IMPERVA®

Imperva CounterBreach

DATASHEET

Protect Your Data from Insider Threats

The greatest threat to enterprise security is the people already on the payroll. To do their jobs, employees, contractors, consultants and vendors must have legitimate access to sensitive and valuable data stored in enterprise databases and file shares. However, when insiders abuse this access, or when insiders are exploited by outside attackers, enterprise data is exposed. Detection and containment of insider threats requires an expert understanding of both users and how they use enterprise data.

Employees require access to information assets to perform their jobs, but malicious or ignorant abuse of authorized access is difficult to detect and high-risk.

GARTNER, BEST PRACTICES FOR MANAGING 'INSIDER' SECURITY THREATS, ANDREW WALLS, 17 JUNE, 2014

Imperva CounterBreach

Imperva CounterBreach protects enterprise data stored in enterprise databases and file shares from the theft and loss caused by compromised, careless or malicious users. By dynamically learning users' normal data access patterns and then identifying inappropriate or abusive access activity, CounterBreach proactively alerts IT teams to dangerous behavior.

Information security strategies need to shift from a bottom-up device and network-centric strategy to a top-down, information-centric strategy focused on the information itself.

GARTNER, PREVENTION IS FUTILE IN 2020: PROTECT INFORMATION VIA PERVASIVE MONITORING AND COLLECTIVE INTELLIGENCE, NEIL MACDONALD, 27 JANUARY, 2016

Detect Dangerous User Data Access

CounterBreach detects potential breaches by pinpointing risky data access events and the user associated with the risky access event.

CounterBreach Behavior Analytics

CounterBreach Behavior Analytics uses machine learning and dynamic peer group analysis to automatically uncover anomalous data access events. This establishes a full contextual baseline of typical user access to database tables and files stored in file shares, and then detects and prioritizes anomalous activity. Combining an expert understanding of users and how they access data equips enterprises with the context and accuracy required to detect data breach incidents. With CounterBreach, security teams can quickly discern between malicious and normal activity so they can immediately identify and act upon risky behavior.

Accurately identifying potential data breaches requires deep contextual understanding of not just user activity, but the data users access and how they access it. Without visibility into the data itself, and an understanding of the indicators of data abuse, one half of the equation is missing. The table below shows examples of common data abuse indicators, and the user and data details needed to do identify them.

DATA ABUSE INDICATORS	LEARNED USER DETAILS	LEARNED DATA ACCESS DETAILS
Suspicious Application Data Access Flags interactive (non-application) users that directly accesses sensitive application table data on a database.	User identity Client IP Server IP Client app	Database name Table name Data sensitivity Schema SQL operation SQL operation type
Excessive Database Record Access Uncovers users that access an unusually high number of database records, as compared to their typical behavior and the actions of their peer group.	User identity User department	Database name Data sensitivity Table name Schema Number of rows involved in operation SQL operation
Service Account Abuse Detects an interactive (non-application) user logs into a database using a service account.	User identity Client IP Server IP Client app	Database name Database table access patterns SQL operation patterns SQL operation type
Slow Rate File Access Pinpoints users that access or copy a certain number of files at an unusually slow rate.	User identity User department	File operation File path File name Folder type File share name Operation response time
Excessive File Access Flags users that access or copy an abnormally high number of files from their personal folder, department folder or network file share from multiple hosts.	User identity User department	File operation File path File name File type File share name

CounterBreach spotlights the riskiest users, client hosts and servers so that security teams can prioritize the most serious incidents.

