Financial Services Connectivity & IT Infrastructure **Playbook**

SEGRA®

SEGRA.COM

Delivering Scalable, Secure and Personalized Financial Services Starts with a **Solid IT Foundation.**

The “one-size-fits-all” approach does not work when selecting IT infrastructure services intended to keep your financial services institution ahead of the competition. The right combination can enhance community engagement, but it’s important to choose wisely. With so many options, analysis paralysis can set in fast.

Let the nature and purpose of your business be your guide.

There’s one thing successful institutions have in common: a sound technology game plan focused on connectivity, cybersecurity, voice, cloud, and colocation. We created this playbook to help you sort through the noise.

SEGRA

A Winning Technology Lineup.

Choosing the right IT foundation for your business is critical. Given the high stakes, it can also be intimidating. There are many options to build your foundation across four key domains.

THE PLAYING FIELD

CONNECTIVITY

The foundational infrastructure enabling fast, secure transactions and communication across branches, data centers, and client touchpoints.

CYBERSECURITY

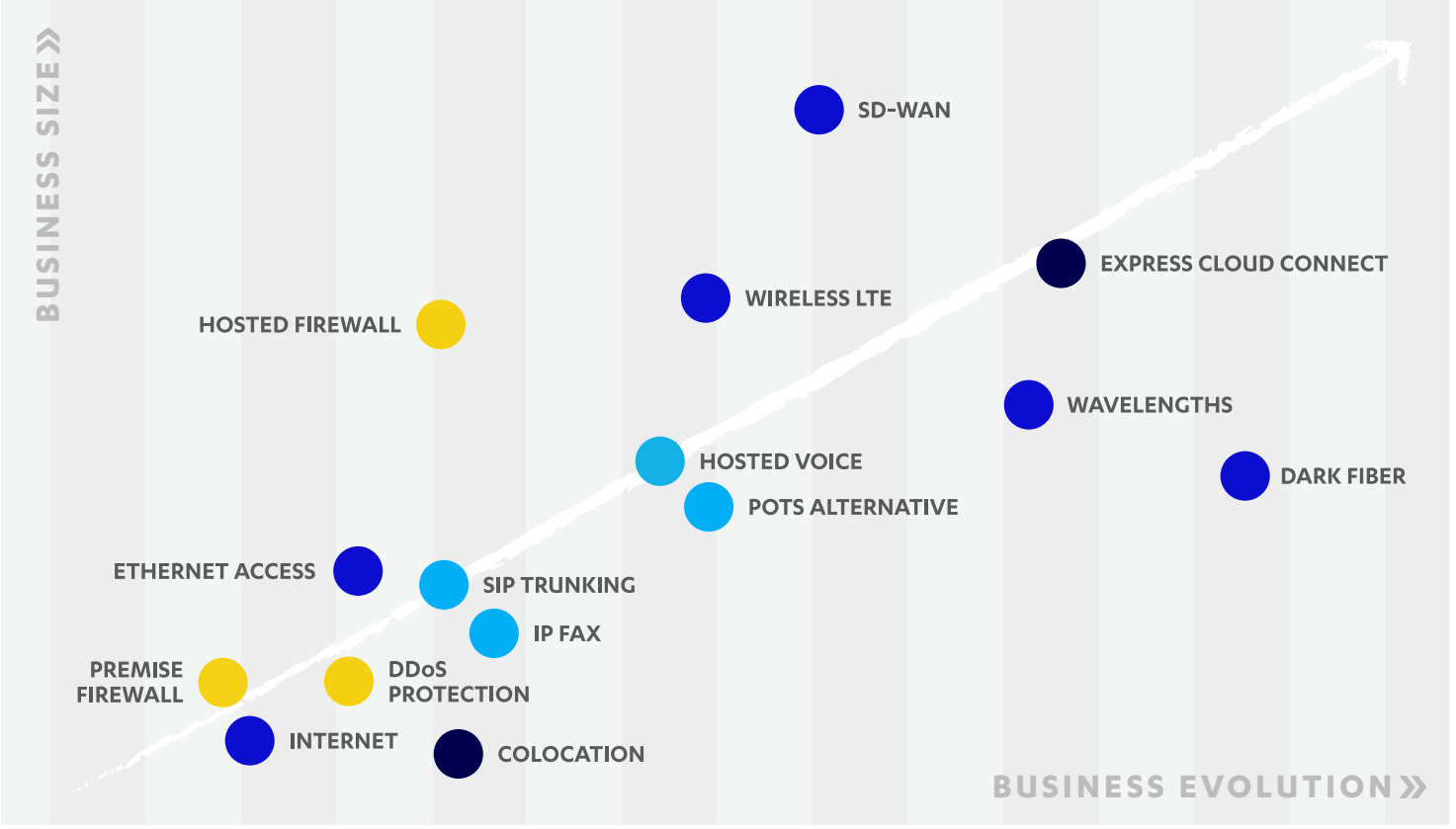
Robust security solutions to protect sensitive data and critical systems from accidental exposure or malicious exploitation.

