US005406260A

# United States Patent [19]

Cummings et al.

[11] Patent Number: 5,406,260

[45] Date of Patent: Apr. 11, 1995

[54] **NETWORK SECURITY SYSTEM FOR DETECTING REMOVAL OF ELECTRONIC EQUIPMENT**

[75] Inventors: **Marshall B. Cummings**, Ann Arbor, Mich.; **Christopher R. Young**, Austin, Tex.

[73] Assignee: **ChriMar Systems, Inc.**, Ann Arbor, Mich.

[21] Appl. No.: **992,924**

[22] Filed: **Dec. 18, 1992**

[51] **Int. Cl.**[6] ..... **G08B 21/00**

[52] **U.S. Cl.** ..... **340/568;** 340/687

[58] **Field of Search** ..... 340/568, 571, 572, 652, 340/664, 687

[56] **References Cited**

U.S. PATENT DOCUMENTS

| | | | |
|---|---|---|---|
| 3,618,065 | 11/1971 | Trip | 340/568 |
| 3,932,857 | 1/1976 | Way et al. | 340/572 |
| 4,654,640 | 3/1987 | Carll et al. | 340/568 |
| 4,686,514 | 8/1987 | Liptak, Jr. et al. | 340/571 |
| 4,736,195 | 4/1988 | McMurtry et al. | 340/568 |
| 4,760,382 | 7/1988 | Faulkner | 340/572 |
| 5,034,723 | 7/1991 | Maman | 340/568 |
| 5,059,948 | 1/1991 | Desmeules | 340/568 |
| 5,066,942 | 11/1991 | Matsuo | 340/568 |
| 5,136,580 | 8/1992 | Videlock et al. | 370/60 |
| 5,231,375 | 7/1993 | Sanders et al. | 340/568 |
| 5,243,328 | 9/1993 | Lee et al. | 340/568 |

FOREIGN PATENT DOCUMENTS

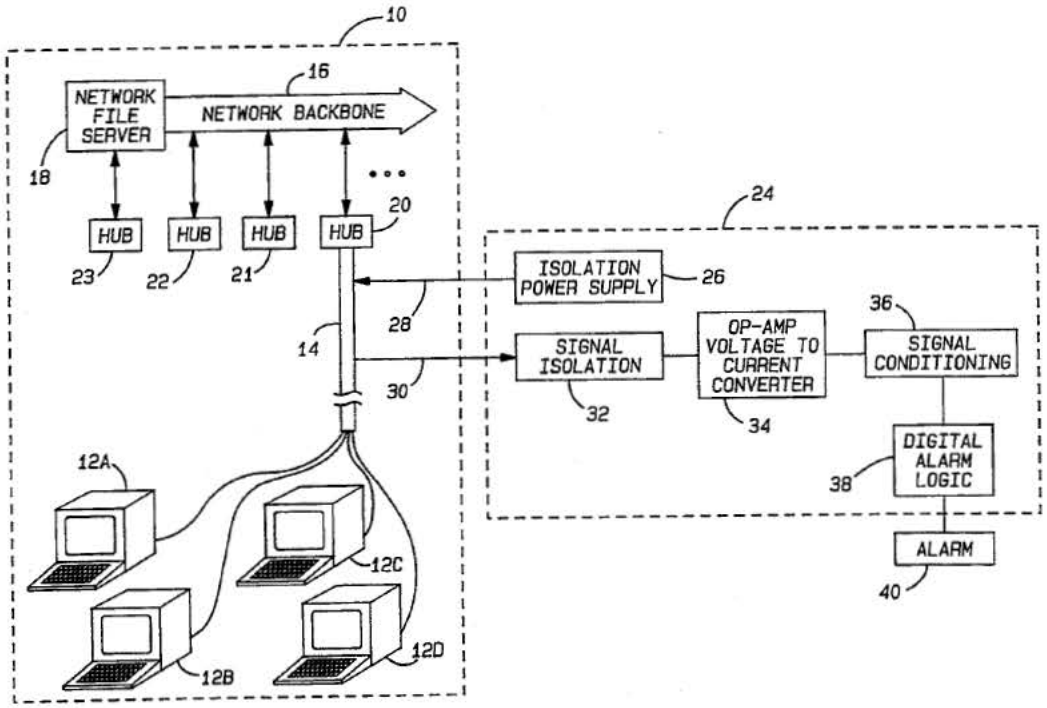
| | | | |
|---|---|---|---|
| 357482 | 3/1990 | European Pat. Off. | 340/568 |
| 4203304 | 8/1992 | Germany | 340/568 |

