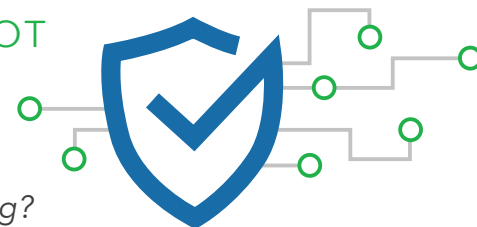# How Organizations Can Tap the Power of Digital Transformation—Safely

DIGITAL TRANSFORMATION IS HERE, READY OR NOT

If your organization hasn't yet embarked on the digital transformation journey, it soon will be. *So what does that mean? And why is it happening?*

Digital transformation starts when an organization begins to tap the power of software—essentially, digital instructions designed to execute on computers—to dramatically improve organizational outcomes.

Increasingly, this software is designed for execution on mobile, IoT and other edge devices—as these devices grow in compute power, storage capacity, and sheer numbers.

Organizations that seek the benefits of transformative technologies like artificial intelligence, machine learning, or augmented / virtual reality must often first achieve some degree of digital transformation.

SOME PRACTICAL EXAMPLES

When field personnel need to access or provide information to customers, edge apps are an obvious move, for improved efficiency and ergonomics. When manufacturers or telecom providers need to monitor and control equipment, smart LAN- or WAN-connected devices can sense and collect data—and even take action—enabling real-time effectiveness and reducing costs.

In other cases, growth objectives, competitive pressures and other market forces may drive organizations to engage more fully with consumers, customers, trading partners, staff, or some combination—and, once again, ubiquitous compute- and connectivity-enabled edge devices, armed with custom-developed or off-the-shelf apps, can fuel engagement in new ways.

Some lines of business will use digital transformation to drive new product launches, push out online catalogs or enable customer self-service. Others will enhance staff capability and productivity with tools that provide real-time information and product or service expertise, while still others will used edge devices and apps to enhance healthcare or medical research.

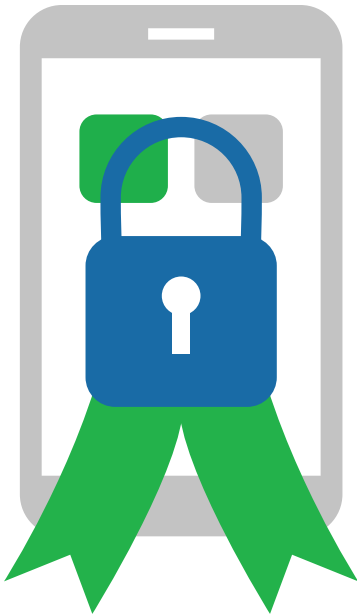## THE COMING REVOLUTION AT THE EDGE

Another key trend that's driving digital transformation is the dramatic increase of computing power being built into edge devices—not just tablets, smartphones and laptops, but in sensors, AI and VR tools, and other endpoints—along with the rapid growth, in terms of sheer numbers, of endpoints. To optimize their digital initiatives, enterprises will push compute cycles from centralized or cloud-based servers out to these endpoints—to leverage their compute power, yes, but also to minimize latency and empower both end users and smart devices.

Analysts at Yardeni Research call out key aspects of this revolution: the increased speed and network traffic reduction realized through reduced latency; fewer connectivity problems (thanks to a reduced need to connect with the cloud); and changes to safety and security as exposure shifts from cloud to edge.[1] Elsewhere, Andreessen Horowitz general partner Peter Levine warns, in "The End of Cloud Computing," that the explosion of data that will be generated by sensors and other devices will choke the cloud (and all its conduits). This will help force repetitive data processing tasks to the edge while more complex analytics and learning remain in the cloud.

1. Source: Morning Briefing, 2/15/2018, Yardeni Research, Inc.

SECURITY ISSUES CAN MAKE OR BREAK YOUR DIGITAL TRANSFORMATION

With all the new capability, of course, comes risk—in this case, security threats to sensitive data, devices, networks, back-end servers and other assets—caused by malicious acts, user errors, or poorly implemented security measures at any architectural point. With mobile and edge computing, an early device-centric security focus has been both challenging and, in some cases, inadequate—especially as unmanaged endpoints (think BYOD and beyond) outnumber those the enterprise "owns." Device-focused security can also degrade the end-user experience. Coding security into apps is an option—but a time-consuming, costly one that distracts enterprises from their core business. Regardless, solving the edge security puzzle is essential for protecting brand reputations, enterprise assets, sensitive data and user adoption rates.

BLUE CEDAR HAS TAKEN ON THIS CHALLENGE—AND WON

Fortunately, there has been a breakthrough: a different, app-centric approach that enables organizations to configure flexible yet powerful security policy—without writing or maintaining any security code—then inject that policy directly into new or existing apps. With their military-grade security policies in place—including user and device authentication, encryption of at-rest and in-transit data, data sharing control and more—the apps are distributed through normal channels (enterprise or public app stores). And their security policies can be adjusted at any time, through a central console, with no need to re-compile or re-distribute them.

The result? By managing security through all the apps that matter—whether off the shelf or custom-developed—the enterprise protects all the users, data, devices and infrastructure that matter. Yet the enterprise retains absolute control of the data and the security functions—and has the important "visibility" capability to easily collect and analyze usage information from millions of edge devices.

Your Digital Transformation, Secured.

When you leverage the Blue Cedar security solution, you free your organization to seize all the advantages that digital transformation offers—confidently. Every stakeholder, every asset is protected, less effort and more flexibility than conventional security methods offer.

Whether your digital transformation initiatives focus on consumers, customers, staff, or trading and business partners, they all enjoy a more seamless, frictionless experience. Your technology staff, enabled (rather than encumbered) by security concerns, can focus on core capability. And your organization can confidently embrace the ongoing revolution in mobile and edge technology.

To learn more about the Blue Cedar security solution for mobile and edge computing, visit www.bluecedar.com or contact info@bluecedar.com.

blue cedar