ebook

The Why, When, and Where of Workforce Protection

Mitigating the Risk of Employee Behavior

FORCEPOINT

Threats from Within Require a Holistic and Sophisticated Strategy

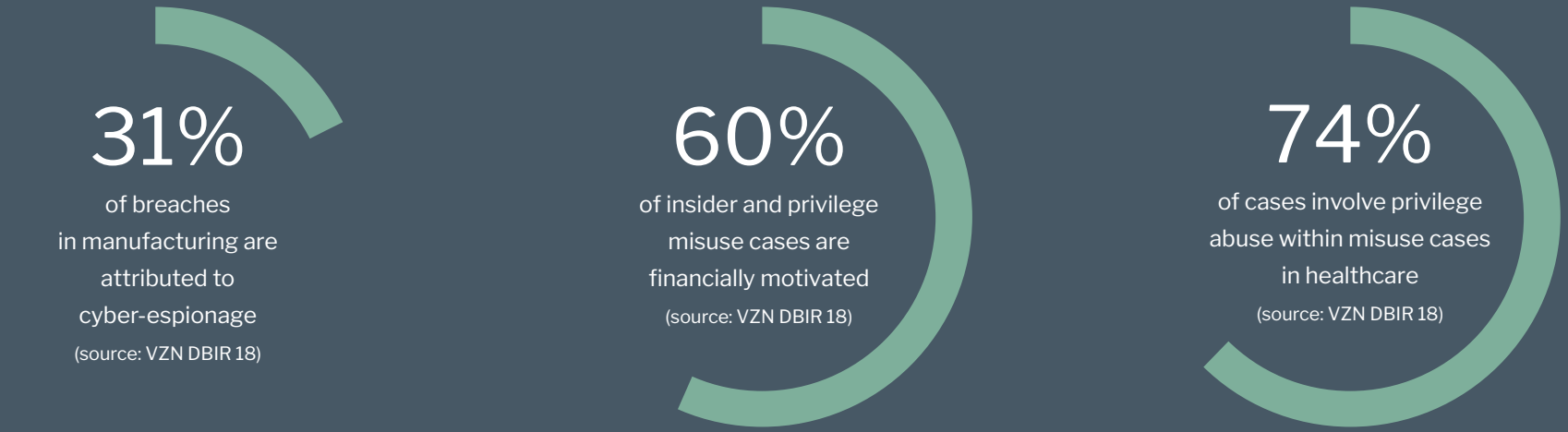
Managing risk

Workforce protection is focused on managing the risk posed by insiders of the organization. These threats have traditionally been managed through the strategy of putting basic safeguards in place and, by and large, assuming that employees were always trustworthy and never engaged in risky behavior. This reliance on strategy over organizational culture is unwise and unfounded. As Troels Oerting, Group CSO and CISO at Barclays recently noted, quoting Peter Drucker at an FS-ISAC meeting, "Culture eats strategy for breakfast."

That said, strategy and culture remain intimately linked; a workforce protection or insider threat strategy with strong ties to an organization's culture is vital for managing the potential risks posed by employees. To this must be added security awareness metrics that help tailor education to individuals operating within different business units and the appropriate monitoring and recording of high risk activities to identify why, when or where an employee's behavior has increased the likelihood of a data breach.

Inspiring change

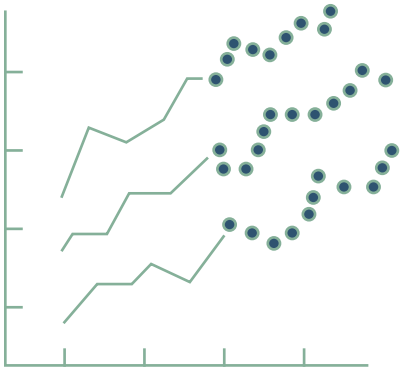
Institutions with IP and sensitive data must understand that, while the right "Why," "When," and "Where" questions will typically highlight behavioral risks to the business, continuous behavioral analysis is both difficult and time consuming. Automation can help, but with it comes the constant challenge of verifying and supervising any decisions being made without previous knowledge of the supporting data. Disruptive technologies such as Blockchain 2.0, aligned with risk-based and data-centric strategies, will offer some assurance, but insider threats remain difficult to manage through technology alone. What's needed is a smarter, more comprehensive approach that combines business and compliance processes so that the level of protection keeps pace with an ever-expanding and evolving digital threat space.



