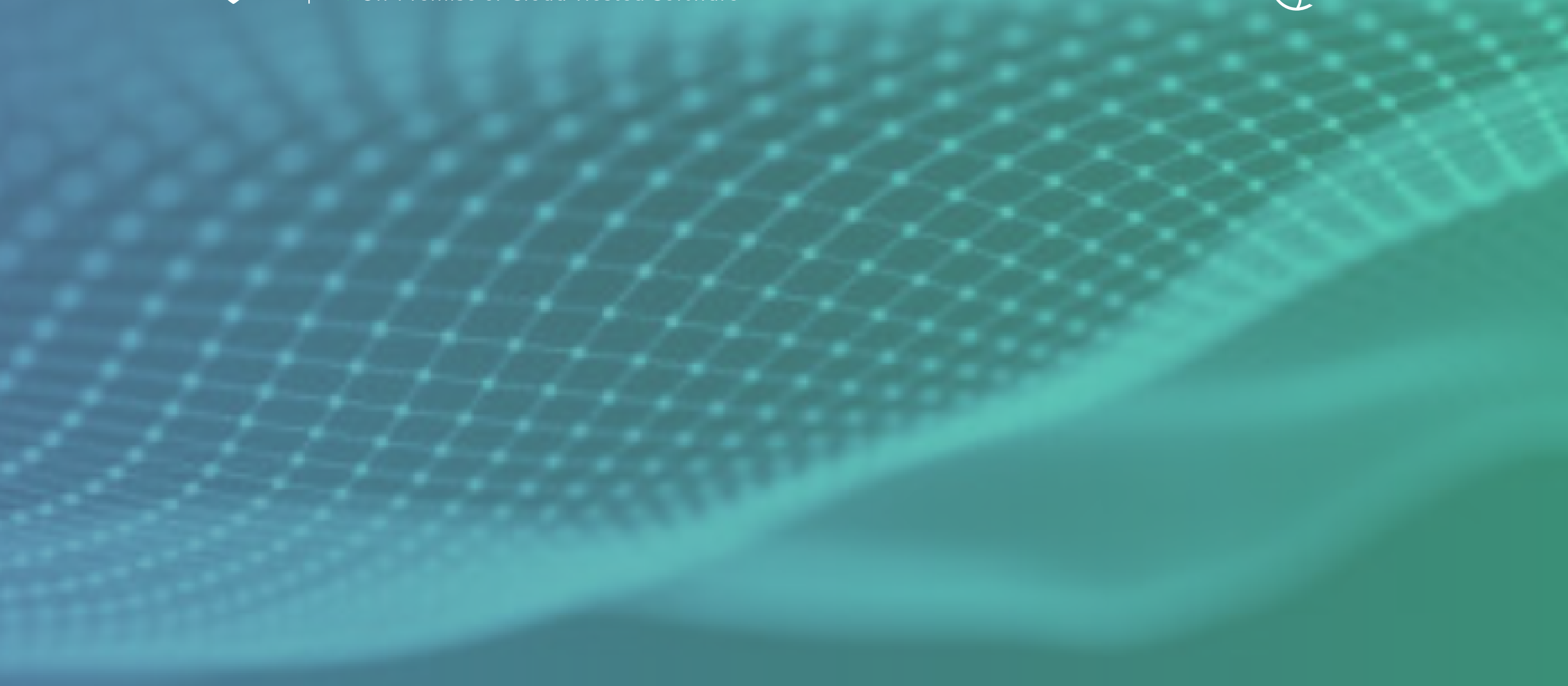
- Detect Disrupt Disarm Defeat
- Preemptive Fraud Loss Prevention
- On-Premise or Cloud-Hosted Software



CT6.® Fraud Preventer

Stop Fraud. Restore Confidence.

Cybercrime Prevention software to defeat cyber-enabled fraud and theft.

Protect your customers, remote workforce, and supply chain.

CT6.® Fraud Preventer Technology

CT6.® Fraud Preventer technology (U.S. patent pending) delivers the next generation of fraud loss prevention. Rooted in the experience of federal investigators of organized cybercrime and adversarial nation-state actors, CT6.® Fraud Preventer creates end-to-end preemptive on-premise or cloud-hosted software solutions powerful enough to alter the risk calculus of adversaries and elevate the enterprise anti-fraud ecosystem.

