FORCEPOINT
POWERED BY Raytheon

Whitepaper

Unlocking Business Success: The Five Pillars of User Risk Mitigation

When desktops ruled the enterprise, employers may not have claimed to have absolute control over their workers' usage of technology and data. But they surely could contain it.

They empowered IT to determine which computers and software programs to acquire and provision. Then, IT decreed what constituted "appropriate use" of its technology. Workers, for the most part, acquiesced. And when they finished for the day, they turned their computers off and went home. They stayed offline until the next morning.

Today, this seems like something from a far-away age, even though it was accepted as reality just a decade ago.

Contents

ERA OF EMPLOYEE EMPOWERMENT INVITES RISKS

When desktops ruled the enterprise, employers may not have claimed to have absolute control over their workers' usage of technology and data. But they surely could contain it.

They empowered IT to determine which computers and software programs to acquire and provision. Then, IT decreed what constituted "appropriate use" of its technology. Workers, for the most part, acquiesced. And when they finished for the day, they turned their computers off and went home. They stayed offline until the next morning.

Today, this seems like something from a far-away age, even though it was accepted as reality just a decade ago.

Whether overtly or tacitly, leadership has now empowered its employees. Thanks to mobility, the cloud and other advancements, workers decide what devices to use and when they will use them. Indeed, Bring Your Own Device (BYOD) and what is called "shadow IT" keeps tech staffers awake at night, as 41 percent of these professionals say their users frequently leverage technologies that are neither implemented nor managed by IT, according to research from PMG. Demand for the most compact and "cool" gadgets is rising so swiftly, that the number of active Internet-connected devices will triple the number of people on earth by 2019[1]. In addition, users select their own business apps to support day-to-day productivity goals, downloading them by the dozens: There are more than 26 apps on the average smartphone, according to a Nielsen study[2].

CATEGORY OF INSIDERS THAT MOST THREATEN ORGANIZATIONS

Negligent Employees..... 52%

Malicious Employees..... 22%

Source: "Insider Threats and the Need for Fast and Directed Response," SANS Institute

With the insatiable appetite for devices, apps and social media, the likelihood of compromise increases: One-third of enterprises have suffered from an insider incident, with the possible loss from such a threat amounting to more than $5 million, according to the SANS Institute[3].

The insider attack players break down into two categories, according to SANS:

- **The malicious employee.** Jaded, disgruntled, or perhaps simply a person of low character, the malicious employee seeks to steal sensitive and/or proprietary data on the network. About one-fifth of organizations consider this worker as the greatest of threats.
- **The negligent employee.** A.K.A. the "accidental" threat, negligent employees invite risk through uninformed, highly questionable behaviors. Via social media and email scams, adversaries target them, to con them into doing something that appears legitimate, but actually allows the adversary to slip "inside the gate" of the network. One-half of organizations view these staffers as their biggest threat.

A lack of awareness accounts for much of the negligent employee's behaviors, as 45 percent of workers receive no cybersecurity training on the job, according to CompTIA[4]. Nearly two-thirds depend upon business-intended devices for personal activities like shopping, banking and social media surfing. Virtually all of them connect their devices to public Wi-Fi networks, with seven of ten calling up company-related data while doing so. And when USB storage drives are involved, the results can be frightening.

Clearly, traditional security tools – while still playing a key role in safeguarding systems – no longer suffice as a sole remedy. IT purchase decision-makers and their tech teams must acquire solutions which enable them to match technology with human oversight, paving the way for 24/7/365 visibility into how users behave, no matter when or where they're connecting to the network. Then, they have to prioritize each risk and launch remediation/mitigation measures.

Relatively few organizations have ascended to this level of a protected state. But they can get there – with less time and cost investment than they realize – to the benefit of their information assurance and business strategies. In this paper, we will explain how.