Insider Risk and the Financial Services Industry

Internal fraud, money laundering, employee discrimination, regulation, and ethics are some of the typical areas financial services organizations focus on when defining, identifying, and managing an insider threat policy. In part, this has been in response to regulatory requirements, including the U.S. Sarbanes-Oxley (SOX) Act and the UK Financial Services Act 2012, which have been enacted to protect consumers from any intentional or negligent wrongdoings.

Challenges caused by new capital markets with lax policies or insufficient security in place, the modularization of financial products, and the increasing pace of data connectivity are also disrupting the industry. They often heighten the risk of employee negligence, which, in turn, has to be carefully managed to maintain the integrity of data security and privacy capabilities. GDPR requires the processing of personal records with stricter monitoring. In the event of a personal data breach, for example, the relevant supervisory authorities as well as the victim must be notified within 72 hours.



Workforce Protection: The Why

Employees inside the organization are able to side-step security policies to cause harm or, more commonly, are users whose actions can unwittingly compromise even the most impressive external threat defenses.

Insider—three behavioral types

1. Compromised—Can refer to technology (e.g., a specific device has been compromised, often without the user's full knowledge), or to an individual (the consequences of blackmail, etc.).
2. Malicious—Includes both premeditated acts of sabotage for purposes of financial gain or retribution, and deliberate behavior that leads to a breach.
3. Accidental—Defined as unintentional employee carelessness that can expose your network—from emailing customer data to the wrong recipient, to being duped by the latest phishing scam.

Why invest in workforce protection?

There are three principal reasons why organizations introduce insider threat technology:

- **Compliance**
  To ensure the effective identification, evidence collection, and reporting of a breach, and to demonstrate that proactive capabilities are in place for mitigating risk.
- **Threat visibility**
  To gain the necessary, actionable intelligence into the risk landscape to plug any gaps and ensure that the necessary monitoring is in place.
- **Managing risk**
  To establish greater control over potential threats by introducing the ability to predict events, rather than just reporting on them after they've happened.

In each scenario, as a growing body of research suggests, it's not your data, network or system failures that pose the biggest risk to critical data. Rather, it's the human point, where people access your critical data every day.

An early warning system

It's not enough to simply know that certain behaviors are occurring. You also need to understand the context and intent of user behavior–hence, the importance of establishing an early warning system, and proactively searching for abnormal behavior across a range of risk indicators that might point to a potential breach in the near future.

Which threats and vulnerabilities have most increased your risk exposure over the last 12 months?

EY 20th Global Information Security Survey 2017-18

Vulnerabilities	2013	2014	2015	2016	2017
Careless or unaware employees	53%	57%	44%	55%	60%
Outdated infosec controls or architecture	51%	52%	34%	48%	46%
Unauthorized access	34%	34%	32%	44%	37%

The chart shows a total percentage figure for those items rated 1 (highest) and 2 (high), from 2013-2017

Workforce Protection: The When

Following the “Why” is the “When,”, i.e., the urgency with which insider threats should be prioritized. Three reasons point to an immediate need:

- **Avoiding financial and reputational damage**
  On average, it takes 170 days to detect a cyber crime; when an insider is involved, that number jumps to 259 days.
- **Meeting regulatory commitments**
  UK and EU regulations define both data security requirements and how organizations should respond to a data breach.
- **Reducing cost to the business**
  According to recent studies, IT professionals spend almost three hours a day dealing with the security risks caused by employee mistakes or negligence.

Technology goes hand in hand with insider threat detection

The biggest driver for workforce protection is simple: the risk is already here, compromising your business clients and putting their reputations at risk each and every day.

For many CISOs, such knowledge raises two urgent questions:

- How can I find out which individuals in my organization are engaging in potentially risky behavior?
- If I identify a potential risk, how can I quickly understand the context surrounding that behavior in order to take immediate action?

