VERTIV WHITEPAPER

How to Protect your Data Center from Environmental Threats

Environmental factors like heat, humidity, airflow, smoke, and electricity can be devastating to data center equipment.

Heat Humidity Airflow

Smoke Electricity

Physical Threats to Data Center Infrastructure

Viruses, spyware and network threats get most of the attention, but environmental factors like heat, humidity, airflow, smoke and electricity can be equally devastating to data center equipment, and thus to a company's IT operations.

Depending on the size of a company and its industry, downtime can cost millions of dollars each hour. If your website is down and a competitor's isn't, you've not only lost the immediate transaction, you've also relinquished an opportunity for repeat business. If the outage causes your company to break a service-level agreement with a customer, the associated fees and potential lost business add up quickly. This is especially true in industries with many compliance requirements such as health care and finance.

Every server room and data center – even those of household-name companies and websites – is vulnerable to environmental damage. One of the most recent examples occurred in January 2016 when a flood knocked a large data center in Leeds offline in the U.K.

A few years before that, two extremely popular email platforms experienced outages lasting 16 hours after a cluster of servers overheated. The amount of opportunity lost in both scenarios is difficult to quantify. However, Ponemon Institute's estimate for the average cost-per-minute of downtime is $7,900, which equates to nearly $475,000 per hour. Lost opportunity aside, you must also consider the cost of replacing expensive equipment.

THE AVERAGE ESTIMATED COST-PER-MINUTE OF DOWNTIME IS $7,900, WHICH EQUATES TO NEARLY $475,000 PER HOUR.
- Ponemon Institute

What's clear is that companies of every size must protect their IT investments from environmental threats like overheating, power outages and excessive moisture – all of which may result from flooding, condensation, leaks, poor airflow management or poorly configured computer room air conditioning (CRAC) units.

Preempt Data Center Danger with Environmental Monitoring

Individual servers now come with built-in temperature sensors that issue alerts if the level of heat surrounding the individual unit rises above a certain threshold, or if an internal fan breaks down. But these are hardly enough to ensure that data center climate conditions are optimized for strong equipment performance and ongoing uptime.

Data center temperatures can vary from one zone to another. Even if there's a clear reading for the overall room temperature, the area nearest the output vents may be cooler than the space behind server nodes. Airflow problems in particular are notorious for creating higher temperature pockets of still air in some aisles, precipitating hot spots that can damage sensitive components.

A better approach involves temperature, humidity and airflow sensors installed on or near individual racks and critical devices. Logging and graphing these measurements in real time can help administrators spot long-term trends, such as temperature spikes during peak operating hours or fluctuations when the building's HVAC systems are throttled back on weekends.

Ponemon: Ponemon 2011 Data center Outages Report

With comprehensive monitoring in place, if an internal fan breaks or an air conditioning unit fails, the spike in operating temperature will be noticed quickly. Probes with internal microprocessors are easy to configure and highly reliable.

Similar sensors can track humidity and moisture in the air and the floor. Much like the temperature may vary in a facility, humidity levels might change depending on factors such as where the vents are located in an open-air cooling model, or how much condensation builds up in water-based cooling. In the event of severe moisture buildup causing puddles, or worse, floods, detective cabling laid along floors will immediately alert data center operators.

Airflow is also a potential problem. Sensors built into cabinet-based cooling components can respond to pressure changes that indicate rising temperatures, helping to ensure that fan speeds adjust to maintain proper airflow.

Even sound sensors can help in the early detection and remediation of component failures. For example, a fan that is wearing out may get louder over time, which could be spotted at an early stage on a device that graphs relative measurements. A properly calibrated sensor would send out alerts for either condition and help IT staff resolve the issue quickly.

THE BENEFIT OF MICROPROCESSOR-BASED SENSORS IS THAT THEY CAN BE MONITORED VIA A WEB BROWSER, WITHOUT REQUIRING PROPRIETARY SOFTWARE INSTALLATIONS.

