Tausight® Situational PHI Awareness

Reducing Risk in the Information Sharing Age

PHI Accountability, inside and outside of your organization

Distributed care, remote working, telehealth, and the drive towards nation-wide sharing of electronic health information are expanding the attack surface at a rapid pace. Traditional models of layering on solutions designed to lock data inside the firewall are insufficient and outdated.

The 21st Century Cures Act is driving the sharing of structured and unstructured data between providers, patients, organizations and applications. This will decrease costs, improve efficiency and improve the quality of care, but will also greatly expand the attack surface and increase risk. To help mitigate risk, the U.S. Department of Health and Human Services (HHS) established the 405(d) Health Industry Cybersecurity Practices (HICP) Guide, which aligns with the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF) and identifies ten practices that are tailored to small, medium, and large organizations.

Tausight's fully automated, ML-native situational awareness platform was built by healthcare experts specifically for healthcare's information sharing age. Our SaaS-based platform provides real-time visibility into structured and unstructured PHI and activity across all endpoints and servers in your healthcare ecosystem. All PHI access, movement, and security status are readily available in self-service dashboards and customizable reports that indicate whether data are secured and defended in accordance with 405(d) HICP. Healthcare providers benefit from:

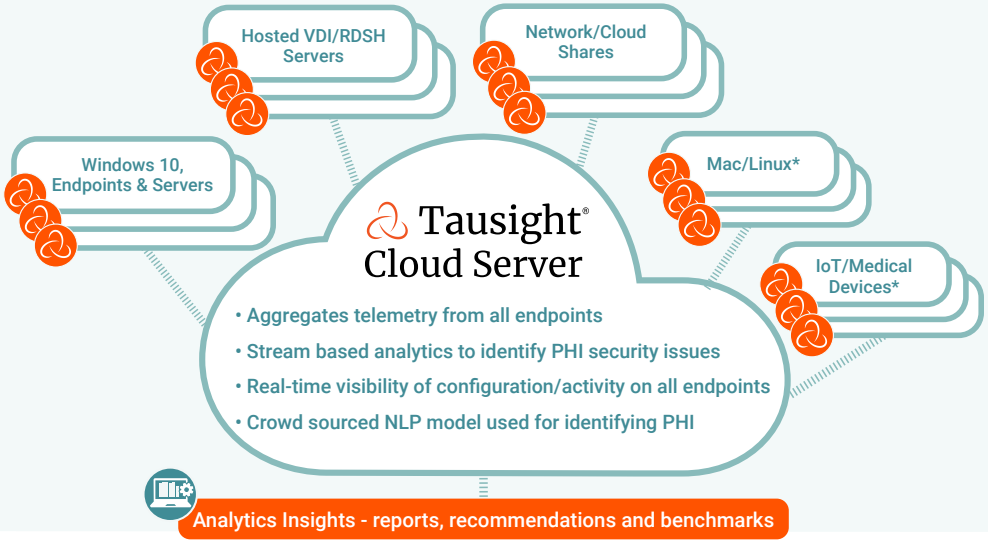
- Stronger PHI protection
- Improved patient safety
- Reduced workload for IT Security teams
- Compliance with regulations
- Faster recovery and lower potential fines
- Cybersecurity insurance rates

Benefits of the platform

- **Reduced PHI risk across the healthcare continuum** — One consolidated, real-time view into structured and unstructured PHI as it is being created, copied, stored, moved and shared between providers, patients, third parties and applications.
- **Continuous, omnipresent validation of cyber preparedness and compliance** — 24/7 telemetry and reporting on PHI activity, including adherence to 405(d) Health Industry Cybersecurity Practices (HICP) to support qualifying for lower cybersecurity insurance rates and reduced OCR penalties in the event of a breach.
- **Faster, less costly time to cyber recovery** – Immutable, off-site audit trail provides forensic-level details across all endpoints; before, during and after a cyber incident, including the information needed to quickly reconstitute the system and reconstruct any incident.

Real-time Situational Awareness

Designed on a modern cloud-based infrastructure and provided as a SaaS service, Tausight is the first PHI protection model developed using leading-edge IoT and NLP/ML technologies. The system provides 24x7 telemetry on the creation, access, storage, movement, replication, and endpoint security status of all PHI, and automatically produces actionable reports. Tausight's patented sensor detects, tracks, and analyzes PHI activity and risk in your data center and on any endpoint devices in the care continuum, in real-time, in any workflow in today's decentralized care delivery ecosystem. No custom rules to be written. No specialized skills required. Zero touch maintenance.



