eGuide

FROM IDG

CIO CSO InfoWorld NETWORKWORLD

BlackBerry

presents

Communicating Security in the Age of IoT

Communications Platform as a Service (CPaaS) and peer-to-peer (P2P) networking make it possible to bake privacy and functionality directly into IoT devices and applications.

How to Secure Human–to–Machine Communications

Security must be addressed for consumers and industries to place their trust in devices and applications that communicate with them.

CONSUMERS ARE OFTEN the driving force behind human-to-machine interaction. They are adopting a range of devices and applications letting them check the status of their home, feed their pets, order groceries, start a playlist, and more.

That adoption is now crossing over to industrial applications as well, as enterprises see its business value. For example, farmers who use drones to capture real-time crop information have increased yield while minimizing waste.

That said, building security into these human-to-machine communications has been lacking, and the vulnerabilities, when exposed, have generated concerns from consumers and government entities.

"The Internet of Things is highly fragmented, and emerging standards are focusing on communication interoperability such as MQTT and CoAP. The overarching question is, 'what about security and privacy?' It's often a second thought, since go-to-market time is important," says Shiladitya Sircar, Vice President of Identity and Messaging at BlackBerry.

Security must be addressed for broader adoption to take place. More parents might adopt apps that let them see their children at daycare, for example, if they feel confident the streaming video is authenticated and secure. Alternatively, more power companies might incorporate drones outfitted with flamethrowers to clean power lines if they are sure the technology can't be hacked.

Users getting savvy to security risks

In terms of complexity, security is one of the most significant challenges facing human-to-machine communications.

Devices like home surveillance cameras or smart door locks are embedded with web-based components or applications that enable users to communicate with them. Simply having to connect to the Internet naturally increases the risk of vulnerabilities. Associated with this, users are not always connecting via a traditional, trusted network; they might be controlling their home thermostats, for example, from their mobile devices via a coffee shop Wi-Fi network.

"From a technology perspective, many IoT and web-enabled devices are built with a Wild West mentality," said Brent Thornton, Director of Enterprise Solutions at BlackBerry. In other words, get it to market fast, don't worry about building in security protocols.

"The problem is, we are rushing to deploy insecure products to support business needs, and then deciding that we need security," said Christopher Conrad, practice manager, critical infrastructure at NSS Labs, in a statement.

"From a technology perspective, many IoT and web-enabled devices are built with a Wild West mentality."

Brent Thornton
Director of Enterprise Solutions
BlackBerry

One woman recently learned this the hard way when she realized her IoT baby monitor had been hacked and she was being spied on.

Herein lies the other challenge: user perspective. This mother regretfully said her decision to purchase the monitor was naïve, that she had no idea of the security risks. She trusted the retail shop and manufacturer, including a no-risk claim, that the product was secure.

As these cases go viral, users become more sensitized to the potential risks. For example, when the mother was abruptly exposed to the device's vulnerability, she quickly took to social media to warn others. And when a Portland, Oregon couple discovered their voice-assistant device had recorded their conversations, it became national news with ensuing governmental intervention.

No one wants to be associated with a negative headline. That's why security must be baked-in from the ground up, using trusted communications technology.

Creating a circle of trust

Trust is the first critical ingredient for securing real-time, human-to-machine communications. Data must be transmitted so it can be trusted and verified. That includes ensuring:

- The integrity of the data, so the user and recipient trust the message has not been intercepted or modified while in transit;
- The authenticity of the sender or initiator as well as the recipient;
- Only the intended recipient can read or interpret the message.

The circle of trust begins and ends with the user experience. From a developer's point of view, start by giving users more granular information than they may need, including specific tasks within the interface, without overwhelming them or adding unnecessary security steps.

"The user is going to make a decision on whether to use the interface you've created, probably within the first few minutes of using the application," says BlackBerry's Thornton. "And part of that user experience is security, privacy, and being somewhat transparent with them. They're going to want to know that their data is protected and the communication between them and the machine isn't going to be intercepted."

This process includes building in contextual security—embedding it where it belongs. For example, with a smart door lock, the user would understand the need to enter a password or perhaps have a geo-location identifier in her smartphone to unlock the door. But she wouldn't expect to go through the same process to lock that door.

The circle of trust is an ongoing loop. The device or application must continually evolve and adapt to both user and machine changes to get the most benefit from the system.