- **Detect** Detect threats using Fraud Incident Event Management (FEIM)® criminal behavioral analytics-based detection to hunt and identify targeted data from premier all-threat intelligence sources.
- **Disrupt** Disrupt nefarious networks or nation state actors through Indicators of Financial Compromise (IoFC)® Matching Logic that connects dissimilar dots across multiple internal and external data sets across disparate platforms.
- **Disarm** Disarm cybercriminals and nation state actors through proactive data matches to preemptively mitigate events before a criminal event occurs.
- **Defeat** Defeat cybercriminals by rendering stolen or compromised data useless or continue to monitor activity for future engagement undetected.

How it Works

1. **Within 30 days:** CT6.® customized Readiness Evaluation will establish an integration plan focused on four areas: Cyber Threat Intelligence Collection, Fraud Analytics, Fraud Prevention, and Compliance & Investigations..

2. **The next 30-60 days:** Customized integration and implementation completed. Fraud Preventer is an on-premise or cloud-hosted software. CT6.® trains your experts to maximize Fraud Preventer outputs.

3. **Immediately after:** Fraud Preventer is up and running in-house by your team of experts. CT6.® remains available to assist for any follow-on needs.

Preemptive:

Discover compromised customers before the criminal fraud or theft event occurs.

Automated Delivery:

Results delivered without human interaction.

Private:

U.S. DOJ & E.U. GDPR privacy law compliant.

Secure:

No PII is exported from your network.

Invisible:

Frictionless with no added burdens or processes to slow users or networks.

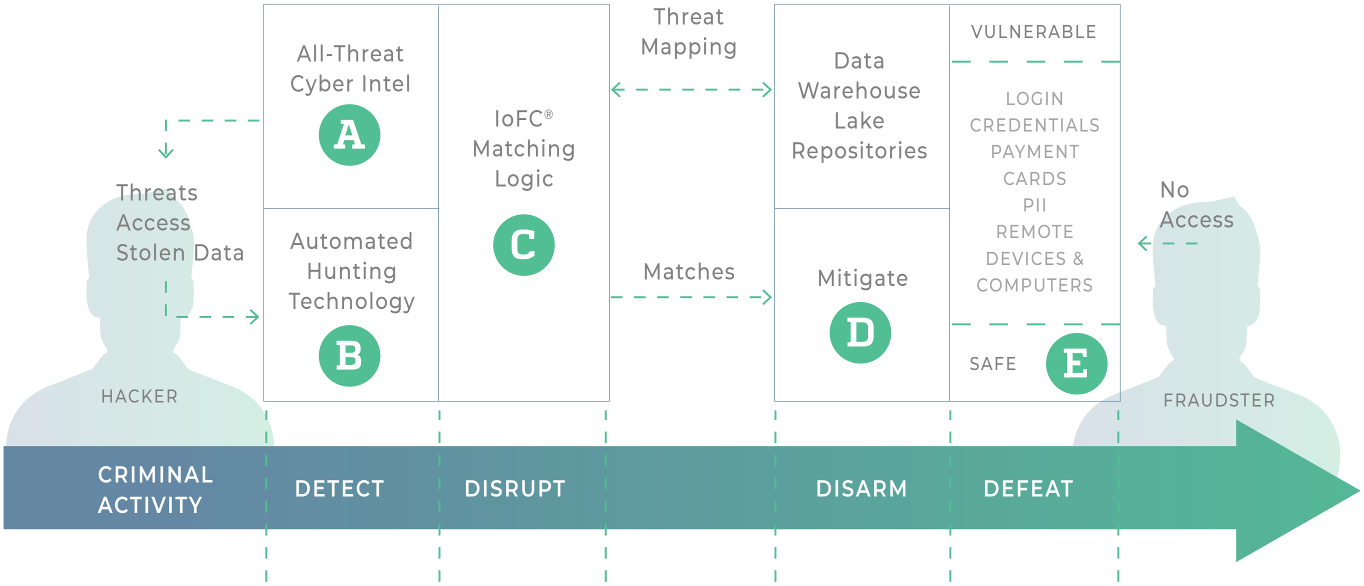
Ethical:

Criminals do not profit in stolen data acquisitions and Fraud Preventer users do not traffic stolen data. U.S. DOJ Compliant.

