PROFICIO
SECURITY AND NETWORKING SOLUTIONS

Whitepaper

# Improving Productivity and Uptime with a Tier 1 NOC


## Summary

This paper's in-depth analysis of IT support activities shows the value of segmenting and delegating activities based on skill level and illustrates the benefits of using a NOC for first-level support. Historical data was gathered from Proficio's 24x7 advanced NOC, industry research, and interviews with IT support engineers. Results showed that **65% of support activities can be performed by a first-level support team,** leading to increased overall productivity and enabling more senior specialists to focus on strategic business initiatives.

A tiered IT support structure utilizing a 24x7 Tier 1 NOC allows incidents to be detected, prioritized, escalated, and efficiently resolved, directly reducing Mean Time to Resolution (MTTR). For organizations that cannot justify the expense of setting up and operating an internal 24x7 NOC, outsourcing NOC services can be a financially and strategically prudent decision. NOC service companies provide inherent economies of scale, making outsourcing a cost-effective option for IT system support.


A **NOC** (Network Operations Center, pronounced "nock") is the central location from which an organization supports its computer network and telecommunications infrastructure—servers, applications, routers, switches, circuits, UPS, environmental sensors, security cameras and other devices. The NOC monitors, detects and resolves infrastructure events as they happen by interacting with monitoring systems, technical specialists and external equipment/carrier vendors.

A NOC is not a help desk. A help desk in an enterprise is primarily set up to handle end-user issues and provide PC/laptop, application and basic network connectivity support.

## Industry Challenges

Organizations that rely on IT infrastructure to keep their core business activities functioning face many challenges in their IT support groups, including:

- Burnout of IT support personnel due to inadequate staffing
- Impaired off-hour coverage
- Lack of proper tools and a structured, process-oriented approach
- Lack of accountability
- Slow response and high resolution times
- High costs of supporting IT infrastructure

From a business standpoint, these problems can result in poor end-user experience, low productivity, the delay of strategic initiatives, and employee attrition. Organizations commonly underestimate the amount of support activity performed by IT staff due to the absence of defined metrics, appropriate data collection and a process-oriented support system. Moreover, a lack of visibility into the nature and types of support activities can lead to the inefficient utilization of staff.

## Analysis of IT Support Activities

An analysis of the common support activities and their duration reveals the benefits of a 24x7 tiered support structure.

### Common IT support activities

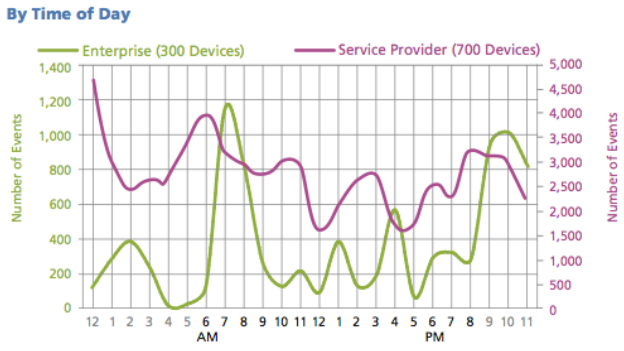
1. Monitoring events from IT infrastructure
2. Managing support requests from end users
3. Managing incidents resulting from events and support requests
4. Maintaining documentation and managing patches, configurations and changes
5. Reviewing periodic service reports

Data related to IT support activities was gathered from our internal 24x7 NOC, industry research and interviews with IT support engineers. A detailed analysis was performed to identify the major time and cost drivers, including frequency and duration of occurrence and also the skill level required to perform each activity.

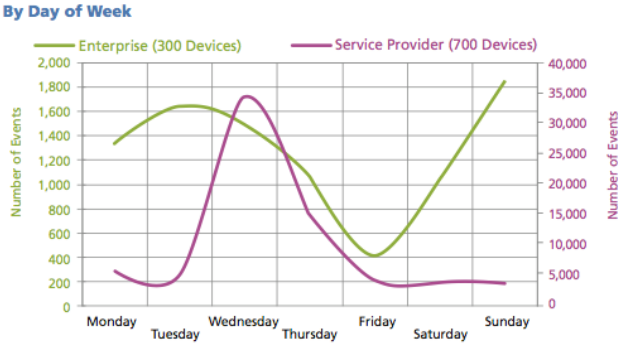
In a traditional IT support environment, staff react to support issue notifications generated by either the IT help desk, end users or an automated alert. In a 24x7 proactive support environment, events (alarms) generated by servers, applications, networks and carrier circuits can be detected, classified and recorded by monitoring tools. They are sent to support staff in the form of alerts, e-mails, text messages, or other automated notifications. To improve efficiency, intelligent and customizable monitoring tools are used to filter out false positives and extraneous events.

