Everyone as a Trusted Insider

AN INTELLIGENT REPLACEMENT FOR EMPLOYEE MONITORING

INTRODUCTION

With a seemingly infinite number of vulnerabilities and the threat of a data breach around every corner, cybersecurity is top of mind for every business and technology leader across the enterprise. And they're no longer just battling the malicious actors lurking outside, but also the threats that now run rampant inside of every organization – regardless of size, industry, or geography.

Data shows that the insider threat remains the top concern, and point of anxiety, for nearly half of today's IT and security teams – and rightfully so, with the monetary damage from insider threats estimated to be upwards of $8 million annually. There are also the harmful effects of a tarnished brand or reputation to be concerned about; more than 60 percent of consumers say that if a company loses their personal information, they're more inclined to blame the company even over a hacker.

Perhaps unsurprisingly then, worldwide enterprise security spending is also at an all-time high and expected to top $96 billion in 2018. But, it's estimated that more than half of that spending is in reaction to the high-profile cyberattacks and data breaches – and associated stream of headlines – plaguing organizations across the globe.

It's worry and fear, rather than strategy, that have been largely driving our security investments and approaches.

The pressure and urgency to retain or regain a sense of control has prompted the purchase of whatever technologies are available, affordable, and seemingly capable at the time of need… namely, legacy employee monitoring solutions. Methods like keystroke logging, video surveillance, and screenshot capture promised to shine a light on any and all suspicious employee behavior – and make organizations more secure in the process.

But, the world is quickly evolving - far beyond the heavy, intrusive methods of traditonal monitoring solutions.

From the scandal surrounding major technology companies like Facebook to the repeal of US consumer data protections and emergence of the EU's General Data Protection Regulation (GDPR), recent events have people on high alert. Consumers are now dedicating a significant amount of time and attention carefully weighing the exchange of personal data and privacy – or the new 'currency' - for access, advantage, or convenience.

Nearly **80 percent of major companies** monitor employees' email, internet, or phone activity.

(American Management Associa ion)

Despite increased concern and hyper awareness, there's certainly still a willingness to engage in these transactions. In fact, 79 percent of consumers in a recent survey agreed that they would be willing to share their data if there was a clear benefit for them. But they're being more vocal in their demands for a mutual, fair value exchange.

It's only practical to acknowledge that the same concerns and newly de ined expectations around privacy and transparency are translating over to the workplace.

Employees are now taking a more active role in understanding how their data is being collected and stored, and where invasions of their personal privacy might exist. While there is a growing understanding and comfort level with the need for employers to monitor in order to prevent security incidents and data breaches, there's also an increasing intolerance for unnecessary or unwarranted invasions of privacy. And this shift in mindset is having widespread effects across the enterprise - from human resources and company culture to security, and perhaps most notably, employee monitoring.

While full visibility into employee behaviors and actions (as well as those of all insiders) remains integral to effective and comprehensive enterprise security, the legacy tactics and technologies deployed to gain that visibility have been rendered unusable and unsustainable. A recent Gartner blog post notes that inquiries on insider threat detection in the early months of 2018 were up over 50 percent year-over-year, with clients 'seeking solutions - both technical and non-technical – for a problem that legacy solutions are not effectively addressing. **And it's become more critical than ever that we evolve our employee monitoring approaches and mindsets.**

» **43 percent** of Facebook users are concerned about invasion of privacy, **up from 30 percent** in January 2011.

» **25 percent** of consumers believe that companies handle their personal data responsibly.

» **10 percent** of consumers believe that companies handle their personal data responsibly.
(Gallup / Deloitte)

NEW: RESPECT FOR EMPLOYEE PRIVACY BY FAULT, AND BY DESIGN

OLD: THE BELIEF THAT SECURITY AND PRIVACY CANNOT CO-EXIST

The good news is that there is a wide range of user-centric, behavior-based technologies now available that make it entirely possible for organizations to gain full visibility without invading employee privacy (or impeding productivity, performance, or efficiency.) And, the investment in these technologies can go a long a way in alleviating angst at a time when monitoring is a sticky topic among employees.

