



# Raytheon Oakley Systems

## USE CASE — PROTECT AND MONITOR CUSTOMER DATA

### The Challenge

Financial services groups, insurance companies, and retailers, store thousands, if not millions, of records on confidential customer data. Usually, the majority of incidents that put the data at risk are inadvertent. This is often, the result of the workforce not understanding the risk or being unaware of the policy. But malicious data theft or even erroneous disclosures can result in brand damage, loss of customer confidence, fines, and legal liabilities. A [comprehensive solution](#) should cover all scenarios.

### Customer Data is at Risk

Nearly every large enterprise stores thousands, if not millions, of confidential customer data records. These records are handled daily by customer service representatives. Sometimes the representatives are outsourced employees. In some cases, these representatives are located in a different country.

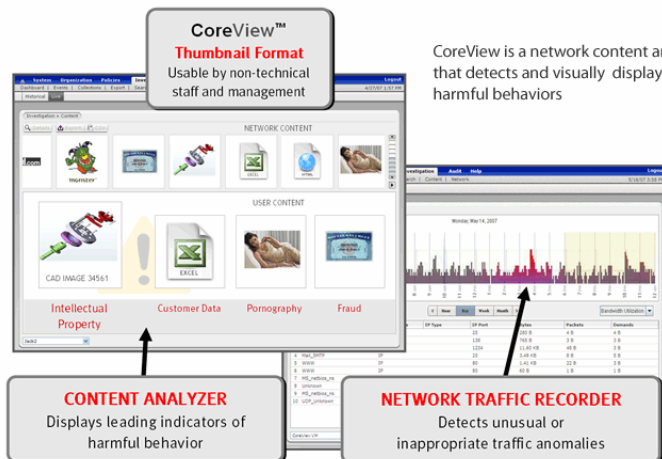
The greatest risk management challenge is that any one of these representatives could become a weak point in the organization's security if they are not aware of risks and don't follow risk management policy.

Unfortunately, it's also a fact that any one of the call center representatives could decide to make some extra money from selling a batch of credit card and Social Security numbers to a criminal third party.

### Oakley Monitors the Enterprise to Reduce Exposure of Customer Data

Oakley's [Monitoring and Investigation](#) solution can be deployed across the enterprise with general policies that help the organization proactively manage risk to customer data by watching for leading indicators of potential problems, such as a large volume of unmonitored USB drive copies, and also keep vigilant watch to detect when specific policies are being violated such as customer Personally Identifiable Information (PII) being sent through emails.

Ultimately, to effectively manage the risk, the organization wants to reinforce behavior that complies with policy and eliminate situations in which there are serious or recurring problems. Oakley's automated controls help risk managers do that by detecting and alerting them of leading indicators, detecting actual violations, and initiating automated remediation responses when specified.



## USE CASE

## PROTECT AND MONITOR CUSTOMER DATA

One extremely useful capability of Oakley's solution is the ability to prompt users in response to an actual or potential policy violation. The prompt will display as a message pop-up on the user's screen and can be used to educate the user about the risk he is taking, to educate the user on the organization's policy, and to allow the user to provide feedback. Sometimes user feedback will reveal a problem with a policy or a productivity impact of the policy of which management was not aware. So the prompting can have a two-way educational benefit.

For all employees who carry customer data on mobile laptops, the company can deploy a technology called [SureFind](#), which will tell you whether the data has been compromised in the event of a loss or theft, and will allow you to set a policy that will remotely destroy the data if you desire.

### Investigating Incidents

Over time, prompting can help an organization reduce accidental and erroneous disclosure or loss of customer data. But it is not always clear whether an incident is unintentional or deliberate. In these situations, it's generally prudent for risk managers to do further [investigation](#).

With Oakley's solution, any individual incident can be quickly investigated through its unique end-point replay capability, which allows an investigator or analyst to see the complete context in which the incident occurred as if he was there watching over the user's shoulder as it happened. In fact, the replay feature will capture activity up to 60 minutes before and after the actual violation occurred. The solution will also capture any data files or Input/Output streams involved in the incident so that it can be forensically reconstructed. With the context Oakley provides, the organization can fully understand the user intent so that the appropriate remediation can be taken, whether it's deploying a training program so the user better understands the consequences of the incident or documenting the actions so stronger action can be taken.

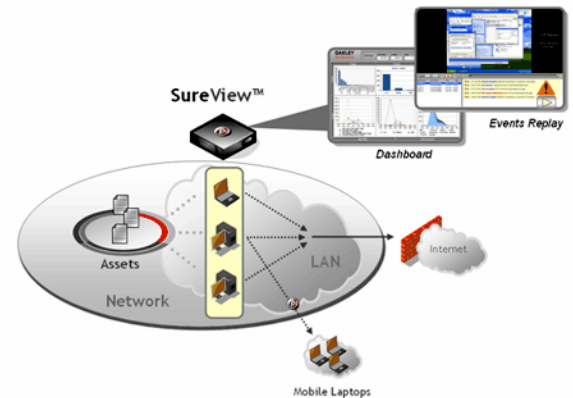
### Oakley Exposes Even the Most Sophisticated Customer Theft

One of the greatest fears in many organizations have are employees extracting customer records and selling the data. When this risk is high more stringent policies can be deployed to the call center employees. Policies can record whenever customer data is being "cut and pasted" between applications using

the clipboard, alert whenever instant messages are sent while the user has the customer database open, or enable additional monitoring if a user deliberately disables his network connection to hide his actions.

As an example, at one Oakley customer it became evident that a particular user was cutting and pasting data from the customer database, which was strictly against corporate policy. Further investigation revealed that the user was dropping the customer data into a Word document, saving the file under an ambiguous name, encrypting the file and saving it to a USB drive. It also revealed he notified his accomplice by instant message when the entire transaction was complete.

These obfuscation steps would easily bypass many data protection solutions since any one of the individual actions appears relatively harmless. But with Oakley's SureView technology, the administrator was able to deploy one of Oakley's hundreds of pre-built policies to monitor anytime customer data was copied from the database application; the policy was also customized to trigger if any data was copied to a USB drive. All user activity was then collected 30 minutes before and after the data was copied to the USB drive. Using Oakley's [SureView Replay](#), the administrator was able to view video-like replay of the entire incident, from the original data copy all the way through to the instant message.



### Additional Resources:

View an actual customer data theft incident capture and replay using Oakley:

[http:// www.raytheonOakleySystems.com /demo/CustomerData/CustomerDataDemo.html](http://www.raytheonOakleySystems.com/demo/CustomerData/CustomerDataDemo.html)  
 Additional Oakley Product Info: [http:// www.raytheonOakleySystems.com /products/Oakley Solutions Brief: http://www.raytheonOakleySystems.com /resources/index.php](http://www.raytheonOakleySystems.com /products/Oakley Solutions Brief: http://www.raytheonOakleySystems.com /resources/index.php)

Raytheon Oakley Systems, Inc.  
 2755 Cottonwood Pkwy., Ste. 600  
 Salt Lake City, UT 84121

T 1.800.662.9120  
 E [info@oakleynetworks.com](mailto:info@oakleynetworks.com)

[www.raytheonOakleySystems.com](http://www.raytheonOakleySystems.com)

**Raytheon**  
**Oakley Systems**