1 Source: http://www.pmg.net/portfolio-items/2015-pmg-it-and-ux-survey/

2 Source: http://www.nielsen.com/us/en/insights/news/2015/so-many-apps-so-much-more-time-for-entertainment.html

3 Source: https://www.sans.org/reading-room/whitepapers/analyst/insider-threats-fast-directed-response-35892

4 Source: https://www.comptia.org/resources/cyber-secure-a-look-at-employee-cybersecurity-habits-in-the-workplace

LACK OF VISIBILITY AND CONTEXT LEAVES ORGANIZATIONS EXPOSED

Currently, the response to user risk is dictated by where organizations stand on the awareness spectrum, which is defined by two opposite ends:

Total awareness. IT teams and leadership recognize that user dynamics have completely changed – it's a major source of anxiety among security staffers, in fact. With a state of urgency justified, tech budgets now set aside funding to address user risk.

Denial. There is a reluctance to acknowledge that the worst can happen from the inside. Leadership dismisses such concerns by saying, "We hire good people. They do terrific work for us, and they have earned our unchallenged trust."

Most organizations are situated somewhere in between the two extremes. They are united, however, by market forces which drive their pursuit of strategic objectives. The Information Economy dominates the landscape, after all. Knowledge workers obtain access, autonomy and authority over sensitive data to do their jobs, requiring management to grant them a broad extension of trust.

Therein lies the tension, with leadership executives conceding that – without the liberation of data to knowledge workers – they will lose their ability to compete. Yet, with the liberation comes risk, whether triggered by intentional or unintentional actions. Thus, risk emerges as a necessary evil that's critical to business success. If you choose to "play it safe" by locking down data, you'll eventually cease to exist.

All of which begs the question: What do we do now?

The answer begins with the establishment of total visibility and context.

Presently, most organizations cannot "see" the extent of their user behavior. If they can, they typically lack context into what they are looking at, to separate acceptable activities from potentially dangerous ones. Yes, they gather large volumes of log data and may be capable of aggregating it into a security information and event management (SIEM) repository. But they don't have the visibility and contextual intelligence to decide which events merit further examination and which can be disregarded. It's not enough to know what employees are doing on the network. You need to know why they're doing it.

Stick-y Situation

Users apparently can't get enough of USB storage drives. And their subsequent practices are jaw-dropping...

- Three-of-five employees rely upon potentially insecure USB storage drives to transfer files among devices.
- Thirty-five percent have borrowed someone else's USB stick to transfer files.
- More than one-fifth would pick up a stick they found in public.
- An astonishing 84 percent of those who'd pick up a stick they found would plug it into one of their work devices.

Source: "CyberSecure: The State of Employee Cybersecurity2015," CompTIA

Because such intelligence remains elusive, IT teams are insufficiently equipped to adequately respond to insider risk: Seven of ten organizations rely upon products which do not provide enough contextual information, according to research from the Ponemon Institute[5]. What's more, alerts "flood the zone" of security monitoring teams' oversight, as 56 percent of security professionals say they encounter too many false positives. At first, they plead for additional manpower – security analysts in particular. But then the finance department tells them that they don't have the funding to hire experienced analysts.

This leaves the teams feeling like they're trapped in a corner, with no "rescue plan" in sight.

Fortunately, there is a rescue plan, and it's readily available in the form of analytics-based solutions. By 2018, enterprises will discover at least one-quarter of self-identified breaches through user behavior analytics, according to research from Gartner[6]. These tools represent the pathway to optimal user visibility and context. But – for unquestioned success – security teams have to combine the new technologies with a human-led, step-by-step strategic plan, one that we call the Five Pillars of User Risk Mitigation. In the next section, we will elaborate upon each of the pillars.

5 Source: http://www.ponemon.org/blog/ponemon-institute-and-raytheon-release-new-study-on-the-insider-threat

6 Source: https://www.gartner.com/doc/2998124/best-practices-success-stories-user

THE FIVE PILLARS OF USER RISK MITIGATION

By building a program through our pillars, organizations develop immeasurable user visibility and behavioral context:

Pillar #1: Behavioral Auditing

With behavioral auditing, you establish a baseline of "normal" and/or acceptable activity. To do so, you must account for a range of typical and atypical (but not threatening) circumstances.

Why? Because for most of us, our schedules are filled with the routine: We log on to a desktop computer, laptop or mobile device. We check our emails. We call up the files we worked on the day before, and pick up where we left off on various reports, projects, etc.