The solution: Baking in security

Embedding security into human-to-machine interactive devices and applications doesn't have to be difficult or time-consuming for developers. Communications Platform as a Service (CPaaS) is a framework that enables the seamless integration of secure, real-time communications—voice, video, messaging, and data transfer—into endpoint devices or applications. CPaaS includes all the standards-based application programming interfaces, code, and support for enterprise-grade communications.

Consider the importance of privilege and access rights in the smart door lock example. Designing and developing the relevant commands and credentials—including encryption and authentication—while ensuring ease of use, can be a complex set of tasks. CPaaS has those capabilities baked right in, including authentication messaging from the recipient to the machine (door lock) and confirmation messaging from the machine to the recipient.

CPaaS abstracts security from the development process. And with pre-built communications features like chat and a back-end communications framework, it saves valuable development time that can be used to focus on the user experience. By increasing the level of connectivity and functionality, CPaaS increases productivity while enhancing data security.

Even better, CPaaS addresses the vulnerability concerns that consumers and enterprises have about human-to-machine interactions. When the application or device has a built-in framework for security from a trusted name, they are more likely to adopt these systems.

By increasing the level of connectivity and functionality, CPaaS increases productivity while enhancing data security.

The Power of BlackBerry Spark Communications Services

The BlackBerry Spark Communications Services offers a comprehensive framework for secure human-to-machine communications. It includes rich features such as messaging, voice, video, read notifications, and data transfer.

"At BlackBerry we think about security, with privacy as the first tenet. We're creating technologies that enable machines and humans to interoperate seamlessly and safely," says Shiladitya Sircar, Vice President of Identity and Messaging at BlackBerry.

With end-to-end encryption, digitally signed messages, and guaranteed data delivery, Spark Communications Services is a secure CPaaS solution that's easy to integrate.

Find out more at BlackBerry.com/sparkcpaas

Core Communications: Creating an Ecosystem for Collaboration

A secure, contained environment for communications generates true business value.

COLLABORATION IS CRITICAL to organizational success. Having and sharing information in real time improves customer relations, productivity, and efficiency.

Yet the challenge lies in ensuring individuals have access to all relevant information in a secure, trusted manner. For example, doctors and nurses who are instant messaging about a patient's care must be confident that health information is protected according to HIPAA regulations. On the flip side, their ability to improve the patient's care increases when vital-sign data can be streamed directly from bedside machines into the chat app they're using.

Solving this requires an ecosystem for collaboration. By embedding secure communications and data sharing inside traditional business applications and devices, organizations have the opportunity to significantly improve collaboration. A self-contained environment—where all communications funnel together—has individual and business rewards.

The benefits of secure, connected collaboration

Embedding secure communication capabilities into core business systems and apps—e.g., ERP, payroll, case management software—has many benefits, including: streamlining workflow processes, breaking down departmental silos, reducing complexity, and improving security.

Consider the specifics of each:

Streamlining workflows: Organizations improve processes by integrating communications within devices and apps. Take for example, a patient who has had an MRI scan. The machine could automatically and securely transmit the results to the patient's electronic health record (EHR), while at the same time sending an alert to the corresponding doctor, triggering the physician to establish a follow-up appointment.

Breaking down departmental silos: Many daily processes involve interaction both internally and externally, yet often information gets lost or missed when communications aren't shared. A salesperson, for example, might not be aware of billing issues with one of her clients based on information within her customer relationship management (CRM) app. She must step outside CRM to send an email to the accounts payable department asking for an update. Similarly, she likely emails the client outside of CRM. Embedding communications directly into that app improves collaboration both internally and externally. It saves time and, by keeping all communications within a contained environment, avoids the risk that pertinent information gets lost.

A self-contained environment—where all communications funnel together—has individual and business rewards.

Reducing complexity: A secure contained communications environment can eliminate the need for multiple messaging and file-sharing apps. Having to license and customize each solution and build in privacy and security protocols can drain IT resources. The integration of systems allows IT to focus on higher-level initiatives, while also furthering digital transformation efforts.

Improving security: A standalone messaging app typically has its own security risks and challenges. Embedding a secure communications framework directly into existing business apps and systems immediately applies security and privacy protocols. That makes it easier for development and IT security teams to ensure policies and audit trails are in place.

Secure and connected: A case for improved care

One of the more data-sensitive and data-intense industries is healthcare. It's also a sector where communications can directly affect someone's well-being. To improve the flow of information among medical teams and patients, a hospital group recently deployed a secure communications platform-as-a-service (CPaaS) solution.

