observe IT
a division of Proofpoint

SOLUTION BRIEF

Insider Threat Management

Securing the Remote Worker and Enabling Business Continuity

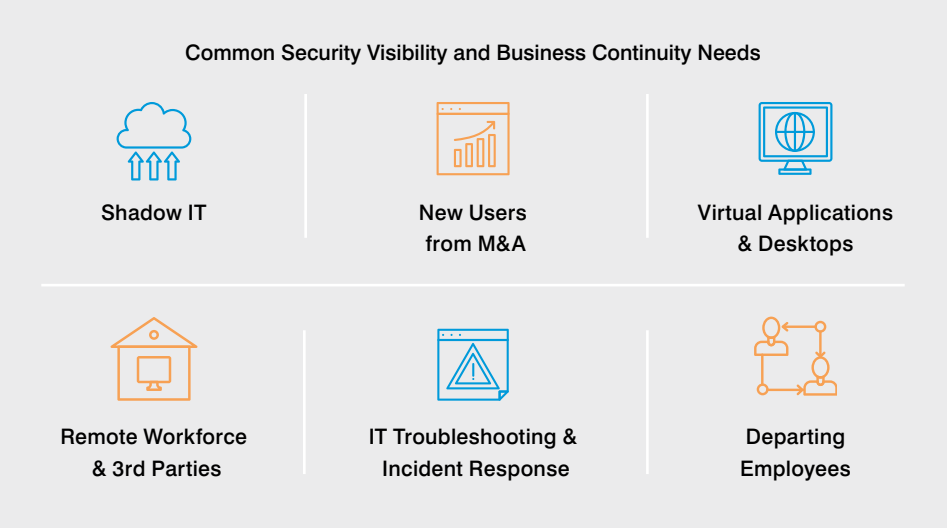
KEY BENEFITS

- Protect against endpoint data loss caused by remote insiders
- Speed up response to remote user-driven incidents
- Get visibility into activity on virtual desktops, jump servers, legacy applications and remote endpoints

Nearly every workforce is mobile and remote friendly now, yet many security teams are stuck with tools built for an office-only era.

Summary

Remote work has many benefits, and the tools that have arisen to enable collaboration help teams get work done and achieve success, no matter where employees and other insiders are located at any given point in time. However, the risks of security mistakes and malicious insider behaviors are only growing as businesses rely ever more on remote work tools and processes. Traditional perimeter-based security solutions do not provide the visibility or context that security and IT teams need to reduce this risk. A people-centric Insider Threat Management solution provides the necessary context around user and data activity to protect against costly data loss, system misuse and/or brand damage that can be caused by remote insiders.



The Challenge: Lack of Security Visibility and Increased Risk Due to Remote Work Conditions

Increased Shadow IT & Pressure on IT Teams

Remote work has increased the propensity of shadow IT, which has left security teams with decreased visibility into data movement and user activity. We cannot rely on the corporate perimeter when it no longer exists, and traditional endpoint data loss prevention (DLP) tools are too easy to bypass. These legacy security tools do not give security and IT teams the visibility they need to understand:

- When users are interacting with sensitive data off-network
- What departing employees and other insiders they do with data after they leave
- What happens after successful disabling of security restrictions on removable media.

Heightened Risks During and After Mergers and Acquisitions

Mergers and acquisitions are a sensitive moment for any organization, and a common time when data exfiltration and other types of insider threat risks are particularly common.

There are two main timeframes when security and IT teams need to ensure complete visibility to protect sensitive assets and data from theft or misuse:

During a merger or acquisition:

- This is a period of high collaboration, often involving highly sensitive information. Stakeholders include bankers, legal counsel, and the firms involved in the deal. Moreover, this takes place within what amounts to a virtual data room.
- Legacy tools make it hard to keep track of who's touching what data and often make it impossible to detect data loss with the necessary user activity context to understand what happened.

After a merger or acquisition is complete:

- In the aftermath of an M&A event, it's common to see user errors, data loss and application misuse. This is a natural result of combining multiple organizations that may have differing security policies and varying levels of security awareness. While security programs are being harmonized, the combined organization faces greater insider risks.

Patchy Security Visibility with Virtual Applications and Virtual Desktops (VDIs)

Virtual applications and desktops (VDIs) are very popular among organizations with large, on-the-go workforces. However, they weren't built with insider threats in mind. The visibility provided by, for example, Citrix and VMWare VDIs doesn't help to detect data exfiltration and system misuse in real-time by insiders with legitimate access. Security teams must painstakingly piece together the user's identity and their actions with data activity and any application(s) in question from hard to understand VDI logs.

