VERTIV EBOOK

4 Ways to Improve Data Center Security This Year

Reduce Risks by Automating Processes and Using Secure Vertiv Solutions

Data center owners and operators are bringing on new capacity to meet voracious business demand and enable business's digital transformation. In the U.S. alone, there are 526 megawatts under construction.[i] *As a result, colocation providers, hyperscalers, and enterprise IT and data center teams are managing a larger footprint than ever. Much of this work is happening remotely, creating new pressures and challenges to navigate.*

> *"Among IT and security teams' top priorities are improving security* **(69%)**, *and environmental management* **(65%)**, *power/energy management* **(61%)**, *and asset tracking/ management* **(60%)**.[ii]*"*

As a result, data center and IT teams are rapidly evolving their approach to device management. They'd like to simplify processes by adopting best-of-breed platforms and tools that:

- Enable secure remote access to devices
- Improve network visibility and control
- Centralize and standardize IT management
- Protect data by using secure information handling tools

The time to start is now. As companies' digitization strategies accelerate, infrastructures are becoming more complex and introducing new gaps others can exploit. Data center and IT teams can use centralized, automated processes to bring new levels of consistency and control to management practices. By so doing, they can deliver the high availability and resiliency their business demands.

Enable secure remote access to devices

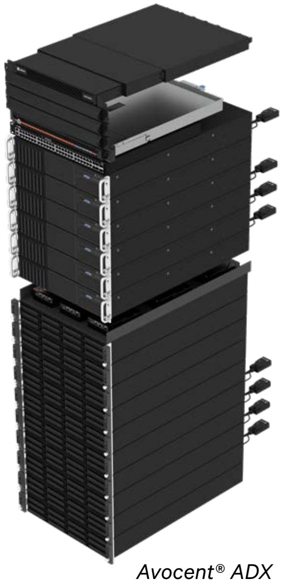
Data center and IT teams need to view, access, control, and manage a wide array of servers, networking, and serial-based devices that make their business run.

While these teams used to work onsite, many staff are now working remotely due to the pandemic – and will likely do so indefinitely. These users are prime targets for attacks, as they have elevated privileges malicious outsiders can use to gain access to organizations' networks. Compromised credentials were used in 20 percent of all attacks in 2021.[iii] It's no surprise then, that organizations are adopting an identity-first approach to security.[iv]

> *"Misused credentials are now the top technique used in breaches.... Identity infrastructure must be properly configured, maintained and monitored with an elevated importance."*
>
> *- Source: Gartner* [v]

Teams can use Vertiv solutions to:

- **Provide secure remote access to devices based on role and group:** IT administrators can use the Vertiv™ Avocent® ADX Ecosystem to authorize users to perform key duties aligned with their roles, such as monitoring and managing specific types of devices. IT administrators can grant privileges to different teams, such as IT, security, applications, and testing, that need to access servers and other networking access devices. Avocent ADX Ecosystem integrates seamlessly with Vertiv™ Avocent® ACS 8000 Serial Console to provide similar secure access to serial-based devices, so that teams can manage devices, gather data, and automate configurations.
- **Centralize third-party authentication:** IT teams can dynamically assign privileges to key third parties
- **Ensure consistency in granting access:** Most organizations use the concept of least-privilege granted, while also empowering users to perform authorized roles. By so doing, they can avoid the issues that occur when access rights aren't proactively managed, such as when individuals roam across networks and perform unauthorized actions on devices.