**Figure 1** shows observed total events by day of the week and by time of day for a service provider with 700 devices and an enterprise with 300 devices. Data was collected over a period of four weeks.

FIGURE 1 Events Generated from IT Infrastructure




Monitoring IT infrastructure events requires preliminary processing by qualified technical people which can take anywhere from a few seconds to over two minutes depending on the type of event. This time is used for acknowledging the event, classifying it as an incident if warranted and creating a trouble ticket for further investigation. Therefore, from a work management perspective, it is necessary to measure the event load during various hours of the day and days of the week.




Events occur around the clock and should be monitored and processed 24x7. Figure 1 clearly shows that the number of events is highest on Wednesdays for the service provider. This is usually because downtime windows are set for that day and the downtime windows have exceeded the allocated times or the changes made to the IT infrastructure have generated events past the downtime window. The figure also reveals that the number of Enterprise events is particularly high around 7:00am. This is due to users signing on at that time, resulting in threshold-based alerts and events generated beyond the change

window from previous changes made to the IT infrastructure. The above analysis highlights the need for a 24x7 proactive support environment, helps us understand trends in event volume over time and allows for proper IT decision making (e.g., support staffing levels).

### Managing Support Requests from End Users

Requests for support, primarily in the form of telephone calls and e-mails, constitute another time-consuming activity for IT staff. Types of requests include service issues, issue updates, password resets and documentation. To measure this type of activity, an Automated Call Distribution (ACD) system can provide reports on the call volume and duration. Statistics on e-mail can be obtained from most messaging software applications. All requests for support related to service issues need to be logged as incidents in the trouble ticket system. Tracking the number and duration of phone calls and e-mail activity reveals the amount of time involved in performing this activity.

FIGURE 2 IT Support Calls

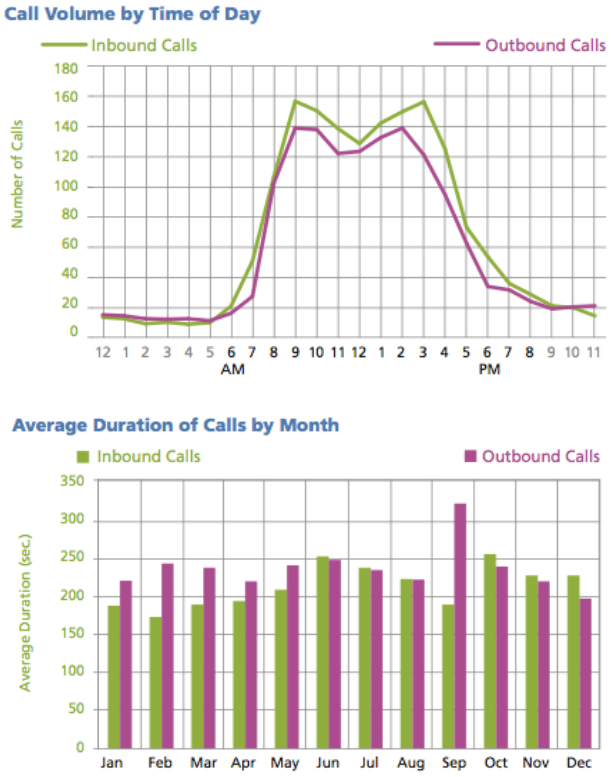



**Figure 2** shows the IT support call duration by month and call volume by time of day based on data collected over a one-year period from a sample of enterprises and service providers. Data for inbound and outbound calls is tracked. Both inbound and outbound call durations average about four minutes with call volume being highest between 6:00 a.m. and 8:00 p.m.

If the average call is four minutes long and the number of calls in a month is 3,000, the amount of actual labor involved in handling support requests would be about 200 hours per month, spread over various times of day and days of the week. Similarly, one can measure the amount of time spent on e-mail activity from statistics generated by the messaging application. Clearly, business hours account for the most support requests in the form of phone calls and e-mails. Quantifying service requests, an integral part of IT support activity, helps us understand how to improve resource allocation and scheduling of support staff.

