Why Data Center and Edge Site Business Continuity Is Now a C-Suite Priority

Vertiv™ Avocent® ADX Platform Provides Remote Access and Centralized Management Capabilities

Business continuity is no longer just the focus of IT and risk management. Now, it's a C-suite priority. Some 50 percent of senior leaders fully support IT's work to prevent and manage unplanned outages[1]. These executives are justly concerned about their organizations' ability to maintain operations, deliver essential services and scale amidst market volatility.

Organizations now need to be ready for anything and everything, including unexpected extended crises. During the pandemic, organizations have scrambled to enable remote workers and digitize business models, products and services, compressing years of work into just a few months. Now, the race is on to drive digital further and faster throughout the business.

IT Teams Need Remote Monitoring and Management Capabilities

So, what does this mean for IT? IT leaders and technology teams are rethinking business continuity and disaster recovery (BC/DR) for a cloud-first, digital era. Data centers are fast becoming a corporate "utility," providing foundational services that ensure the business's very existence and survival[3].

There are multiple strategies that organizations can take to improve BC/DR, including improving infrastructure redundancy, scaling uninterruptible power supplies (UPSs) wherever they're needed, adopting long-lasting lithium-ion batteries and optimizing power distribution design at data center and edge sites[4]. All of these strategies can and do prevent unplanned downtime.

> *"During 2020, organizations experienced an average of 2.4 unplanned total outages at core data centers, lasting a total of 331 minutes, and 2.7 at edge sites, lasting a total of 122 minutes[2]."*

1 "Data Center Outages at the Core and the Edge," infographic, Vertiv, 2021, https://www.vertiv.com/49052c/globalassets/documents/infographics/vertiv-datacenterdowntimecost-ig_322710_0.pdf
2 "Data Center Outages," ibid.
3 "Vertiv Experts Foresee Utility-Like Criticality for Data Centers in 2021," press release, Vertiv, January 5, 2021, https://www.vertiv.com/en-in/about/news-and-insights/news-releases/vertiv-experts-foresee-utility-like-criticality-for-data-centers-in-20212/
4 "Data Center Outages," ibid.

Why Data Center and Edge Site Business Continuity Is Now a C-Suite Priority

Vertiv™ Avocent® ADX Platform Provides Remote Access and Centralized Management Capabilities

However, the ongoing pandemic has proven that IT teams also need secure remote monitoring and management capabilities to scale their time and talent, ensure continuity of services and reduce risks on an ongoing basis. Here's how Vertiv™ Avocent® ADX Ecosystem is uniquely designed to help your IT teams improve your organization's BC/DR:

Trade physical for remote access: IT staff can no longer count on their ability to access data center sites at will. In addition, edge sites may be located across multiple geographies, meaning that teams can't easily travel there to perform onsite support. With Vertiv™ Avocent® ADX Platform, IT can securely and remotely access devices across sites, controlling, configuring, updating and troubleshooting them.

Ensure high availability of compute resources: As your business becomes more digital, ensuring high availability of online services is essential, at both the core and the edge. While hyperscale cloud and colocation facilities can easily move workloads to another site in the event of an emergency, the same is not true for edge sites. However, edge sites are becoming more integral to the business as they support more users, enable critical applications, and gain hyperscale and enterprise-level capabilities. It's absolutely vital, then, to ensure constant connectivity to all your sites. Unplanned outages or latency harm the customer experience and take workers offline, causing reputational harm, lost productivity and revenue losses.

While IT teams build redundancy into core and edge sites, even redundant infrastructure such as UPSs and their batteries can fail if not monitored and managed effectively. With Vertiv™ Avocent® ADX Platform, you gain a centralized platform for managing critical devices, including servers, service processors, and virtual machines and containers; routers, switches, firewalls and storage device; and environmental and device sensors. With dozens of sensors on a single rack, the IT team can easily detect and address device issues before they harm the business and cause an outage. If corporate networks and storage aren't available, IT
staff can use out-of-band management capabilities to perform routine maintenance and troubleshoot issues, ensuring exceptional edge site performance.

Scale with business growth: It's likely that the demands on your IT organization are outpacing your ability to add staff and budget. If your team is using manual processes to manage devices, they're also experiencing significant work strain, which could introduce delays and errors into your processes.

Vertiv Avocent ADX Platform provides secure remote access, enabling your existing team to manage more sites and devices. IT staff can tap the automated processes Vertiv Avocent ADX Platform provides to configure and update devices at scale. In addition, you can update Vertiv Avocent ADX Platform without taking the platform offline. All of these capabilities can help you improve performance and uptime.

Design for simplicity: As you add more devices, you'll also need to navigate a wide array of vendor tools. Vertiv Avocent ADX Platformenables your team to simplify processes, using a single platform to manage all your devices. You also can streamline further with Vertiv™ Avocent® ADX Platform, by using a single IP to access all your devices, reducing power and cabling with power over ethernet (PoE), and harnessing APIs to accelerate the deployment and configuration of devices.

Improve device security: Remote work has increased cyber risks, as attackers take advantage of IT's lack of holistic visibility into expanded network activity and new processes. IT teams need to ensure the security of their processes, while also monitoring devices for anomalies that could indicate unauthorized access and manipulation.

Vertiv™ Avocent® ADX Platform provides a private network for all device operations. It safeguards access to IT devices, enabling your IT team to control and restrict device operations. Vertiv Avocent ADX Platform also secures keyboard, video and mouse (KVM) and serial sessions and provides a detailed user history of actions. With Vertiv Avocent ADX Platform, your IT team can be confident that through role based authorization, only approved IT users are managing and changing device configurations. You also can grant and control 4K KVM over IP access to key users who need access to on-premises applications, enabling critical business actions in a secure environment.

"60 percent of enterprises will phase out most of their remote access VPNs in favor of zero-trust architectures. That's because VPNs are used in 68 percent of major incidents using remote access tools[5]."

Conclusion

As demand for data center and edge resources grow, IT organizations need to rapidly evolve management processes. Vertiv Avocent ADX Ecosystem helps your IT team build processes for simplicity, scale and accuracy. With the centralized visibility and control, secure processes and automation that Avocent ADX Ecosystem provides, your IT organization will be able to deliver the high availability and connectivity that your business seeks. By so doing, you will serve as a valued partner to the business in ensuring the stability of key operations amidst challenging conditions.

Get started with Vertiv™ Avocent® ADX Ecosystem today.

5 Alex Wells, "How to Choose a Zero Trust architecture: SDP or Reverse-Proxy?," blog, Cloud Security Alliance, February 15, 2021, https://cloudsecurityalliance.org/blog/2021/02/15/how-to-choose-a-zero-trust-architecture-sdp-or-reverse-proxy

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

AV-20205 (R01/23)