CLEVER Mobile® for DNS 1.1

Empowering IT Cloud Security Management Anywhere, Anytime

Key Features

- **Mobile app provides access to CLEVERDetect for DNS** alert notifications
- Mobile OS includes **iOS** and **Android**
- Ensures real-time notification of DNS record changes to the appropriate IT knowledge worker with **structured alert levels** and **alert notification reports**
- Identifies who will receive specific alert details for decision making with the **user authorization level function**
- **Rearm** capability avoids flooding mobile device with repetitive alerts
- **Audit report** displays historical details on when a DNS record was different from the baseline
- **Commands** provides access to common TCP/IP functions like Ping and Traceroute to aid in forensic diagnosis
- Assists in the detection of **cache poisoning**, **amplification**, and **redirection** vulnerabilities
- **DNS Monitor** shows real-time changes in DNS records compared to a baseline

AES
149 Commonwealth Drive
Menlo Park, CA 94025
650-617-2400 or 650-617-2401
www.aesclever.com
info@aesclever.com

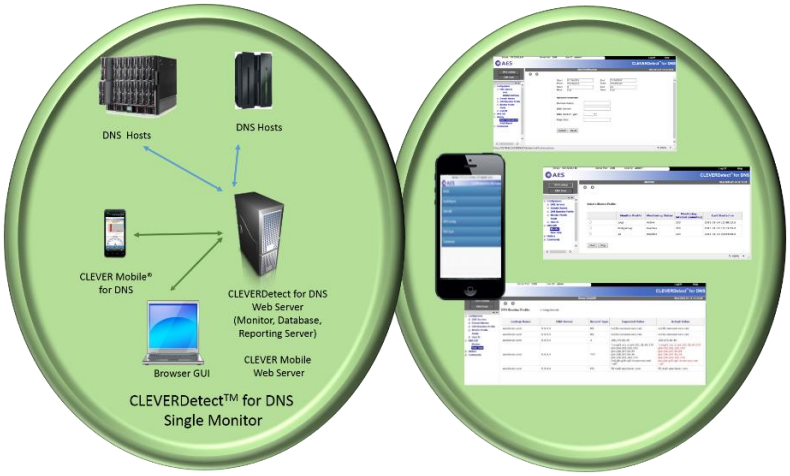
CLEVER® Business Cloud Service and Security Management

Enterprise mobility has come of age with measurable business value available to early adopters. Mobile technology is transforming the business at a dizzying pace, far exceeding the business impact of the change to IP back in the late 1990's. The computing power now in the hands of business people through mobile devices is awe-inspiring.

One of the few things everyone agrees about on cybersecurity is that it is all about reducing and managing risk. The major components of risk are threats and vulnerabilities, and risk levels go through cycles as threats and vulnerabilities wax and wane. The major factors that cause those elements to vary are changes in technology and changes in business processes.

DNS vulnerabilities are second only to HTTP in the number and frequency of exploitation by hackers. With DNS being the 'Internet's Directory Assistance', gaining control of a DNS server can run havoc on your business sending users, clients, and employees to the wrong servers. This can result in misinformation being relayed, userids and passwords or confidential information being acquired by cyber thieves, or malware being placed on unsuspecting systems. Understanding if your DNS servers have been compromised by techniques like cache poisoning, amplification, or redirection is essential to protecting your business, employees, clients and users in general.

CLEVER Mobile® for DNS empowers IT staff members to provide exceptional service to the business with their iOS ® and Android® powered mobile devices. The added access capability ensures real-time notification of changes in DNS records leading to increased awareness of potential security vulnerabilities. Historical information access through these mobile devices improves forensics management of security threats globally.



Applied Expert Systems - The Business Cloud Service and Security Management Company

Highlights of CLEVER Mobile® for DNS

- **Mobile app provides access to CLEVERDetect for DNS** alert notifications
- Mobile OS includes **iOS** and **Android**
- Ensures real-time notification of DNS record changes to the appropriate IT knowledge worker with **structured alert levels** and **alert notification reports**
- Identifies who will receive specific alert details for decision making with the **user authorization level function**
- **Rearm** capability avoids flooding mobile device with repetitive alerts
- **Audit report** displays historical details on when a DNS record was different from the baseline
- **Commands** provides access to common TCP/IP functions like Ping and Traceroute to aid in forensic diagnosis
- Assists in the detection of **cache poisoning**, **amplification**, and **redirection** vulnerabilities
- **DNS Monitor** shows real-time changes in DNS records compared to a baseline

CLEVER Mobile for DNS v1.1 is scheduled to enter managed availability March 2015.
CLEVERDetect for DNS v1.1 entered managed availability January 27, 2015.

System Requirements

CLEVER Mobile for DNS System Requirements

- **Android:** 4.x
- **iOS:** 5.x and above
- **CLEVERDetect for DNS v1.1**

CLEVERDetect for DNS System Requirements

- **Web Server:** For Windows/Linux - 4 GB of RAM, 1 GHz processor or higher, 1 GB of hard disk space
  - Operating Systems - z/OS V1R12 or later, Windows Server 2008 and 2012, Windows 8 and 7, Red Hat Enterprise Linux 6, and SUSE Linux Enterprise Server 11
  - JAVA Platform: WebSphere for z/OS 7.0 or later, Apache Tomcat 7.0 or later, JRE **must** be 7.0 or higher
- **PC Workstation:** 2 GB RAM, 1 GHz processor or higher, 1 GB hard disk space
  - : Windows Server 2008, Windows Server 2012, Windows 8, Windows 7, RHEL 6, SLES 11
- **Browser Applications:** Internet Explorer 8.0 or later, Firefox 31 or later

AES
149 Commonwealth Drive, Menlo Park, CA 94025 USA
phone: (650) 617-2400 or (650) 617-2401
Fax: (650) 617-2420
Website: www.aesclever.com Email: info@aesclever.com

MM-10-1501-DS2