



DNA Enterprise™

"DNA Enterprise provides the real-time network awareness and corrective measures we need to be one step ahead of the threat at our headquarters and in the datacenter." **Banking CIO**



The Problem with Network Security Today

The four key pillars of network security: Anti-virus, Firewall/VPN, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) do not protect your network assets from hackers, viruses, worms and spyware. Nor do they help you comply with government regulations. In addition, none of these solutions can properly alert, block and remediate against dirty laptops, untrusted and malicious insiders or rogue wireless devices.

In summary:

1. INTERNAL VULNERABILITIES CAUSE DOWNTIME

From 2000 to 2005, reported vulnerabilities increased over 90%

From 2000 to 2005, reported security breaches as a result of vulnerabilities increased 10x (tenfold).

95% of all security breaches result from known vulnerabilities and misconfigurations (Source: 2005 Ecrime Survey, CSO Magazine and CERT)

2. CORPORATE NETWORKS ARE NOW DYNAMIC, MOBILE AND WIRELESS, CREATING MORE RISK

According to Forrester Research, 35 million remote users this year (2005) and 14 billion devices on the Internet by 2010. The need to quarantine high risk, vulnerable systems or untrusted malicious insiders in complicated non-homogenous networking environments is growing dramatically.

3. LACK OF DUE CARE AND DUE DILIGENCE IS VERY COSTLY

CERT calculates the financial damage from these security intrusions worldwide at around \$15 billion annually. Of the 90 percent of CSI/FBI survey respondents detecting computer security breaches within the last year, 80 percent acknowledged financial losses.

"NetClarity picks up where firewall, anti-virus, intrusion detection and intrusion prevention leave off."

- John Gallant, President, NetworkWorld - May, 2006

The Solution- DNA Enterprise Appliance

What is Dynamic Network Awareness (DNA)? DNA is a turnkey security appliance loaded with a robust suite of sophisticated, proprietary software solutions that enables you to secure, manage, and control the information on your network and systems environment effectively.

With a DNA appliance, administrators can monitor their network for security breaches and network integrity, problems, analyze event data in real time, quickly review important event data archive files and generate event reports.

Whether you are managing a large, complex network, or multiple systems on a LAN/WAN or SOHO environment, NetClarity products can provide you with unparalleled solutions to protect the integrity of your information and systems.

DNA will proactively detect and alert using advanced tracking technology. It helps you block and mitigate attacks in real-time with discrimination between usage errors and unauthorized access.

It provides an early warning system for enterprise-wide event correlation coupled with intrusion detection and intrusion prevention measures.

All of these features are built-into one network-based intrusion prevention appliance (NIPS).

By deploying DNA Appliances and Protection for Windows, our Host-based Intrusion Prevention System (HIPS), along with our award-winning Auditor vulnerability management appliances, you'll always be one step ahead of threats in a more preemptive, proactive way.



Secure, Turnkey, Plug-and-Play Appliance

With our uniquely easy to use solution, you will be up and running in five minutes. Within your first hour, you will have a DNA Enterprise solution up and running. It will only generate reports and alert you when you need to be alerted. No false positives:

- Plug it in, turn it on.
- Connect to it securely, with standard web browser using HTTPS (SSL)
- Log in and watch as DNA keeps an eye on your network with no fuss.
- Set up the IDS/IPS engines in minutes.

Key Features

- Advanced tracking technology captures MAC and IP addresses and tracks source of issue
- Discriminates between usage errors and unauthorized access
- Early warning system provides enterprise-wide correlation of event data
- Sophisticated Event Wizard provides threat analysis and event management support in real time
- Alerts indicate multi-site attacks
- Automated event notification by email and pager
- Link to remote sites in real-time with proprietary and SNMP systems
- Auto compression and archiving of event data to local and remote storage
- Easy maintenance of data files
- Provides multiple adapter support, including dial-up, AOL and Ethernet
- Multi-protocol analyzer with support for TCP/IP, IPX/SPX, LocalTalk, NETBEUI, NETBIOS and DECNET and more
- Uses sophisticated encryption and armoring technology to protect DNA Appliances from being compromised.
- Rejects attacks with real-time dynamic filtering protection

NetClarity's advanced tracking technology is multi-protocol and uses sophisticated methods to track and trace security problems and error conditions in complex enterprise networks.

Users control multiple options to set the sensitivity level to desired event tracking operations. Tracks and displays source of event, including user name and machine name. Threat analysis distinguishes between events and attack behaviors.

MACtrack™ observes all connections. Target tracking covers all monitored segments.



Appliance Specifications

- 2.5 GHz Pentium 4 processor (or higher).
- 80 GB of built-in high speed HD storage (or higher).
- 1U rack mountable chassis with universal rails included.
- 1 GB of high speed memory (or more).
- Built-in keyboard, video, mouse and serial ports for initial setup.
- Dual Intel 10/100/Gigabit Ethernet controllers (NICs).
- Audits networks from hundreds to thousands of IP Addresses.

System Requirements

Works with any Web browser running HTTPS (SSL) including Opera, Internet Explorer, Netscape and Firefox. **Can easily manage DNA Branch™ appliances through the built-in Command Center dashboard.**

Benefits

With DNA Enterprise, you will be able to quickly and easily defend against attacks which target all of your Common Vulnerabilities and Exposures (CVEs®) - The root cause of network downtime. All hackers, worms, viruses and spyware use CVEs® to break into your network, behind your firewall. DNA's patent-pending technology consists of data analysis, event management, and notification management, pattern-matching, data archives and report generation functions coupled with Firewall and SmartSwitch plug-ins (optional) for full Network-based Intrusion Prevention System (NIPS) functionality.

DNA Technology features include:

- Notification management with fail-close feature
- Enterprise-wide MACtrack availability
- Expert system automatically generates new rules from local network data
- Built-in security defense management
- Sophisticated probe and trace capability to operate at MAC level
- Multi-level sensitivity controls
- Support for 802.3 compliant networks and multiple ASYNC adapters
- Support for local or network attached printer
- Proprietary and SNMP built-in communications
- Integrated replay function with sophisticated archive management
- Multiple encryption techniques for DNA product branding

AVAILABLE NOW:

Call: 781-276-4555

Email: sales@netclarity.net