CLOUD & COLOCATION

Secure, reliable data center solutions for traditional and hybrid environments, and a fast, dedicated connection.

VOICE

Combined voice and data solutions and tools to enable shared, seamless conversations across multiple platforms.



SEGRA

Modern financial services institutions need fast, reliable and secure IT in order to thrive.

- Hyper-personalizing services and automating operations through AI while defending against AI-powered fraud and cyber attacks
- Processing real-time payments and instant transactions across domestic and cross-border networks
- Migrating to hybrid and multi-cloud environments while maintaining operational resilience
- Protecting sensitive financial data end-to-end against ransomware, deepfake fraud, and sophisticated cyber threats
- Enabling and securing open banking connections and API integrations
- Maintaining regulatory compliance across evolving frameworks like DORA, PCI DSS V.4, and data sovereignty requirements
- Digitalizing smart retail branches with seamless omnichannel experiences

Successful execution across these strategic imperatives supports growth while maintaining regulatory compliance.

A solid IT infrastructure foundation must be flexible enough to support evolving demands, scalable enough to accelerate data transfers and secure enough to thwart bad actors.

USE CASE 1:

Large Banking Institution

Tier 1 banks operate at massive scale, processing millions of transactions daily across global networks. Meeting customer expectations and regulatory requirements demands a sophisticated IT strategy built on high-performance connectivity, including dark fiber for ultra-low-latency trading connections, internet for branch operations, and SD-WAN for secure multi-site networks. Combined with robust security, redundant systems, and reliable voice services, the right technology foundation ensures both operational excellence and the personalized service that builds lasting customer relationships. A "belt and suspenders" approach to network redundancy guarantees maximum uptime, protecting both reputation and revenue while maintaining the competitive edge needed in the digital-first banking landscape.

CONNECTIVITY: Ethernet Access + DIA + Wavelengths + SD-WAN

- A fast, secure, private ethernet network provides the foundation for delivering mission-critical applications and highly sensitive client data to branches and offices across the institution.
- For high-bandwidth data center interconnections, disaster recovery links, and cloud connectivity requiring dedicated circuits with speeds from 10 Gbps to 400 Gbps, wavelengths deliver the capacity and low latency needed for large-scale data transfers, real-time financial transactions, and mission-critical operations.
- SD-WAN load balancing ensures connectivity never goes down and optimizes network performance across all locations.