CPaaS is a framework that enables developers to seamlessly integrate secure, real-time communications—voice, video, messaging, and data transfer—into endpoint devices or applications. It includes all the standards-based application programming interfaces, code, support, etc., for enterprise-grade communications.

The hospital had several critical considerations that the CPaaS solution needed to address:

- Privacy and confidentiality. Healthcare is among the most regulated sectors. HIPAA legislation alone adds complexity to ensuring privacy. Messaging must be protected, and all parties must be authenticated.
- Data integrity. It's imperative that data can't be tampered with or modified during transmission or at rest, for both internal and external communications. This includes multiple points of presence (patients, caregivers, machines, applications).
- User experience. Healthcare is a 24/7 business, with medical staff often consulting on patient care outside of the traditional four walls of the facility. Mobility and ease of use had to be considered.

The hospital chose a CPaaS solution with embedded security and privacy. It includes end-to-end encryption, using standards such as the FIPS 140-2 libraries—a set of U.S. government cryptography standards.

Yet the solution goes well beyond encryption to ensure a secure connection by addressing the following:

- Identity—includes identity and entitlement controls for access authorizations
- Integrity—uses digital signatures and message fingerprinting to verify intended recipients, regardless of whether the data is voice, video, messaging, or alerts
- Confidentiality—employs two layers of content encryption: one at the transport layer and one at the data layer
- Availability—ensures each endpoint (e.g., a doctor's tablet device, smartphone, and desktop) is confirmed and associated with the trusted identity so the user can securely access, transmit, and receive
- Non-repudiation—uses a combination of digital signature and identity verification to assert the authenticity of the

CPaaS enables developers to seamlessly integrate secure, real-time communications into endpoint devices or applications. It includes all the standards-based application programming interfaces, code, support, etc., for enterprise-grade

communication's origin

All of these features assured the hospital's IT and development teams that data communications would be secure, confidential, and available both in transit and at a rest.

Doctors, nurses, and medical staff can now communicate within a private, self-contained environment. They can chat, share patient images, and view test results in real time from any location. Their notes and conversations, as well as medical device data—for example, from MRI or CT machines, heart monitors, temperature indicators, etc.—are automatically logged in the EHR system. This information can populate in the chat window as a patient's health status is being reviewed.

Patients too can access and interact with their physicians via the private communications environment. "The ability to share information securely isn't the only challenge. You also have to control what was already shared. Ultimate control comes when you can retract content or mark time to live," says Shiladitya Sircar, Vice President of Identity and Messaging at BlackBerry.

The ultimate reward is better patient care and communications. Access to comprehensive patient files has improved medical professionals' decision making, while knowing the information is secure and confidential.

The power of CPaaS

Embedding secure communication in a collaborative space puts permanence into what has been an ephemeral process. Standalone messaging apps can't capture the full context of a patient's health status or a customer's purchase history.

"A general-purpose messaging platform not only has security challenges," says David Wiseman, Vice President, Secure Communications, BlackBerry. "But also, when you use a standalone environment like that, you can't tailor and customize the user experience like you can with CPaaS model, where you can truly embed it into your systems and start to digitally transform your business."

Learn more about the communications ecosystem at BlackBerry.com/sparkcpaas

IoT + P2P = Private Communications

The traditional cloud–based store–and–forward distribution model for communications puts Internet–of–Things devices at risk. There's another way to ensure privacy.

THE INTERNET OF THINGS (IoT) proliferation is here, and it's embedded across consumer, enterprise, and industrial markets. It's estimated there are currently approximately 20 billion IoT-connected devices in the world, and that will scale to 75 billion by 2025.

But as adoption increases, privacy concerns are also escalating. For example, Consumer Reports recently advised readers to take precautions before purchasing any IoT-equipped, web-connected home device. And the Federal Trade Commission has waded in, suggesting more must be done to protect information that is shared on these devices.

The primary challenge is that sensitive data is often sent through and/or stored on a server somewhere, using the Internet. And the Internet can be hacked. But imagine if there was another way to send communications via IoT devices. One that bypasses the cloud completely to eliminate those privacy risks and uses fewer resources to boot.

There is: peer-to-peer (P2P) networking.

Conventional IoT sharing today

Nowadays, data created on IoT devices is typically processed, shared via the Internet, and commonly stored in the cloud. Even if it's stored on-premises, the store-and-forward distribution model typically includes cloud routing, where sensitive data is vulnerable. With data breaches and hack attacks always a threat, that information is at risk both in transit and at rest.