### Managing Incidents Resulting from Events and Support Requests

Events and service requests can be logged into a trouble ticket system as incidents. Once an incident is recorded, the primary goal of the IT staff is to resolve it as quickly as possible. This is usually the most time-consuming activity performed by the support staff. To perform incident management effectively, aside from tools and training, it is essential to have good troubleshooting processes and a trouble ticketing system to record and track the details of each incident until resolution. The trouble ticketing system also provides visibility to other groups or users involved with resolving the incident.

The ability to quickly respond to and resolve incidents depends on the tools, structured processes and training available to the IT support staff. On average, Tier 1 activities last 15 minutes, while Tier 2 and 3 activities can last an hour or more for each specific incident depending on an organization's IT environment. A repeatable support process, an available knowledge base, accurate documentation, skilled IT support personnel, available spare parts and access to specialists are all factors that contribute toward reducing the MTTR.

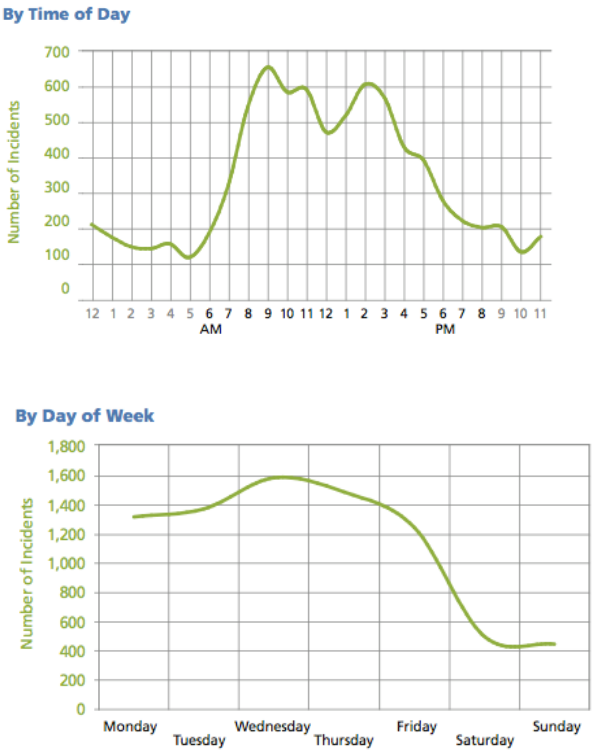
By far, managing incidents is the most time-consuming aspect of IT support. The analysis above shows that staff utilization can be optimized by dividing the support tasks among different tiers of support.

## Maintaining Documentation and Managing Patches, Configurations and Changes

The IT service and infrastructure environment reaches across various internal departments and external groups. To react quickly to events and support requests, the IT support group must not only keep accurate records of the IT infrastructure but also keep track of the various service levels that each group or department needs. Each group may need a different level of service which is documented in a Service Level Agreement (SLA). Service levels are defined by factors such as uptime for e-mail, web and database services; response times; latency; jitter; packet loss; network availability and MTTR.

Routine patches and upgrades of software revisions need to be performed and configurations need to be backed up to enable quick recovery from a failure. A majority of these tasks can be performed by first-level technicians. Changes to the infrastructure are routine and must be recorded as they happen.

**FIGURE 3** Incidents Generated from Events and Support Requests




The IT infrastructure required to deliver services to end users is complex and consists of a combination of applications, servers, network and security devices, external WAN circuits and environmental equipment. All of these assets, their configurations and their relationships need to be identified, recorded and maintained.

Maintaining an accurate repository of the network diagrams and asset details, including configurations and support service levels, allows the IT support group to prioritize incidents appropriately and resolve them quickly and efficiently. A controlled change management process and a routine patch and configuration management procedure are essential for preventing unnecessary downtime.

## Reviewing Periodic Service Reports

Periodic review of reports plays an important role in the analysis of support issues and can lead to reducing downtime in the future. Although periodic reports are usually customized to a specific IT support environment, most reports are published weekly, monthly, quarterly and annually. These reports contain information about the number of events, incidents, phone calls, e-mails, response times, uptime and MTTR and can be grouped by reason codes, physical locations, departments, type of equipment and so on.