Since American companies generally aren't required by law to disclose how they monitor employees using company-issued devices, the best-case scenario in most workplace environments today is including a catch-all clause in employment contracts. This ambiguity, along with the concept of self-policing, has allowed organizations to treat the

privacy and protection of employees as an after-thought (at best). And it has opened the doors for employer manipulation and abuses of power, overreaching and overstepping without much consequence.

But with the emergence of the General Data Protection Regulation (GDPR) and similar regulations in other geographies, it's quickly becoming evident that any global business hoping to sustain and thrive must adopt the mindset that views privacy as a 'fundamental right of every human being.' This is necessary not only to avoid considerable penalties, but also to be competitive in attracting and retaining skilled, talented employees.

It is also worth noting that all signs point to additional regulation and compliance requirements coming, both to the US and across the globe, and the emphasis on employee personal data protection should have all businesses paying attention. The recently passed California Consumer Privacy Act of 2018 gives Californians more control over the use of their personal information to protect their fundamental right to privacy, and imposes new data collection requirements and prohibitions on businesses.

So, how do we identify and deploy solutions designed with privacy in mind? **there must be complete visibility into employee behavior and the ability to generate a high- idelity signal into where suspicious behavior or activity is taking place.** The ability to be reliably and immediately informed when an employee or device may be compromised means it is no longer necessary to try to see and capture everything… just what is deemed a potential risk.

There has also been significant innovation in capabilities like data anonymization, which can keep a user's identity hidden until suspicious activity is detected. This not only helps address employee privacy concerns, but also provides a layer of protection at a time when behavioral data is increasingly being labeled as sensitive, personally identifiable information.

"The CCPA is considered one of the toughest data privacy laws in the United States and will dramatically impact how businesses handle data."

(Gordon & Rees)

64 percent of Americans

say they would be comfortable with their employer monitoring their digital activities on work-issued devices if it was for security purposes and the data was anonymized.

(Dtex / Harris Poll)

NEW: A LAYERED APPROACH SPANNING PREVENTION, DETECTION, MITIGATION, AND INVESTIGATION

OLD: A FOCUS ON RESTRICTION AND INVESTIGATION, IN HOPES OF PREVENTION

The sheer volume of threats, both internal and external, has rendered prevention-centric approaches to security unsustainable. Compounded by the increasingly diverse and sophisticated tools of today's bad actors, allowing them to stealthily evade detection and steal corporate data, organizations can no longer afford to take a purely reactive approach either.

Traditional employee monitoring solutions are notorious for their heavy footprint - generating excessive amounts of data and requiring a significant investment in people and resources to analyze it before it can be acted upon. Without sufficient resources or infrastructure to support, organizations have been forced to resort to an investigative, forensics-only style of security - piecing together events after a threat, compromise, or data breach has been identified. Once an investigation is completed, punishment or restriction are used in hopes of preventing future occurrences.

The security of an organization's data is directly dependent on the security and protection of its users. It's unreasonable to expect to minimize insider-related incidents without a layered approach, encompassing prevention and detection as well as mitigation and response – and without equal investment in both technology and human-readiness.

Empowering employees with consistent and comprehensive education is an absolute must, given the volatility and sophistication of today's threat landscape, as is equipping them with the tools needed to build responsible security habits.

But, even in the best-case scenario – with a commitment to employee education and training, and high levels of employee awareness – human behaviors will eventually put an organization at risk. This further emphasizes the need to have a continuous monitoring system in place that delivers unobstructed, real-time visibility into user behavior.

80% of organizations don't measure the success of security awareness training and cyber hygiene programs.

(Thycotic, The 2017 State of Cybersecurity Metrics Report)

Last year, businesses had to address an average of 40 new vulnerabilities every single day.

