Reaching for the Cloud Apps

Cloud application delivery is business-critical. So how can IT make using apps via the cloud as safe and secure as possible?
Cloud App Delivery Is Front and Center

If this age of mobility really is, as Craig Mathias maintains in our opening chapter, all about the apps, then IT today must be all about app delivery, which inevitably means cloud app delivery. It doesn’t matter if workers in your company use apps delivered via private cloud, public cloud or (most likely) a combination of the two—aka, hybrid cloud. Company employees use apps, so it’s up to the company’s networking team to make that app use effective and secure.

In this three-part technical guide, our experts look at the challenges facing secure and efficient cloud app delivery today. We open with Mathias’ handy checklist for managing apps via cloud. Then, Sean Kerner looks at both cloud app management success stories as well as key challenges. Finally, because in IT cost is always a concern, Nick Martin considers the expenses involved with a cloud migration. Cloud apps may offer cost savings, but it’s not a guarantee, Martin finds.

Apps are in the enterprise today. People who use apps outside work often use the same apps on the job as well. That’s not news anymore. But the precise ways in which cloud can deliver apps safely and effectively is a timely topic. It’s essential that networking pros know how to ensure cloud application delivery while guaranteeing that company data and systems stay secure.

Brenda L. Horrigan, Ph.D.
Managing Editor, Security Media Group
Making Private and Public Cloud App Delivery
Both Smooth and Secure

Given the dominance of mobility in organizational IT strategies today, it’s not surprising that “it’s all about the apps” has become a mantra. While one might argue that it’s really all about the information those apps manage and transform, the importance of the functionality, security and integrity of those apps cannot be overestimated. So it’s vital that organizations have a strategy for managing an increasing number of mission-critical apps across an ever-more distributed and growing user base.

Though they run locally on mobile devices, apps are distributed via public or private—or sometimes both—cloud providers. Delivery options for public cloud applications include vendor app stores and related sites, and the process involved is intuitive, reliable and proven. But proprietary or otherwise private apps distributed within an organization also require special consideration regarding how they are managed, supported and secured.

Cloud App-Management Checklist
Here are the key items to keep in mind for your app-management checklist:

- Enterprise app stores. These are the repositories for apps distributed directly by the organization. They provide a single point of distribution, control and management; a catalog of available apps and a log of their use; and authentication of apps to minimize the possibility of success in attempts at theft or tampering. Effective app stores can be customized to fit the needs of specific users or groups, often in conjunction with directory services and identity management tools. Many app stores also provide the management of vendor licensing requirements for redistributed apps, such as Apple’s volume purchase program.
- **Mobile application management (MAM).** This element of modern enterprise mobility management (EMM) software assures that only authorized apps can run on a given mobile device. MAM is typically implemented via a whitelist or blacklist mechanism and must also provide broad support for BYOD. The latter is important because devices owned by the end user cannot be as tightly managed as their company-owned counterparts, and the opportunities for errant private or public cloud apps attempting to compromise sensitive organizational data and facilities must always be considered.

- **Security and integrity.** The most common technique applied to private or public cloud applications on mobile devices today is the use of software containers—increasingly a facility implemented directly in the mobile operating system—to enable operational management to be limited to the containers themselves. With this approach, distribution of apps and especially sensitive data onto arbitrary mobile devices is much less risky—again, assuming that an appropriate MAM platform is in place.

Note that there is always a degree of risk associated with the availability of any third-party app; there is no way to determine exactly what that app might be doing at any given moment in time. MAM, combined with containers, can offer a compelling bulwark against malicious use.

- **Management and administration.** Management visibility through MAM and EMM dashboards is essential to shed light on who is using a given app and identifying any possible unauthorized activity. The level of effort here, however, is really no different from any other IT management activity, and it will continue to be eased by the increasing application of analytics techniques. It’s also important to consider the support effort and costs associated with proprietary app distribution, including training materials, help desk and related activities.

- **Cross-platform considerations.** All app distribution strategies must consider the multiplatform nature of today’s IT landscape. At a minimum, support for iOS, Android, Windows, Mac OS and perhaps one or two flavors...
of Linux is required. Note that restricting the universe of available (supported) device and mobile-OS pairs always lowers costs and risks, so updates and upgrades may be required by policy in order for a given user to have access to a given app.