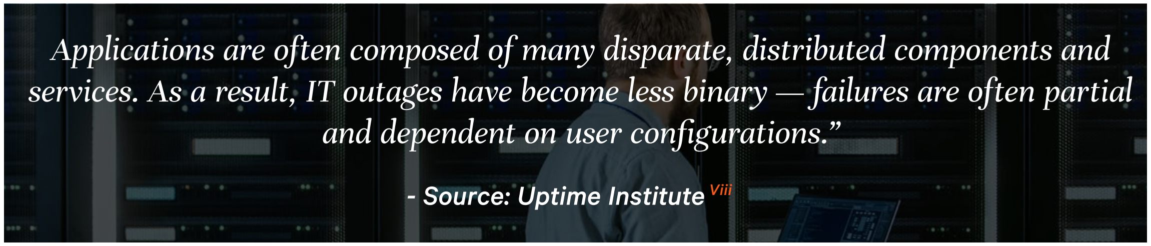
Avocent® ADX Ecosystem

Avocent® ACS 8000

Improve network visibility and control

Across enterprise data centers and edge sites, hyperscalers' thousands of cloud services, and colocation provider's infrastructure, networking is happening everywhere. By 2025, 85% of infrastructure strategies will integrate on-premises, colocation, cloud and edge delivery options, compared with 20% in 2020.[vi] That's because IT teams are placing workloads strategically to drive the best outcomes.[vii]

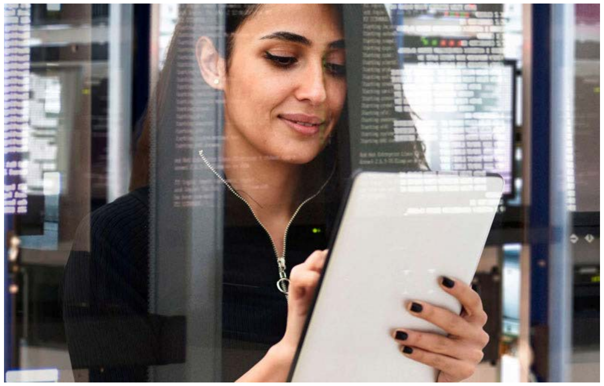
Data center and IT teams need to improve visibility and control, wherever they work and whatever they manage. That's even more important at third-party providers, as human error or exploited security gaps can cause business-critical impacts and harm tens of thousands or millions of customers.



> *Applications are often composed of many disparate, distributed components and services. As a result, IT outages have become less binary — failures are often partial and dependent on user configurations."*
>
> ***- Source: Uptime Institute*** [viii]

Teams can use Vertiv solutions to:

- **Use a single point for authentication:** Teams can use Avocent® ADX Ecosystem to gain single point access to server and other IT devices, while Avocent® ACS 8000 also provides aggregated access to serial-based devices. By centralizing visibility and access, data center and IT professionals can work more efficiently, performing both in-band and out-of-band management duties.
- **Control what users can see:** Avocent ADX Ecosystem enables teams to control the devices individual users can see. This is especially critical for colocation or hyperscale providers, which will want to segment access so that customers can only see their own devices. Similarly, superusers can control what teams at other business units, third parties, and other authorized parties can see.