CYBERSECURITY: Firewall + DDoS Protection

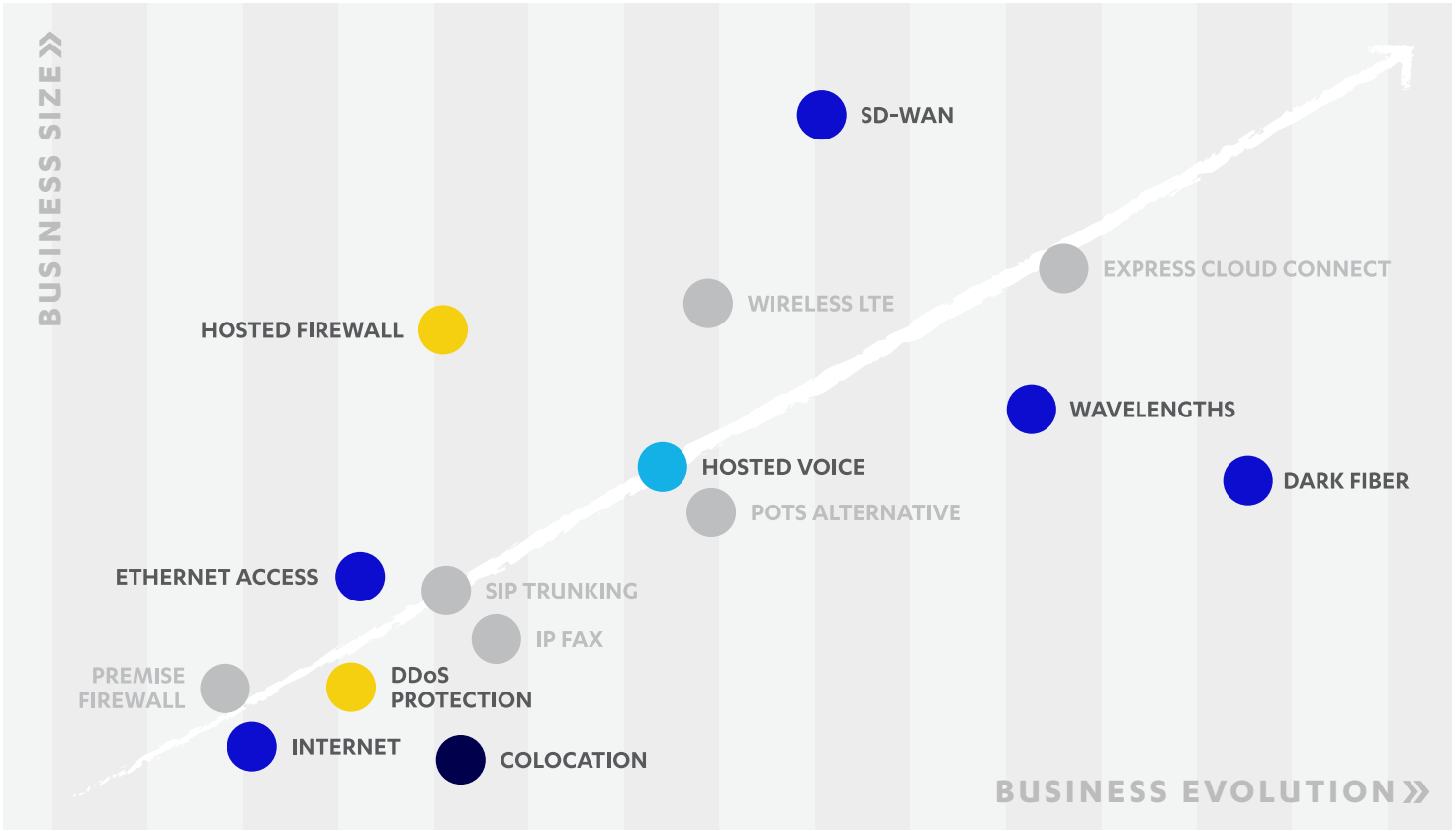
- Nothing tarnishes a bank's reputation and risks regulatory fines like data breaches. A comprehensive approach that keeps sensitive information private starts by preventing bad actors from breaching the network perimeter.
- A bank's website is a visible target. Bad actors often target them to tarnish their brand and distract scarce IT resources from other more devious cyberattacks. DDoS mitigation deters these bad actors, ensuring your security team stays focused on the right priorities.

CLOUD & COLOCATION

- Secure, reliable data center solutions for traditional and hybrid environments, and a fast, dedicated connection.

VOICE: Hosted Voice

- While digital banking services are the primary way most consumers prefer to connect, branch offices and phone services continue to play an important touchpoint for clients. Make sure your phone conversations are clear and dependable to deliver a positive impression.



SEGRA

USE CASE 2:

Regional Credit Union

Serving the community's financial needs and sustaining growth means moving away from a transactional orientation and delivering a broad portfolio of services tailored to the needs of local consumers and businesses.

