FORCEPOINT
POWERED BY Raytheon

Whitepaper

Defeating the Threat Within

HOW IT SECURITY TEAMS BATTLE THE NEW WAVE OF EMPLOYEE BEHAVIOR TO THWART INSIDER THREATS EARLY AND OFTEN.

Joe in accounting is about to put all your confidential data at risk, cost the company millions of dollars, and likely get someone fired.

As a technology professional, you know that data, network and system failures aren't your biggest problems. It's the humans who interact with these systems that cause your biggest headaches.

High-risk insider threats – malicious, careless or "negligent" employees – are one of the main causes of data breaches. Most of the time, these are simply ordinary users focusing on getting their job done. They're not thinking, minute by minute, about protecting the company's sensitive or confidential information.

Whether employees are negligent or malicious, IT security teams (and ultimately, CISOs) are responsible for protecting the organization from breaches and risky behavior. But outdated, traditional security solutions don't offer enough protection from threats inside organizations. Security professionals need a new playbook for dealing with insider threats.

Insiders are the new threat. Here's what to avoid.

It's easy to believe that your workforce is "too smart" to avoid breaches, but it's a mistake to think so. You have hundreds or even thousands of employees, and while you trust them, 94% of your employees will potentially be duped by a socially-engineered, targeted phishing scam . This applies to every organization, regardless of size or industry.

"94% of your employees will potentially be duped by a socially-engineered, targeted phishing scam"

Employee education and automated security feedback helps, but it's not foolproof. As quickly as training ends, new threats come your way. What's more, individuals respond or react differently to threats and education falls on deaf ears if a disgruntled employee is out to do harm.

Hackers create phishing lures because they work. Targeted lures are designed to fool people; they're well-researched, highly plausible and difficult to discern. Traditional endpoint defenses won't always work with such dangerous lures. Sometimes, the people who fall hardest for these tricks are among the most highly placed in your organization – people who likely know the rules of security but still get pulled in.

You can't afford a 6- or 7-month breach. The average "dwell time," the amount of time between infiltration and remediation of a breach, is over 200 days in most organizations. And remediation costs precious time and resources. The good news is you can hope that you may have almost seven months before data is stolen. The bad news is you may not. But in either case, hope isn't a strategy, is it?

All networks are vulnerable because they have people using them. Reality check: Your network will be breached. Even if you have the strictest protocols for email and web security, for example, there's a 94% probability that some of your employees will blend personal data on their work devices – and vice versa. The key is finding and securing those breaches early and keep your data – the ultimate target – secure.

Hackers keep getting more creative. Hackers create, disseminate and mutate their threat techniques faster than most IT security teams can effectively react. Risks posed by all threats – external and internal – are rising daily and not going away. At some point, you'll be a target.

Be ready.

Like most knowledgeable security professionals, you know your network will be breached at some point. That's probably one of the reasons why you likely have a robust data loss prevention solution in place.

While data loss prevention is an important part of your day-to-day defenses, the key to full protection is having a system that can see new threats before they become a problem.

Having good data security is like having healthy habits. If you keep an eye on your diet and exercise regularly, you're less likely to catch the virus that's spreading among your co-workers. Or, if you do catch it, it will likely be short-lived and not have a huge impact on your health.

But sometimes, new illnesses can strike even if you're in the best of health. You may not even know you caught the virus because you feel OK on most days. By the time you realize you're sick, you're really sick. The virus has turned into an infection. Wait much longer to take care of yourself and you could develop the flu or pneumonia.

It's the same with data security breaches. You need robust defenses, but that's just the start. To truly be prepared, you also need strong diagnostic systems that can keep watch over your users, your network and your data to detect abnormal behavior as soon as it happens. Combining that with automated systems that provide the context in which problems are occurring enables you to more rapidly and accurately decide what actions to take to correct the problem and get back to feeling — and performing — better.

It's not enough to train employees, rely on web and email filtering and employ data loss prevention. Just like with your health, you need an "early warning system" for insider threats.

Visibility, Context and Time: Your Insider Threat Defense Allies

The key to thwarting breaches from your biggest threat, your most vulnerable "endpoints" – your employees – is knowledge. It's critical to detect breaches, understand the intent or context and then act quickly.

