
Prevention, Patrols, and Public Health in the Information Age

Today, large companies, agencies and organizations are expanding and updating their internal infrastructure of networked computers. These increasingly complicated networks are interconnected with the global information infrastructure through the Internet and business partner networks. These interconnections are increasingly vulnerable to attacks. At the same time, information technology (IT) is proliferating, and "electronic borders" are increasingly hard to define and protect.

The solution is to create an "immune system" to protect the entire IT infrastructure against external and internal threats by making security pervasive and preventing incidents where possible, and detecting and responding appropriately when necessary. Just as immune system constantly monitors the health of a body and uses a range of means to prevent, detect, intercept, and defeat disease, an Internet Immune System must be equally aggressive in controlling attacks.

Threat Vectors

The threats to a communications network, internal network (intranet), or the Internet can come from both outside of the system or from within. External threats, while getting the most publicity, are not the most severe problems. Internal attacks have historically proven to be the most serious problem for any organization. Whether they come from outside or inside, there are four major types of activities that can threaten the health of your core business systems and networks:

- **Sites & Services:** certain locations and applications violate legal, regulatory, or other policies.
- **Events & Activities:** specific network incidents are often highly correlated with attacks and not legitimate operations.
- **Data & Content:** viruses and other forms of malicious code can threaten a network and certain forms of data, such as pornography, may be prohibited.
- **Individuals & Behaviors:** people and their actions are ultimately the source of all threats and violations of policies, laws, and norms of behavior.

External Security

Well-defined borders at network boundaries and gateways need to be protected using standard means such as firewalls, virus and active content scanning, as well as intrusion detection and protection and other traditional security methods. Because of the fluidity of modern networks, your core assets need better protection. Our **High Assurance Core™** services define the products, services, procedures, and integration methods that can surround your core systems – just as there is a barrier between the circulatory system for the body and the brain. All core systems and networks protected by our High Assurance Core products and services operate cooperatively to ensure the security within core systems. These core systems will also have improved security integrated with their interfaces with the remaining portions of the internal network as well as external communications and computers. While network and computer security techniques are useful, these key assets must have a full security program including physical security and careful choices made to ensure the availability and robustness in the face of natural and manmade disasters. This security program for your technical staff is an integral part of our High Assurance Core services. Our High Assurance Core services also define practices and recommend equipment or software modifications that will strengthen your internal security and business infrastructure.

Internal Security

Many of the security measures that are used at the border should permeate a network infrastructure. Virus and active content scanning as well as intrusion detection and even firewalls should be distributed throughout. These measures are needed to help minimize the impact of internal threats but also to address the constant changes and violations of the system's border. Filtering, Traffic and Access Control, and suspicious activity Monitoring become more important within the infrastructure. These techniques ensure that activities within the network are consistent with all of the owner's policies and the means are in place to identify violations.

Security Management Infrastructure

The users, computers, applications, and network all participate in ensuring that legal, regulatory, security, and other policies and procedures are followed. Tools such as public key infrastructures as well as biometrics and other access control techniques and security tools help implement these policies and procedures.

Immune System Infrastructure

The Internet Immune System itself has elements contained within a **High Assurance Core™** architecture: Agents that link applications to the immune system as well as stand-alone platforms and software; an internal Immune System Network with points of presence that link the immune system to the operational network and Security Management Infrastructure; and an Immune System Management System that monitors and controls the entire Internet Immune System as well as providing analytic and other support functions.

Creating the Immune System

An Internet Immune System is not a technology or suite of technologies, it is a basic change to the management of IT infrastructures. Threat Assessment, Requirements Analysis, Design, Integration, Deployment and Operation must all be linked by strong Technical Leadership and effective Project Management.

If you are interested in protecting your IT Infrastructure with our High Assurance Core™ products and services, contact us at info@itglobalsecure.com, or call U.S. Toll Free at 1-866-ITARMOR (+1 202. 332. 5878). Direct Sales: 1.202.425.422