*Primary Examiner*—John K. Peng
*Assistant Examiner*—Thomas J. Mullen, Jr.
*Attorney, Agent, or Firm*—Harness, Dickey & Pierce

[57] **ABSTRACT**

A system and method are provided for monitoring the connection of electronic equipment, such as remote computer workstations, to a network via a communication link and detecting the disconnection of such equipment from the network. The system includes current loops internally coupled to protected pieces of equipment so that each piece of associated equipment has an associated current loop. A low current power signal is provided to each of the current loops. A sensor monitors the current flow through each current loop to detect removal of the equipment from the network. Removal of a piece of hardware breaks the current flow through the associated current loop which in turn may activate an alarm. This invention is particularly adapted to be used with an existing 10BaseT communication link or equivalent thereof, employing existing wiring to form the current loops.

**19 Claims, 3 Drawing Sheets**




DOCKET ALARM

Find authenticated court documents without watermarks at docketalarm.com.

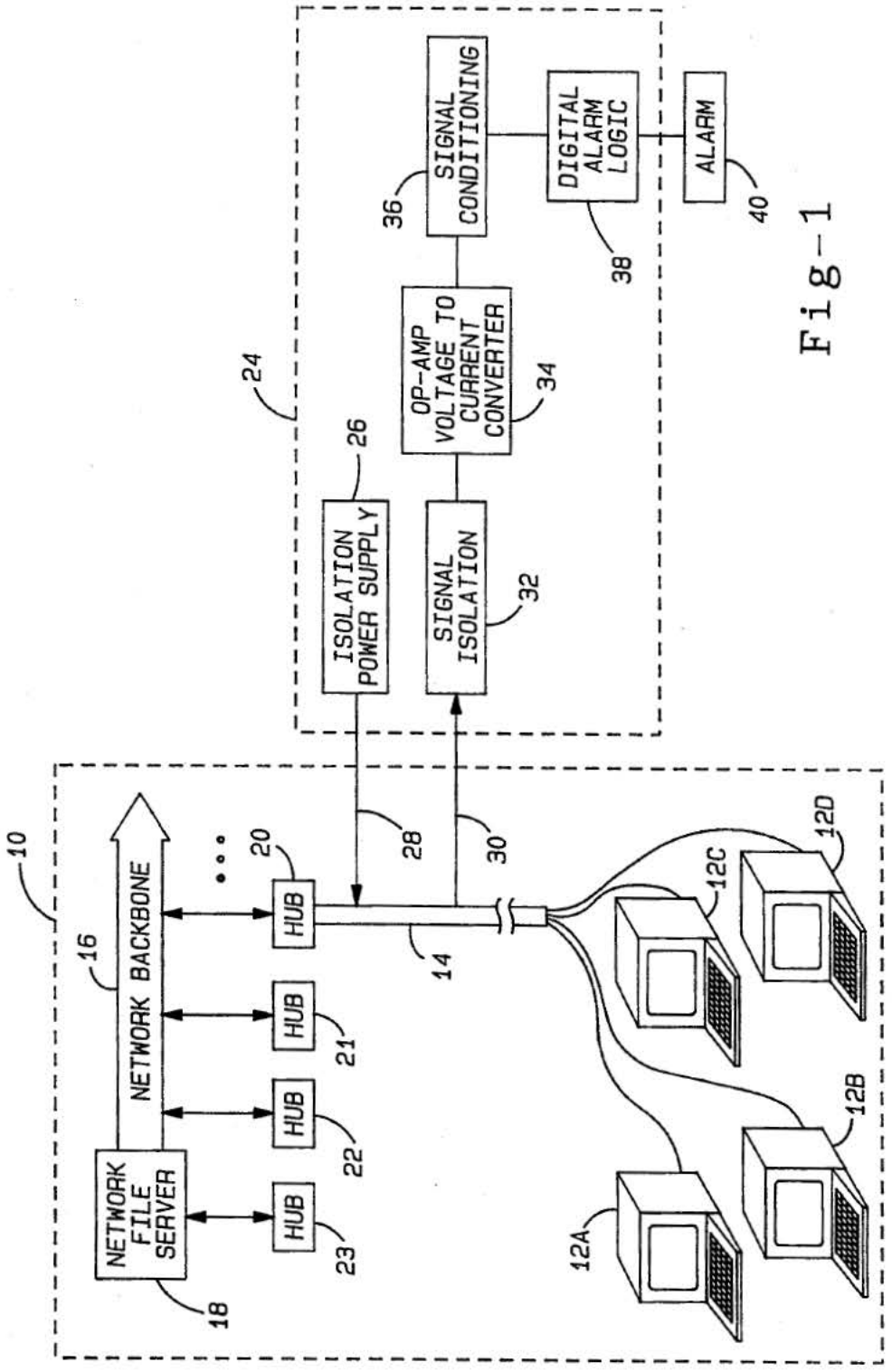



Fig-1