Reports are reviewed primarily to identify trends and patterns in support issues. For example, a specific location or device could be prone to outages. Power-related issues could be causing a majority of the downtime due to lack of sufficient backup power. A server may be nearing CPU or memory capacity utilization, or the bandwidth between sites may be maxed out, resulting in latency and packet loss.

**Figure 4** represents examples of periodic service reports. Outage information over a period of one month for an enterprise with 300 devices reveals that about a third of the outages are related to power issues.

Review of such reports allows the IT staff to identify recurring problems, monitor potential capacity issues and track availability and uptime on a consistent basis.

FIGURE 4 Periodic Service Report Examples

**Monthly Outage Report by Reason**

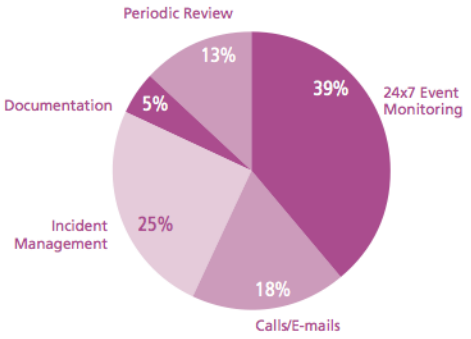
| Reason | Number of Tickets | Outage Minutes |
|---|---|---|
| Circuit Outage | 5 | 853 |
| Device Failure | 5 | 1,122 |
| Link Unstable | 2 | 1 |
| Power Outage | 23 | 1,934 |
| Scheduled Maintenance | 6 | 802 |
| Threshold Alert | 2 | 1 |
| Unknown | 1 | 1 |
| Unscheduled Maintenance | 2 | 791 |
| Uptime Alert | 23 | 16 |
| Other | 6 | 2,146 |
| **Total** | **75** | **7,667** |

## Example – IT Support Activity Summary for an Enterprise

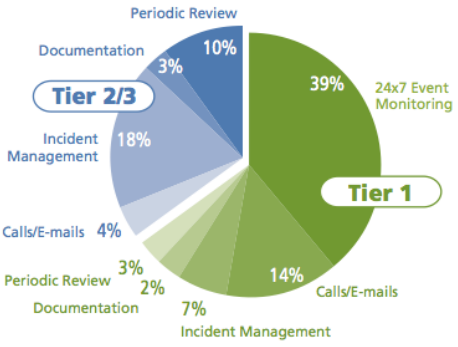
To better illustrate the activities discussed in the previous sections, Proficio performed an internal customer study of an enterprise with an IT infrastructure consisting of servers, network devices and environmental equipment. The total number of devices monitored for this particular enterprise was 312 with 10,411 interfaces and 647 IP addresses. A total of 13,464 services were monitored along with 951 thresholds. Examples of services include web, e-mail, database and various customized services for in-house applications. Thresholds were set for CPU, memory, disk, bandwidth and numerous other variables.

FIGURE 5 IT Support Activity Summary

**By Category**




**By Tier**




The duration of activities such as monitoring events and managing incidents was tracked at the Tier 1 and Tier 2/3 levels. **Figure 5** summarizes the IT support activities for the enterprise over a period of one month.

Figure 5 shows that the greatest proportion of time, 39%, was spent on 24x7 event monitoring, followed by incident management at 25% and handling calls and e-mails at 18%. The statistics by tier show that 65% of the total time spent on support was related to Tier 1 support activity, with a majority of time spent on 24x7 event monitoring and handling calls and e-mails. Tier 2/3 activity required 35% of the total support time, with most of the time being spent on incident management and periodic review.

This IT support activity analysis provides the basis for meaningful change to the IT support structure in order to improve customer service and infrastructure uptime cost-effectively. The following section provides recommendations.

## Solution – Tiered IT Support Structure

Previous sections discussed activities that IT personnel need to perform to fulfill the support function. Most of these are 24x7 activities that require dedicated resources. These activities need to be continuously measured and analyzed to optimize resource allocation. A tiered IT support structure will enable IT managers to leverage the lower-cost first-level or Tier 1 NOC to perform routine activities and free up higher-level or Tier 2/3 IT support engineers to focus on more advanced issues and implement strategic initiatives for the organization.

