VECTORUSA

```
h3>Ready to Ship</h3>
  <p class="text-muted">
</div>
</div>
<div class="col-lg-3 col-
  <div class="service-box">
    <i class="fa fa-4x fa-
    <h3>Up to Date</h3>
    <p class="text-muted">
  </div>
</div>
<div class="col-lg-3 col-
  <div class="service-box">
    <i class="fa fa-4x fa-
    <h3>Made with Love</h3>
    <p class="text-muted">
  </div>
/div>
```

Infrastructure You Need to **Take Your Business Digital**

As the business environment that developed in 2020 has shown, digital transformation isn't just a trend. Every employee—from corner office executives to the most junior of employees—had to make dramatic shifts in how, where, and when they got their work done. Fortunately for them, IT departments were able to make it all happen.

However, the way that many organizations began (or accelerated) their digital transformation journey likely was not the way that they would have preferred to achieve such dramatic change. Now that the digital dust has fallen in the wake of this dramatic change, organizations are trying to find their technical footing and maintain the right balance between productivity and security, especially as organizations continue to scrutinize budgets.

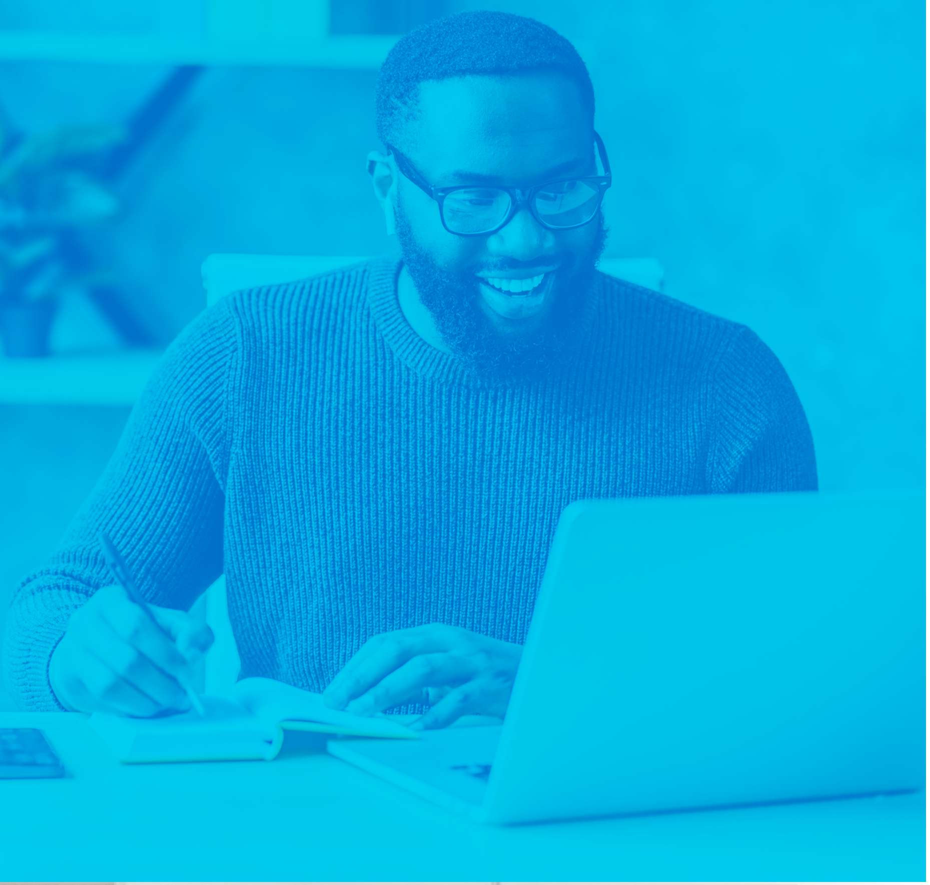
So how can your organization find that sweet spot and put the right infrastructure into place, to take your business digital the way you and your employees need it?

> Every employee—from corner office executives to the most junior of employees—had to make dramatic shifts in how, where, and when they got their work done.

Defining the Foundation of Your Digital Strategy

No matter the size and scope of your business, IT leaders have to walk a fine line between usability and security. How can you design and employ technology platforms that enable employees to be productive, collaborative, and efficient while also ensuring your data and digital assets are protected?

Instead of thinking of this as a zero-sum challenge or beginning with a complex system of hardware and software, keep things simple. This is especially important when you consider usability. Work with your business partners to find out what your employees are trying to do, and make it easy for them to do.



Some of the steps in this usability evaluation process include:

- ☑ Defining core business functions and recovery requirements
- ☑ Defining key business roles and responsibilities
- ☑ Identifying and prioritizing key business systems
- ☑ Documenting key functional and performance requirements

Although this isn’t an exhaustive list, it will give you the information that you need to strike the right balance between what your users need to achieve your mission and the potential security risks that they may be facing.

Key Systems That Balance Both

When it comes to creating balance between usability and security, what security tools and systems does your organization need to help implement that balance? Here are five key components that should be a part of your digital strategy.

1. Network Access Control (NAC)

Organizations now have to account for dramatic growth of mobile, tablet, and end-user devices accessing their networks, locally and remotely—and the security risks that come with it. A network access control (NAC) system can provide the visibility, network access control, policy management, and security compliance that you need to protect your network security infrastructure.

2. Identity and Access Management (IAM)

Identity and access management (IAM) policies and tools give organizations the power to identify and validate users, applications, systems, and devices attempting to access their digital assets. Then they can grant the appropriate authorities and permissions. Some IAM solutions can also be used to further define and enforce policies for user groups that include roles and responsibilities, streamlining and enabling access while simplifying back-end management.

3. Endpoint Protection

With a distributed workforce and a wide range of business platforms, unified endpoint management tools help with the administration of multiple end-user devices into one system. They facilitate the configuration, management, and monitoring of mobile, tablet, and computer systems, streamlining device maintenance and policy enforcement.

4. Intrusion Detection (IDS) and Intrusion Prevention (IPS) Systems

An intrusion detection system (IDS) monitors network and system traffic and patterns for any suspicious behavior, notifying administrators of abnormal activity. Intrusion prevention systems (IPS) enable the proactive quarantining of suspicious traffic. Ultimately, an effective IDS and IPS solution should allow normal user activity without any disruption, discovering threats before they fully infiltrate the system.

5. Disaster Recovery (DR) and Backup

Backup and disaster recovery (DR) are core pieces to ensuring that your critical business systems and data are backed up and safely stored so that operations can come back online as fast as you need them to.

> Intrusion prevention systems (IPS) enable the proactive quarantining of suspicious traffic.

A Partner for Your Key Systems

Unfortunately, in today's digital world, there will always be a push and pull between the need for both security and accessibility. Add in a rapidly changing technology landscape—complete with new tools, apps, and devices, and an evolving cyberthreat surface—and there is plenty to keep IT leaders up at night.

As a technology leader in your organization, it is important to remember that you don't have to tackle this challenge alone. Industry-leading IT services partners like those at VectorUSA have a deep bench of technology experience, connections with best of breed technology vendors, and a broad range of services—all available to help your business deliver for your end users while protecting your most important assets.

VECTORUSA

Ready to learn more?

Schedule a free consultation with the VectorUSA team now.

Schedule a Consultation