SEE WHAT'S HAPPENING

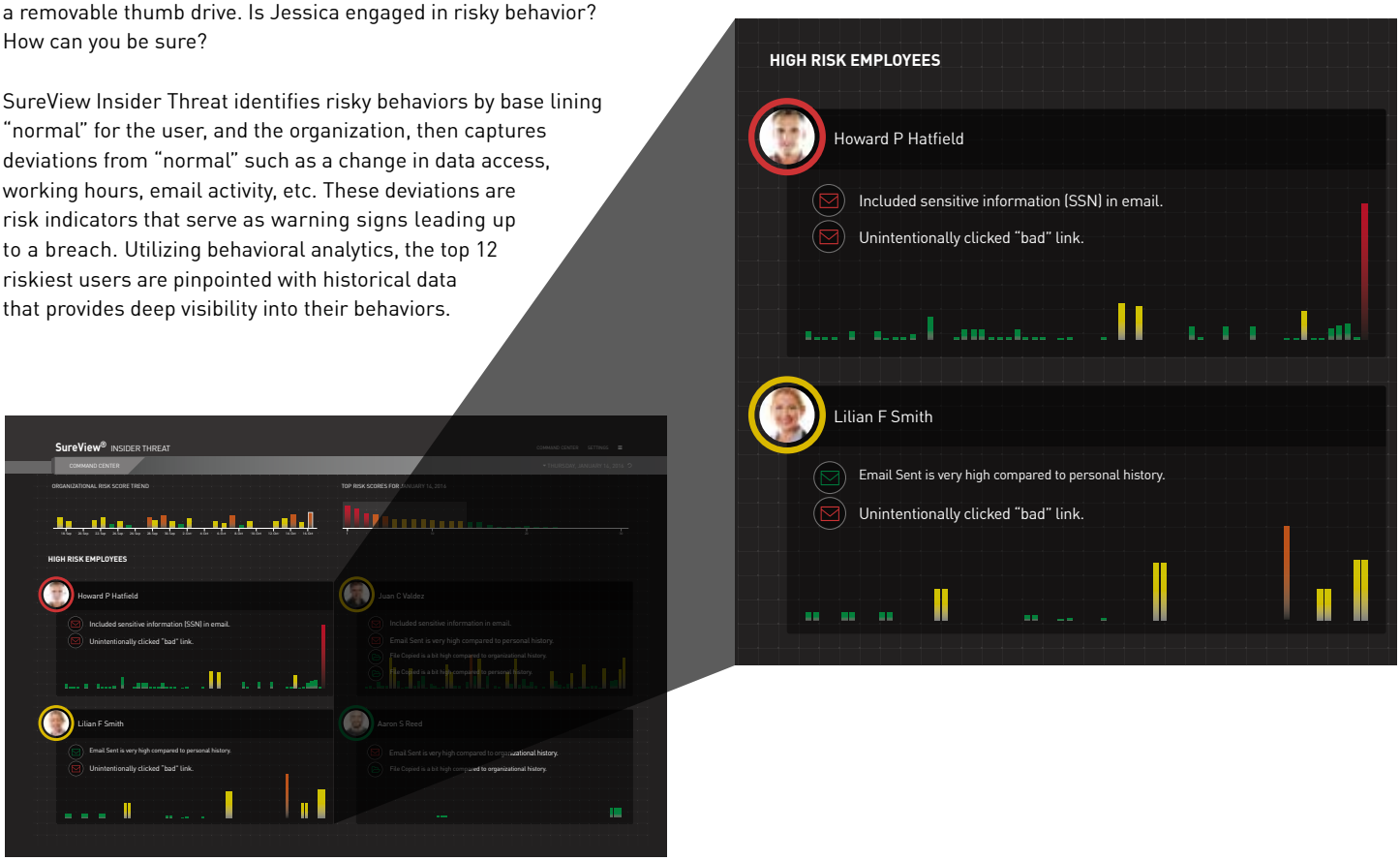
Forcepoint™'s SureView® Insider Threat watches user behavior and alerts your team to any suspicious, risky, or data-exposing activities. Within moments of risky behavior taking place, you'll know. And, you can set up your own definitions of "risky" behavior or use policies Forcepoint has developed in working with large enterprises, including major federal agencies.