The benefit of microprocessor-based sensors is that they can be monitored via a web browser, without requiring proprietary software installations. With a web-enabled monitoring system, you can measure temperature, humidity, airflow, water leaks, power, door/cabinet position and more, setting alert thresholds and escalation schemes in case an anomaly is detected.

Optimal sensor equipment can send alerts in numerous formats, including SNMP (Simple Network Management Protocol) traps for integration with network monitoring software, email messages to pertinent staff and even text messages.

NOT ALL DATA CENTER ISSUES CAN BE PREEMPTED, ESPECIALLY WHEN THEY RESULT FROM ACTS OF NATURE – BUT THEY CAN BE DETECTED EARLY.

Best Practices for Optimal Monitoring

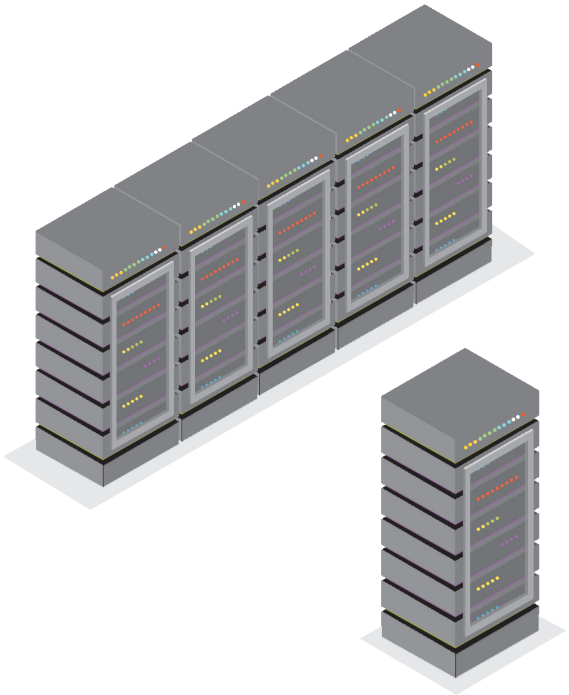
Heat: Temperature sensors should be placed on the top, middle and bottom of individual racks to measure the heat being generated by equipment, and at the air conditioning system's intake and discharge vents to measure efficiency. Sensors should also be placed around critical devices, because the temperature inside a rack-mounted device could be as much as 20 degrees higher than the surrounding area. A probe near the room's thermostat can help monitor what the thermostat is 'seeing' as it controls the air conditioner.

Once these sensors are in place and being monitored centrally from a browser, emergency alert policies should be set up to ensure that the right personnel are informed of potential problems. Remediation procedures should also be mapped out ahead of time.

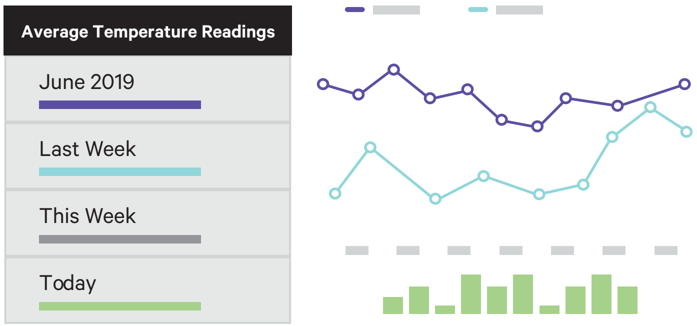
Tracking temperature over time is also helpful. IT managers can review data logs over a weekly or monthly span to identify spikes that occur during off hours or slow periods. Additionally, testing the sensors every month is an important step to making sure the system will function properly if an event occurs.

Beyond simply preventing overheating, doing all of the above can also improve resource efficiency throughout the data center. Not only will data center management be protecting the equipment in their facility, they'll also be protecting their interests by cooling more effectively.

SENSORS SHOULD ALSO BE PLACED AROUND CRITICAL DEVICES, BECAUSE THE TEMPERATURE INSIDE A RACK-MOUNTED DEVICE COULD BE AS MUCH AS 20 DEGREES HIGHER THAN THE SURROUNDING AREA.