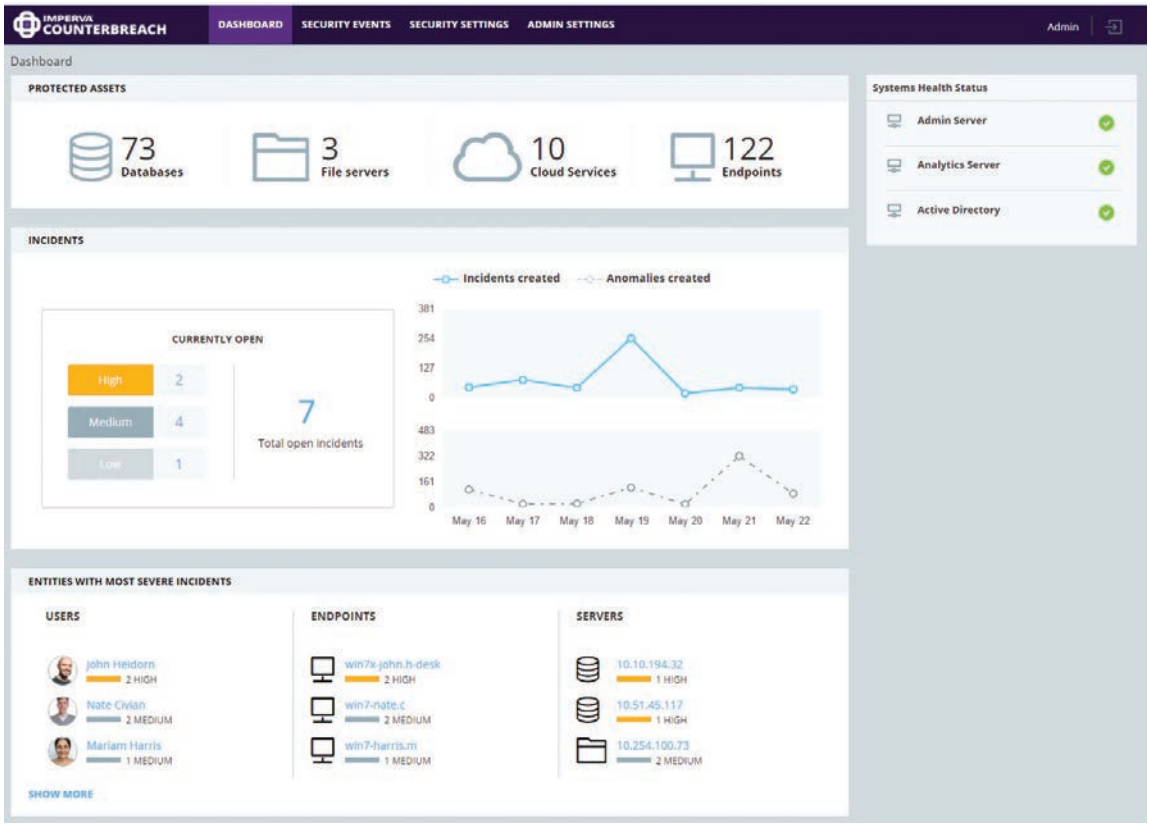
Key Capabilities

- Detect critical data misuse
- Accelerate incident response time
- Simplify investigations

CounterBreach Key Capabilities

Detect Critical Data Misuse

Incidents detected by Behavior Analytics are populated into an easy-to-navigate dashboard. CounterBreach spotlights the riskiest users, client hosts and servers so that IT staff can prioritize the most serious data access incidents. Security analysts can also drill down into a view of all open incidents and investigate all the details pertaining to an event.



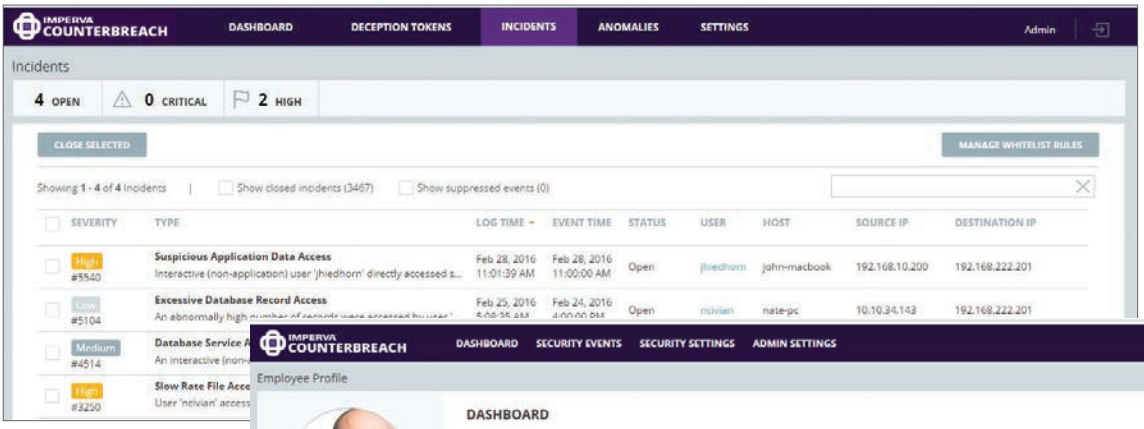
The CounterBreach dashboard aggregates threat indicators across all enterprise data.