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

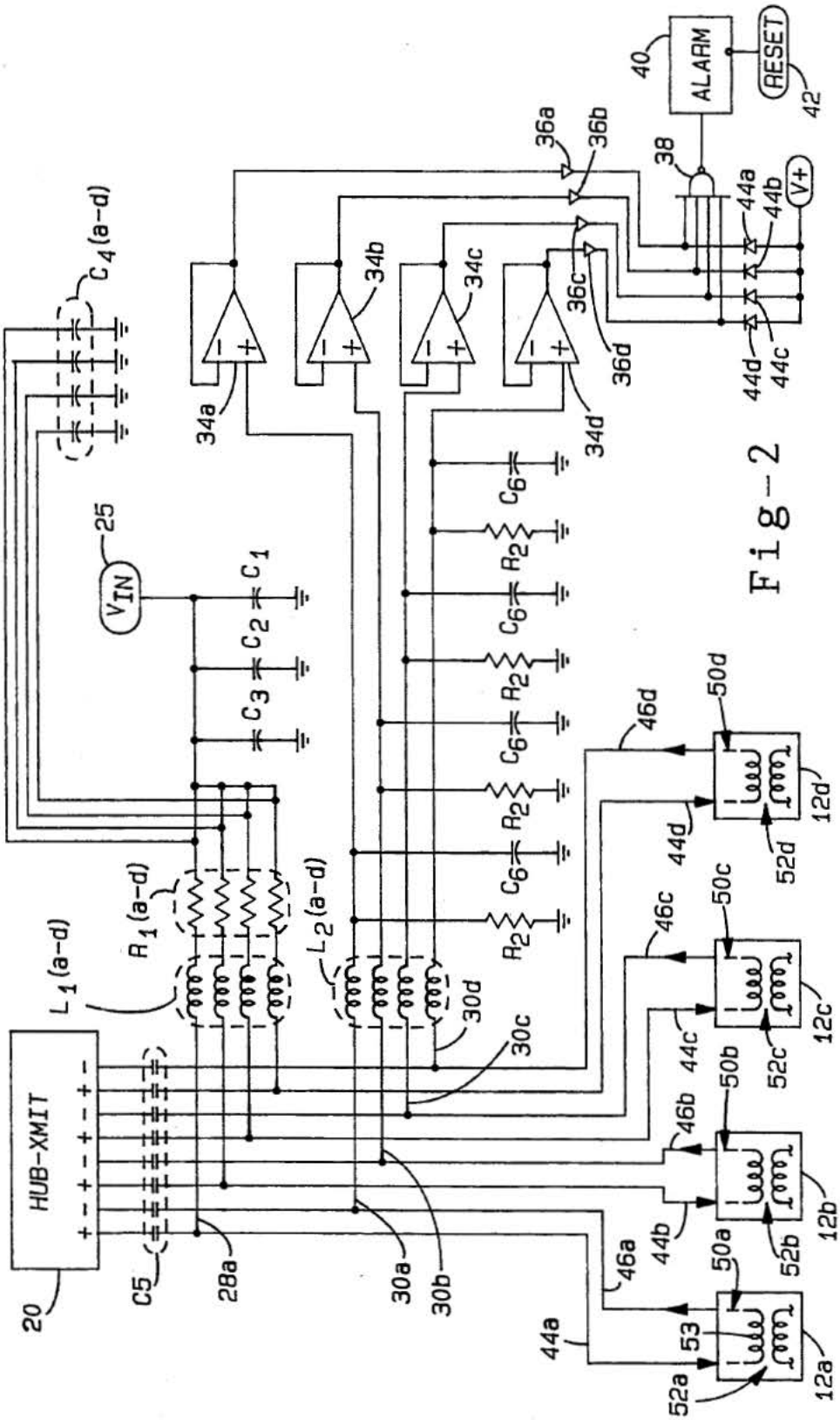



Fig-2

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

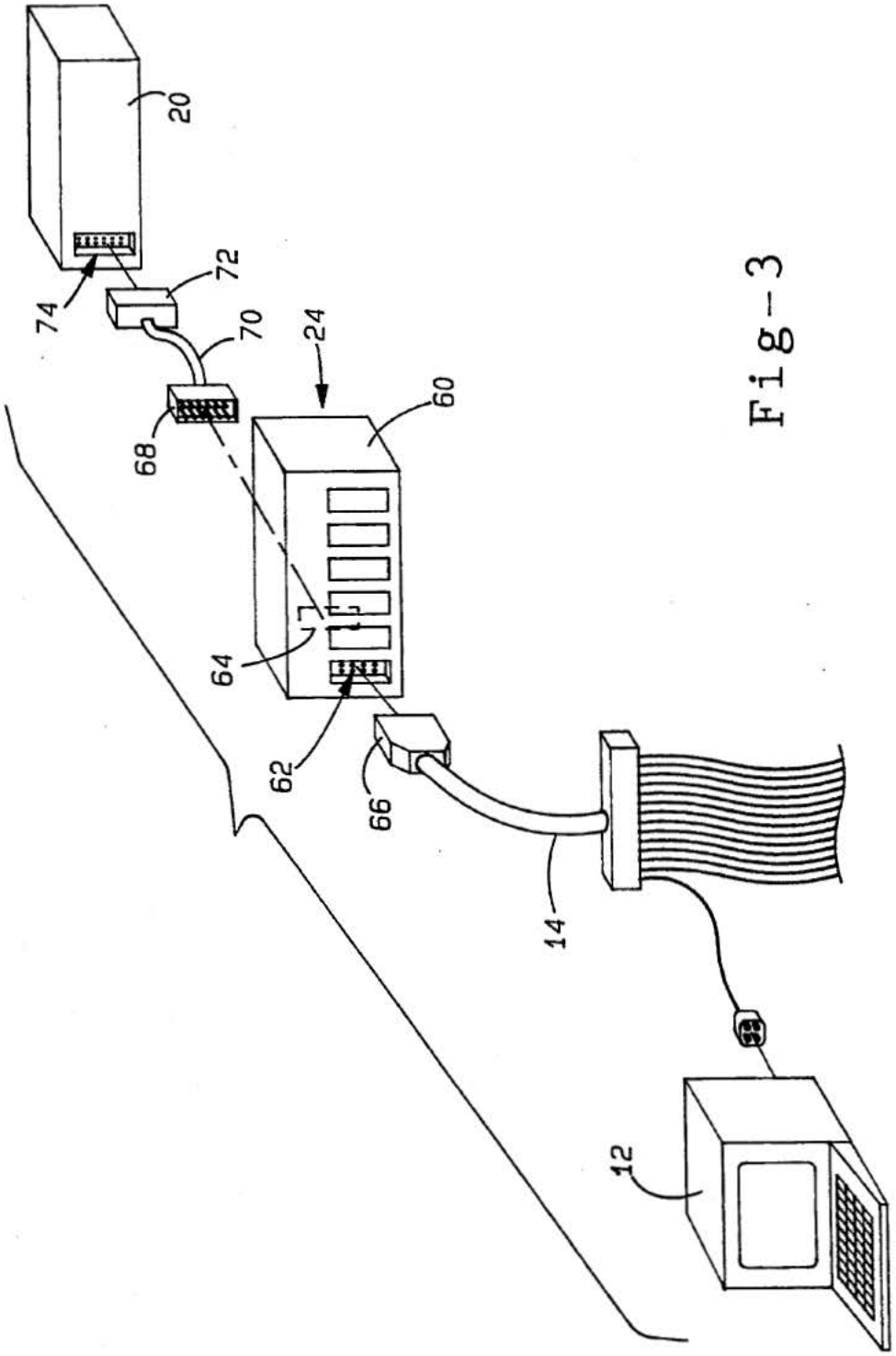



Fig-3

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

# NETWORK SECURITY SYSTEM FOR DETECTING REMOVAL OF ELECTRONIC EQUIPMENT

## BACKGROUND OF THE INVENTION

1. Technical Field

This invention relates generally to theft protection security systems and, more particularly, to a network security system for detecting the unauthorized removal of remotely located electronic equipment from a network.