We’re at the point where organizations of any size are able to leverage a broad range of approaches to meet their private and public cloud app-distribution needs. As always, though, it’s best to start with objectives, strategies, policies and procedures, and then back all these up with end-user education and training.

Properly implemented, distribution of both private and public cloud applications can be transparent, working its magic without bothering either IT staff or the end users benefiting from access to those increasingly essential programs. —Craig Mathias
The Challenges and Successes of Cloud App Delivery

Enterprises are trying to make the best use of computing resources wherever they may reside, which ultimately is what the promise of hybrid cloud—notwithstanding the sea of confusion over its true definition—is all about.

Things only got murkier in 2014 when VMware abandoned its vCloud Hybrid Service branding, renaming it vCloud Air. This compounded the fact that many organizations, including companies that sell cloud services, still mistake simple hosting as being synonymous with cloud.

Despite the market’s inability to settle on a definition of hybrid cloud—which the U.S. National Institute of Science and Technology identified as an environment with two or more interconnected cloud infrastructures—its goal is more clear cut: enable enterprises to get the best of both worlds from public and private clouds.

Historically, however, networking in hybrid clouds has been tricky at best. Now that cloud adoption is becoming the norm, there are multiple sets of challenges around ensuring cloud application delivery and performance over hybrid cloud networks.

Jason Cornell is the manager of cloud and infrastructure automation at Cox Automotive, an Atlanta-based subsidiary of Cox Enterprises that sells digital marketing, software and other services to the automotive industry. He said he wants to treat the cloud as a platform—not another data center. To accomplish that, his IT department aims to develop applications that are cloud-aware, meaning they can benefit from cloud resources and capabilities as needed. And if those applications need resources in his data centers, Cox Automotive’s IT team taps into APIs to access those resources.

Cornell and his team are familiar with the challenges around networking and application delivery between their public and private...
clouds. As a result, they have a relatively straightforward approach: avoid the hybrid model and all its headaches.

“We attempt to not couple on-premises and cloud solutions together where possible,” Cornell said.

**APPS SHOULD BE ‘CLOUD NATIVE’**
The key to success in cloud app delivery—be it public, private or hybrid—is to first understand that cloud isn’t just hosting; it’s about agility and applications **decoupled** from physical infrastructure. Enabling applications to run in either public or private cloud is fundamentally about enabling applications to be what is sometimes referred to as **cloud native**, which means the application can scale up or down on demand and is designed to run in a cloud environment.

“When we refer to ‘cloud-native,’ it’s about how you build your app and think about how your app is laid out in a cloud environment, rather than just the packaging and shipping,” said Lachlan Evenson, who was the team lead for cloud platform engineering at Lithium Technologies, a social software company based in San Francisco, at the time of this interview.

Lithium maintains two data centers: one in North America and one in the Europe, Middle East and Africa (EMEA) region. The company also uses Amazon Web Services (AWS) in both the United States and EMEA.

Joseph Sandoval, while director of cloud engineering at Lithium, saw that company begin to take its applications into OpenStack. (Sandoval now is cloud platform manager at TubeMogul Inc.)

The OpenStack cloud platform was deployed in Lithium’s data center to help enable the cloud-native approach to application delivery. Sandoval said that migrating applications from **bare-metal servers** to a cloud-native deployment isn’t just a “lift and shift” from one type of infrastructure to another.

“You’re best off just first automating your application monolith before you even start thinking about moving to cloud,” Sandoval said.

Given that the cloud is elastic, a cloud-native application also needs to be able to scale across nodes. When determining what workloads should run on premises and which ones should run in a public cloud, there are several
factors to consider. For example, some workloads have data that needs to reside in a private data center for security, privacy or regulatory requirements.

“We’re very specific about which workloads run where,” Sandoval said.

**CONTAINERS GAIN FAVOR IN HYBRID CLOUDS**

To truly be cloud-native, an application needs to be built with the assumption that it will live in the cloud, according to Evenson. The use of Docker containers is also becoming a core element of many cloud-native applications.

Prior to Lithium’s Docker use, the company used and maintained deployment templates for both AWS and OpenStack for cloud application delivery, in addition to an orchestration system on top of them. By using Docker containers, Lithium is refining the deployment process for its resources in both Amazon’s public cloud and its own private OpenStack cloud.