Accelerate Incident Response Time

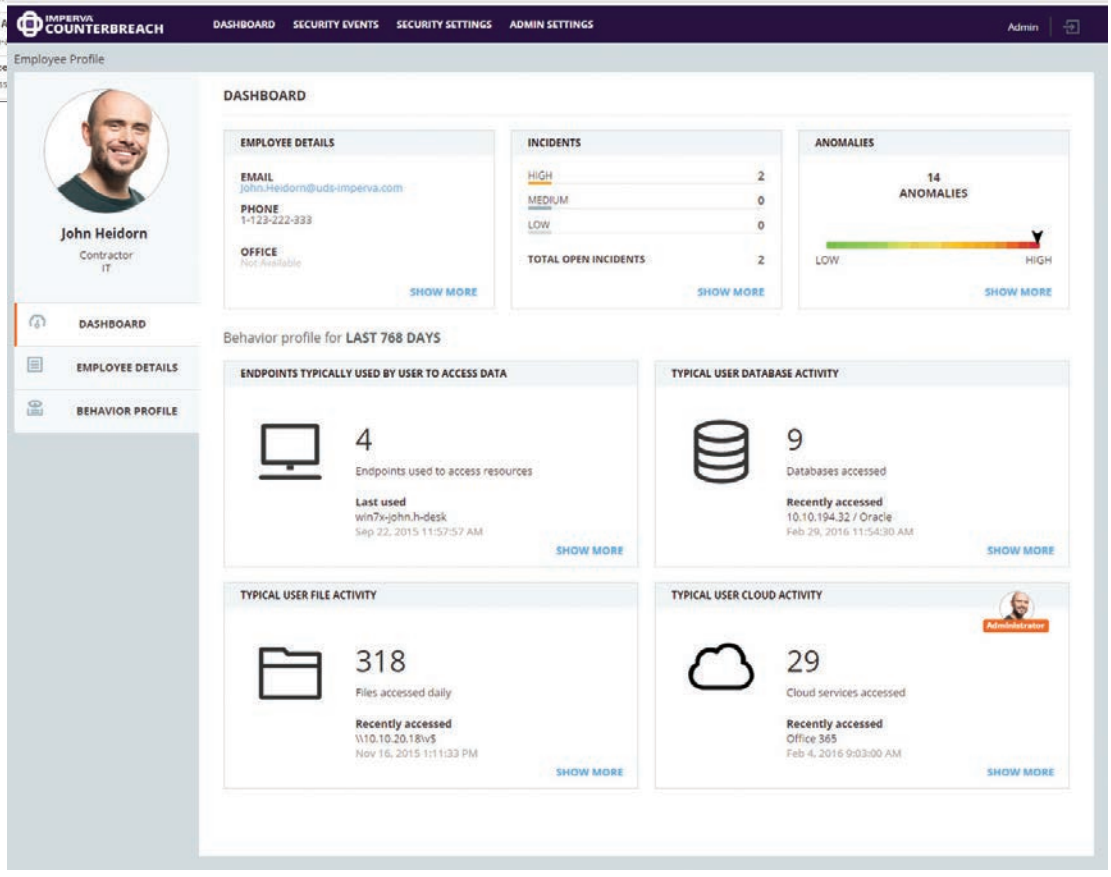
Security teams can efficiently investigate the most risky data access events by filtering open incidents by severity as well as by a specific user, server or client host. Users can then drill deeper into a specific incident to review a detailed description of the event and view granular information about the use and the data that was accessed. From here, SOC staff can close the incident or whitelist behavior that is authorized or unable to be remediated right away.

Simplify Investigations

Security teams can analyze the data access behavior of particular users with the user dashboard. With a consolidated view into database and file activity, security analysts have a full picture of the user's data access across the organization. Security teams can investigate incidents and anomalies specific to the individual, and then drill down to the behavior profile to the view baseline of typical user activity and compare a given user with that user's peer group.



