EVERFOX

DATASHEET

EverShield User Activity Monitoring (UAM)

Deep Visibility of User Activity

Benefits

- → Collect from over 15 channels such as web, file operations, keyboards, and email for full context of user activity
- → Explore meaningful data using a powerful dashboard built for analysts, by analysts
- → Transparent to the end-user, preserving the user experience
- → Privacy protection features, including “do not collect” policies
- → Robust endpoint sensor for out-of-the-box and configurable policy-driven data collection
- → Proven authentic, relevant, and original records for use in legal proceedings
- → Scalable and enterprise ready for centralized management for multiple network environments and domains

The EverShield UAM is designed to support the needs of security analysts and investigative professionals by collecting behavioral data from multiple endpoint channels for full context of user activity.

Host-based user activity monitoring

Through its easy-to-use Policy Workbench, EverShield supports a risk-managed approach and provides analysts with the ability to succinctly define policy-based criteria, determining which behaviors to monitor and what information to collect. EverShield UAM also enables analysts to minimize or block the collection of sensitive information such as PII, user passwords, or privileged communications.

Organizations require a UAM solution to align with requirements and policies published by the National Insider Threat Task Force (NITTF) that demand a capability that can observe and record the actions of human behaviors on computer workstations. Traditional network defense tools are simply not designed to do this.

Full-context event replay

EverShield delivers a unique session playback capability that provides the contextual insight needed to discern malicious from benign activity in a manner that can be easily understood by non-technical personnel.

The playback capability offers unambiguous and irrefutable attribution of all computer end-user activity and provides context to the user’s behavior both before and after a specific event.

Strong management controls

Originally designed to support the unique requirements of the counterintelligence community and the sensitivity of their mission. EverShield UAM provides features to ensure separation of critical or sensitive duties with role-based access and operations, two-factor authentication using hard and soft tokens, and two-person authorization for sensitive functions such as modifying user monitoring policies or exporting activity records.

In addition, EverShield immutable audit logs provide a “watch the watcher” feature to support the independent oversight of the operator’s activities within the tool, ensuring that monitoring programs are conducted in accordance with your organization’s legal and privacy requirements.

Comprehensive coverage with high stability and low impact to networks

EverShield UAM facilitates host-based monitoring for a range of user interactions with computer endpoints. This includes all keystroke activity, communication channels, application usage, processes, and use of removable media and peripheral devices. Everfox accomplishes all these tasks without adversely affecting mission, network, or system performance.

The highly stable agent has been designed to minimize adverse impact to workstation bandwidth usage and storage. Configurable throttling mechanisms regulate CPU utilization and the transfer of collected data. EverShield agents are also able to collect data in a persistent manner, even when workstations are disconnected from the network.

