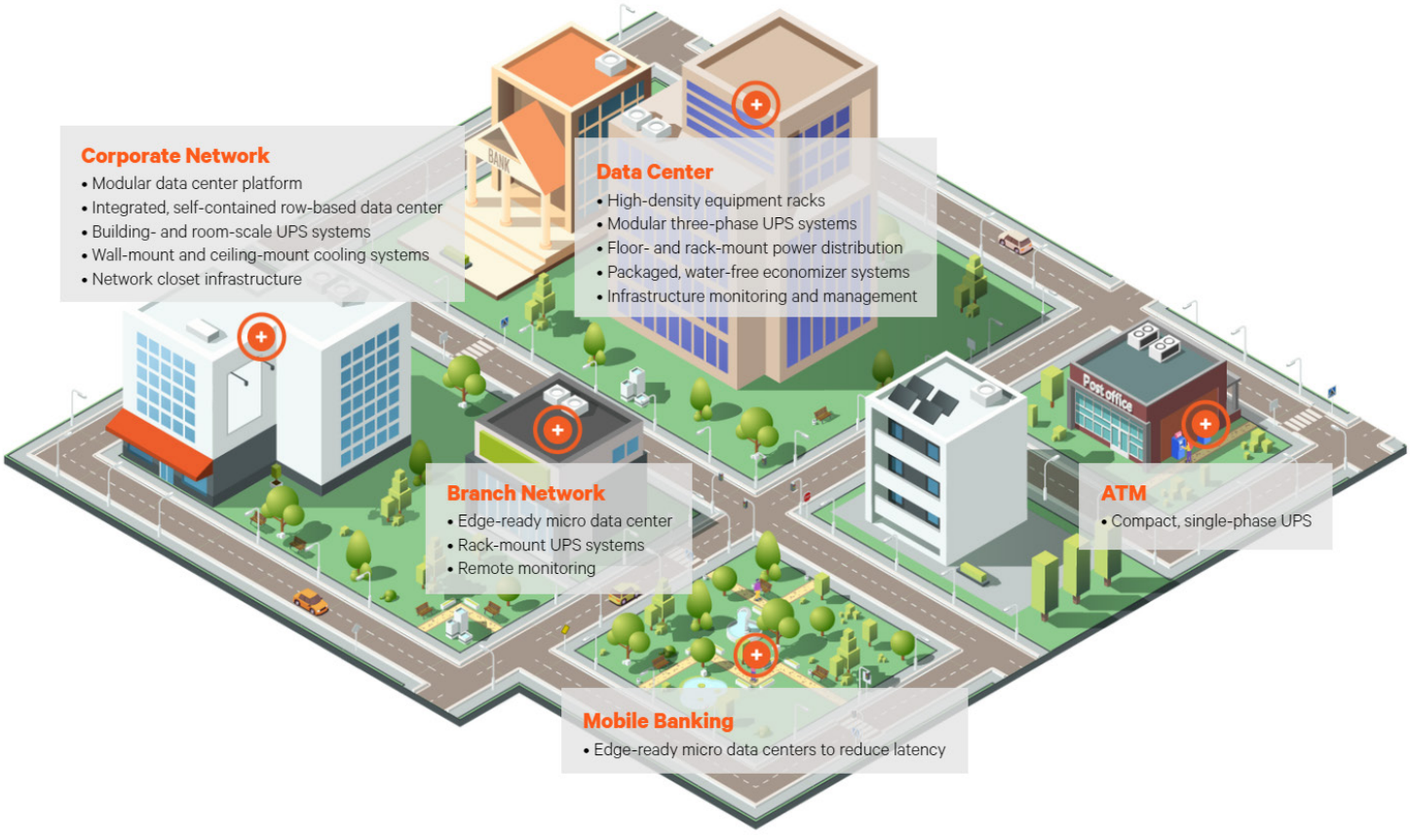
Securing Your Banking Edge

The financial world is rapidly changing, from disruptive service offerings to new forms of currency. At the same time, customers consider around-the-clock access to mobile banking and other digital tools the norm. Managing operations across all spaces requires seamless data integration, which is often not possible with outdated legacy infrastructure. Further complicating matters is the lack of in-house IT expertise.

Meeting these challenges requires a protected, resilient IT network. There's a need for availability and security across the financial ecosystem, but changes are having their biggest impact at the branch level, as one of the key touchpoints to the customer. Downtime at the branch can not only damage customer relationships but can be extremely costly!

Dispersed banking environments need to ensure the security of critical infrastructure in all locations with appropriate physical security measures, as well as access, control, and visibility into IT systems.

Banking Critical Infrastructure



Security Checklist:

- All systems and software applications should be behind a virtual private network and not accessible from the public internet.
- No systems should use factory default credentials.
- Use strong, long passwords or passphrases in accordance with your region's standards, such as the **National Institute of Standards and Technology Special Publication SP 800-63B guidelines** in the United States.
- Credentials for all UPS units and similar systems should adhere to strong password length requirements and adopt login timeout/lockout features.
- A dedicated, secure space for equipment or enclosures can ensure the physical security of equipment.
- Leverage key IT management solutions to assure visibility and control of any issues at the branch level.
- Make sure your IT manager has secure remote access and management to provide visibility of all IT assets and to control the physical access to equipment.

Vertiv Solutions:

The **Vertiv™ Liebert® GXT5**, an online double conversion UPS solution, offers premium power outage protection and continuous power conditioning in a compact and flexible rack/tower design, helping protect your bank branches against downtime. Its remote management capability makes it ideally suited to protect your bank's critical infrastructure at the edge. And the Liebert GXT5 UPS is now available with **lithium-ion battery technology**, providing a longer life and the lowest total cost of ownership over the lifetime of the UPS.

Financial institutions cannot afford any kind of downtime since they support 24x7 online transactions. Having a reliable power distribution unit that also provides redundant power can help your IT equipment stay online. All **Vertiv™ Geist™ rack power distribution units (rPDUs)** undergo individual testing for reliability, helping ensure your business is powered by a rPDU that passes the test.

Computing at edge sites in banks is becoming more prevalent and critical, but space is limited, and on-site staff are usually not IT experts. The **Vertiv™ Avocent® ACS 800 Serial Console** ensures network security at your bank branches while delivering visibility and connectivity at all times.

Efficiently manage your IT infrastructure with the **Vertiv™ Avocent® ADX Ecosystem**, which provides network resiliency. It is capable of deploying feature upgrades without requiring downtime, ensuring continued productivity. Additionally, the ecosystem allows you to securely manage your devices across the network, supporting more than 100 simultaneous users.

With full protection against data leakage, **Vertiv™ Cybex™ Secure MultiViewer KVM Switches** provide reliable and secure switching for IT applications in office environments and operation centers. Fast switching among desktops also enhances productivity.

Contact a Vertiv partner today for a solution that is right for your financial institution.

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