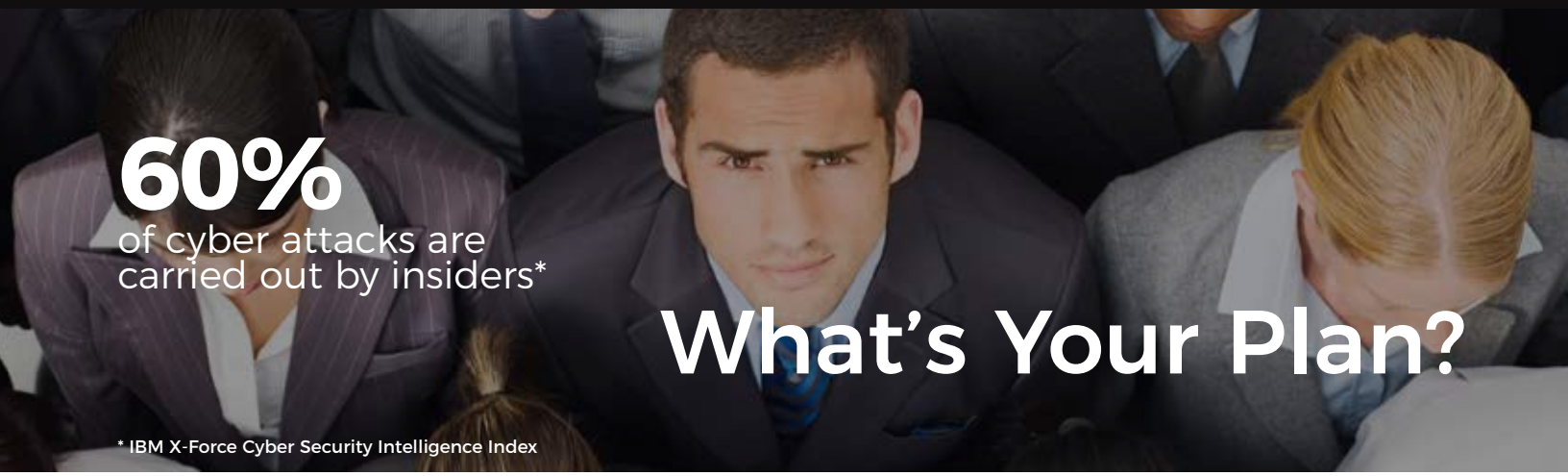
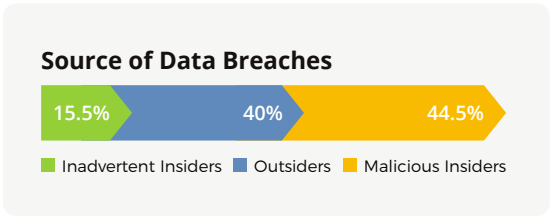


Security's Achilles' Heel

Insider security has become the Achilles' heel of most corporate security strategies. Many rely primarily on access management, network data (SIEM) or locking down documents (DLP). The volume of breaches shows that this is simply an incomplete security strategy when protecting a corporation's critical data. The impact of losing patient data, private customer data (PII) or Intellectual Property (IP) can be devastating for a corporation.



Cerebral
INSIDER THREAT INTELLIGENCE PLATFORM

Integrated & Intelligent

Cerebral is an AI powered security platform that integrates User & Entity Behavior Analytics (UEBA) with User Activity Monitoring (UAM) and Data Breach Response (DBR).

The Need for Speed

When a breach occurs, the ability to immediately recognize it, pin point who is involved and lock it down is crucial. Unlike standalone monitoring or analytics tools, Cerebral's integrated and intelligent capabilities provide an end-to-end security solution that immediately identifies a threat coming from anyone in a network, lets security rapidly take action with 100% confidence and provides the evidence essential to taking legal action.

A Holistic Strategy

Because you never know where an attack will come from, it's critical that every endpoint is protected from both external and internal attacks. Best practice dictates an in-depth defense strategy against external threats (antimalware, firewalls, etc.) and internal threats (behavioral analytics and direct visibility).

Internal threats can be malicious or accidental and can come from employees, former employees, contractors, business partners as well as an external attacker who's posing as an insider (stolen credentials).

51%

of CISOs say insider threats are the greatest security threat they are facing.

Cyberark Global Advanced Threat Landscape Report 2018

"Advanced forensic data analytics is becoming an indispensable tool to detect Insider Threats."

Ernst & Young Managing Insider Threats, a holistic approach to dealing with risk from within

71%

of U.S. Workers are so unhappy at work they are looking for a new job.

Mental Health America 2017 Survey

Predictive Analytics powered by Veriato AI

Endpoint Monitoring and User Behavior Analytics

Veriato AI continually monitors every endpoint and builds a digital fingerprint for each user and group. When there are anomalies, pattern variations or significant variations from the established baselines, an alert is triggered so that the investigation and remediation can begin immediately, often before real damage is done.

Veriato AI

To create the dynamic digital fingerprint for all users on a network, Veriato AI analyzes;

- File & document activity
- Web & Dark Web activity
- Network usage
- Chats & IMs
- Emails activity
- Program usage
- Geolocation
- Imposter indicators
- and more...

Psycholinguistics

Veriato's proprietary AI algorithm detects disgruntled users by monitoring their sentiment for possible threats.

1 WATCHING

Cerebral continually watches the behavior of all users on the network. Cerebral protects physical and virtualized environments and can be deployed on Windows workstations and servers, Macs and Android devices.

2 ANALYZING

Veriato AI continually analyzes all user behavior for signs of threat, including indications of stolen credentials.

3 ALERTING

As soon as a threat is detected, Cerebral alerts the security team. Additionally, integrated alerting minimizes the security team's workload.

4 SEEING

Cerebral's Time-Capsule DVR gives you an immediate video playback of the user's on-screen actions. This allows you to quickly see the nature of the threat.

5 REACTING

Video playback lets you react immediately and with 100% confidence, notifying building security and management while you isolate the endpoint from the network. Additionally Cerebral's video evidence is crucial for legal action.

Eyes On Glass

Watch video playback of a user's on-screen actions from 5 minutes ago or 5 days ago. These videos can be exported as JPG or AVI files and used as legal evidence.

The Impact of Veriato

The ability to predict and react with speed and confidence is at the core of a mature, internal threat detection and data protection strategy.

Speed of Discovery is critical in minimizing damage. Without AI to rapidly detect anomalies (e.g. imposters in the network or unusual user activities), vast amounts of data can be siphoned over weeks or months. Veriato uses the most advanced AI algorithms to analyze and predict risk from the vast amounts of endpoint data that's continually collected. However, discovery alone is not enough.

Speed of Remediation is governed by your ability to determine exactly what's happening. Veriato gives you an immediate view into the actual on-screen actions so that you can rapidly determine if the alert is signaling a security breach or just an uncommon, but harmless, business activity.

This direct visibility allows you to take action rapidly and with 100% confidence by providing the visual evidence crucial for remediation as well as criminal and legal action.