

The APC NetBotz® Solution

NetBotz is an active monitoring system designed to protect against the physical threats of interruption in distributed, understaffed locations. Three critical data points are monitored—environmental, visual and audio—to deliver the industry's most robust monitoring and protection solution over an IP network.

The system includes a base station appliance, environmental sensors, color camera, and integrated software that assesses the severity of threats and provides notification. The Centralized Management console is a central station platform (application) that can communicate with, configure, manage, archive, and provide trend analysis on data coming from as many as 500 NetBotz appliances throughout a distributed enterprise. Users receive alarms and notification via e-mail, phone or pager, and in the form of text messages or video clips.

Until NetBotz, there really hasn't been a solution that effectively addresses the unique needs of a remote, understaffed location.

NetBotz is the only product available today that leverages your current IT infrastructure and the power of the Web. Our award-winning, patented IP-based technology means no custom install, no hassles, and no extra expense. The solution integrates fully with industry-leading network monitoring systems. Best of all, the system is housed in a self-contained plug-n-play package and can be installed

©2006. All rights reserved. All APC trademarks are property of American Power Conversion. Other trademarks are property of their respective owners. Specifications are subject to change without notice. 998-0295B



NetBotz customers routinely report these immediate results:

- ***Improved response time to incident via troubleshooting, early detection, and automated threat response***
- ***Reduced staffing requirements by augmenting with remote eyes and ears***
- ***Reduced operating costs with early problem detection before cost of remediation becomes significant***
- ***Reduced operating costs through fewer service calls, eliminating unnecessary site visits***
- ***Improved business decision support via trend monitoring***
- ***Improved customer service through increased system and information availability***
- ***ROI in 12 months, often less***
- ***Peace of mind***

APC phone contact: 1-800-788-2208

Ensuring IT Availability In The Data Center And Beyond

Four Key Risk Areas And How To Protect Against Them

APC[®]
Legendary Reliability[®]

NETBOTZ[®]

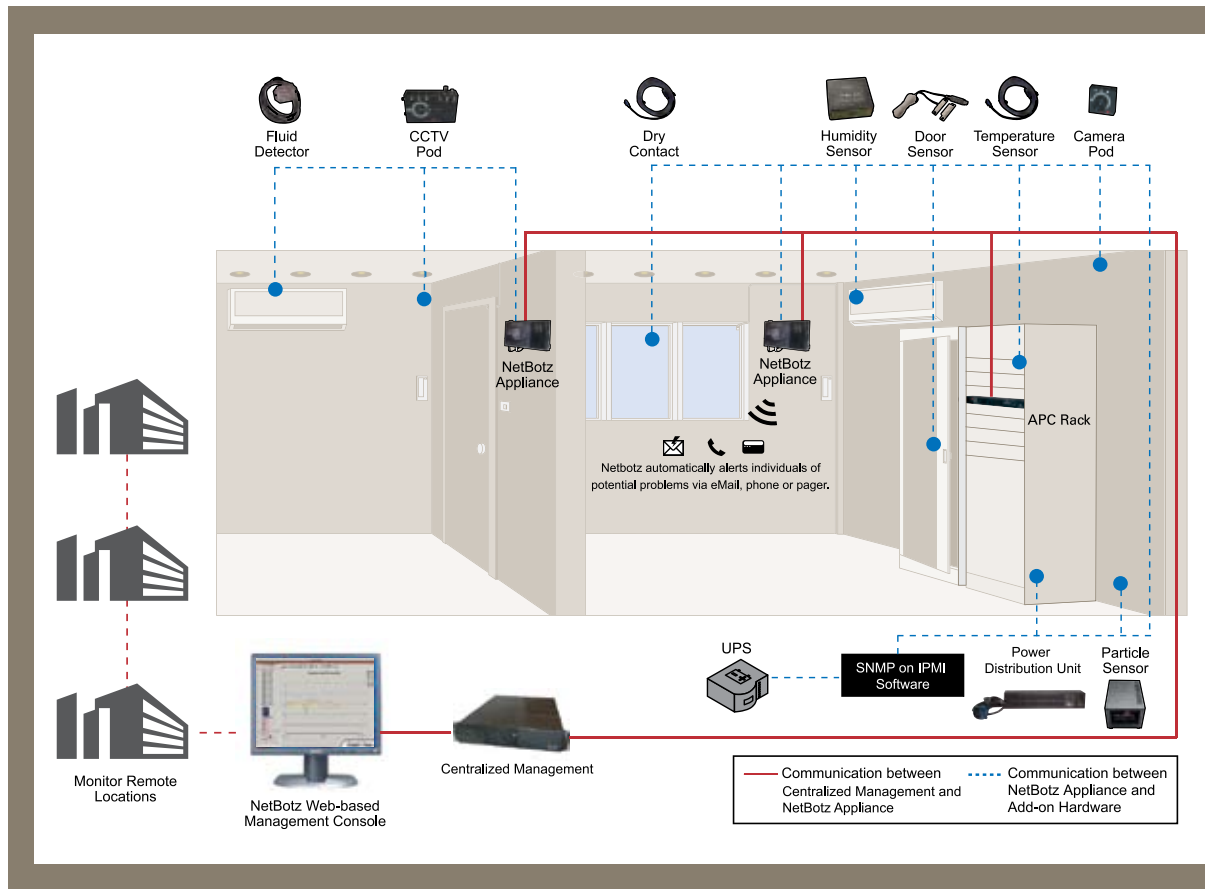
Where are your IT assets?

As an IT professional, you're the first to understand the pressures associated with information and system availability. When everything is functioning properly, you're doing your job. When they go awry, well, let's just say you're the first in line to hear about it.

In today's IT-centric climate, planning for the unexpected is a monumental task. It is tough enough protecting assets in the data center. Your challenges are compounded when you consider that a fast-growing percentage of the IT assets you manage are in less than desirable environments.

- **There are more systems performing mission-critical tasks than ever before.**
- **These systems are being deployed in sub-optimal environments without the proper environmental infrastructure to support them.**
- **Equipment density in these locations is increasing exponentially, producing more stress on ventilation and power.**
- **These systems are often unattended or managed by non-IT professionals.**

The fact is, as much as 30% of a company's mission-critical infrastructure fits into the category of being in environmental conditions that were not properly prepared for technology use, and/or do not have optimal IT supervision.



The four risk areas

1 Environmental disruption.

The #1 cause of downtime for remote locations, environmental problems go beyond worries of fires and floods. Cooling and power are key points of exposure and become more so as equipment density increases.

2 Human error.

We call this the "unspoken epidemic" because no one likes to discuss human error and the tremendous impact it can have on availability. But the fact is, it's the second greatest cause of downtime in remote or unsupervised locations because systems are often housed in janitor closets, wiring closets, and other less than optimal settings.

3 Physical theft.

As assets become smaller and more efficient with hot swappable drives, they become more attractive targets that are easier to steal. Physical attacks against digital assets are often overlooked and are a source of real concern.

4 Sabotage.

Thrust into the forefront of everyone's minds as a result of current events, terrorism is now something each of us must plan for, regardless of the probability. But there are very real threats within your own building from disgruntled employees who are far more likely to strike – and succeed.