For some markets and industries, this risk is untenable. For example, a patient's MRI scan data is subject to strict HIPAA regulations about how it is stored. Or consider defense drones capturing and transmitting sensitive images; even encrypted, if that information is hacked during transmission, it could cause serious ramifications.

Enterprises are not immune, either. "People will be installing smart devices in their offices that automatically connect to the Internet," says Kevin Curran, Senior IEEE Member and Professor of Cybersecurity and Intelligent Systems at Ulster University. "But what if a builder hasn't checked if it's secure? We're heading for a nightmare down the road as things cannot be patched and secured."

The benefits of IoT + P2P

IoT devices must be built so that highly sensitive data can be shared privately. One way to achieve that is using P2P networking.

"With P2P, you're not leaving fingerprints on the Internet," says David Wiseman, Vice President, Secure Communications at BlackBerry. "When you use server-based information sharing, it can be secure—but depending on how you're doing it, there can still be cached copies or residual metadata that are vulnerable. With P2P, you're able to eliminate a lot of that and have a higher privacy standard."

In a P2P streaming scenario, encrypted content is directly uploaded to the receiving client—there's no server in the middle. All that information is available to the sender and receiver on their own private connection. Eliminating a mediator for the content transfer ensures privacy, while

It's estimated there are currently approximately 20 billion IoT–connected devices in the world, and that will scale to 75 billion by 2025.

reducing vulnerability risks.

P2P also offers an advantage in instances where a strong communications network is not available for IoT devices. "With the P2P model, you can set up a localized communications infrastructure that can gather data, independent of whether you have cellular coverage," Wiseman said. "That might mean using a mesh network among sensors. But the overall advantage is that with P2P, you're not relying on an external network being available to transmit and share information."

Another benefit: Large content streams can be moved more efficiently at lower costs. "In the land of video, that's a lot of data to be uploading and streaming," says Brent Thornton, Director of Enterprise Solutions at BlackBerry. "Cloud systems typically charge per megabyte or gigabyte not only for the storage but also for the processing. There's some least-cost routing efficiencies that you can build into your app from a logistics standpoint that large data transfers happen via P2P, so that saves time and money."

The last benefit of P2P mode for data stream transfer is "protecting data sovereignty, since data never strays outside two connected endpoints," adds Shiladitya Sircar, Vice President of Identity and Messaging at BlackBerry.

P2P + IoT in the field: Practical use cases

There are many applications where the use of peer-to-peer capabilities built into IoT devices benefits users and enterprises.

For example, an MRI machine requires diagnostic testing, but the manufacturer is unable to get a technician to the hospital site in a timely manner. Fixing the machine remotely via cloud streaming could run afoul of HIPAA's strict data-sharing regulations. With a P2P microservices model, the diagnostics information can be streamed from the MRI device directly to a technician in a private connection, ensuring that data is private and secure.

On the consumer side, individuals with smart camera systems in their homes might want the ability to monitor different rooms or to see who is at the front door. However, they don't want that private data continually flowing over the Internet where a hacker could intercept it. Secure P2P functionality built into the cameras ensures the content remains private by never leaving the actual environment.

The solution: Baking privacy into IoT devices

Embedding privacy functionality right into IoT devices and applications doesn't have to be difficult or time-consuming. Communications Platform-as-a-Service (CPaaS) is a framework that seamlessly integrates secure, private, real-time communications—voice, video, messaging, and data transfer. CPaaS includes all the standards-based application programming interfaces, code, and support for enterprise-grade communications.

There is considerable complexity, for example, developing end-to-end encryption at government-level standards, which is a necessity for a surveillance drone used by defense contractors. With the right CPaaS solution, companies can directly embed that degree of privacy into the drone and instead focus on the device's user experience and P2P networking capabilities.

Building private, secure P2P functionality right into IoT devices not only simplifies the development process, it also creates an embedded layer of trust that users—and governmental regulators—are clamoring for.

"P2P is a perfect play in the IoT space," Thornton says. "It's a direct connection, so you're going to get faster speeds, and there's no possibility of man-in-the-middle attacks."

How Bots and Machine Learning Provide Better Communications

There's an opportunity for businesses to increase value with enhanced, secure

ORGANIZATIONS RECOGNIZE the business value of satisfied users and customers. They are constantly seeking ways to improve interactions with them—increasingly through applications or devices.

To simplify these communications while reducing operational costs, many companies have deployed bots (short for "robots"), or applications that perform automated tasks. Bots are typically used for customer support, such as answering frequently asked questions.

