

# iBeast Business Solutions, Inc.

## **Implement Intrusion Detection Software:**

The installation of Intrusion Detection Software, IDS, is a vital step in the overall process of securing a network. IDS does exactly what its name describes. It detects intrusion attempts. The vast majority of IDS solutions do not have the ability to stop or prevent an intrusion; the ones that can are very expensive and very limited to the systems they can control. IDS deployment should be part of an overall security project. Servers and desktops should be made as secure as possible in order to assist in the prevention of unauthorized access to sensitive data.

Intrusion Detection Software falls into two main categories. These are:

- Network based systems (NIDS)
- These types of systems are placed on the network, nearby the system or systems being monitored. They examine the network traffic and determine whether it falls within acceptable boundaries.
- Network based software can be fairly easy to deploy. However, it can generate false positives about threats, and that means headaches for nothing. Another downside is that the software is not typically integrated into larger network management systems so net managers can't gain an integrated view without proliferating more monitors.
- Host based systems (HIDS)
- These types of systems actually run on the system being monitored. They examine the system to determine whether the activity on the system is acceptable.
- Host-based intrusion-detection software may provide better application-layer security than can network-based tools because the host software can detect failed access attempts. It can monitor the number of files or directories accessed by a user.

Intrusion detection is the attempt to monitor and possibly prevent attempts to intrude into or otherwise compromise your system and network resources. Typically, a firewall or authentication system of some kind will be employed to prevent unauthorized access from the Internet. Sometimes, however, a firewall or authentication system can be broken. Intrusion detection is the set of mechanisms that you put in place to warn of attempted unauthorized access to the computer. Intrusion detection systems can also take some steps to deny access to would-be intruders.

## **What iBeast Can Do For You:**

More than ever, Credit Unions need to protect themselves and their members from hackers and cyber-terrorists. You must defend against viruses and worms, lost data, customer erosion, lawsuits, and loss of revenue. iBeast has the expertise, not only in network and network security, but also in Credit Unions and their special needs to deliver the right solutions for the right price.

## **How can iBeast do this?**

By giving you intrusion detection at an affordable price. Installing intrusion detection software is only the start. With the iBeast Cave monitoring and protecting your Credit Union and enhancing your peace-of-mind, you can focus on serving your members instead of on what cyber-problem might come next. The Cave monitors networks 24/7 and is operated by skilled network and security professionals. Attacks are responded to immediately and detailed escalation procedures are followed to prevent any mistakes. You can rest easy knowing your networks are being watched, even while you're sleeping.

---

## **Firewall Management**

iBeast provides the essentials you need to establish your firewall security. Stop worrying about costly investments in personnel or technology. And even more critical, this solution provides around-the-clock monitoring and management - along with continual upgrading to keep your data secure and keep you ahead of changing technology.

- Proactive monitoring 24 hours per day, seven days per week
- Minimized capital expenditures and investment in personnel training
- Simplicity and flexibility
- Maximum availability and reliability

## **Complete Managed Security Package\***

The complete security management package includes the IDS Monitoring and Response and the Firewall Management. This package has all the features of the above, but lowers the monthly fees by more than 25%.

Also included in this package is our Windows NT/2000 Security Maintenance Service. Every month Microsoft releases fixes for security issues as well as other operating system issues. Keeping up with these changes and analyzing if they fit the needs of your Credit Union is a time consuming task. Installing a Hotfix or a Service Pack can have negative effects on your systems and can cause serious downtime and business interruption. iBeast researches and tests all Hotfixes and Service Packs prior to installation on any production system. We'll make sure you stay current and get only the patches you need.

As the world has become acutely aware, the threat of viruses to business has grown to an enormous liability. Not properly maintaining your virus protection creates an invitation for disaster. A virus infection at even a small Credit Union can cause thousands of dollars in damage as well as result in lost business and can cause expensive equipment loss. Infection repairs can cost thousands in hourly fees from expensive consultants or take the precious time of your in-house staff. iBeast will manage and maintain your virus software making sure that it is configured for optimum security and that updates are done regularly. In the case of a virus outbreak, iBeast analysts will notify the Credit Union and make sure that all updates are performed and that the network is secure. If updates are not readily available we will work with the Credit Union to minimize the possibility of an infection. iBeast works with all major vendors to ensure timely notification and resolution of virus outbreaks.