IT MANAGERS CAN REVIEW DATA LOGS OVER A WEEKLY OR MONTHLY SPAN TO IDENTIFY SPIKES THAT OCCUR DURING OFF HOURS OR SLOW PERIODS.



Water: Moisture and humidity sensors should monitor for leaks inside cooling equipment, potential leaks that come from nearby pipes, or water caused by a flood or other disaster. Water sensors should be placed at the lowest point (wherever water would tend to pool) on the floor, and underneath any pipe junctions. Air-conditioning condensation trays should also be equipped with sensors to detect overflow.

Power: Electrical failures can cause air-conditioning equipment to shut down even while an uninterruptible power supply (UPS) ensures that servers stay up and running – a sure recipe for overheating a server room in short order. Something like this actually happened in 2014 after a severe rain storm knocked a Toronto data center offline. The UPS kicked into action, but the facility experienced cooling problems, resulting in high temperatures. The best approach is to monitor current coming into the data center, and arrange for an orderly shutdown of IT equipment in case power is lost. The hour or two of downtime, while certainly not ideal, is far preferable to the widespread device failures that would result from overheating.

Smoke: Smoke alarms can trigger power shutdowns, but haven't historically been tied to an alerting system that contacts IT personnel. Alarms may be noticed by building owners – or the local fire department – but the maintenance of sensitive server equipment is not their priority. Here, the best approach is to wire the smoke alarms directly into the climate monitoring and alerting system, essentially extending the functionality of the climate sensors to the smoke alarm.

Doors: A final concern for data center monitoring is unauthorized entry. Dry-contact sensors that detect the opening and closing of a door should be installed at the room entry points and on the doors of server and UPS cabinets. On a busy day, these sensors can send alerts numerous times and present a time-consuming irritation, but managers can configure alerts to account for weekday vs. weekend operations, work hours vs. overnights, and other factors to help reduce the number of false alarms.

The Vertiv Geist Solution to Monitoring

An environmental monitoring solution requires a comprehensive portfolio of sensors and appliances, as well as an intuitive, remotely accessible dashboard that can alert operators up to the second as conditions exceed thresholds.

The Geist Environmental Monitoring products and Rack Power Distribution Units (rPDUs) provide environmental monitoring capabilities to track temperature, humidity, water leaks, power usage, door position and more. While these products come in a wide variety of models and options to fit different requirements and room sizes, they're all based on standard hardware and software monitored via a web browser.

The environmental monitoring units are designed to take up very little space; the largest models are 1U high rack-mount units, while the smallest is only 4 inches long by 1.5 inches wide and deep. For especially large data centers, models with built-in Power over Ethernet (POE) capability can be helpful. The Geist environmental monitoring products have built-in temperature, humidity, and dewpoint sensors. Depending on the environmental monitor or rPDU, a user can connect any where from 4 to 16 external sensors.

Lastly, Vertiv stands behind all of its products, with firmware updates available free on its website, and free technical support available for life.

THE END RESULT IS RELIABLE ENVIRONMENTAL MONITORING BACKED UP BY RELIABLE EXPERTS.

Conclusion

Data center equipment is sensitive and susceptible to environmental damage from excessive heat, moisture and unauthorized access, among other variables. Power outages that knock out cooling systems can lead to overheated servers in a matter of minutes. Should any of these scenarios occur, the result could be higher operational costs, lost opportunity and lower profit margins.

Simple thermostats and server-based temperature sensors are therefore no longer enough to ensure comprehensive protection. It takes temperature and water sensors strategically placed throughout the data center, especially near potential trouble spots, paired with the ability to tie the data from these sensors into a cohesive display, and to set alarm parameters in case a threshold is exceeded. The result of these capabilities is real-time insight that can nourish facility optimization and uninterrupted uptime.

VERTIV™

Vertiv.com | **Vertiv Headquarters,** 1050 Dearborn Drive, Columbus, OH, 43085, USA