With containers, an organization can build, package and ship a cloud-native application that can run in any Docker-ready cloud. And by overlaying Google’s open source container technology, Kubernetes, on top of Docker, an organization can run the same code in two different places in the same way.

“One of the things we’re doing with hybrid cloud is using it to enable another availability zone,” Evenson said. “We have on-premises OpenStack and then we can augment a second running version of the same application in AWS, where we have [a dedicated network connection via] Direct Connect.”

The ability to run the same application in both the public cloud and on-premises OpenStack cloud was enabled by Lithium’s abstraction of applications into Docker containers. Lithium’s IT team makes an app-by-app policy decision on where things will run, based on data issues, service level-agreements (SLAs) and availability.

Deploying Docker with Kubernetes also provides a way to manage the hybrid cloud in scalable fashion. In the pre-cloud era, Evenson explained, developers always wanted to be able to tunnel into their applications via Secure Shell (SSH). But in an environment with a thousand servers, for instance, it’s just not feasible to tunnel into them all. With Kubernetes,
an administrator can get a single location to view how the thousand containers are running, including logging information.

Analytics software company FICO, based in San Jose, Calif., is also a big believer in a hybrid cloud enabled by Docker containers. Nicholas Gerasimatos, former senior director of cloud services engineering at FICO, said the company has a very broad and diverse architecture that includes “big and blocky” infrastructure, such as EMC (now Dell EMC) storage and IBM mainframes. The next-generation architecture that FICO is building is all based on OpenStack and Docker containers.

“How FICO, traditionally, has always been an on-premises company, so we would acquire hardware, load our software on it and then ship it to a customer and do integration,” said Gerasimatos, who is currently a certified cloud service provider at Red Hat. “We realized that model only worked for large organizations.”

FICO’s smaller customers didn’t want hardware deployed, which is where the FICO Analytic Cloud came into play. It’s a customer-facing, multi-tenant cloud service that can reside in a FICO data center, a public cloud or a combination of the two.

“So we might do our own data center and then we might have something for high availability in AWS,” Gerasimatos said.

“Some countries won’t let you take data across borders, and there isn’t a cloud in every single country.”
—NICHOLAS GERASIMATOS, Red Hat

The main driving factor is availability for deployment.

“Some countries won’t let you take data across borders, and there isn’t a cloud in every single country,” he said.

Like the IT team at Lithium, Gerasimatos said he uses Docker containers at FICO as much as he can now.

“Part of the reason we do that is because we can ship the containers to any location and it doesn’t matter from an underlying hardware perspective,” Gerasimatos said.

To help manage application availability across both public and private cloud
deployments, FICO uses Amazon’s Route 53 managed DNS service as well as some home-grown technology.

“We have something we have built internally that validates that services are available from an external perspective,” Gerasimatos said. FICO’s IT team keeps tabs on its clouds with a mix of commercial and open source network monitoring tools, including Nagios, Splunk and Zabbix, along with open source server search tool ElasticSearch. It then ties all those sources of data together to automate cloud application delivery. Additionally, FICO makes use of Red Hat’s CloudForms technology to get a single pane of glass for application deployment that bridges its Amazon, OpenStack and VMware environments.

“Our developers don’t know where the apps are running and they shouldn’t care,” he said. “We want to make it simple for them to deploy, and it doesn’t matter if it’s OpenStack, VMware or Amazon; it just runs and the app is getting the performance it needs.”

**SDN TAKES ON HYBRID CLOUD SECURITY**

The network also has a role to play in securing hybrid clouds. Evenson said software-defined networking (SDN) is a key element in providing network-level isolation so that each application interface is on a different network.

Lithium needs to provide the same level of security, if not a better one, inside of AWS as it does with its on-premises cloud.

“There is a common baseline for all our infrastructure that is enforced,” Evenson said. “We are providing secure multi-tenancy using SDN and are able to provide the same security in AWS as we do on premises.”

Going a step further, Lithium also now encrypts everything in its own data centers as well as its Amazon deployment. In the past, however, Lithium didn’t always fully encrypt the data inside its own data centers. Essentially, the best practices that grew out of securing the public cloud are now being pulled back into the private, on-premises deployment to improve security everywhere.

**SDN is a key element in providing network-level isolation so that each application interface is on a different network.**
CLOUD APP DELIVERY ALL ABOUT LOCATION

There’s a lot to consider when deciding where an application should run. At Lithium, real-time services have strict SLAs that need to be adhered to. With the public cloud, however, Evenson said it’s not always possible to guarantee performance across a network.

