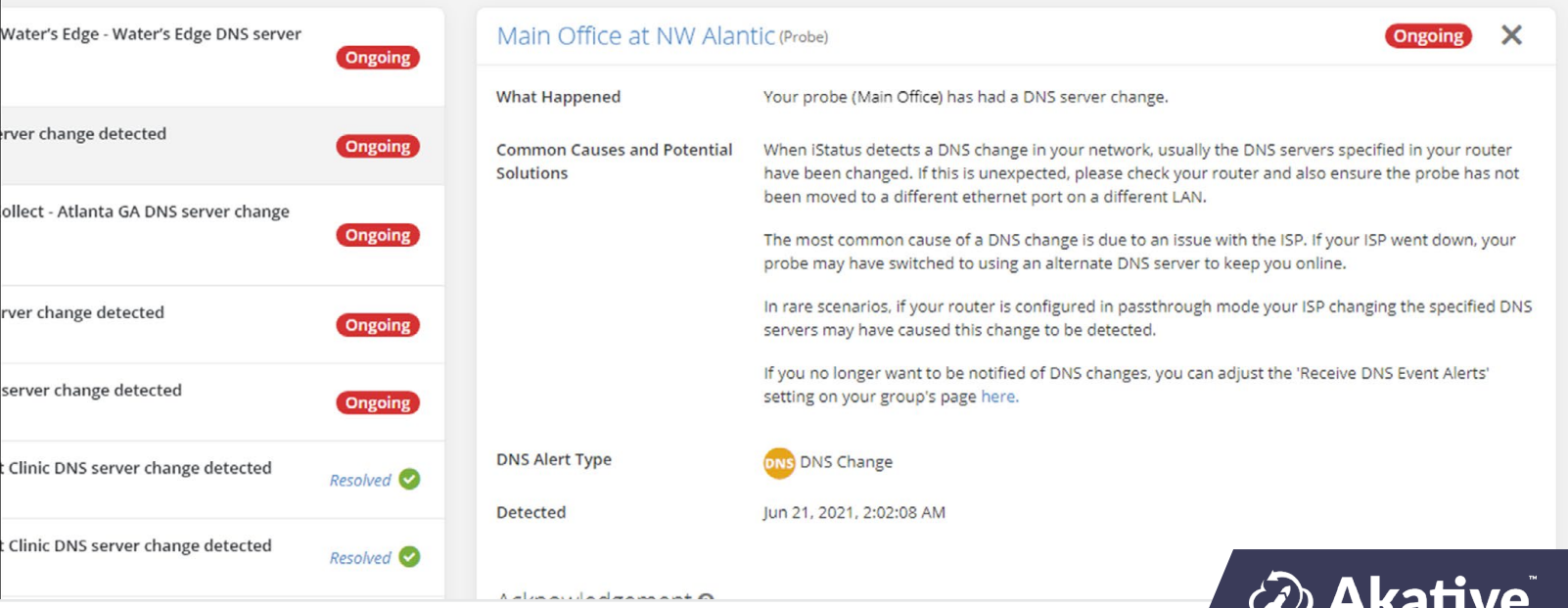


# iStatus® DNS Change Detection

## Built-in iStaus Network Security Layer

### How DNS Change Detection Help You Manage Networks Better?

With the DNS Change Detection feature, iStatus helps you maintain the security of your network. This built-in feature alerts you when the DNS is altered, indicating a misconfiguration, or worse, a cyberattack.

iStatus detects two of the most critical and most common DNS hijacking attacks, router DNS hijacks (using the DNS Change Detection Feature) and man-in-the-middle attacks (using the iStatus ArpWatch™ Feature). Using these two iStatus features is among the easiest ways to protect your network today.

With real-time IntelligentAlerts™ keeping you informed, you can quickly and proactively take action to keep your network secure and operating optimally.

- **To Enable DNS Change Detection and ArpWatch:** you can easily add-on these iStatus security features to your current monthly service or upgrade your monthly service plan to the Professional or Enterprise service plan. Please reach out to our support team or an Akative representative.

### What is DNS Hijacking?

A Domain Name System (DNS) is essential to all companies that depend on the Internet—it is a crucial element to the performance and legitimacy of an organization's web-based applications and cloud services.

A DNS attack/hijack is a cyberattack in which the attacker exploits vulnerabilities in the Domain Name System. A loophole in your customer's DNS could translate to major loss and frustration.

There are many different ways in which DNS can be attacked. However, there are four basic types of DNS redirection:

- **Local DNS hijack** — attackers install Trojan malware on a user's computer, and change the local DNS settings to redirect the user to malicious sites.
- **Router DNS hijack** — many routers have default passwords or firmware vulnerabilities. Attackers can take over a router and overwrite DNS settings, affecting all users connected to that router. (Detected by DNS Change Detection)
- **Man-in-the-middle DNS attacks** — attackers intercept communication between a user and a DNS server and provide different destination IP addresses pointing to malicious sites. (Detected by ArpWatch)
- **Rogue DNS server** — attackers can hack a DNS server and change DNS records to redirect DNS requests to malicious sites.