- SaaS service, self-updating sensor for Windows & VDI endpoints either inside/ outside the firewall
- Real-time, full-stack ground truth telemetry for system, user, application, device, network, hardware, activity
- Content inspection detects PHI at rest (files), in use (apps) and in transit (network, cloud)
- Natural language processing identifies PHI in structured and unstructured PHI without pattern matching complexity
- Forensic audit trail for all activity events back to user accounts

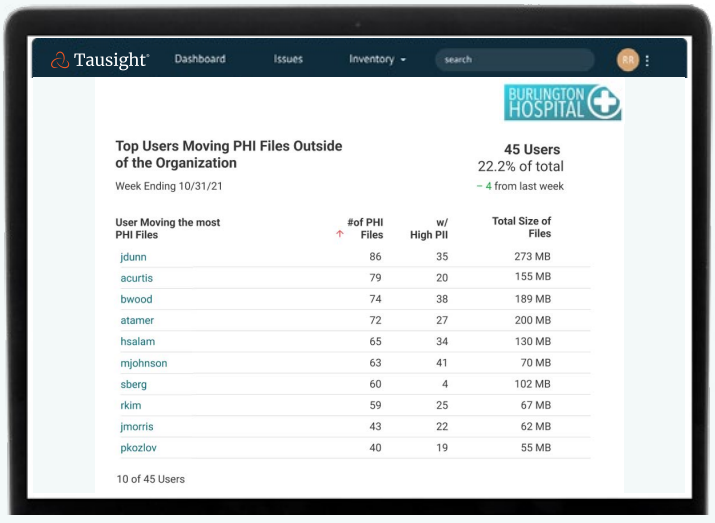
Tausight Patented Sensors * Future offerings

Tausight's Situational Awareness Platform provides:

- The ability to detect the presence of PHI, both at rest and in transit, allowing real-time visibility into data as it is being created, copied, accessed, stored, and moved.
- Context around how PHI is used; including applications involved, email destinations, and endpoint configurations, monitoring resources and streamlined audit and compliance.
- Insights into applications; application usage, which can expose misuse and underuse, potentially reducing license costs; and patching levels, identifying risk.
- Insights into user behavior including shared workstation usage, application usage, and interaction with PHI at rest and in transit, which can reveal risky or malicious actions.
- User configurable alerts for information on what is happening in your environment to signal inappropriate activity as it occurs, minimizing damage, recovery time and fines. Alerts can be real-time, asynchronous, email or text.
- Generated ServiceNow tickets to manage action items.

Technical Overview – Tausight consists of four major components:

1. The Tausight Service is a smart telemetry hardened sensor that is deployed on endpoints. As the heart of the overall platform, this sensor uses two separate machine learning-driven engines that actively learn, sense, and monitor vulnerabilities across the entire IT system to detect and classify PHI on a continuous, real-time basis. Once deployed, the sensor is invisible and self-updating. There is no need for system downtime or reboots.
2. The Tausight Server, a private, cloud-based server, leverages the Google Cloud Platform (GCP) and serves as the brain of Tausight. It utilizes Google Cloud Analytics and Tausight's proprietary, ML-driven Risk Prioritization engine that creates and prioritizes risk and threat scenarios from the raw telemetry vulnerability metadata generated by the Tausight Sensor.
3. The Tausight Telemetry Transport Framework is an IoT-based transport system that collects and delivers raw IT system vulnerability data to the Tausight Service and Server with minimal effect on CPU usage, bandwidth, and connectivity.
4. The Tausight Administrator/User Interface has been designed to instantly categorize and display all the critical telemetry data in simple and easy-to-view tile dashboards. Easy drill downs allow IT Security staff to mine specific details, while customized alerts and reports provide the option of real-time visibility for IT Security, Compliance, executives, or boards.



The Tausight UI provides dashboard views into a healthcare organization's PHI Landscape as well as an inventory of devices, users, and applications.

With Tausight, IT Security, Privacy and Compliance teams can easily produce real-time reports on their organization's status in many areas, including: Data Protection and Loss Prevention, End Point Protection, Incident Response Preparedness, IT Asset Management, Identity/Access Management, Vulnerability Management and more. An example is this view of Top Users Moving PHI files outside of the Organization. Reporting to the board, auditors, OCR or cyber insurers on alignment with 405(d) or other best practices is as simple as grabbing a screen shot.

Tausight's Situational PHI Awareness Platform is the tool that IT Security, Privacy and Compliance teams need to protect PHI and ensure compliance in the information sharing age.

For more information or to find out where all your PHI is, visit www.tausight.com.