Say, for example, that SureView Insider Threat has noticed that Jessica in marketing has downloaded a huge file from the company network. Further review reveals that she then transferred the file to a removable thumb drive. Is Jessica engaged in risky behavior? How can you be sure?

SureView Insider Threat identifies risky behaviors by base lining "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. Utilizing behavioral analytics, the top 12 riskiest users are pinpointed with historical data that provides deep visibility into their behaviors.

Insider Threat will not only flag Jessica's behavior, but it will also record her screen for playback, like a DVR. You will not only see what's happening in near real-time, but you can review what happened around it.

In Jessica's case, the CFO asked for her to download a large presentation onto a thumb drive. Jessica wasn't doing anything malicious, but this alert is important. The technology team can take this opportunity, for example, to ensure the thumb drive doesn't contain any harmful files before it goes into the CFO's laptop. Or they can load the presentation onto a laptop that's not connected to the network so that the CFO can use the file without attaching an external device.



PUT BEHAVIOR IN CONTEXT

It's not enough to know that certain user behavior is happening. You need to understand the intent behind risky user behavior. Is it intentional or accidental? Where is it happening and when? Most major breaches begin with a well-crafted email that circumvents traditional email security and fools the end user into risky behavior.

It's not just seeing what is happening in a narrow context, but in a broader, more accurate one. For example, imagine a photograph of a person running in the street. You may initially think he's running from a crime. But if you see a bit more of the picture, such as seeing another man running behind him, you might assume he's being chased or make other assumptions. If you could see the whole picture, you would see that they're both escaping from a burning building.

SureView Insider Threat provides context and user intent quickly and definitively, now and in the past. In Jessica's example above, her actions were shown to be non-malicious; the context shows that she is an unintentional threat and needs some training so she doesn't do that again. This data can help you create guidelines that alert you to future risky types of behaviors, making early detection more relevant and effective to your business.

MONITOR MULTIPLE VECTORS IN REAL TIME

Without all the information – the visibility to the breach, understanding the intent of the user, and seeing the full context – identifying an infection can take a lot longer and put your critical data at risk for weeks, if not months.

Insider Threat gives you a comprehensive monitoring of multiple attack vectors – internal and external. It signals potential risky behavior – large file transfers, responses to lures or infected URLs, for example – in near real-time, giving you the details you need to contain threats immediately.

When you're able to review your employees' actions promptly, you're not playing catch-up. You're seeing a potential problem, identifying the threat, analyzing it and remediating it quickly before the threat has the opportunity to steal your data.

You can be sure that you won't discover a threat months later when it may be too late. You can mitigate the threat before it becomes a headline about your company losing customers' private data, proprietary data and valuable market share.

DEPLOY AN "EARLY WARNING SYSTEM"

This monitoring and intelligence defense capability is an "early warning system" that identifies and potentially deters inappropriate behavior before data theft or leakage can occur. In addition to providing opportunities to quickly educate people about behavior that can pose risks, it also helps indicate similar risky behaviors to uncover trends for employees and teams. For instance, if you know that accounting does a huge file transfer at the end of each month, you can mitigate risks ahead of these activities, and then get better and safer over time.

Forcepoint SureView Insider Threat helps you identify negligent employees quickly and apply the appropriate restrictions on their actions and their system access. This early warning system allows CISOs and security teams to make informed decisions on policies that are directly applied to preventing and containing insider threats.

HELP EMPLOYEES USE TECHNOLOGY AND DATA TO ITS FULLEST ADVANTAGE

Employees' risky behavior – whether intentional or innocent – won't ever completely go away. They'll never be as vigilant about protecting data as you are; they're too busy doing great work.

Your team helps protect the employees by protecting the valuable data they use every day. But just as importantly, you also empower them to perform their jobs as best as possible by enabling them safe access to the data, tools and technology they need.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[SOLUTION_BRIEF_CISO_INSIDER_DEFEATING_THE_THREAT_EN] 200036.011416