2. Discussion

There has been an ever increasing need to provide security for electronic equipment against the unauthorized removal or theft thereof. Computer systems have become a major capital expenditure for users which commonly include businesses, educational institutions and governmental entities, among other users. Advancements in technology have significantly reduced the size and weight of complex computer equipment, thus making expensive computer equipment more easily portable. As a consequence, modern computer equipment is generally more compact and more easily transportable, which further makes it more difficult to secure against the unauthorized removal or theft thereof.

Today, computer network systems are frequently employed to provide efficient computing capabilities throughout a large work area. Existing computer network systems generally include a number of remotely located work stations coupled via a data communication link to a central processing center. For instance, many educational institutions such as universities commonly provide a large number of individual work stations at different locations throughout the university campus so as to allow easy computing access to the computer network system. However, the wide dissemination of such equipment at remote locations has made the equipment an accessible target for computer thieves.

Accordingly, a number of methods have been developed for guarding against the unauthorized removal of electronic equipment. Early methods of protection have included the physical attachment of a security cord to each piece of protected equipment. However, the security cord generally may be cut or physically detached from its secured position and is usually considered to be a non-appealing aesthetic addition to the equipment. Another method of protection includes the attachment of a non-removal tag to the equipment which also requires cooperating sensing devices responsive to the tag which are properly located at exit locations from the premises. However, this approach requires rather expensive sensing devices and is generally not very feasible especially when multiple exit points exist.

Other methods of theft protection have included installing a special electronic card inside each computer machine which responds to polls from an external monitoring station. Upon removal of the machine, the card stops responding to the polling of the central station and an alarm is initiated. Another approach involves mounting a sensing device on or into the machine to detect movement of the machines. These approaches, however, are generally undesirable since they require the incorporation of additional components into each machine.

More recent methods of theft protection have included the sensing of a current loop coupled to the protected equipment. One such method is discussed in U.S. Pat. No. 4,654,640 issued to Carll et al which discloses a theft alarm system for use with a digital signal PBX telephone system. This method includes a plurality of electronic tethers which are connected to individual pieces of protected equipment by way of connectors which in turn are bonded to the surface of the protected equipment. Each tether includes a pair of conductors which are connected together to form a closed current loop via a series resistor and conductive foil which is adhesively bonded to the outside of the equipment. However, this method requires the addition of an externally mounted current loop, and it is conceivable that the current loop may be carefully removed without any detection.

It is therefore desirable to provide for an enhanced network security system which detects unauthorized removal of remotely located pieces of hardware from a network. More particularly, it is desirable to provide for such a security system which feasibly employs separate current loops provided through an existing data communication link to monitor the presence of remotely located computer equipment. In addition, it is desirable to provide for a security network system which may be easily and inexpensively implemented in an existing network system and may not be easily physically removed or detached from tile system without detection.

## SUMMARY OF THE INVENTION

In accordance with the teachings of the present invention, a security system is provided for detecting unauthorized removal of electronic equipment from a network. The system includes current loops internally coupled to protected pieces of equipment so that each piece of associated equipment has an associated current loop. A low current power signal is applied to each of the current loops. A detector monitors current flow through each of the current loops so as to detect a drop in current flow which represents removal of equipment from the network. Detection of removal of a piece of equipment may in turn activate an alarm. This invention is particularly adapted to be used in conjunction with a computer network having an existing communication wiring scheme coupling each piece of equipment to the network, and which may be used to form the current loops.

## BRIEF DESCRIPTION OF THE DRAWINGS

Other objects and advantages of the present invention will become apparent to those skilled in the art upon reading the following detailed description and upon reference to the drawings in which:

FIG. **1** is a block diagram which illustrates a network security system coupled in to a computer network in accordance with the present invention;

FIG. **2** is a circuit diagram which illustrates the network security system coupled to the computer network in accordance with the present invention; and

FIG. **3** is a schematic diagram which illustrates installation of the network security system into an existing computer network in accordance with the present invention.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Turning now to FIGS. **1** and **2** a network security system **24** is provided therein for achieving theft protection of electronic computer equipment associated with a computer network **10**. In general, the network security

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

**LAW FIRMS**
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

**FINANCIAL INSTITUTIONS**
Litigation and bankruptcy checks for companies and debtors.

**E-DISCOVERY AND LEGAL VENDORS**
Sync your system to PACER to automate legal marketing.