FIGURE 6 Enterprise IT Support Structure

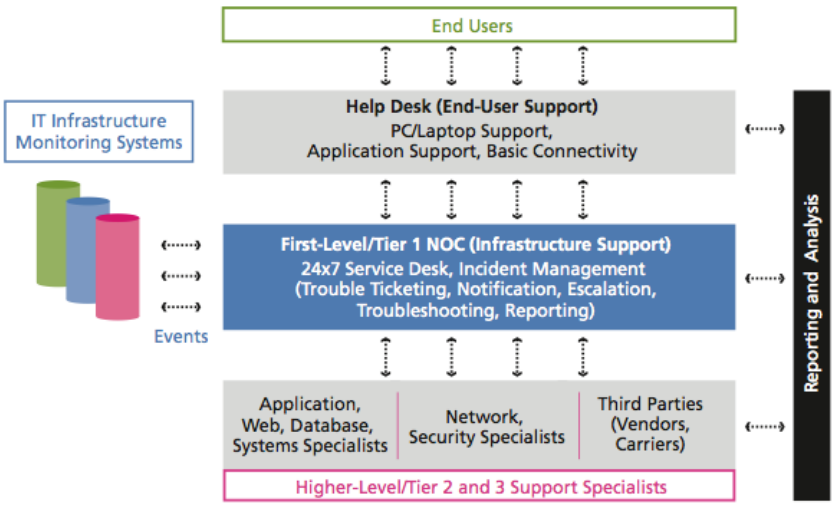



**Figure 6** is a tiered support structure, central to which is the Tier 1 NOC that interacts with monitoring tools, an end-user help desk and specialist engineers. Information flows between the various tools and entities within a well-defined process framework. Depending on the size and complexity of the infrastructure, there may be different ways to implement this strategy. For example, a carrier that is primarily concerned with network support may not need a help desk.

It is important to distinguish between a help desk and a NOC. In an enterprise, the help desk is primarily set up to handle end-user issues and provide PC support, application support and basic network connectivity support. On the other hand, the NOC supports IT infrastructure such as servers, applications, networks, security, and WAN circuits and interacts with monitoring systems, technical specialists, engineers and external equipment/carrier vendors.

The tiered IT support structure can effectively resolve 65% of incidents at the Tier 1 level and escalate advanced issues to specialized IT staff. This enables the support group to handle the events, service requests and incidents at the appropriate tier while achieving resolution as quickly as possible.

### Tier 1 NOC – Central to IT Support

Most organizations have high-level specialist engineering staff but lack a 24x7 Tier 1 NOC. The example above reveals that approximately 65% of the time spent in supporting IT infrastructure can be accomplished at the Tier 1 level. These results are further validated by a recent benchmarking report of service desk practices reporting that 60% of incidents are resolved at first contact by front-line support personnel.

Industry studies show that the average hourly compensation for first-level support staff is one-half that of second and third-level support engineers. It is neither productive nor cost effective for expensive Tier 2/3 engineers to perform activities that can be handled by front-line or Tier 1 NOC support personnel.

An organization can cost-effectively improve the support function by utilizing a 24x7 Tier 1 NOC service to perform basic support activities that can be escalated to the Tier 2/3 support personnel when necessary.

Figure 6 illustrates the tiered support structure with the Tier 1 NOC providing 24x7 support activity. Monitoring infrastructure events, handling support requests from end users, creating and updating trouble tickets, escalating issues and working with external carriers all fall directly in the realm of Tier 1 NOC support activity.

## Benefits of Utilizing a 24x7 Tier 1 NOC Service

The benefits of utilizing a 24x7 Tier 1 NOC service are summarized below.

- ✓ **Reduces the overall cost of delivering IT support.** About 65% of IT support activity can be performed on a 24x7 basis by Tier 1 NOC personnel resources that cost considerably less than specialist Tier 2/3 resources.
- ✓ **Reduces the organization's MTTR.** By having a 24x7 NOC that follows a repeatable process for managing incidents, not only is the response time to an alarm lower, but the resolution process is repeatable and acted upon and escalated in a consistent, formal way.
- ✓ **Improves efficiency and utilization of Tier 2/3 personnel.** Interruptions in the form of support activity are a distraction to strategic projects performed by specialist engineers. Diverting resources off a project and re-engaging after interruptions results in lost productivity. Resource utilization is improved significantly by engaging the Tier 2/3 engineers appropriately when their specialized knowledge is needed. (As the example above shows, nearly two-thirds of all support activities can be performed by the Tier 1 NOC and thus Tier 2/3 personnel remain available for other activities.)
- ✓ **Improves the end-user experience.** By providing a 24x7 service desk, the NOC service ensures that incidents are detected, prioritized and resolved around the clock. The end users are notified with a time to resolution. Thus, proactive management of the IT infrastructure results in a higher quality of support to the end user.