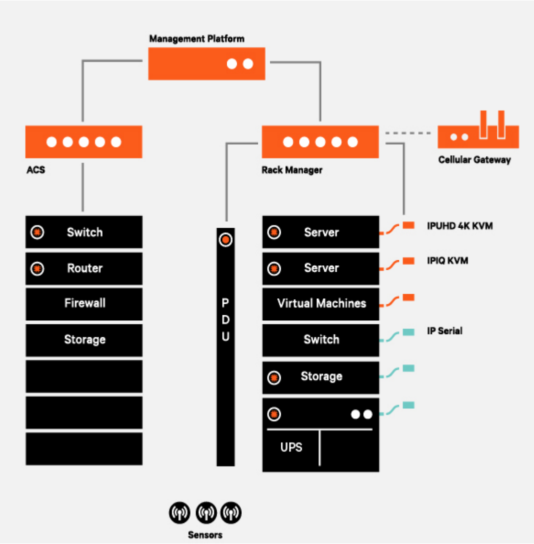


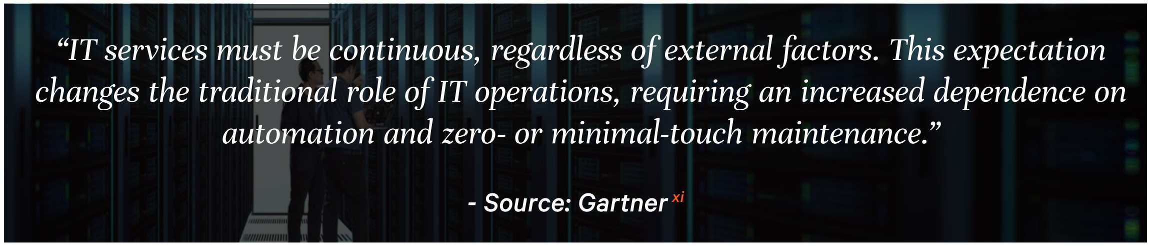
- **Audit user behavior:** Many companies need to provide reporting on user access and device actions for auditing and regulatory compliance purposes. The Avocent ADX Ecosystem enables administrators to monitor who does what, when, and how. They can monitor every keystroke that users make, when accessing devices via Avocent ACS 8000. It's also easy to set alerts for strings to get early-warnings of high-profile actions. Finally, IT staff can provide access to online and offline data logging with time stamps from Avocent ACS 8000 for analysis and reporting purposes.

Centralize and standardize IT management

Network device proliferation has created greater complexity for data center and IT teams. Most vendors offer their own tools for managing their devices. As a result, 64 percent of enterprises now use between four and 10 tools to manage networks.[ix] Using too many tools can introduce security gaps into processes or increase the risk of human error, both from actions that are taken and those left undone.

IT and data center teams want to centralize and automate the management of server, networking, and serial devices.



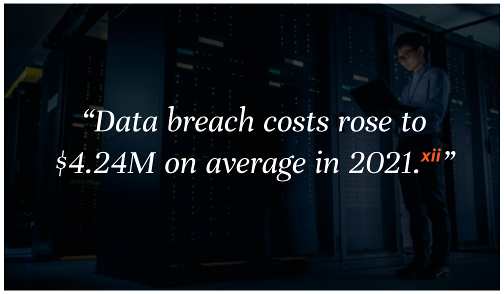


> *"IT services must be continuous, regardless of external factors. This expectation changes the traditional role of IT operations, requiring an increased dependence on automation and zero- or minimal-touch maintenance."*
>
> *- Source: Gartner*[xi]

Teams that deploy Vertiv solutions can:

- **Aggregate devices to improve security:** Connecting each device to the internet dramatically increases the attack surface, increasing risks. Teams can use the Vertiv™ Avocent® ADX Rack Manager to connect up to 48 devices. They can then hide them from network view and outside access by putting them on a private network. Only authorized users can then access the devices and perform the actions they're authorized to do.
- **Quickly diagnose and address any issues:** IT teams are expected to deliver continuous uptime and application availability to enable digital business processes. As a result, the pressure is on to proactively identify and address issues, as well as identify and resolve network outages. Teams can utilize Avocent® ACS 8000 to perform in-band and out-of-band management processes, using cellular, Ethernet, or analog modem connectivity to gain access to devices.
- **Automate firmware upgrades:** Out-of-date firmware is a prime target for cybercriminals, who are actively monitoring networks for these issues. Yet, despite this reality, security teams say they spend 41 percent of their time on manual firmware patches that could be updated. IT and security can use Avocent ADX Management Platform to automate server firmware upgrades, closing this security gap for good.

Protect data by using secure information handling tools



"Data breach costs rose to $4.24M on average in 2021.[xii]"

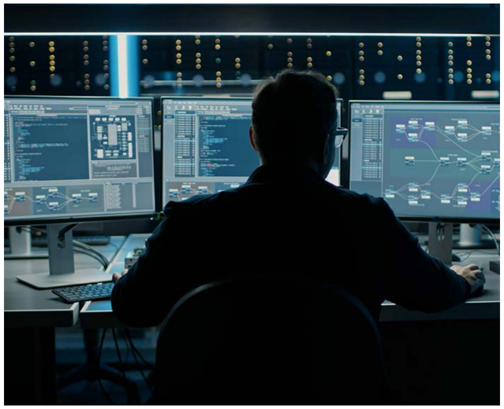
Data is the lifeblood of industries, powering key operations and driving business growth. Companies produce and manage a wealth of confidential and sensitive data that is typically tightly governed by industry regulations.

