FINLEY ENGINEERING
INTEGRITY INTO EVERYTHING

Finley Active NOC

Network Monitoring & Management Service

External customers expect your services to be available at any time. But staffing and managing a proactive 24/7 NOC is a large draw-down on margins for small and medium service providers, and a large expense for similarly sized businesses too. Outsourcing support to the right team can save much of this cost without reducing the quality of your customer's experience with your service. Finley has the right team.

Finley Active NOC© Service ensures you have around the clock proactive management of your network and critical servers with a staffed network operations center. Our staffed NOC monitors your equipment via proactive alerts for most common performance impacting conditions and failure events. Most often, the NOC can handle those conditions before they impact services. Even if the failure does impact services, the Finley Active NOC staff often will have begun troubleshooting and escalation before the first customer call. Finley Active NOC monitoring and management is of course fully customizable to your business case.

The Process

Software agents monitor servers and collect data from network devices. If the agent discovers a problem with the server or an associated network device, the agent generates an alert to the Finley Active NOC.

This alert triggers the creation of an incident ticket, which is then worked to resolution by the NOC. More complex incidents may require escalation to engineering staff or may require interaction with you, the customer. In any case, you will be kept appraised of any open tickets that impact services to your customers.

While a large majority of tickets should be created through this process, if you have an issue you need to escalate and there is no open ticket, you may call the NOC's toll-free number.

Network Assessment Enhancements

Service Provider Network

Prior to engagement for network operations, Finley recommends a network assessment and documentation review prior to the engagement. Finley IP Services can provide a detailed assessment of your current service provide network architecture and implementation. At the end of the assessment Finley Engineering will deliver a detailed list of findings and recommendations, along with drawings of the current physical and logical architecture.

FINLEY ENGINEERING
INTEGRITY INTO EVERYTHING

Corporate Server Network

The Finley Active NOC can perform a server-centric network assessment to identify the current state of your server network and any risk points found within your server implementation. The outcome of this process is a pair of reports including an Executive summary report that is seven pages, and a detailed technical report that is often over 50 pages long. While optional, this assessment is a great enhancement to the Active NOC service, and is often the best starting point for an engagement. The table below outlines the elements of a server network assessment.

The network assessment is the first step in setting up our Remote Monitoring Support Services. This includes a required audit of your network devices. Next, a system will be identified for hosting the Finley remote monitoring agent. This could be a network management platform, but any Windows or Linux system is acceptable. Through this agent, Finley is able to continually monitor and react to any network or server problems 24/7.

Task	Description
Detect Domain Controllers	Identifies domain controllers and online status
FSMO Role Analysis	Enumerates FSMO roles at the site
Enumerate Organization Units and Security Groups	Lists the Organizational units and Security Groups with members
User Analysis	List of users in AD, status, and last login/use, which helps identify potential security risks
Detect Local Mail Servers	Mail server(s) found on the network
Detect Time Servers	Time server(s) found on the network
Discover Network Shares	Comprehensive list of Network Shares by Server
Detect Major Applications	Major apps / versions and count of installations
Web Server Discovery and Identification	List of web servers and type
System by System Event Log Analysis	Last 5 System and App Event Log errors for servers
Detailed Domain Controller Event Log Analysis	List of event log entries from the past 24 hours for the Directory Service, DNS Server and File
Replication Service event logs	
Network Discovery for Non-A/D Devices	List of Non Active Directory devices responding to network requests
SQL Server Analysis	List of SQL Servers and associated database(s)
Internet Domain Analysis	"WHOIS" check for company domain(s)
Password Strength Analysis	Uses MBSA to identify computers with weak passwords that may pose a security risk
Missing Security Updates	Uses MBSA to identify computers missing security updates
Internet Access and Speed Test	Test of internet access and performance
External Security Vulnerabilities	List of Security Holes and Warnings from External Vulnerability Scan

FINLEY ENGINEERING
INTEGRITY INTO EVERYTHING

Finley also has a backup service for 24/7 backups on critical servers that provides bare metal restores in the event of a server failure.

Finley network monitoring includes device availability, utilization levels on memory, CPU, and interfaces (as specified by the customer). Network reporting is included and provides a historical view showing the network utilization over time and giving you a baseline view of network health. Any changes like utilization spikes or sudden abnormal activity can be quickly identified which is especially important for identifying security vulnerabilities. Having this information quickly available puts you in control of your network and able to react to any event or issue.

Finley understands that all networks are not the same and we size our support according to the requirements of our
customers.

Being able to have critical systems monitored 24/7 and servers with backup and performance monitoring allows you to have peace of mind, and enables you to deliver upon the
expectations of your valuable customers. Minimize downtime, become proactive and save time and money while keeping your customers happy.

For more information contact Mike Ockenga at m.ockenga@fecinc.com or call 952-582-2912.

Server care includes:

- Application, performance and hardware monitoring
- Intelligent alert monitoring (thresholds set by management)
- Alert filtering and validation
- Ticketing system with escalation and resolution tracking
- Full remote access problem resolution
- Remote restart of services and reboot
- Server maintenance, server health, application performance and issue reporting
- The patch levels including a white listing patching service
- An antivirus and malware service
- Reports that show server utilization and availability, application and performance monitoring
- Additional reporting services include MS Exchange, security, HIPAA, and network audits