Yet, as individuals become more accustomed to interacting with bots, there's an opportunity to advance these communications. By integrating bot and machine learning technologies with business systems, enterprises can deliver a higher level of communication: context-sensitive, conversational dialogues. A critical element in doing so will be ensuring the security and privacy of this shared information.

The evolution of digital communications

Traditional telephone conversations between customers and businesses are slowly being replaced by digital communications. Millennials' comfort with technology coupled with their desire "to communicate faster and get better answers," are accelerating this transformation.

At first, these new digital "conversations" took place by email and text messaging. But as companies discovered how to streamline FAQs into digital conversations, they have started deferring to chatbots to carry the bulk of the dialogue. And with the fast uptick of artificial intelligence (AI) and machine learning, these technologies are now revolutionizing communications.

For example, an Accenture-led pilot program at a European telecom company found the use of chatbots led to "successful resolution of 82% of customer interactions through automation and artificial intelligence alone," says Shiladitya Sircar, Vice President of Identity and Messaging at BlackBerry. "Machines are great at learning statistically significant repetitive tasks, so fairly supplicated workflow automation is possible just by enabling machine learning in a communication framework."

A similar evolution is happening in the consumer space. IBM Watson's victory on Jeopardy awakened consumers' interest in the possibilities of AI and machine learning. That curiosity blossomed as consumers turned to digital assistant devices like Siri or Alexa for answers. And now, many consumers are comfortable using machine learning-enabled devices to smartly open home door locks and stream time-sensitive video of their children at daycare facilities.

These instances provide some level of contextually aware communications. For example, if the smart door lock has geo-location identifiers, presence capabilities kick in when the user activates his device or application near the door lock.

However, to achieve true business value, bot interactions need to become both conversational and anticipatory—for example, to

Millennials' comfort with technology coupled with their desire "to communicate faster and get better answers," are accelerating digital transformation.

provide service or support before the customer gets frustrated. Here's one example: A customer-service chatbot can be trained by machine learning to recognize when a customer is getting frustrated and then forward that call to human support.

Taking communications to the next level

The large volumes of data in business systems like ERP and CRM can be mined to provide high-value, customized communications. When integrated with bots that include machine learning capabilities, bots can find and use more contextually aware, relevant information.

For example, bots now do some pre-processing work to answer voice or chat messages that come through a bank's website. They can either answer the customer's question or route him to an account services representative. Now that customer support process can be automated using conversational interfaces. Machine learning can first determine if the same set of questions resolve into the same set of answers. And then a textual analysis of a question suggests possible outcomes based on previous results and auxiliary information.

Taking the next step, if a customer-support bot can interact with a specialized bot in the bank's CRM system, together they can gather relevant data that is directly pertinent to the customer making contact. Once the conversation is contextual and specific, it can become personalized and anticipatory—potentially suggesting additional services or products.

At this point, a world of opportunities opens for businesses. Rather than just having a digital assistant make restaurant reservations for example, it can activate a series of bots that integrate data from a myriad of applications and environments to drastically simplify tasks.

For example, a user could tell his digital assistant he wants to go on vacation. Based on the user's preferences and history, that bot talks to a whole series of other bots embedded in applications to come up with vacation options—with possibilities for airlines, accommodations, tours, and restaurants.

Ensuring secure bot communications

Of course, a critical element in this bot-machine learning story is security.

"There's more privacy and security risks if you haven't set up the protocols for communication and information sharing between these bots," says David Wiseman, Vice President, Secure Communications at BlackBerry. "We've got to make messaging secure, make sure you're talking to the right bot, because someone could put a fake bot in there to intercept communications."

By embedding secure communications directly into business applications and devices, organizations can protect bot-to-bot interactions. And doing so doesn't have to involve a complex development process. Communications Platform-as-a-Service (CPaaS) is a framework that enables the seamless integration of secure, real-time communications—voice, video, messaging, and data transfer—into endpoint devices or applications. CPaaS includes all the standards-based application programming interfaces, code, and support for enterprise-grade communications.

CPaaS abstracts security from the development process, making communications between bots more secure than traditional bot-to-standalone messaging app interactions, which may have vulnerabilities.