Scalability

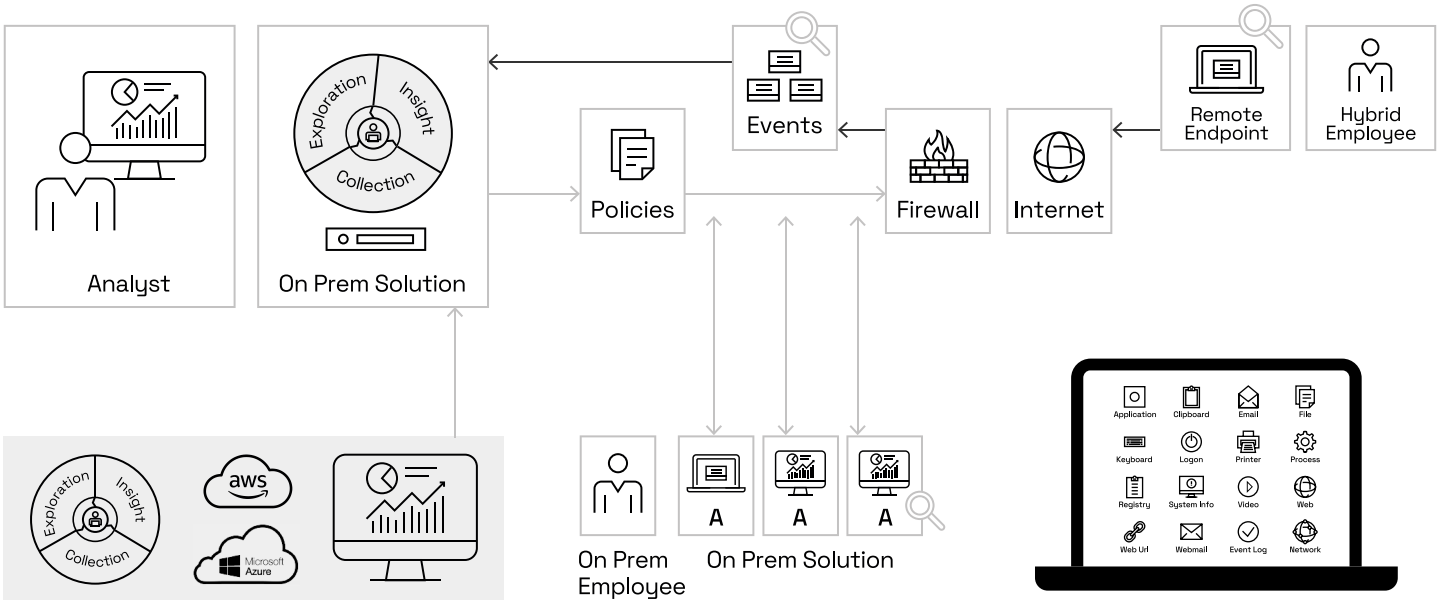
EverShield UAM is a fully scalable, enterprise-wide solution that has been deployed to hundreds of thousands of endpoints across government, critical infrastructure, retail, healthcare, and other major organizations. Everfox cluster-based architecture enables server nodes to be added as needed, to scale the system from small network environments to large enterprise networks spanning multiple security domains.

Security

Out-of-the-box, EverShield meets all risk management framework requirements and our customers have obtained Authority to Operate (ATO) on networks across global commercial and government enterprises.

Everfox employs validated NIST FIPS 140-2 encryption modules for cryptographic functions, including storage of data on agents, agent-to-server communication, server-to-server communication, and storage of data in the centralized database. EverShield UAM is a widely deployed and trusted solution operating in some of the most sensitive and complex environments.

Collect



Cloud
Hosted options for private or public cloud

Robust endpoint sensor for policy driven data collection

Collect & Explore
Visualize, explore and investigate

About EverShield Insider Risk Management Platform

User Activity Monitoring • Behavioral Analytics • Case Management

Beyond detection: Comprehensive insider threat protection

Built by analysts for analysts, Everfox EverShield is trusted by Fortune 500 companies and 100+ government entities around the world to detect, prevent, and manage insider threats at scale.

As a design partner with the U.S. Government for 20 years, we have developed more nuanced and advanced methods of identifying indicators of impending insider threat activity. We also provide a streamlined version of this platform for commercial enterprises.

Everfox EverShield can help you establish a mature Insider Risk Management (IRM) program. Combine deep user activity monitoring, data-source agnostic behavior analytics, advanced linguistic analysis, and case management to improve your ability to prevent insider threat events.

User activity monitoring

EverView utilizes a lightweight, policy-driven endpoint agent that collects behavioral telemetry from over 15 monitored channels, including file access, web activity, email, chat, keyboard usage, and application behavior. It is always on, even when a device is offline. However, the way data is collected allows you to preserve risk relevant evidence longer with less storage burden.

Behavioral analytics & linguistic analysis

EverInsight is an AI/ML-driven analytics engine for behavioral baselining, anomaly detection, and psycholinguistic analysis. It supports more than 100 models, including indicators of isgruntlement, data staging, lateral movement, and hostile communications. More nuanced linguistic analysis, 100+ models and a unique hybrid analysis approach improve your ability to get ahead of threats.

Case management

EverCase is a secure, centralized case management system designed for classified or sensitive environments. It supports collaborative investigations with built-in privacy enforcement, chain-of-custody tracking, and role-based access.

About Everfox

Everfox, formerly Forcepoint Federal, has been a trailblazer in defense-grade cybersecurity for more than two decades. Leading the way in delivering innovative, high-assurance solutions. But we're just getting started.