Insider Risks with Remote Third-Party Contractors

Many organizations rely on third-party vendors and contractors to keep up with changing economic conditions. Resource-strapped security teams are manually crawling through jump (host) server logs as contractors access applications within the corporate data centers. Additionally, many industries—such as financial services, healthcare and government services—mandate monitoring of third parties that work with sensitive financial, health and otherwise classified data.

Slow, Manual IT Troubleshooting and Incident Response

Remote IT teams must often work around the clock to maintain business continuity, doing so with restricted access to physical servers and data centers. With limited visibility and context, their troubleshooting and incident response processes take far longer than ideal. Moreover, under significant pressure, administrators may take risky shortcuts, such as storing passwords on notepad files, leaving servers unprotected, or misconfiguring certificates with little documentation.

Data Loss with Departing Employees

According to Osterman Research, 69% of organizations say they have experienced data loss when an employee leaves.[1] Mass furloughs and layoffs create even more confusion and can lead to disgruntled employees stealing data, conducting unauthorized activity, or even committing sabotage. Security teams need proactive visibility and detection of risky insider behavior, especially remote workers, during these sensitive times.

"The first tool I go to for investigations is ObserveIT. We get alerts from other tools, but ultimately use ObserveIT for full context around various incidents."

-Bill Duenges, SVP, IT

AIRCASTLE

THE SOLUTION: OBSERVEIT. THE LEADING INSIDER THREAT MANAGEMENT PLATFORM

USER AND DATA ACTIVITY VISIBILITY AND INCIDENT DETECTION.

Complete User and Data Visibility

- Gain comprehensive support of virtualized environments: Citrix Ready, VMWare vSphere, AWS, Azure and 27 flavors of UNIX/Linux server distributions
- Achieve granular visibility into published applications and desktops
- Deploy silently, with easy installs
- Contextualize "who, what, where, when, why" within seconds during incident response

Real-time Alert Notifications

- Detect data exfiltration, account compromise, system misuse and policy violations in real-time with 400+ real-world insider threat scenarios
- Detect contractors misusing systems, departing employees exfiltrating sensitive data and remote users logging on at odd hours, which may indicate insider threats
- Adjust alerts based on threat profiles of user and endpoint groups

Incident Replay

- View timelines of user activity to troubleshoot root cause of IT issues
- Access easy-to-understand, irrefutable incident evidence for HR and legal, with visual activity replay
- Achieve "privacy by design," with compliance-ready features including user anonymization, data exclusion policies, and more

Out-of-the-Box Reporting

- Comply with user monitoring security standards with full metadata audit and screen capture of user actions (e.g. PCI-DSS, NISPOM Change 2 and FISMA)
- Access easy to understand reports and share with non-technical internal audit, compliance and HR teams
- Audit reports of administrator activity to meet internal audit and privacy requirements

Forced Identification on Shared Accounts

- Gain full visibility into user identity on shared accounts on terminal servers and jump servers
- Force secondary login authentication to identify individual users when multiple users share credentials to systems
- Enable granular context when users access a Windows server desktop or published application in your environment

Easy Integration with Service Desk Systems

- Require IT administrators or remote vendors to enter a valid ticket number to complete the login process to a corporate server
- Improve security by limiting server access to administrators and remote vendors with valid IT tickets
- Quickly locate all system and user activity with IT ticket number search instead of keywords or manual crawling through incomplete server logs
- Speed up IT troubleshooting by reviewing the specific actions performed by administrators leading to the error by linking the screenshots of the relevant server session to the IT ticket

Privacy by Design

- Anonymize users to protect identities, unless risk thresholds of agreed-upon policies are breached
- Implement application and data exclusion policies to ensure personal applications and personal data are not tracked
- Focus on user activity & data movement only where your sensitive data lives
- Ensure safeguards against administrators of ObserveIT misusing their access by recording all their actions within out-of-the-box audit logs and screen capture (“watch the watchers”)

PREVENTION ON SERVERS

Linux Prevent Rules

- Prevent unauthorized Linux commands before execution based on flexible prevent rules

  For example, two popular rules include:

  1. block commands to manipulate sensitive protection policy files
  2. block SFTP commands sent from remote servers with intent to bypass security controls

Note: Supported SFTP commands include: MKDIR, RMDIR, LS, RM, GET, PUT, LN, RENAME, CHOWN, CHMOD

Forcing Application Closure

- Block users running harmful applications by closing down the application
- Force closure of applications after severe policy violations on browsers and databases, such as when users browse forbidden websites or execute potentially harmful SQL commands.

LEARN MORE

For more information, visit https://www.observeit.com/solutions/securing-the-remote-worker-use-case/

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