus
A KYOCERA GROUP COMPANY
Interfocus.us | Info@Interfocus.us

The time is now to have conversations about employee monitoring with your operations teams, your IT teams and your workforce.

Malicious actors certainly aren't waiting and neither should you. By thinking critically about your employee monitoring needs, setting a transparent process and communicating effectively to your workforce, you will ensure that employee monitoring is a net positive for your organization

from the start.



Manage your IT *before* it gets out of control.

Get Started with LanScope Cat

Interfocus
A KYOCERA GROUP COMPANY

Interfocus, a Kyocera Group Company, provides LanScope Cat, a unified endpoint management and security solution in the cloud that simplifies and automates how you control your team's devices in the workplace. LanScope Cat automatically inventories your PCs, laptops, peripherals and software licenses to provide visibility into how users interact with your proprietary data. LanScope Cat's dashboard and reporting capabilities are used by over 10,000 companies and 8.6 million users, protecting their digital data and assets and ensuring compliance with both internal policies and external regulations.

Start your free 14-day trial of LanScope Cat today!

INTERFOCUS.US

3565 CADILLAC AVENUE
COSTA MESA, CA 92626

INFO@INTERFOCUS.US