Both answers begin with increased visibility into user activity. This means gaining the insight to identify risky behavior, coupled with the broader intelligence needed to understand the intent behind user behavior. Only then will you know you’re using the right controls and that they’re being used to uncover trends relating to wider, systemic failings.

A question of confidence and support

Today, the scale of any breach is no longer limited by what can be physically carried out of a building. Even one negligent or malicious employee can severely damage or even destroy an organization's market advantage and reputation. Demonstrating to the board solutions that are able to identify which individuals pose the greatest risk and why will go a long way toward building both internal and external confidence.

At Forcepoint, we fully appreciate the power of reassurance and deliver the products and services that enable financial services organizations to perform in the marketplace with security and confidence. As your security partner, we provide the necessary insights and advice for ensuring that an effective insider threat detection and prevention platform is in place to help mitigate enterprise intellectual property theft, data loss, and other potential threats.

Workforce Protection: The Where

The "Where" of workforce protection is relatively simple: where should you focus your attention and security investments? In part, this requires knowing where the threats are likely to emerge and recognizing that they're not just limited to the network. For example, when your employees leave the network, they effectively become invisible. Your now-remote employees can access your critical data on devices that are outside any of your security controls.

For complete coverage, insider threat capabilities must monitor continually in real time, even when devices are used offline. Monitoring must provide both the visibility and context to help you immediately assess the severity of a potential threat and address the problem.

At Forcepoint, we believe that establishing your controls and understanding context are vitally important. That's why we adopt a unique approach that brings together both unrivaled data loss prevention (DLP), User Activity Monitoring (UAM) for deep collection, and behavioral analytics solutions to directly link data movement with user behavior to ensure data protection and provide an early warning system to other threats on the horizon.

Made to measure

Endpoint monitoring is a key component for building a robust defense. Another is detecting abnormal behavior as soon as it happens, using strong diagnostic systems. Armed with such behavioral analytics, you can create statistical baselines for user activities and then use them to conduct volumetric anomaly detection. Mapped against your definitions of high risk behavior, you'll also be able to minimize false positives and false negatives to ensure you're analyzing the truly meaningful events—not thousands of non-substantive alerts.

The result will be a broader, more accurate perspective of cause and effect. You'll also have the necessary context to not only explore the root behavior, but to confidently take the appropriate measures.

Only Forcepoint has the ability to immediately detect when intellectual property is leaked or stolen via accidental or deliberate methods.

Built from the ground up as your first line of visibility into user activities, Forcepoint Insider Threat provides deep collection and streamlined investigation of insider activities through video cache capabilities and beyond. Combined with the power of Forcepoint Behavioral Analytics, it provides early indicators of data exfiltration events such as stockpiling, negative or illicit behavior, malicious use of resources, and even compromised user credentials.

When combined with Forcepoint DLP (Gartner Magic Quadrant DLP leader since 2008), these tools comprehensively provide the control of and visibility into user activities needed to run an effective Workforce Protection Program. This solution detects threats normally hidden by encrypted traffic, and files, and continues monitoring even when devices are disconnected from the network. The result is proactive visibility into user behavior and an ability to prevent data theft and loss by hijacked systems, rogue insiders, and negligent users.