Biopharmaceutical companies want to protect drug research and data; leaks can harm their ability to keep and win regulatory approval for their drugs and lose ground to competitors. Financial services teams work with customer and trade data that is protected by regulations such as GDPR, GLBA, NYDFS, and PCI-DSS. Government workers need to use sensitive, classified, and non-classified data that travels over network such as JWICS, SIPRNet, and NIPRNet. Finally, in healthcare, clinicians access electronic healthcare records that contains personally identifiable information (PII) and personal health information (PII) protected by HIPAA.

Whatever the industry, Vertiv™ Cybex™ SC Secure Desktop KVMs can help workers to access sensitive data, within the bounds of strict security controls:

- **Easily navigate among information sources:** Cursor Navigation Switching enables workers to securely view information with multiple classification levels on the same screen. That is especially ideal for sensitive government operations, such as managing critical infrastructures or performing intelligence or military work.

- **Prevent information cross-contamination:** Information gets contaminated and potentially leaked when users take unapproved actions. Organizations can use Cybex™ SC Secure Desktop KVMs to prevent copying, cutting, and pasting of information across classification levels. While government agencies need this type of protection routinely, other industries could use it for work such as reviewing confidential product development data or target company financials during M&As.



- **Prevent device tampering:** Cybex SC Secure Desktop KVMs offer the following safeguards to prevent tampering. Active tamper detection causes the KVM to become inoperable if its seals are penetrated. In addition, locked firmware prevents users from performing unauthorized actions on KVM operations.

Conclusion

Network complexity is growing, creating pressures on data center and IT teams to streamline current processes and improve security. These professionals can help accomplish those goals by enabling secure remote access to devices, improving network availability and control, centralizing and standardizing IT management, and protecting data by using secure information handling tools.

Let this be the year you benefit from increased security and control, bring greater consistency to management processes, and simplify daily administration with automation.

Improve data center security four ways with Vertiv.

Learn more about:

Vertiv™ Avocent® ADX Ecosystem

Avocent® ACS 8000 Serial Console Server

Vertiv™ Cybex™ SC Secure Desktop KVMs

Resources

Want to learn more about improving data center security? Check out these Vertiv resources:

- Enable Workers to Safely and Securely Handle Sensitive and Confidential Information
- Setting Granular Controls for IT Networking Devices Is Now Easier Than Ever
- How IT and Cyber Teams Can Work Hand-in-Hand to Strengthen Server Management Security

[i] "Data Centers," chapter 8, U.S. Real Estate Market Outlet 2022, report CBRE, undated, https://www.cbre.com/insights/books/us-real-estate-market-outlook-2022/data-centers#.

[ii] Ibid.

[iii] "How much does a data breach cost?" webpage, IBM, https://www.ibm.com/security/data-breach

[iv] Kasey Panetta, "The Top 8 Security and Risk Trends We're Watching," article, Gartner, November 21, 2021, https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021

[v] Ibid.

[vi] Add reference

[vii] David Cappuccio, Henrique Cecci, Your Data Center May Not Be Dead, but It's Morphing, Gartner, report, September 17, 2020, https://www.equinix.com/resources/analyst-reports/data-center-not-dead-morphing-changing?

[viii] Rich Miller, "The Eight Trends That Will Shape the Data Center in 2022," Data Center Frontier, January 10, 2022, https://datacenterfrontier.com/the-eight-trends-that-will-shape-the-data-center-industry-in-2022/

[ix] EMA: Network Management Megatrends, 2020, Kentik, page 4, https://www.kentik.com/resources/ema-network-management-megatrends-2020-report/

[x] "New Security Signals study shows firmware attacks on the rise; here's how Microsoft is working to help eliminate this entire class of threats," article, Microsoft, March 30, 2021, https://www.microsoft.com/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/

[xi] "Gartner Top 6 Trends," ibid.

[xii] "How much does a data breach cost?" IBM, ibid.

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