“In a bare-metal [server] deployment, you take the networking for granted, while in cloud you can’t,” Evenson said. “You could be sharing with others, so you need to make better decisions on how to service SLAs.”

Ensuring the highest levels of performance is not just about putting the most vital SLA-bound workloads on bare-metal servers. In cases where there is a cloud data center closer to a customer than a Lithium data center, Evenson found the public cloud can actually provide better performance.

“I don’t like to think about [our architecture as] hybrid, because it’s just something we just do,” Sandoval said. “I don’t care whether the infrastructure is public or private; I want a data center fabric that gives me the best of both and can run my workloads anywhere.”

—Sean M. Kerner
Discovering the Most Cost-Effective App Delivery Method

**Consuming resources only** when you need them seems like the most obvious way to increase efficiency. While you can shut down a server to save pennies on power and cooling when it’s not in use, you can’t recoup any of the capital costs. And most OS or software licensing models don’t care how often you use the application. So, when you’re able to pay for the bundled resource, delivered as a service, only when you need it, of course you save money—except when you don’t.

Many applications just aren’t suited to run in a public cloud, for either technological or financial reasons, said David Linthicum, senior vice president at Cloud Technology Partners, based in Boston. To avoid paying more than they need to, organizations should carefully consider their application costs in a cloud vs. on-premises environment.

“It could be as many as 50% of applications in a traditional enterprise, and the average is about 30% to 40%,” Linthicum said. “You have to do the triage and understand the application portfolio—otherwise you will end up making dumb decisions and moving workloads to the cloud that will end up costing you more money.”

Applications that are tightly coupled to a database, or that would require a large amount of redevelopment work to run efficiently in a cloud provider, are workloads that are best left running on-premises, Linthicum said.

“So some applications were just built less efficient and are going to use more resources than they should in a cloud provider,” he said. “So, very much like a 30-year-old refrigerator, it’s going to take more power than a new model.”

Ultimately, much of the on-premises vs. cloud cost comparison comes down to whether the application is designed to run in the cloud, or how much work it will take to redesign it, said Erik Peterson, who was director of
technology strategy at Veracode, an application security company based in Burlington, Mass., that runs on Amazon Web Services (AWS). (Peterson has since gone on to found Cloud-Zero Inc.)

“Some applications were just built less efficient and are going to use more resources than they should in a cloud provider.”
—DAVID LINTHICUM, Cloud Technology Partners

“Most people think they’re going to start by lifting and shifting an existing application into AWS,” Peterson said. “But they often don’t realize the mental shift that’s required with the move to cloud.”

For decades, companies have spent a lot of money to ensure their critical workloads remained functioning in the event of a failure, investing in redundant systems sized to meet peak demand. In many ways, public clouds turn this dynamic on its head, offering an elastic platform with the expectation of failure. Unsurprisingly, workloads designed for one infrastructure paradigm often don’t easily translate to the other. For example, when deploying on-premises workloads, administrators commonly allocate enough resources to accommodate expected demand spikes. But if you apply this same principle to public cloud workloads, you end up paying—often per hour—for much more than you need.

Organizations should first evaluate their reasons, aside from cost, for moving an existing application to the cloud. Then, if there are compelling business reasons to proceed, businesses should approach a cost comparison skeptically, said Mindy Cancila, research director for cloud computing at Gartner.

“Typically, when I talk with clients who want to build a model for comparing costs, the first thing we recommend is they look for other benefits that are driving cloud adoption first,” Cancila said. “The reason being that cost models are layered with inaccuracies.”

Overlooked costs, such as facilities and power delivery, can skew comparisons if they aren’t accounted for. Gartner has built a cost comparison model for clients to understand the economics of on-premises vs. cloud
environments. But an accurate comparison from any model requires that organizations crunch the numbers and look closely at everything that goes into delivering a workload to end users.

Gartner recommended an enterprise moves to a per-virtual machine (VM) cost component for compute because it is the most logical comparison for on premises and the public cloud. “But, again, most companies don’t have that level of clarity or transparency,” Cancila said. “Most are not tying spending to VMs or even to different teams.”