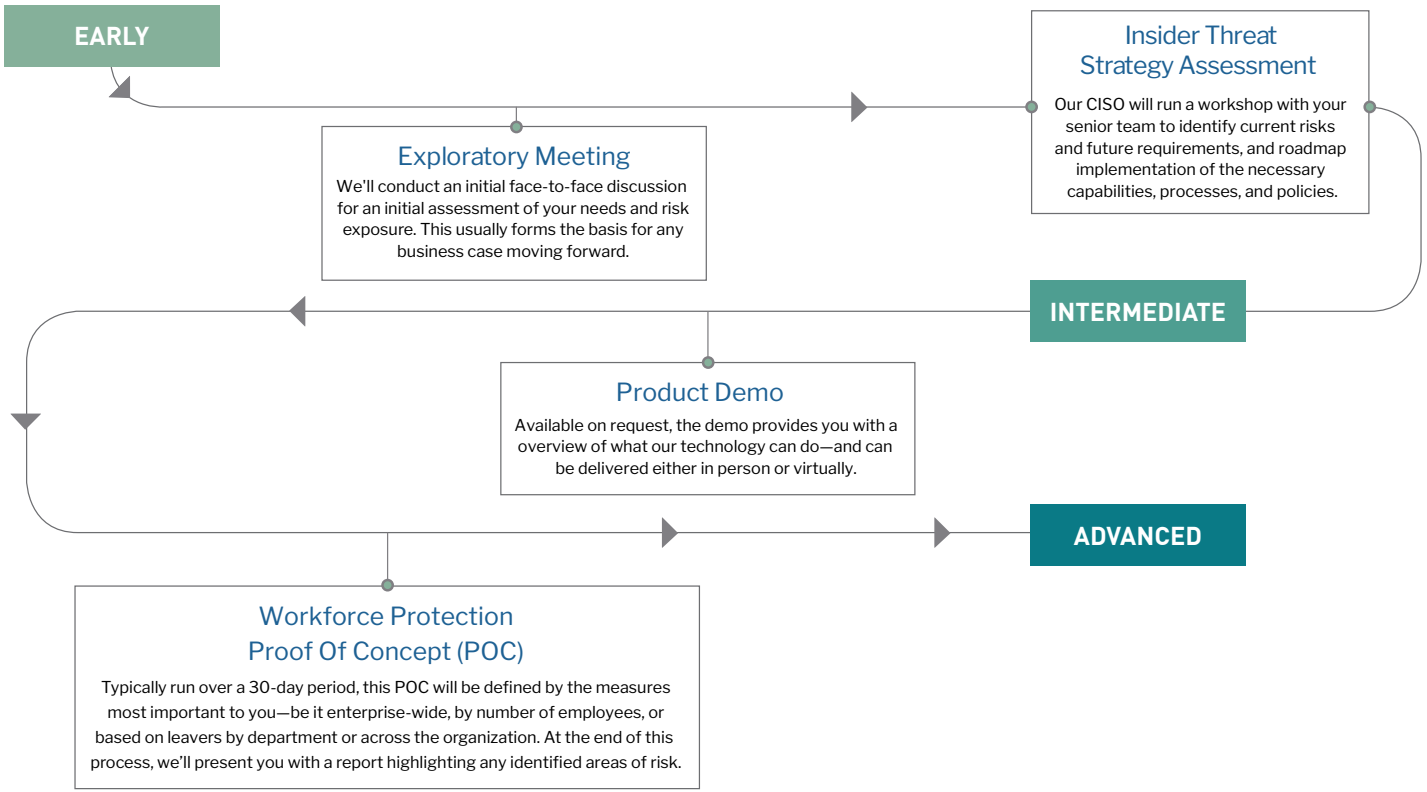
Next Steps

Managing insider threats is a process, not an event. For organizations, it's also a journey, as they steadily build up their capabilities to effectively mitigate risk.

Forcepoint is a proven leader in the field with more than 1 million endpoints already protected—including many Fortune 500 companies in industries ranging from banking to commercial infrastructure.

What are you doing to defend against the threats inside your organization?

Whatever your current level of progress, Forcepoint can offer you a range of valuable services:



Only Forcepoint has the ability to immediately detect when intellectual property is leaked or stolen via accidental or deliberate methods.

About Forcepoint

Forcepoint is transforming cybersecurity by focusing on what matters most: people's behavior as they interact with critical data and systems. This human-centric approach to cybersecurity frees employees to innovate by understanding the normal rhythm of user behavior and the flow of data in and out of an organization. Forcepoint behavior-based solutions adapt to risk in real time and are delivered via a converged security platform to protect network users and cloud access, prevent confidential data from leaving the corporate network, and eliminate breaches caused by insiders. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries.

Contact

forcepoint.com/contact

[EBOOK_WHY_WHEN_WHERE_INSIDER_THREATS_EN] 800004.021219