**65%** of time spent in supporting IT infrastructure can be accomplished by first-level or **Tier 1** skilled personnel. Tier 1 staff has basic technical certifications such as (CCNA, A+, MCTS or similar) and customer service experience. This function receives a support request (alarm or call), logs the issue and assists with simple configuration and problem resolution activities. Issues that are not resolved by Tier 1 support are escalated to Tier 2/3 support.

**35%** of support activity is performed by higher-level or Tier 2/3 staff. **Tier 2/3** engineers have several years of technical experience, possess advanced certifications (CCNP, CCIE, MCPD, MCA or similar), maintain service-specific knowledge and attempt to resolve integration issues. Tier 2/3 support performs routine diagnostics, configuration, problem identification and analysis.

**Considerations for Building a 24x7 NOC**

- Volume of events, support requests and incidents
- Initial software and ongoing support
- Initial server hardware and ongoing support
- Implementation, customization and integration of software
- Systems and application engineers
- NOC staffing requirements
  - Hours of coverage (for example, 24x7, 8-to-5)
  - Number of personnel per shift
  - Challenge of maintaining consistent staffing
- Training costs
- Miscellaneous costs
  - Disaster recovery site for redundancy
  - Office space, monitoring stations, telephone, network connectivity and power

## Considerations for Building a 24x7 Tier 1 NOC

The decision to utilize or build an internal NOC depends on a number of economic and strategic factors. The following elements represent the basic cost drivers required to run or build an internal NOC.

For organizations that cannot justify the high expense of setting up or operating an internal 24x7 NOC, it is economically feasible to outsource the Tier 1 NOC service to a qualified company. Outsourcing is a cost-effective option because of the inherent economies of scale that NOC service companies provide.

## Conclusion

IT Support Managers and staff face ever-increasing demands as enterprises and service providers stress lower time to resolution, higher service availability and increased end-user satisfaction while controlling costs. To perform the IT infrastructure support function effectively, it is important to understand and proactively monitor and quantify IT support activities that include event and incident management, processing of service requests, maintenance of documentation and periodic review of the service performance.

Utilization of IT support capacity and resources can be optimized by measuring and classifying support activities into Tier 1, 2 and 3 activities. By utilizing a skilled internal or outsourced 24x7 Tier 1 NOC service that consistently monitors, records and manages events and incidents, IT Support Managers can ensure that 60% or more of their support issues are resolved at the front line. For escalated cases, the IT specialist engineers are able to respond to and resolve issues in a systematic and timely manner. This results in significant cost savings from improved staff efficiency, reduced mean time to resolution and a much better end-user experience.

### About Proficio and ProNOC

Proficio is a leading provider of networking and security solutions. Enterprises benefit from Proficio's real world experience in delivering large successful projects and rely on our team for security assessments, consulting, project management, implementation, and support.

Proficio's ProNOC service provides 24x7 monitoring of networks, servers, circuits, and applications ensuring continuous uptime. We can advise how to respond to problems or take direct responsibility for remediation. Our approach saves costs (typically 1/3 of equivalent in-house cost), delivers the highest levels of availability and performance.

ProSOC is our security monitoring and analysis service. Using leading SIEM technology, security experts monitor and respond to your security alerts 24x7. Our experts have managed some of the largest and most respected Security Operation Centers in America.  Instead of being overwhelmed by alerts, we will identify the short list that matter and then work with you to respond.

For more information see www.proficio.com.

While every effort has been made to ensure the accuracy of the information presented in this publication, Proficio Inc. does not warrant or assume any liability or responsibility for the accuracy, completeness, or usefulness of the information or processes disclosed in its publications or those of its partners. All information is subject to change without notice. Pro**NOC** is a trademark of Proficio Inc. Other product and company names may be trademarks or registered trademarks of their respective owners.