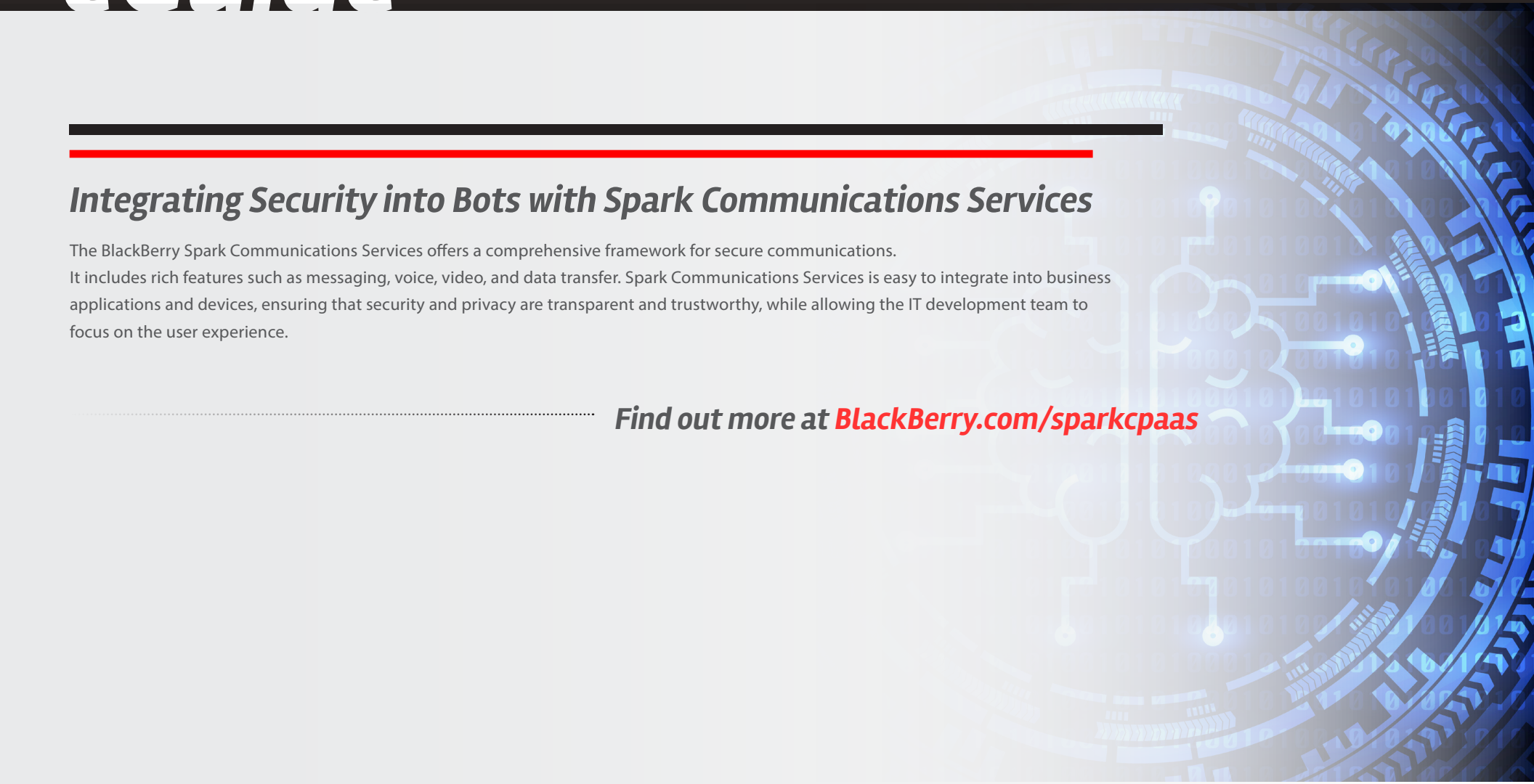
By increasing the level of connectivity and functionality, CPaaS also increases business value through conversational dialogues that strengthen customer relationships.

Bots using machine learning is "an opportunity to drive productivity through automation, provide useful results and information to customers, and even sell additional services with enhanced communications," Wiseman says. "The key is making sure privacy and security are transparent."

"There's more privacy and security risk if you haven't set up the protocols for communication and information sharing between bots. We've got to make messaging secure ..."

David Wiseman

Vice President, Secure Communications



Integrating Security into Bots with Spark Communications Services

The BlackBerry Spark Communications Services offers a comprehensive framework for secure communications. It includes rich features such as messaging, voice, video, and data transfer. Spark Communications Services is easy to integrate into business applications and devices, ensuring that security and privacy are transparent and trustworthy, while allowing the IT development team to focus on the user experience.

Find out more at BlackBerry.com/sparkcpaas