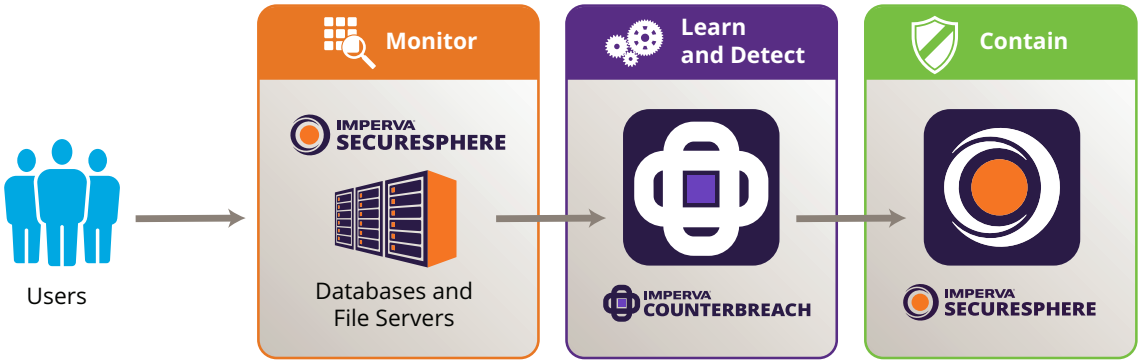
The CounterBreach incident screen shows critical data access anomalies prioritized from critical to low severity.



The CounterBreach user screen provides an at-a-glance look at individual access to enterprise data and highlights risky user behavior.

Prevent Data Breaches with Imperva

To detect and contain data breaches, organizations need to have visibility into who is accessing enterprise data, understand if that access is legitimate and respond immediately if it's not. CounterBreach integrates with Imperva SecureSphere solutions to pinpoint critical anomalies that indicate misuse of enterprise data stored in databases and file servers.



Monitor

Imperva data protection solutions directly monitor all user access to on-prem data repositories. SecureSphere provides visibility into which users access database and file servers, giving IT organizations insight into the 'who,' 'what' and 'when' of access to sensitive information.

Learn and Detect

CounterBreach combines Imperva expertise in monitoring and protecting data with advanced machine learning to uncover dangerous user data access activity. Based on granular inputs from SecureSphere, CounterBreach develops a behavioral baseline of typical user data access and then detects critical deviations from the norm. CounterBreach proactively flags these dangerous actions for immediate investigation.

CounterBreach integrates with Imperva SecureSphere to pinpoint critical anomalies that indicate misuse of enterprise data

Contain

With the CounterBreach solution, security teams can contain potential data leaks before they become major events. Once dangerous anomalies are detected, enterprises can quickly quarantine risky users in order to proactively prevent or contain data breaches.

Imperva CounterBreach Cyber Security

Imperva CounterBreach protects enterprise data stored in enterprise databases and file shares from the theft and loss caused by compromised, careless or malicious users. By dynamically learning users' normal data access patterns and then identifying inappropriate or abusive access activity, CounterBreach proactively alerts IT teams to dangerous behavior.

IMPERVA COUNTERBREACH

System Requirements

CounterBreach Prerequisites

CounterBreach requires one of the following Imperva products performing monitoring and containment functions: SecureSphere Database Activity Monitor, Database Firewall, and File Firewall.

CounterBreach Virtual Appliances

CounterBreach is deployed as virtual appliances that are simple to deploy and do not interfere with existing SecureSphere implementations. The minimum requirements per physical host and for each guest virtual appliance are shown below.

	PHYSICAL HOST		GUEST VIRTUAL APPLIANCE				
	Hypervisor	Processor	CPU	Memory	Disk Space	Operating System	File System
CounterBreach Admin Server[1]	Dual-core server Intel VTx or AMD-V	VMWare ESX/ESXi 4.x/5.x/6.x	2	4 GB	50 GB		
CounterBreach Analytics Server[2]			4	16 GB	1 TB		

[1] The Admin Server is required for Behavior Analytics. Imperva will deliver software on pre-configured virtual appliances with the specifications shown above.

Supported Platforms

COUNTERBREACH BEHAVIOR ANALYTICS	
Database Platforms	Oracle, Microsoft SQL Server, DB2 for LUW, Sybase ASE
File Systems	CIFS file storage systems, NAS devices
File Operating Systems	Microsoft Windows Server
SIEM Integration	Splunk, ArcSight
Supported Syslog Formats	CEF, LEEF, Raw