CONNECTIVITY: Internet + SD-WAN + Wireless LTE

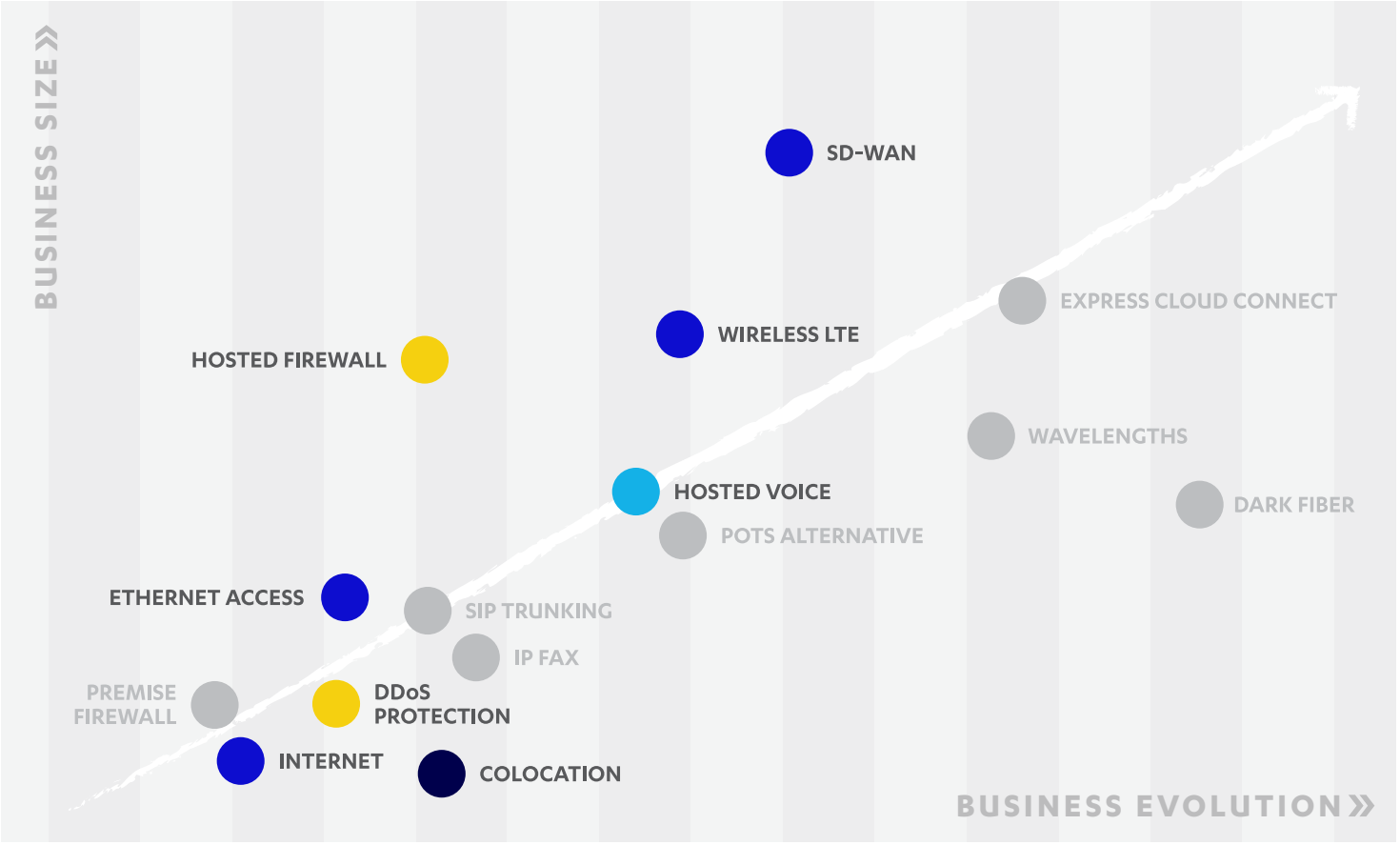
- Delivering interactive services and ensuring systems function to spec for bank branches demands the guaranteed bandwidth and symmetrical service delivered by fiber-based dedicated internet services.
- An SD-WAN overlay guarantees connectivity for hard-to-reach locations, providing optimal capacity utilization and optimizes the resilience of multiple connections for any eventuality.

CYBERSECURITY: Firewall + DDoS Protection

- Financial services institutions are consistently one of the top two targets for bad actors. Client data is highly prized, and keeping it secure mut be a top priority. A comprehensive approach must include a strong firewall to keep bad actors at bay.
- Web properties and IT connections must also pre-empt "smoke screen" DDoS attacks designed to distract credit union's IT resources and tarnish their reputation with clients.

VOICE: Hosted Voice

- Phone banking is a key element credit union customers continue to rely upon. Never miss a call and stay connected with your customers. Deliver superior support with the confidence your conversations are private and your connection is clear.



What's **Your Play?**

These are the most widely used connectivity plays successful financial services institutions swear by. Refer to this playbook every time you're thinking of adopting new innovations and use these plays as building blocks to put together your technology game plan. It can help you think through every move to ensure your business is set up for success.

The plays contained in this document address broad use cases. Some products in a play may not be ideal for specific use cases or situations, and some products not included in the playbook may work better for other business scenarios.

Segra offers a broad portfolio of technology services and will help you design a winning technology game plan tailored to your unique business needs.

Let's start a conversation today.

10/25