

24/7 Monitoring

OneSquared Monitoring and Reporting tests all network connections, servers, and even services running on servers both in our data centres and on your premises.

What is it?

OneSquared Monitoring and Reporting consists of three elements:

1. Monitoring of your:
 - a. Server devices
 - b. Network connections
 - c. Services running on servers and devices
2. Reporting on all aspects of performance, usage, and availability of your:
 - a. Servers
 - b. Network and internet connections
 - c. Web site activity
 - d. Service issues such as job tickets and service level agreement (SLA)
 - e. Mobile messaging activities
 - f. Email
 - g. Domain names
3. Alerts. When things go wrong, you need to know. Depending on your contract with us, you may be notified by email, SMS text message or by phone.

Why should I use it?

OneSquared monitoring provides a permanent, remote watch on your server(s), network connections and the processes operating on them. If anything fails to respond to tests, we know about it.

Real-time web-based reporting gives you a full understanding of user activities and performance management.

How does it work?

Monitoring tests not just whether a device on a particular IP address responds to a PING request, but also whether the SMTP, HTTP and IMAP services are responding on that device.

Each test includes a number of configurable parameters:

- Test Parameters – availability and protocol
- Test Interval
- Threshold – Warning, Critical, Recovery
- Threshold Action

When services meet certain “failure” parameters, alerts are sent out in an escalating manner depending on your SLA and the nature of the issue.

You can also log in at any time to the web-based reporting tools get an overview of all of your services.

Monitored Fault Response?

With an appropriate SLA and system management contract, OneSquared also offers a fault response service which includes your choice of:

- Investigation of ‘non-availability’ incidents
- Server or service restarts
- Service restoration and root cause analysis in the event of catastrophic failures (these are carried out in association with appropriate third parties)
- Service incident logging
- Reviewing of event logs (security, application errors) and monitoring for unusual activity