InteliSecure

At a Glance

Customer:
- Nationally recognized Cancer Research and Treatment Center

Critical Assets:
- Genomic Research
- Health Records

Industry:
- Healthcare

Solution:
- Critical Asset Protection Program development and Managed Services

Results:
- Managed DLP Program implemented successfully in phases
- DLP technology deployed and tuned with minimal noise from false positives
- Ongoing alerting, reporting and Incident Response processes

MAKING THE CASE FOR CRITICAL ASSET PROTECTION

Major Cancer Center Safeguards More Than Just Patient Data with InteliSecure

THE BUSINESS CHALLENGE

A well-known, nationally recognized Cancer Research and Treatment Center affiliated with a state university system was initially seeking to update and align its information security posture to comply with healthcare regulations and policies that safeguard patient privacy and data. Like many healthcare institutions, the Cancer Center had made significant investments in cybersecurity to protect its perimeter and was committed to improving security in the wake of growing threats from both inside and outside the organization.

Because of the "open" nature of the affiliated university's network, the Cancer Center's security management team was especially interested in DLP technologies for safeguarding both structured and unstructured data. The Cancer Center engaged InteliSecure in discussions to help identify and prioritize their critical assets, evaluate and recommend technologies that could meet their specific requirements and implement and managed a comprehensive security program.

DEVELOPING A CRITICAL ASSET PROTECTION PROGRAM™ (CAPP)

InteliSecure Critical Asset Protection Programs are implemented in phases to maximize their success - a proven approach that guides customers in the identification and protection of their most critical assets. In this case, InteliSecure Professional Services worked with the Cancer Center to first identify and prioritize critical information that not only included patient data, but also other intellectual property such as research and other key assets. The program established security policies and workflows specific to the customer's needs.

"One of our most important tasks was to work with InteliSecure in the planning phases to learn and thoroughly understand how people use our information technology" said the center's information security project leader. "We both learned a lot about our business during that initial consulting and technology evaluation phase."

Multiple DLP technologies were assessed by InteliSecure and the customer, with each vendor subjected to a 700 point use-case evaluation matrix. The results helped identify the best DLP solution for the Cancer Center's specific requirements and included technology for protecting data in motion, in use and at rest.

Going beyond the standard patient data and compliance security requirements, InteliSecure helped identify the Cancer Center's intellectual property in the form of genomic research as a priority for protection. Based on requirements for all key assets, a set of policies was developed for their DLP implementation.

By understanding how Cancer Center employees created, stored and transmitted their critical assets, InteliSecure Professional Services was able to properly tune technology settings from the start, helping to ensure the security staff would not be overwhelmed with the noise from hundreds or even thousands of alerts. From day one there were very few false positives. Tuning technologies properly also ensured that security analysts could review the information most relevant to the Cancer Center as quickly and accurately as possible; an essential condition of effective ongoing monitoring, reporting and incident response.

> ***"We were able to deploy a very complex set of technologies in a very short time thanks to the expert skills of InteliSecure's Professional Services team. Not only are they experts in DLP, but they have an in-depth knowledge of how virtualization and network technologies operate that has proven very valuable in the planning and operation of our program."***

OPERATIONALIZING THE CAPP WITH UNIQUE MANAGED SECURITY SERVICES

With the Cancer Center's Critical Asset Protection Program developed and deployed, InteliSecure commenced managing the program through its innovative Managed Security Services. InteliSecure provides a team of experts for each of its clients to interface with their Information Security Team. InteliSecure's SOC includes security monitoring and analytics (SM&A) experts as well as a security platform engineering (SPE) group to manage critical asset protection programs.

The Security Monitoring and Analytics team members intimately know the client's CAPP and are constantly observing, extracting and correlating data on how information is moving in and out of the client organization. This ongoing effort is essential in gaining a clear and accurate picture of the client's security posture in order to provide actionable recommendations as the program evolves. Knowing the business drivers for the client CAPP allows the team to quickly identify, triage, remediate and report on any suspicious events exponentially faster than traditional MSSPs.

The platform engineering group supports the SM&A team members by providing expert technical support in terms of ensuring solution components have 100% uptime as well as developing, maintaining and making configuration adjustments in scope and policy governance relating to the CAPP.

As part of its Managed Security Service, reports for the Cancer Center address overall security posture and intelligence issues. Policy reports help their governance group assess the accuracy of alerts and the severity of incidents, as well as discuss lessons learned and highlight trouble areas that may need more attention. Compliance reports provide auditing stakeholders with information necessary to help demonstrate compliance with policies and regulations.

THE ERRANT DOCTOR TRANSMITTING IP OUTSIDE THE ORGANIZATION

Within the first few days of implementing Managed Security Services, the client's SOC team identified and flagged the behavior of one specific doctor involved in genomic research at the Center's campus. Whether by accident or malicious intent, it appeared the doctor was transferring proprietary research information to a university outside the United States; a clear violation of policy. At this point, the SOC alerted key customer stakeholders, including legal and compliance, who decided how best to respond to the situation in consultation with InteliSecure.

Regardless of specific actions taken in response to this incident, SOC teams are constantly analyzing the impact of incidents or violations of policy to assess how existing policies may need to change in order to minimize or eliminate vulnerabilities. In this case, policies no longer permit auto-forwarding of specific documents by users.

“We have not had any problems in our initial implementation, which I attribute in large part to the technical design and planning service from InteliSecure.

“InteliSecure reports contain a lot of very useful information that contributes to improving our operating performance. They give our non-technical stakeholders a way to understand the issues and give us a much higher level of confidence in making decisions.”

KEY BENEFITS OF A CRITICAL ASSET PROTECTION PROGRAMTM

Utilizing InteliSecure Professional Services, the Cancer Center was able to identify and prioritize critical assets, develop processes and workflows customized to its specific way of doing business, select the best DLP technology and then operationalize its program through InteliSecure’s SOC. As a result, the Cancer Center gained:

- A proven, successful process for implementing and leveraging DLP.
- Unmatched expertise as an extension of its security team for daily tasks in monitoring both structured and unstructured data.
- A clear, more accurate picture of its security posture and how data is moving in and out of the organization.
- Analytics and reporting to help make more informed and effective decisions about priorities and resource allocation for information security.

ABOUT INTELISECURE

InteliSecure specializes in making data protection easy, fast, and cost-effective for companies of nearly every size. More than 500 clients with over 2 million managed users rely on our services and specialists to protect the integrity and safety of their sensitive information. With more than 15 years’ experience and partnerships with some of the world’s biggest names in cyber defense, we make data security and compliance easy by providing effective data protection at a lower cost, eliminating the strain on IT organizations and reducing the risk of confidential information getting into the wrong hands. Unlike other security providers, we focus on business outcomes—providing data and reports that make sense to business and security executives alike. InteliSecure serves clients globally with security operations centers in the United States and the United Kingdom.

InteliSecure

5613 DTC Parkway, Suite 1250 Greenwood Village, CO 80111 | + 1 (720) 227-0990 | sales@intelisecure.com | www.intelisecure.com
1 Lindenwood, Chineham Business Park Crockford Lane, Basingstoke, RG24 8QY, UK | +44 118 976 8960