InteliSecure

CRITICAL ASSET PROTECTION PROGRAMS™

InteliSecure.com

Today's advanced and persistent threats continue to create problems for security organizations throughout the world. The traditional perimeter-only, blanket approach to security continues to fail us as evidenced by large and very public breaches. While important for any security program, firewalls and other perimeter-focused technologies are only a part of an effective security program.

InteliSecure goes beyond traditional security programs to focus on the most critical assets in an organization's environment. Organizations are swimming in data and becoming more interconnected with partners and vendors in the "Global Electronic Nervous System" every day. The rapid and dispersive nature of data today makes it increasingly harder for people to protect their information. Critical Asset Protection Programs™ (CAPPs) focus on the data assets of an organzation that if breached, or otherwise compromised, would dramatically impact their bottom line. Examples could include: product design schematics, drug formulae, personal health information or even manufacturing processes.

CRITICAL ASSET PROTECTION PROGRAMS™	TRADITIONAL SECURITY PROGRAMS
Combine perimeter security with data protection that monitors the movement of data throughout your environment	Focus on an organization's perimeter with limited visibility as to how information flows through an organzation
Clearly define what assets are most critical to the health of your organization based on revenue, income, reputation and core operational impact	Designed as a blanket approach
Multi-dimensional to protect against internal and external threats	One dimensional perspective typically focused on external threats
Based on ISO 27001 standards	Generally based on a specific industry standard or a corporate requirement
Designed to help you move from a Compliance-based security posture to a Committment-based one	Often difficult to align people, processes and technologies to have employees view security as a competitive advantage and not a hindrance to their jobs

IDENTIFYING YOUR CRITICAL ASSETS

CAPPs clearly define what assets are deemed most important to your organization based on revenue, income, reputation and core operational impact. Whether those assets are intangible (e.g. a CAD file of a new product design) or tangible (e.g. a server farm providing transaction processing) we have developed a methodology that provides a risk-based, cost-effective solution.

Content

The actual information that makes up the asset.

Examples: Engineering specifications, drug formulae, PHI, manufacturing processes

Community

Who should and should not have access to the asset.

Examples: All employees, specific departments, outside vendors or partners, customers

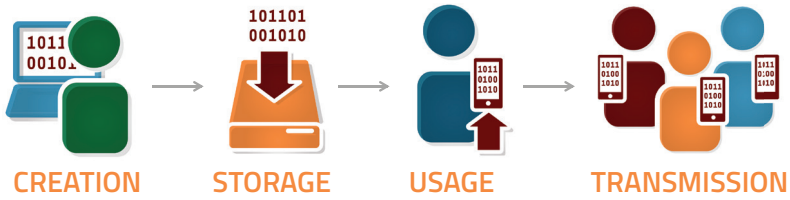
Channel

How the asset is allowed to move throughout an internal network and whether or not it is allowed outside of the organization.

Examples: Email, removable media, FTP, Print/fax, web postings

CRITICAL ASSET PROTECTION PROGRAM SCOPE

Most information and network security programs are doomed from inception because of the failure to develop a scope that is accepted, acknowledged and supported by senior leadership. Through a comprehensive interview and information gathering process, we work with you to develop a realistic CAPP scope that not only defines your critical assets but also their core attributes in regards to their creation, storage, usage and transmission.



Creation: The point in time when the asset is created. This could be the first swipe of a credit card, the initial lines of code for a new application or the acquisition of a new VM cluster. Today, asset creation can be the product of multiple groups or systems, creating the need for a laser-focused scope imperative for a successful protection program.

Storage: Once an asset is created it is then stored somewhere. For intangible assets this may be on a hard disk, RAM, NAS, SharePoint or other type of storage media. Tangible assets like servers, routers or laptops may be racked in data centers, placed in a remote office closet or maintained in a home office.

Usage: Mapping the authorized use of the asset is essential when developing a CAPP. After mapping the authorized use characteristics of the assets within the program scope and applying the optimal combination of people, process and technology, the task of successfully protecting the assets becomes a more manageable endeavour.

Transmission: Assessing how critical asset information is shared within and outside the organization provides key insight to the required protection mechanisms. The transmission threat vector is constantly utilized for authorized operations and can present some of the greatest challenges to inadvertent or malicious asset exposure.

THE RESULT

By taking into consideration not only what your most critical assets are, but also how they are used and moved about your environment, you end up with a customized Critical Asset Protection Program that helps you secure current and future revenue and earnings with enhanced confidentiality while maintaining optimal operational efficiency and reputational integrity.

Contact us to learn more.

Phone:
US+1 720 227 0990
UK +44 (0) 118 976 8960

Email: sales@intelisecure.com
Web: www.intelisecure.com