

# CipherTrust Security Intelligence



## Challenge: Gaining organization-wide visibility into threats to sensitive data

To avoid merely recognizing data security events, such as breaches, after they occur, IT managers require a simple way to identify and correlate all relevant data about potential security events, so they can mitigate threats quickly and in real time. Some of the most effective tools for this are Security Intelligence and Event Management (SIEM) solutions.

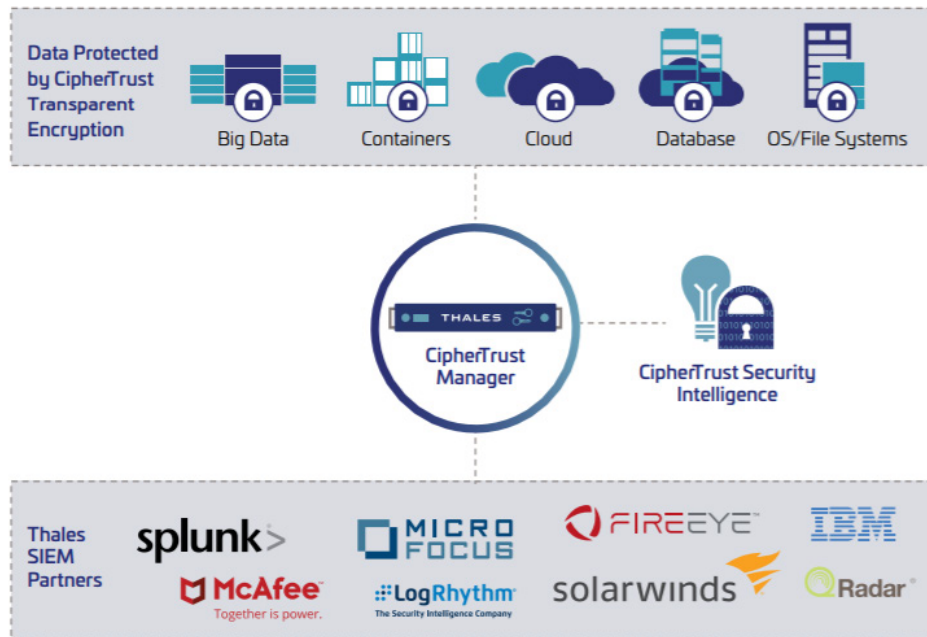
## Solution: CipherTrust Security Intelligence efficiently tracks and investigates suspicious activities across the organization

However, SIEM solutions can be blind to possible threats to your protected data without the detailed data provided by CipherTrust Transparent Encryption's Security Intelligence. CipherTrust Security Intelligence logs and reports streamline compliance reporting and speed up threat detection using leading Security Information and Event Management (SIEM) systems.

CipherTrust Security Intelligence is available for sale to the U.S. Federal Government exclusively through Thales Trusted Cyber Technologies.

## Benefits

- **Deliver granular, actionable security intelligence**  
Traditionally, SIEMs have relied on logs from firewalls, IPS, and NetFlow devices. Because this intelligence is captured at the network layer, these systems can generate massive volumes of data making it challenging for administrators to identify the events that matter. These systems also leave a commonly exploited blind spot: They don't provide any visibility into data access attempts and events occurring on servers. CipherTrust Security Intelligence eliminates this blind spot, delivering targeted, critical insights into file access activities. As a result, the solution helps eliminate the threat of an unauthorized or compromised user account gaining stealthy access to sensitive data. CipherTrust Security Intelligence logs produce an auditable trail of permitted and denied access attempts from users and processes. The solution's detailed logs can be reviewed to specify when users and processes accessed data, under which policies, and if access requests were allowed or denied.
- **Streamlining auditing and compliance.** With its detailed visibility and integration, CipherTrust Security Intelligence helps streamline the effort associated with audits and ongoing compliance reporting. To adhere to many compliance mandates and regulations, organizations must demonstrate that data protection is in place and operational. CipherTrust Security Intelligence can be used to prove to an auditor that encryption, key management, and access policies are working effectively.



- **Pre-built SIEM Integrations** Collected at the system level, CipherTrust Transparent Encryption logs report authorized and unauthorized access attempts to encrypted files and volumes, including user, process, and more. CipherTrust Security Intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and event management (SIEM) systems. Authorized user access data is available to create baselines for user data usage and can be integrated with other security data, such as user location and access points, for pinpoint threat identification.

## CipherTrust Data Security Platform

CipherTrust Security Intelligence is part of the CipherTrust Data Security Platform. The CipherTrust platform unifies data discovery, classification, data protection, and provides unprecedented granular access controls, all with centralized key management. This simplifies data security operations, accelerates time to compliance, secures cloud migrations, and reduces risk across your business. You can rely on Thales CipherTrust Data Security Platform to help you discover, protect and control your organization's sensitive data, wherever it resides.

## About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit [www.thalestct.com](http://www.thalestct.com)

## Features

CipherTrust Security Intelligence logs:

- Produce an auditable trail of permitted and denied access attempts from users and processes. These logs can be efficiently shared with your SIEM platform to help uncover anomalous process and user access patterns, which can prompt further investigation.
- Detect possible malware or malicious insiders making unauthorized access attempts.
- Pinpoint unusual patterns of user access to protected data that indicate malware (or a malicious internal user) could be stealing data.
- Monitor process access to protected data for anomalous patterns of use that could indicate a process has been co-opted by malware.
- Identify attacks on the CipherTrust Manager appliance from unauthorized users.