Still, there are times when we diverge into uncharted yet benign territory: A coworker from another department – one with whom we seldom engage – suddenly asks us to forward research that we recently completed. We accompany our child on a field trip to a place we've never been to, and access the network during a break in the schedule. We have trouble sleeping after 3 a.m., so we go to a diner with public Wi-Fi to get a head start on the day over eggs and bacon.

To security staffers, the situations may seem unusual. Yet, through effective behavioral auditing, they should still fall within a baseline of accepted behavior, a baseline which covers routines, job roles and occasional but hardly alarming deviations from given patterns.

Organizations have access to a great deal of data to determine baselines – to the degree that the data overwhelms them and they can't begin to analyze it. So much of it is unstructured, scattered about in emails, PDFs, spreadsheets, videos, etc. This is the "digital exhaust" of the enterprise, created by an abundance of logging and sensors and endpoints communicating with other endpoints.

Consolidation will help your security teams better manage the wealth of data. Once you put it all together in one place, you want to focus on data that brings you as close to the user as you can get. Toward this end, system logs are revealing, but even more so are sensors detailing a daily flurry of network activities. And most telling of all is endpoint data – a comprehensive roadmap of each employee's practices, whether ordinary or extraordinary, whether authorized or not. When you are this close to the user, you know who does what – with whom – and when, where and how often it happens, i.e., the behavioral baseline you seek.

Pillar #2: Indicators of Risk

You now have user data in one place, to conduct your behavior audit. You can distinguish the routine from the not-so-routine. So it's time to inventory the practices which extend beyond merely harmless deviations, resulting in the loss or destruction of proprietary data, the theft of customers' personally identifiable information (PII), the stealing of sensitive files through unauthorized access, etc.

Executives come to us and say, "I spend lots of money on firewalls, threat detection products and other point solutions … Shouldn't they tell me something about user behavior and risk?" Our response is, "Yes. Absolutely. But we can help you leverage those investments to drive additional value. In other words, we can make what you have even better." Point solutions fulfill a noble purpose. But, when they are combined with behavioral audits and indicators of risk, you gain a richer, more nuanced perspective of risk.

TOP CONCERNS ABOUT INSIDER THREATS	
Compromise of personally identifiable information (PII) relating to customers and clients	67%
Reputational damage	54%
Loss/exposure of confidential business information	51%
Loss/exposure of intellectual property	44%

Source: "Insider Threats and the Need for Fast and Directed Response," SANS Institute

Pillar #3: Risk Scoring

At this point, you have a behavioral audit paired with additional risk indicators. However, it's difficult to keep up with the volume and velocity with which all of the information is coming in. You can't manually process it all, to assess the indicators signifying the gravest dangers.

This is where machine-based analytics enter the picture, to automatically produce a "risk score" for individual user behavior over a defined period of time. With a score, security teams pinpoint which users' behaviors can potentially cause the most damage, and respond accordingly.

The rating can be numerical, the classic "1 to 10," with the "10s" being the most urgent. When employees log in from machines they have never used before, access files they have never needed and correspond via email with new parties who are not associated with work matters – these and other patterns will ratchet up the score.

A "2" or a "3" may amount to little more than a staffer emailing an external party who doesn't appear on the surface to have legitimate business with your organization. An "8" or "9" could involve a finance department executive who is scheduled to work at the office all week, and yet calls up and forwards a classified budget-planning document while connecting from an airport Wi-Fi location in London – a file that has nothing to do with her areas of responsibility, and one for which she used someone else's credentials to obtain.

Would the latter scenario validate immediate intervention? Perhaps, but not necessarily, as our next pillar illustrates...

Pillar #4: Forensic Context

If you have reached our fourth pillar, then congratulate yourself. Most organizations have yet to implement a program that includes an effective behavioral audit, indicators of risk or automated risk scoring.

But if you have come this far, why not push efforts further, to actually solve the problem, reducing organizational risk as related to user behavior over time. Risk scores alone won't get you there. They are like most statistics: They convey part of the picture, but not the entire picture.

Through forensic context, you fill in the missing pieces with a narrative that connects all the numerical dots.