(Cyentia Institute, Prioritization to Prediction: Analyzing Vulnerability Remediation Strategies)

NEW: APPLYING BEHAVIORAL CONTEXT, MACHINE LEARNING & ACTIONABLE INTELLIGENCE

OLD: BUILDING RULES TO ALERT ON EVERY POTENTIALLY RISKY BEHAVIOR AND EVENT

While the visibility and information provided by traditional monitoring solutions are essential, it's critical – and now entirely possible - to go a step beyond that. Visibility, in order to truly be effective, needs be enriched with intelligence and powered by technologies that are capable of continuously learning and self-tuning.

Legacy employee monitoring tools use a rule-based model, where behaviors or events are labeled 'good' or 'bad' and alerts are generated accordingly (when potentially 'bad' activity is detected.) But, what we once thought of as black and white has become shades of grey, thanks to the human element - and what presents as risky or suspicious activity for one person does not necessarily represent suspicious activity for another.

With so many variables to contend with, **it is essentially impossible for the average organization to develop a rule for all potentially risky scenarios.** But because rule-based solutions are only as intelligent as the information being fed into them, they rely completely on the humans who manage them to tell them what to look for.

For many analysts with limited bandwidth, this makes it necessary to cast a wide net – generating potentially hundreds, if not thousands, of alerts that require a manual review to verify if a bona-fide threat exists. And has resulted in a constant state of information overload.

The ability to write rules and policies tailored to our specific needs and environments is absolutely necessary, and the best way to generate immediate value from any monitoring solution. But if alerts and indicators are designed based only on known and available information, without seeking out additional context or intelligence, there will inevitably be things that fall through the cracks. And the simple fact is that if we don't know it presents a risk, we won't know to look for it.

For a monitoring solution to truly have value, it needs to be equipped to understand behavioral context, establish a baseline of normal behavior, and apply advanced analytics and machine-learning to determine if an event or behavior is abnormal. With better anomaly detection comes higher-quality alerts - and reliable, actionable intelligence.

» Organizations can investigate only **56 percent** of the security alerts they receive on a given day.

» Half of the investigated alerts **(28 percent)** are deemed legitimate.

» **Less than half (46 percent)** of legitimate alerts are remediated.

(Cisco, 2017 Security Capabilities Benchmark Study)

NEW: PRIORITIZING CONSISTENT AND ENTERPRISE-WIDE VISIBILITY

OLD: MONITORING THE SELECT FEW INSTEAD OF ALL USERS

The reality is that all users are equally capable of capable of putting the business at risk - whether that's falling prey to malicious actors and their social engineering tactics or engaging in negligent behavior.

But, the heavy footprint of traditional monitoring solutions has largely limited the number of employees that organizations are able to monitor and, in turn, has inhibited their ability to deploy at scale. As a result, many security teams have narrowed their focus, and visibility, to include only their most privileged users.

It's certainly true that with increased access to systems and data comes increased vulnerability and potential for devastation. As with non-privileged users, it's imperative that privileged users don't become exceptions-to-the-rule or security blind spots – especially as they have become a target for manipulation and exploitation with the GDPR coming into effect.

More than 60 percent of insider incidents are the result of user negligence.

(Ponemon Institute, 2018 Cost of Insider Threats Report)

But, the bottom line is that every user is vulnerable.

A common pattern seen in many high profile cyber-attacks - including Yahoo, SWIFT and the Bangladesh Bank, the U.S. Office of Personnel Management (OPM), and many more - begins with a targeted social engineering or phishing attack on a 'semi-privileged and unsuspecting employee.' Once the attacker has successfully stolen the employee's credentials, they are able to compromise an employee's workstation with malware and use privileged credentials harvested from the compromised workstation to expand their attack to other assets within the enterprise.

The success of cybercriminals leveraging privileged credentials is directly related to their ability to move laterally, and subsequently escalate privileges or exfiltrate data, without raising red flags. This means it's critical to choose advanced, behavior-based solutions – which are the only ones capable of recognizing and flagging when someone with seemingly legitimate access is engaging in inappropriate or potentially harmful activity.

