

WHAT EXACTLY IS AN INSIDER THREAT? Most CIOs would agree that the definition of “insider threat” must encompass any digital behavior that poses a threat to shareholder value through:

- Direct financial loss
- Theft or impairment of intellectual property
- Compromise of customer data leading to brand damage
- Lost productivity and misused resources
- Exposure to legal risk and liability
- Creation of a hostile work environment

Dealing with the growing range of insider threats is daunting. Network complexity, dissolving perimeters, the proliferation of alternative communications channels such as instant messaging and VoIP and easy access to removable media all contribute to raise the threat level.

Enterprises cannot afford to respond with anything less than extremely targeted, focused and efficient remediation. Many have responded with security policies that define accepted user behavior, but in many instances insider breaches exploit legitimate user access and functions.

The breadth and depth of the trusted user threat requires proportionally rich and sophisticated solutions. Already stretched to the limit, IT and security organizations must respond to the specific problem with tailored remediation, not generalized reactions—because no business wants to arbitrarily clamp down on legitimate transmission of information.

benefits. Not surprisingly, some IT organizations have reacted to the insider threat with a firewall mentality: If we can stop external threats from entering the net-

VISUALIZE BEHAVIOR

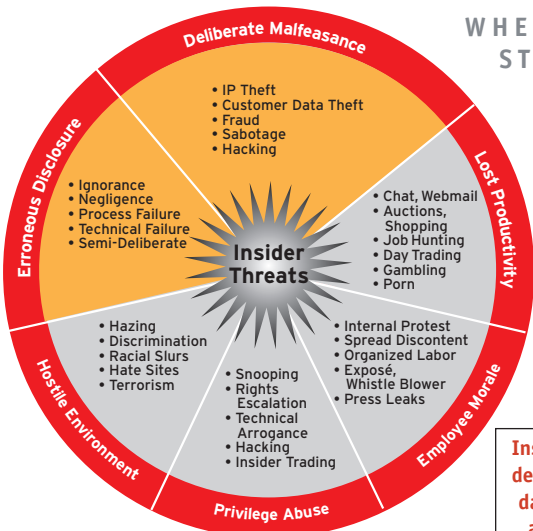


TO STOP INSIDER THREATS

work, the thinking goes, why not implement solutions that prevent information from exiting the network?

These types of solutions, commonly referred to as “content monitoring and filtering” or “information leak prevention” products, address only one vector of insider threats—outbound data streams, mostly e-mail—and can only block data or alert you that it has been transmitted. What’s generally missing from these solutions is:

- Detection of non-e-mail activities, such as copying files to removable media, printer output, and DVD/CD-burning
- Visibility into encrypted transmissions and transactions
- Monitoring off-network and offline user activity, particularly in mobile users
- Ability to detect and prevent deliberately obfuscated multi-vector behaviors
- Situational context for each incident, to minimize false positives and false negatives



WHERE TO START?

Edge security—such as firewalls—is broadly accepted as reasonably easy to deploy with quantifiable

Insider Threats are defined as not just data leakage, but any action that puts shareholder value at risk.

Companies need to be able to detect and respond to the full range of threatening behaviors. The challenge is to implement systems that are constantly vigilant and that can analyze traffic, content and behavior in context to determine whether it is nefarious, serves a legitimate business purpose, or falls into the myriad of activities in between that are on the margin of acceptable behavior.

A solution that provides visibility into behaviors in context provides security professionals with the ability to respond appropriately with policies or practices for near-term remediation or long-term prevention without impeding business.

APPROPRIATE RESPONSES

Most companies would be horrified to discover what percentage of their daily activity involves non-business related activities such as online shopping, stock trading, and travel planning. As headcount is nearly always the largest corporate expense, the impact on profit margins from lost productivity can be substantial. Pornography—much of which easily bypasses most URL filtering solutions—can become a significant legal liability if exposed inappropriately or accidentally.

Employee behavior at the margin of acceptability, or even activities that appear threatening but are in fact legitimate—are almost impossible for automated systems to detect without generation of false positives that disrupt business activity.

Truly contextual activities such as internal harassment, protest, and snooping are nearly impossible to detect, much less prove, with conventional solutions. And detection of truly malicious actions requires sophisticated detection and generation of forensic evidence that can withstand legal review in support of termination or prosecution.

Enterprises need to attack the root cause of the insider threat itself—user behavior—and look at content only as a symptom. Only by moving beyond the reverse firewall mentality—and into the actual root cause of threatening behavior—can organizations achieve the contextual visibility required to mitigate insider threats and truly optimize business processes and procedures.

TAKE ACTION ON YOUR INSIDER THREAT ISSUES TODAY!

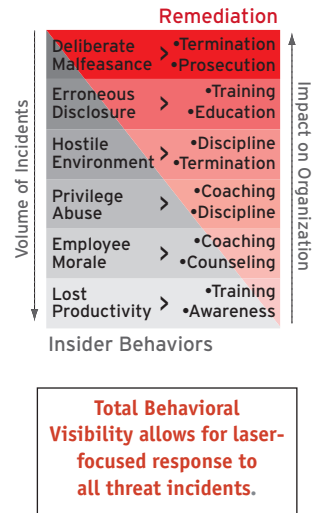
- Download the whitepaper: *Why Content Filtering and Information Leak Prevention Solutions Don't Stop Insider Threats*
- Setup a "Total Behavioral Visibility" Insider Threat Assessment

Register for both at www.oakleynetworks.com/CSO or call toll-free 1-800-662-9120.

OAKLEY DELIVERS BEHAVIORAL VISIBILITY

Oakley Networks, building on a foundation of technology developed for the government, today delivers an integrated solution that addresses the entire spectrum of threatening insider behavior:

- Protection from the network edge to the desktop
- DVR-like incident replay for forensics and investigation
- Detecting incidents even where all traffic is encrypted
- Capturing incidents that take place when a device is not connected to the network
- Allowing anyone, even non-technical staff, to immediately identify threats or unproductive behavior
- Immediately identifying the desktops most at risk, and automatically deploying software to detect more threatening behavior



SUMMARY

Insider behavior—whether unintended or malicious—can carry serious business risks. In today's complex network environment, simple content monitoring and filtering does not provide the context necessary to assess, discover and detect threatening behavior by trusted insiders. It also lacks advanced forensics capabilities, such as capture and playback of incidents. Only Oakley delivers the combination of technologies required to give network managers and security professionals the visibility they need to respond to a range of threats with an efficient range of remediation. The Oakley solution helps you prevent insider threats, implement effective security policies, improve employee training, and target high-risk behavior. ::