In the case of our finance department executive, for instance, forensic tools can examine the employee's email correspondences, web surfing and interactions with coworkers/managers to disclose perfectly appropriate, non-threatening reasons for what she did in London. Forensics would reveal that she had to abruptly leave for Europe due to the unexpected death of a close relative there. While awaiting a connection at the airport, she checked into her work account and called up a voice-to-text message from her CFO, who gave her credential information to access and forward the budget planning document to him. (The CFO was hurriedly driving to an off-site meeting in which the document would be reviewed, and didn't have the time or patience to pull over and retrieve the document himself. In his haste, he also didn't realize that his executive was in Europe when he asked her to forward the document over.)

In addition to crosschecking emails, web surfing and file usage, enterprises can elevate the sophistication of their forensics through desktop video solutions, which deliver an "over the shoulder" view of what users are doing at their stations. Security teams can observe anyone of interest, or they can retrieve video capturing specific times of interest via DVR-like replay.

With these and other forensic methods and technologies, you ascertain what is – and what isn't – the authorized and non-threatening deployment of company computers and devices. That's the "story behind the numbers," signaling whether action steps are warranted.

Pillar #5: Remediation

The action steps, of course, are remediation and mitigation. You have flagged unusual activity. You have concluded that it cannot be "explained away" by a narrative which holds up to scrutiny. You understand that there is too much is at stake – data/informational assets, customer loyalty, brand reputation, etc. – to sit still.

Because the range of user intent is so broad – a human mistake, or something less innocent? – the range of appropriate remediation is broad. Therefore, forensic context should determine the action steps. Without forensic context, you won't know if a user just needs better training, or if the situation warrants a reprimand and/or a performance improvement notice.

If remediation requires more severe and swift action (like a termination), you contact the employee's manager and HR. (And possibly bring in law enforcement.) Then, you minimize any damage by locking down the employee's access to the network. You isolate associated computers and devices until you can bring the situation to its proper conclusion.

As previously indicated, you cannot do this without the assistance of analytics. To learn about a solution that's helping organizations reach an optimal state of visibility, identification, prioritization, contextualization and remediation, read on.

SUREVIEW INSIDER THREAT ENABLES ACTIONABLE AWARENESS

To help security teams implement our Five Pillars, we offer SureView Insider Threat, a solution which identifies questionable behavior and resolves impending incidents before damage is done. SureView Insider Threat goes beyond virus scans, configuration management, log analysis, "dirty word" searches, etc. These functions contribute to determining what's going on. But they can't reveal the "why" behind the "what."

SureView Insider Threat closes the gap as an all-in-one product, with systems administrators and managers gaining comprehensive visibility into the thousands of human and computer exchanges occurring every day. If data is compromised, SureView Insider Threat can assess the intent of the user who caused the issue – was it a simple mistake, or the outcome of ill-will?

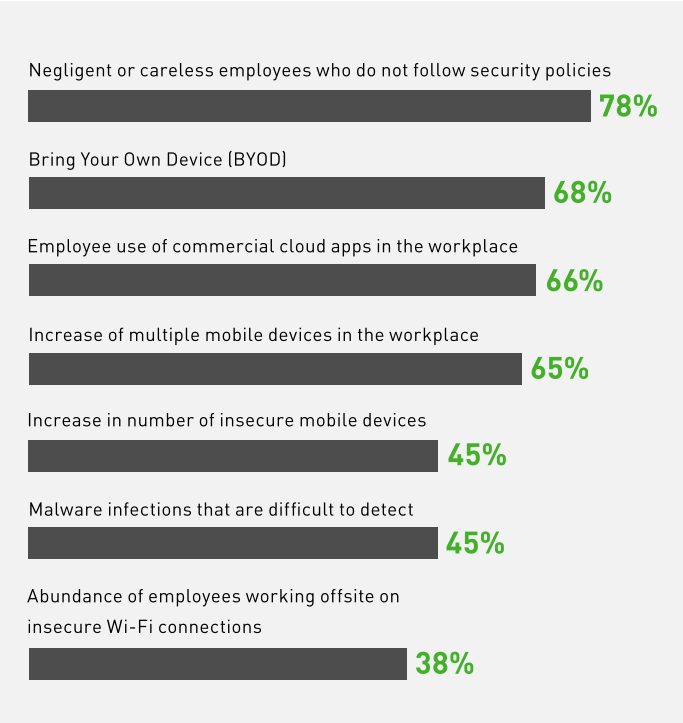
SureView Insider Threat detects incidents that help prevent damage while not presenting obstacles to user productivity or business functions. It is built around the following tenants:

- **Behavior analysis and focused observation:** SureView Insider Threat identifies risky behaviors by baselining "normal" for the user, and the organization then **captures deviations** from "normal" such as a change in data access, working hours, email activity etc. These deviations are risk indicators that serve as warning signs leading up to a breach. The riskiest users are pinpointed with deep visibility into their behaviors. SureView Insider threat applies

user behavior analytics to mitigate the insider threat, resulting in answers and not just more questions—true user risk mitigation.

- **Contextual, actionable awareness.** SureView Insider Threat monitors endpoint communications and applications in real-time. It not only examines data location and movement, but it also monitors the actions of users who access, alter and transport data. SureView Insider Threat interprets meaningful patterns in large sets of audit data through analytics-interface tools, allowing for risk assessment, anomaly detection, user trend analysis and role-based profiling.
- **Threat elimination.** SureView Insider Threat establishes the broad monitoring of your data and assets for risk indicators. If a violation is found, it further targets specific events for investigation. It ascertains when intellectual property is leaked or stolen through accidental or deliberate methods — whether via email, clipboard cut-and-paste, screen captures, printing, copies to USB drives, etc. SureView Insider Threat will detect tampering regardless of an insider's evasion techniques, whether the computer is detached from the network or files are encrypted. Features like disconnected caching and event-correlating analytics bring clarity to the most complex activity. SureView Insider Threat generates the details, insight and context to measure the severity of the compromise, fix the problem and build the policies to prevent it in the future.
- **Total coverage.** Only SureView Insider Threat can thoroughly track all communication vectors at the endpoint to discover threats normally hidden by encrypted traffic and files, and continue monitoring while desktops are offline. Since SureView Insider Threat is on the endpoint, it provides clear-text visibility of the encrypted email, files and web sessions collected immediately pre-encryption and/or post-decryption.
- **Video replay.** You will gain compelling video of workstation activity, including what was going on before, during and after an incident. SureView Insider Threat targets specific occurrences and produces context in the form of DVR-like video replay.
- **"Real" event identification and enterprise scalability.** SureView Insider Threat sends active alerts as to when policy violations are underway. If an employee is pasting confidential report details into a clipboard – whether with good or bad intentions – SureView Insider Threat can give notice (to the employee and/or systems analysts) that such actions violate company rules. SureView Insider Threat's engine and analytics minimize false positives and false negatives. It strictly monitors what approved policies state, and its ability to create fine-grained policies keeps you from sifting through thousands of non-substantive alerts to find the "real" events. Built for speed and simplicity, SureView Insider Threat scales easily to large enterprise installations.
- **Remote user monitoring.** SureView Insider Threat uniquely monitors remote users at their endpoints, identifying violations and collecting events, when remote users are connecting and when they are not.

BIGGEST CAUSES OF ENDPOINT SECURITY THREATS



Source: "2015 State of the Endpoint Report: User-Centric Risk," Ponemon Institute

CONCLUSION

In the last century, we have often participated in debates which pit Man versus Machine. But when it comes to user risk mitigation, we should think in terms of Man and Machine.

That's because analytics technologies are only as good as the people who are developing the strategies, policies and practices which drive their deployment. Leadership must allow and even encourage work teams to thrive within a less restrained data environment. This is a recipe for modern business success. But the recipe requires another ingredient – the implementation of our Five Pillars along with SureView Insider Threat to ensure the following:

- Visibility and context into all user activity
- A formidable defense against malicious and unintentionally harmful insiders
- Elimination of multiple resource solutions
- Enterprise security without productivity disruption

When man and machine come together like this, organizations harbor no fear as employees unleash the complete potential of data. Leadership executives realize security teams are closely monitoring user activity to sort innocuous interactions from threats. They are fully confident that raised visibility and context-enabled awareness will not arrive at the cost of doing business. And – to their extreme comfort – they know they don't need to "control" the use of data to protect it.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[WHITEPAPER_SUREVIEW_INSIDER_THREAT_UBA_PILLARS_EN] 200037.011416