# KNIGHTWATCH



## A View From The Top

KNIGHTWATCH is a highly complex monitoring system that lies upon our management platform. It is a well measured balance between a First Tier Human Response Team and bundles of monitoring tools and techniques that work together to provide an unbeatable service. Because of our framework, Digital Edge is able to insure 100% coverage from all angles from any type of equipment, anywhere-Geographically Independent.

## Our Process...

KNIGHTWATCH collects information from multiple monitoring systems and inputs the information into a centralized repository. Starting here; all of the information gets reviewed on a 10 minute basis, analyzing alerts levels and thresholds. Once our platform LOGIC detects a problem, an alert level is raised. The alert is then populated into the repository display page for the monitoring team to examine.

To minimize the occurrence of false positives, we act on the second alert that is generated. When a first alert is brought up, the monitoring team is notified and examines the signal. Within 5-10 minutes another signal will come in determining whether or not it is an actual warning. In the event that there is an actual warning, an incident will be produced and the specified escalation procedure for that current situation will be followed.

## Our LOGIC...

KNIGHTWATCH is comprised of multiple layers of tools, each used for different pieces of an IT infrastructure that focus on their specific areas. Digital Edge constructed a mixture of methods in order to create a product that would not fail. Our methods include:

- *Constantly analyzing performance statistics on physical servers (Methods vary based on OS)*
- *Using SNMP for Network devices to pull performance information*
- *Constantly confirming servers and network device availability – ICMP*
- *Verifying port availability (requests depend on port protocol)*
- *Constantly checking if monitored processes are up*
- *Scanning event logs to check if there are any monitored events*
- *Hitting clients web pages and performing actions that users would do on a website (which we script) to verify:*
- *How fast systems respond – user experience*
- *If content on pages are correct*
- *If multiple page user's click through produce expected results (for example check out process)*
- *Verifying disk capacities*
- *Calculating database response times*
- *Verifying database capacities and health*
- *Verifying opened ports and checking what services and service versions are running on opened ports*

In addition, we also script "custom" monitoring algorithms to check custom events, business workflow, custom application functionality, etc... We keep full logs of statistics and alerts for historical review or compliance reports; can always produce graphs based on existing statistics and can draw custom graphs showing dependencies of performance alerts helping to troubleshooting bottlenecks

*We collect server performance every 10 minutes,*
*site performance & content every 5 minutes,*
*and check device responses every minute.*

## Alert Levels

We escalate queries into 2 groups, critical and non-critical.
Critical alerts are the notifications that populate in our repository regarding:

- *a process that is down*
- *a device that is down*
- *a port that is down*
- *security foot print changes*
- *disk or database overloads*
- *web pages not loading*
- *pages loading with incorrect content*
- *messages in system logs*
- *hardware critical notifications*

# KNIGHTWATCH



We also classify critical alerts based on custom monitoring logic, such as:

- *Not receiving an email within defined timeframe*
- *Receiving emails*
- *Receiving emails with certain content.*
- *Receiving an HTTP post with certain content.*
- *Receiving # of messages during defined period of time.*

Non-critical alerts are the items that populate into our console, but that we send out to select responsible parties. These are notifications that we only monitor, we do not handle. This could be anything that a client decides to leave responsibilities to either their IT department or another vendor. In this case, our job is to send a notice to the responsible party to make sure it gets escalated. In this scenario, most of our clients find it is very effective to leverage our ability to actually respond to alerts. Unlike automated systems we can actually perform troubleshooting, facilitate recovery processes, start coordinating with vendors or responsible parties, perform initial hardware checkups, and assist hardware vendors in determining cause of failure.

## Our Benefits...

Digital Edge differentiates from competitors by supporting client specifications and by providing an intelligent FIRST TIER HUMAN RESPONSE TEAM to alerts, exceptions, and abnormal operational cases. We learn our client systems, processes, escalation procedures, and integrate with their IT departments to guarantee success. We believe that a service provider should be flexible and be able to work with companies to maximize their goals. By modeling Digital Edge in this fashion, we are able to provide our clients with industry leading support.

Some of our core benefits include:

- *24/7/365 support*
- *100% coverage*
- *20 minutes response time*
- *Intrusion detection, security monitoring, and security footprint*
- *Incident history reporting in real-time (could also be monthly, weekly, daily, etc…)*
- *A customer portal (ability to view al monitoring actions, alerts, and functions in a single consolidated view*
- *Operational history, (log management, events)*
- *Patching history reporting*
- *Controlling change requests*
- *Assistance with compliance regulations and SAS70 certification*
- *A 24/7 human monitoring and response team*
- *Customizable escalation procedures*
- *Ability to use KNIGHTWATCH to monitor current SLA's*

## Our Understanding...

... that clients need a provider that can improve there IT environment and act as their FIRST LEVEL of DEFENSE. Any company can detect a failure; it is bringing a client value by helping expedite alerts, working with hardware/software vendors to access the failures, and working hard to keep the IT as a whole seamless.

## Our Requirements...

List of items we would need to start

- *Number of servers and OS flavors*
- *Number of network devices and ports*
- *List of ports/services*
- *Content monitoring points for web sites including scenarios for user action scripting*
- *List of critical process*
- *Needs for any hardware events*
- *Needs for intrusion detection logging and monitoring*
- *List and description of business processes*
- *Your escalation procedure and/or Level 1 Response*