observeIT
a division of Proofpoint

CUSTOMER STORY

Bain Capitalizes on ObserveIT to Minimize Insider Threat Risk

Investment Firm Realizes Security Gains by Increasing Visibility and Enriching Alert Context

BAIN & COMPANY

THE CHALLENGE

- Enable privileged user access to sensitive data
- Prevent potential theft or misuse of financial information
- Stop potential data exfiltration

THE SOLUTION

- ObserveIT Insider Threat Management Platform
- ObserveIT integrations with SIEM and incident response platforms

THE RESULTS

- Provided complete visibility into data loss and malicious activity
- Enabled context around any Insider Threats that may arise, including root causes, fall-out, and how to proceed with response
- Created context for security alerts

The Company

Bain Capital is a U.S. private investment firm based in Boston, MA. The company specializes in private equity, venture capital, credit, public equity, impact investing, and more. With investments in a wide range of industries, sectors, and geographic regions, the Bain portfolio services more than $100 billion in capital.

The Challenge

Insiders pose a huge risk for companies of all shapes and sizes, but this is especially true for businesses in the financial services sector. With access to massive amounts of capital and troves of sensitive data, this industry is ripe for Insider Threats. Investment firms are relying more on a transient and digitally-savvy workforce, including younger generations or contractors, to work time-sensitive deals and build new funds. Couple that with ever-present regulations and competitive dynamics, and the need to tackle Insider Threats has never been greater. For Bain Capital, legacy tools were not cutting it, as they were too heavy on the endpoint, left many blind spots and were too easy to circumvent.

The Solution

Bain Capital partnered with ObserveIT to bring better visibility on top of existing preventative controls and meet compliance needs with fewer resources. Tightly integrated with their other security tools, ObserveIT is now a key aspect of their security program and enables them to better manage Insider Threat risk. With the complete Insider Threat management platform on board, the Bain team has visibility into high-risk users across the firm, and can now take appropriate and timely action when an Insider Threat incident occurs

"ObserveIT provides a huge value for me and my team. It is unmatched with any other tools I have—visibility across the network, into endpoints, and into user activity. It provides much-needed context to understand alerts, and is huge to us as a piece of the puzzle in our security program."

Mark Sutton, Vice President and Chief Information Security Officer, Bain Capital

The Results

Unmatched Visibility

ObserveIT provides the Bain Capital security team with complete visibility into data loss and malicious activity by users that circumvents existing controls. ObserveIT offers a variety of angles when it comes to that visibility, as well, ranging from an easy-to-read timeline of user activity to visual replay. This enables the team to communicate with other stakeholders in the organization, including non-technical counterparts, with information that is intuitive and quick to interpret.

Complete Context

ObserveIT provides the team with clear and complete context into any Insider Threats that may arise. Whereas previously the team often did not have enough context to understand what happened before, during, and after an Insider Threat incident, they can now quickly determine the root cause, the fall-out, and how to proceed with response.

Enriched Alerts

As with any sophisticated security program, Bain Capital relies on a range of security tools to gather information and alerts. However, prior to using ObserveIT, it was often difficult if not impossible to make sense of certain security alerts. With ObserveIT on board, they have access to much-needed context that empowers them to understand the efficacy of alerts other technology controls create. Using ObserveIT's intuitive search features, they can quickly track down the source of an alert and build rich context around what happened.

LEARN MORE

For more information, visit **observeit.com**.

ABOUT OBSERVEIT

ObserveIT, a division of Proofpoint, is the leading Insider Threat Management (ITM) solution with more than 1200 customers globally. ObserveIT helps organizations protect against data loss, malicious acts, and brand damage involving insiders acting maliciously, negligently, or unknowingly.

The ObserveIT platform correlates activity and data movement, empowering security teams to identify user risk, detect to insider-led data breaches, and accelerate security incident response. Leveraging a powerful contextual intelligence engine and a library of over 400 threat templates drawn from customers and leading cybersecurity frameworks, ObserveIT delivers rapid time to value and proven capability to streamline insider threat programs.

observe IT
a division of Proofpoint

0000-0000-00-00 06/20