Forcepoint

Datasheet

User Activity Monitoring

Deep visibility of user activity

Key Benefits

- Collect behavioral data from multiple endpoint channels for full context of user activity
- Transparent to the end-user, preserving the user experience
- Robust endpoint sensor for out-of-the-box and configurable policy-driven data collection
- DVR-like "playback" feature provides full context of user actions to easily discern malicious from benign intent
- Privacy protection features, including "do not collect" policies
- Proven authentic, relevant, and original records for use in legal proceedings
- Enterprise ready for centralized management and monitoring with a scalable architecture for expanding network environments and support for multiple security domains
- Supported by a team of expert engineers and subject matter experts

Forcepoint User Activity Monitoring (UAM) is an insider risk management solution specifically designed to support the needs of security and investigative professionals:

- Collect behavioral data from channels such as web, file operations, keyboards, and email.
- Explore meaningful data using a powerful dashboard built for analysts, by analysts.

Host-based User Activity Monitoring

Forcepoint User Activity Monitoring provides analysts and investigators with deep visibility by collecting behavioral data from multiple endpoint channels for full context of user activity. Through its easy-to-use Policy Workbench, Forcepoint UAM 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. Forcepoint UAM also enables analysts to minimize or block the collection of sensitive information such as PII, user passwords, or privileged communications.

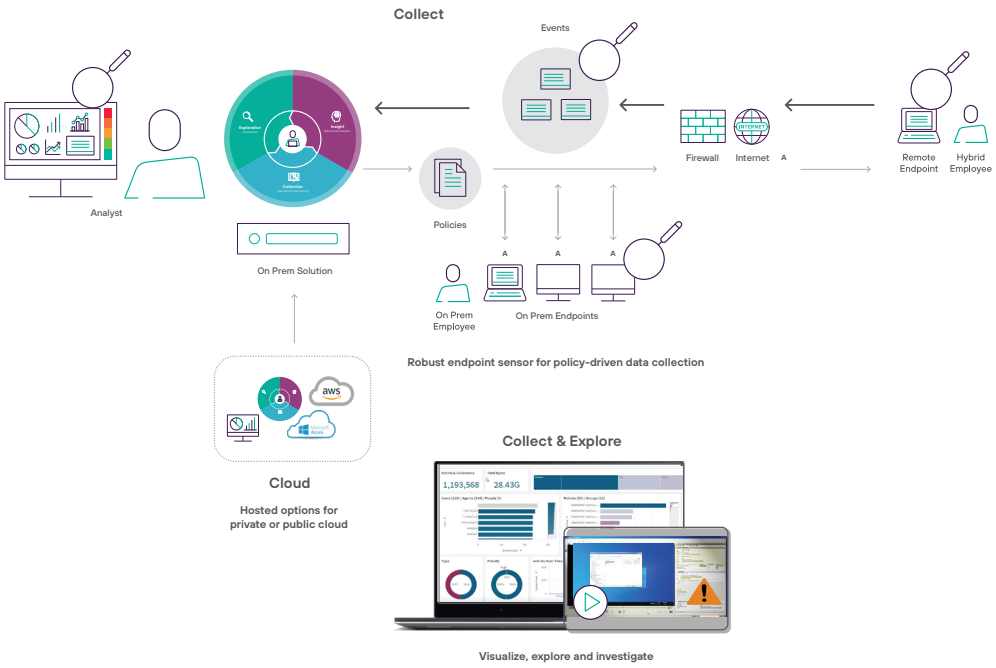
Organizations require a UAM solution to align with requirements and policies published by the National Insider Threat Task Force (NITTF) that demand a capability that can observe and record the actions of human behaviors on computer workstations. Traditional network defense tools are simply not designed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

Full-context event replay

Forcepoint UAM delivers a unique "video 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

Forcepoint UAM was originally designed to support the unique requirements of the counterintelligence community and the sensitivity of their mission. The tool 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, Forcepoint UAM 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

Forcepoint 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. Forcepoint UAM 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. Forcepoint UAM agents are also able to collect data in a persistent manner, even when workstations are disconnected from the network.

Scalability

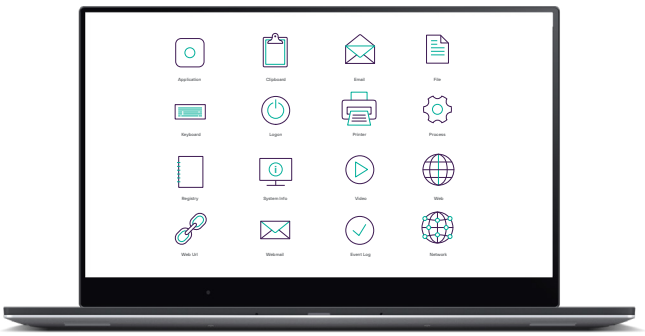
Forcepoint UAM is a fully scalable, enterprise-wide solution that has been deployed to hundreds of thousands of endpoints in across government, critical infrastructure, retail, healthcare, and other major organizations. Forcepoint UAM's cluster-based architecture enables server nodes to be added as needed,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

Security

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

Forcepoint UAM 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. Forcepoint UAM is a widely deployed and trusted solution operating in some of the most sensitive and complex environments.

Collections Channels



Forcepoint

forcepoint.com/contact

[FP-UAM-Datasheet-US-EN] 7Feb2023