It is equally critical for organizations to understand the number of employees with privileged access and apply real-time visibility across all users and environments, regardless of designation of privilege. And this visibility needs to be delivered via technologies that have proven to be scalable, with the ability to grow and adapt as the needs of the business grow.

Only 35 percent of organizations have complete visibility into which insiders have privileged access.

(Bomgar, Privileged Access Threat Report 2018)

NEW: OPEN, TRANSPARENT MONITORING APPROACHES AND POLICIES

OLD: MONITORING APPROACHES ROOTED IN SECRECY AND AMBIGUITY

Companies run the risk of weakening their first and last line of defense if they aren't transparent about how and why they're monitoring employees. The traditional belief is that effective security requires the use of secrecy or the element of surprise - but in a new world that values trust and open communication, this approach is both flawed and potentially dangerous.

A transparency-led environment, built on mutual trust and open communication, is much more likely to make well-intentioned employees feel more comfortable and empowered. On the flip side, those wishing to engage in malicious activity will have a much harder time finding dark corners to hide or lurk in.

And whether careless or malicious, **risky employee behaviors have a much better chance of being addressed before resulting in potentially devastating consequences.**

Only 12% of employees are fully aware of their organization's IT security policies and rules.

(Kapersky Labs)

There's also research that shows transparency of information can 'breed self-correcting behavior,' which supports the theory that people are more likely to be at their best when they know they're being held accountable. The employees who understand what monitoring technologies and practices are in place, and how their employees generate and use data, will ultimately be in a better position to understand what types of online activities and behaviors are potentially harmful.

77 percent of employed Americans
say they would be less concerned with their employer monitoring their digital activity on personal or work-issued devices they use to conduct work, as long as they are transparent about it and let them know up front.

(Dtex / Harris Poll)

NEW: GREATEST ASSETS ARE EMPOWERED TO REMAIN GREATEST ASSETS

OLD: GREATEST ASSETS ARE IMMEDIATELY ESTABLISHED AS GREATEST VULNERABILITIES

It's been established that having the right systems in place – those that deliver full visibility, use lightweight data collection, and have proven themselves to be scalable - is essential. And yet, the traditional monitoring solutions deployed across the enterprise have not only impeded the speed and reliability of corporate networks, but also employee access and efficiency.

While the technical limitations of heavy monitoring solutions are certainly to blame, so are the 'Zero Trust' methodology and framework embraced alongside. Centered on blocking or severely restricting access to resources and applications, this approach has actually raised our risk levels in many cases - **leading users to engage in risky or irresponsible behaviors simply because they are unable to complete an essential or urgent task.**

With the right technologies in place and the capabilities needed to continuously monitor risky behavior, it becomes truly possible to extend trust and allow employees to move more freely. This type of environment is likely to leave them feeling not only more empowered and accomplished, but also better equipped to make responsible security decisions.

Over 80%
of employers want to have cyber risk management embedded in their company culture within the next three years.

(Willis Towers 2017 Watson Cyber Risk Surveys)

CONCLUSION

The bottom line: yesterday's employee monitoring approaches and technologies do not work today.

Today's solutions must provide complete visibility into everything users do on their work devices, capable of generating intelligence, shining a spotlight on suspicious behavior, and filtering out all the noise. And they must be scalable enough to be deployed enterprise-wide without negative impact to network performance.

Just as importantly, these programs need to be built on transparency, with the utmost respect for personal privacy and data protection. And mutual trust - between companies and their employees, as well as contractors, partners or customers - must be at the core of any program or initiative that requires visibility into behavior or the capture and collection of data.

ABOUT DTEX

Dtex Systems arms enterprises and governments across the globe with revolutionary technology to protect against user threats, data breaches, and outsider infiltration. As the only solution combining unparalleled endpoint visibility with advanced analytics, Dtex is able to pinpoint threats with greater accuracy than traditional security methods without adversely impacting user productivity. To learn more, visit us at www.dtexsystems.com.