**NEW APPS, NEW AGE**
Comparing on-premises vs. cloud costs for many workloads is difficult, but it’s worth the effort, Cancila said. Cloud providers have levels of infrastructure efficiency that are out of reach for most organizations, and they’re benefiting from next-generation hardware that is unavailable to enterprise IT shops. Even if shifting an existing application to the cloud may not always offer a clear financial advantage, businesses looking to build or deploy a new application should consider a cloud deployment first—either hosted at an infrastructure-as-a-service provider or as a software-as-a-service option.

“Over time, we just don’t think you can compete in the type of model where you’re comparing public cloud costs with on premises, and that’s true for most all workloads,” Cancila said.

Increasingly, new companies, or those looking to deliver new workloads, consider cloud services to avoid large capital server or storage expenses.

“We started a new company when [Google] App Engine was in beta—so we never owned a server in our office,” said Dale Hopkins, CTO at Vendasta Technologies, a sales and marketing software provider based in Saskatoon, Sask. “The cost of on-prem is too high for our applications, and we don’t have any IT staff,” Hopkins said. “So, we chose right away that we wanted to use managed cloud as the core to our business from when we first opened the doors.”

Over time, as Google’s cloud services evolved and more competitors emerged, Vendasta continued to reap the financial benefits.

“[Google] has made some significant strides
over the last eight years on their pricing,” Hopkins said. “Basically, across the board, we pay less than we used to.”

While there is money to be saved, most organizations will encounter a variety of challenges, Peterson said. A business also needs to consider that a change in platform should be accompanied by a change in culture. While performing a security audit for a customer’s AWS environment, Peterson’s team helped uncover an unexpected problem in their client’s account.

“We discovered they were spending over $10,000 a month on disk storage volumes that they’d completely forgotten about,” Peterson said. “A developer had created a system that generated disk volumes but never cleaned anything up. There wasn’t a connection between who was paying the bill and who was doing the work.”

Creating policies that enforce accountability and allow organizations to track resources is the most important piece to ensure a company’s cloud investment doesn’t become a liability, he said. Veracode relies on CloudHealth Technologies, a third-party cloud management tool to track and manage AWS resources.

Large customers often rely on multiple AWS accounts, but built-in tools from Amazon don’t allow users to track costs across different accounts. “In our case, we have over 20 different accounts,” Peterson said. “If you want a holistic view across all of your accounts, the only way you’re going to get that is if you have some sort of third-party service or write your own code to do it.”

**COST OPTIMIZATION’S NEXT LEVEL**

It’s not until organizations have a good process to track their cloud spending, employees with the expertise and use cloud services at scale that they start to explore cost optimization techniques. In the future, Cancila said she expects to see a new breed of tools—from both cloud providers and third parties—designed to help organizations optimize cloud spending.

Even today, larger cloud users find ways to slash costs. For example, AWS offers an option called Reserved Instances in which customers prepay for cloud capacity at a discounted rate. Assuming a company can accurately plan
capacity needs, “you can shave 20% to 30% off your bill with some smart Reserved Instances purchasing,” Peterson said.

The next evolution in cloud frugality may build on another EC2 instance type. Amazon EC2 Spot Instances allow a customer to bid on spare computing capacity. This unused capacity on Amazon servers would otherwise go to waste, so, in an effort to further improve efficiency and make a buck, Amazon offers this capacity at rock-bottom prices—or to the highest bidder. Customers specify a price they’re willing to pay, and as long as the market rate, based on other customer bids, is equal to or less than their price, they can purchase capacity at a significant discount. However, when the market price exceeds their bid, their instances are terminated.

“You can have systems that do unbelievable amounts of work for pennies,” Peterson said. “It’s difficult for companies to rearchitect their apps to take advantage of that, but when I’ve seen companies make the investment, it pays back very quickly.”

Spot Instances are geared more towards workloads that aren’t considered critical or time sensitive, Linthicum said, but it is possible to build a resilient application that doesn’t fail if a single instance, or group of instances, is killed. In fact, given the portability advantages containerization offers, the next step could be the movement of workloads across different instance types or even across different cloud providers—automated by cost triggers.

