



## Case Study: American National Bank of DeKalb

American National Bank of DeKalb County's dedication is to provide a consistent level of quality customer service, administered by a strong management team, and supported by long term employee relationships and strong regulatory compliance. To match their goal to deliver first-class banking services to all individuals, families and businesses within the communities they serve, the company must aggressively and proactively protect and secure their customer data from a breach, identity theft or fraud.

"We conducted a lengthy search of several different security tools in the market place and realized there was no other tool that combined the features which the CTH Technologies' tool offers. The tool addresses our regulatory compliance issues, end point protection issues, web filtering and encryption requirements. We didn't know one tool would solve our problem. We definitely were impressed with the SecureCARE solution." stated Jeff Rolczynski, Sr. Vice President, American National Bank of DeKalb.

American National Bank uses CTH Technologies' Data Loss Prevention (DLP) solution, SecureCARE, to protect their sensitive customer data which includes: account information, credit card and Social Security numbers. "The ability of the SecureCARE tool to scan the body of the email and the attachment for sensitive data without impacting our user's productivity was very important to us in selecting the CTH solution. With this tool, we also prevented confidential information, including strategic planning, merger and acquisition, and financial data from accidental or malicious disclosure, while meeting compliance with state and federal regulations" added Rolczynski.

One of American National Bank's highest priorities was to protect their customers' confidential information. The company decided to proactively implement a DLP strategy that would protect internal IP and customer data. Understanding the increasing scrutiny the regulators are now taking when conducting IT Data Audits, American National Bank was determined to find a solution that combined content profiling with email encryption so they could ensure that sensitive data could not be sent out accidentally. During their research, American National Bank discovered that most data breaches today occur internally, caused by accidental disclosure of information within an email or weak end point protection. With a DLP solution like SecureCARE, American National Bank met all their requirements for protecting their sensitive content including auto-encrypting sensitive email, blocking USB drives and securing all of their end points.

"We realized that our encryption policy would be much more effective, if we had a tool that would automatically sense what information should be encrypted instead of relying on our employee's judgment to determine what to encrypt. Unlike the other vendors we looked at, the CTH DLP solution provided comprehensive protection for data at rest, motion and most importantly data in use" added Rolczynski.



CTH Technologies, Inc.



*"Unlike the other vendors we looked at, the CTH Technologies' DLP solution provided comprehensive protection for data at rest, data in motion and most importantly data in use."*

- Jeff Rolczynski  
Senior Vice President

*"Understanding user behavior at the desktop made securing the network that much easier."*

- Brian Truschke  
Vice President  
Information Technology

---

Today, American National Bank uses SecureCARE to mitigate the risk of a data breach, identity theft and fraud by preventing any accidental or malicious information leaks, securing all end points and monitoring employee activity. With these safe guards in place, it allows American National Bank to relax when state or federal regulators conduct their next IT Audit. Jeff knew what the standard minimum regulatory requirements were in passing their IT Data Audits, but he was also smart enough to realize that his banks needed additional security functionality, that the SecureCARE tool provided, to ensure his banks are truly secure and protected from any costly data breach, identity theft or fraudulent activity.

With SecureCARE agents deployed on the PC network, all network communications, desktop applications, PC hard drives and all external devices are monitored for the access or manipulation of sensitive data by the user. Based on policies that are built in the central analysis server, these actions then can be blocked or the data encrypted before leaving the network. SecureCARE's agent technology can even proactively search devices for stored sensitive data, by scanning the network connected desktops, laptops, and servers. Once sensitive data is found, the agent will report the data's location to the server and then optionally encrypt the sensitive data. Through the logging and analysis server, the Security Officer deploys centrally managed policies, monitors real-time events, and generates critical reports on policy violations, user behavior, and compliancy audit data.

"With SecureCARE, we are now able to receive accurate reports such as; File and Data Activity, User Timesheet, Website Access, Alert Summary, and Content Violations, which allows us to better manage our users and secure our data.," said Brian Truschke, Vice President Information Technology, American National Bank. "Understanding user behavior at the desktop made securing the network that much easier. For example, with the user timesheet report we were able to find out what the user was doing and then create policies around the undesired user behaviors.

American National Bank was impressed by SecureCARE's centralized dashboard—which allowed the company to monitor user behavior, identify risk, create and manage policies, and create customized alerts. The company found that SecureCARE was very simple to use and manage. "SecureCARE was really easy to learn, with our computer expertise and this software, we were able to meet our data loss prevention goals while achieving our government compliancy requirements." said Truschke. "It is a very well designed tool, easy to use and easy to deploy."

### How to get started

CTH Technologies' team of data loss prevention experts will work with you to understand your unique data security requirements and priorities while sharing insight into our industries best practices. By auditing a sample of your network desktops and laptops, we will provide your company with our Data Risk Assessment Report from which our team will assist in implementing our recommended Enterprise Security Policy.



### About CTH Technologies

CTH Technologies now offers a unified Business Solutions Management platform that secures, simplifies, and automates IT processes. It also improves decision making, provides performance analytics and integrates data workflows across all technology platforms. Security remains the lead focal point within our solution suite offering. Our technology provides Enterprise Information Protection solutions that enable sensitive customer, patient or company data to move securely within large enterprises or small businesses, greatly increasing collaboration, enabling business processes and meeting regulatory compliance requirements for all of our customers.



### CTH Technologies, Inc.

One Lincoln Centre, 15th Floor  
Oakbrook Terrace, IL 60181

Phone: (630) 613.7070  
Fax: (630) 613.7001  
Email: [sales@cthtech.com](mailto:sales@cthtech.com)  
[www.cthtech.com](http://www.cthtech.com)