Flexible:

Scalable, available as an on-premise software or cloud-hosted solution.

CT6.® Fraud Preventer



Fraud Preventer defeats the hacker-criminal engagement by preventing the criminal from utilizing compromised data before fraud or theft occurs.

A

Privacy and Search Accuracy tool

The proprietary process of creating a partial hash or partial-partial hash (digital fingerprint) of data to erase identifiers while improving data matching capabilities. (U.S. Pat. Pend.)

B

Wide Aperture Data Hunting

A proprietary software-based capability that identifies customer, employee, and vendor points of compromise, independent of a connection to an organization, among 23+ billion of pieces of data. Data types include digital device identifiers, payment cards, login credentials, financial transaction data, and all PII. (U.S. Pat. Pend.)

C

IoFC® Matching Logic

A proprietary methodology used to uncover and map hidden connections between disparate and remote data points to expose customer, remote workers, and vendor/supplier risks. IoFC (Indicators of Financial Compromise)® is trademarked as a new way of discovering cybercrime risk. (U.S. Pat. Pend.)

D

IoFC® Cybercrime Risk Signaling

The product of IoFC® Matching Logic, this proprietary software-based capability produces the early warning cybercrime risk indicator that CT6.® users receive to manage and mitigate risk days, weeks, or months before the criminal can commit fraud, theft or sabotage. (U.S. Pat. Pend.)

E

Criminal Behavioral Analytics

The process that exposes exactly how the criminal business cycle converts data and access into fraud, theft, and sabotage against a business/organization.

CT6.® Fraud Preventer Technology

CT6.® Fraud Preventer can be customized with assistive technologies to fit any corporate enterprise, organization, or government entity. CT6.® assistive technologies enable an optimum Fraud Preventer experienced based on the requirements of any environment.

◆ Business Intelligence

CT6.® Business Intelligence visualization tool transforms structured data into natural language descriptions to provide context and explanations of Indicators of Financial Compromise (IoFC).

- Provides analysts, investigators, managers, and executives with enhanced analyses under near real-time threat conditions.
- Tracks the performance of cyber threat intelligence providers, monitor specific cyber threats, screen content on dark Internet marketplaces, and track criminal activity.
- Embeds into any platform such as Microsoft Power BI, Tableau, or Qlik View. Employs Arria (www.arria.com) Natural Language Generation to enable fully automated production of plain language reporting.

Graph Link-Analysis

CT6.® Graph Link-Analysis provides powerful point and click deep-link analysis on common data attributes (e.g., phone numbers, IPs, device IDs, financial transaction information, etc.).

- Graphs hidden links between points of compromise, threat actors, money mules, and other criminals.
- Employs Kaseware (www.kaseware.com) for extreme configurability with limitless applications using current business structures.

◆ Case Management

Fraud Preventer adapts to case management programs (e.g., Kaseware) to allow organizations to form efficient teams of information security specialists, fraud analysts, and investigators. Fights cybercrime through a single pane of glass.

◆ Artificial Intelligence

Calibrate and hone fraud prevention AI programs with Fraud Preventer to reveal the ground truth of actual cyber-criminal access into remote workers, customers, or vendors. Significantly improve the predictive ability of existing AI models. Empower supervised machine learning algorithms to build highly tuned, threat and actor-specific fraud prevention strategies.

◆ Real-Time Prevention

Fraud Preventer highly predictive signals improve real-time prevention programs to better identify risk. Improve fraud prediction for identified customers, employees, and vendors/suppliers. Create highly focused and predictive threat and actor specific risk rules.

◆ Compliance

Fraud Preventer can connect cyber to other required risk management programs (e.g., money laundering, terrorist financing, supply chain & insider threat), and export specific data to government mandated reporting [e.g., Suspicious Activity Reports (SARs)].