“I could even build out automated processes that seek out the most efficient platform,” Linthicum said. “That’s a little science fiction right now, but it’s certainly possible with the technology we have today.” —Nick Martin
MAKING PRIVATE AND PUBLIC CLOUD APP DELIVERY BOTH SMOOTH AND SECURE

THE CHALLENGES AND SUCCESSES OF CLOUD APP DELIVERY

DISCOVERING THE MOST COST-EFFECTIVE APP DELIVERY METHOD

SEAN M. KERNER is an IT consultant, technology enthusiast and tinkerer. He has pulled Token Ring, configured NetWare and has been known to compile his own Linux kernel. He consults to industry and media organizations on technology issues.

NICK MARTIN is an executive editor for TechTarget’s Modern Infrastructure e-zine and, previously, senior site editor for the company’s site SearchServerVirtualization.com. Prior to joining TechTarget in 2011, he worked as a staff reporter for the Monadnock Ledger-Transcript in New Hampshire. Martin is a graduate of St. Michael’s College with a degree in journalism and mass communication.

CRAIG MATHIAS is a principal with Farpoint Group, a wireless and mobile advisory firm, and an internationally recognized expert on wireless, unified communications and mobile computing technologies. He holds a Bachelor of Science degree in applied mathematics and computer science from Brown University.

SEAN M. KERNER is an IT consultant, technology enthusiast and tinkerer. He has pulled Token Ring, configured NetWare and has been known to compile his own Linux kernel. He consults to industry and media organizations on technology issues.

NICK MARTIN is an executive editor for TechTarget’s Modern Infrastructure e-zine and, previously, senior site editor for the company’s site SearchServerVirtualization.com. Prior to joining TechTarget in 2011, he worked as a staff reporter for the Monadnock Ledger-Transcript in New Hampshire. Martin is a graduate of St. Michael’s College with a degree in journalism and mass communication.

CRAIG MATHIAS is a principal with Farpoint Group, a wireless and mobile advisory firm, and an internationally recognized expert on wireless, unified communications and mobile computing technologies. He holds a Bachelor of Science degree in applied mathematics and computer science from Brown University.

SEAN M. KERNER is an IT consultant, technology enthusiast and tinkerer. He has pulled Token Ring, configured NetWare and has been known to compile his own Linux kernel. He consults to industry and media organizations on technology issues.

NICK MARTIN is an executive editor for TechTarget’s Modern Infrastructure e-zine and, previously, senior site editor for the company’s site SearchServerVirtualization.com. Prior to joining TechTarget in 2011, he worked as a staff reporter for the Monadnock Ledger-Transcript in New Hampshire. Martin is a graduate of St. Michael’s College with a degree in journalism and mass communication.

CRAIG MATHIAS is a principal with Farpoint Group, a wireless and mobile advisory firm, and an internationally recognized expert on wireless, unified communications and mobile computing technologies. He holds a Bachelor of Science degree in applied mathematics and computer science from Brown University.

SEAN M. KERNER is an IT consultant, technology enthusiast and tinkerer. He has pulled Token Ring, configured NetWare and has been known to compile his own Linux kernel. He consults to industry and media organizations on technology issues.

NICK MARTIN is an executive editor for TechTarget’s Modern Infrastructure e-zine and, previously, senior site editor for the company’s site SearchServerVirtualization.com. Prior to joining TechTarget in 2011, he worked as a staff reporter for the Monadnock Ledger-Transcript in New Hampshire. Martin is a graduate of St. Michael’s College with a degree in journalism and mass communication.

CRAIG MATHIAS is a principal with Farpoint Group, a wireless and mobile advisory firm, and an internationally recognized expert on wireless, unified communications and mobile computing technologies. He holds a Bachelor of Science degree in applied mathematics and computer science from Brown University.

SEAN M. KERNER is an IT consultant, technology enthusiast and tinkerer. He has pulled Token Ring, configured NetWare and has been known to compile his own Linux kernel. He consults to industry and media organizations on technology issues.

NICK MARTIN is an executive editor for TechTarget’s Modern Infrastructure e-zine and, previously, senior site editor for the company’s site SearchServerVirtualization.com. Prior to joining TechTarget in 2011, he worked as a staff reporter for the Monadnock Ledger-Transcript in New Hampshire. Martin is a graduate of St. Michael’s College with a degree in journalism and mass communication.

CRAIG MATHIAS is a principal with Farpoint Group, a wireless and mobile advisory firm, and an internationally recognized expert on wireless, unified communications and mobile computing technologies. He holds a Bachelor of Science degree in applied mathematics and computer science from Brown University.