THE SAVVY CIO'S GUIDE TO IOT

CISCO

ACADIA TECHNOLOGY GROUP

TABLE OF CONTENTS

IOT SECURITY CONCERNS AND HOW SDN SHORES UP EXPOSED NETWORKS 4

3 INSURANCE AND FINANCIAL FIRMS THAT ARE GROWING THEIR BUSINESSES WITH IOT SOLUTIONS 7

DIGITAL SIGNAGE AND RETAIL IOT SOLUTIONS FOR STADIUM MONETIZATION 9

RESOURCES 12

INTRODUCTION

Enterprises have a great opportunity to streamline operations, increase revenue, and develop a more customized and efficient workplace experience with IoT solutions. For firms that capitalize on this opportunity, there remains the concern of both end point and overall network security. Acadia Technology Group addresses these concerns while opening the door to software-defined networking (SDN) solutions.

Use this guide to IoT solutions for enterprises to influence your decision-making on how IoT will affect your network performance while enhancing the promotion and delivery of products and services.

IOT SECURITY CONCERNS AND HOW SDN SHORES UP EXPOSED NETWORKS

As enterprises explore ways to integrate IoT-enabled devices into operations, organizations should also evaluate the security vulnerabilities that undoubtedly arise from adding IoT endpoints to the network.

Recent research has revealed IoT devices fall into three security categories:

Disastrous: Usually IoT-enabled security cameras and monitoring systems fall into this category as bad actors can compromise the network to access customer data, allowing break-ins to physical locations and other cyber related crimes.

Disruptive: Video conferencing and VOIP conferencing and connected printers and scanners also open the possibility of cyber spying (listening or watching through IoT devices).

Damaging: IoT devices in the office breakroom such as smart fridges and light bulbs could give industrious hackers access to the enterprise's network. Examples of this phenomena are legion and provide one of the easiest forms of entry because they appear to be innocuous when in fact they expose an organization to enormous risk.

At present, you can say that we have a three-tiered group of IoT devices. Right at the top we have well-protected devices such as smart industrial machinery and laptops.

In the middle, we have moderately complex devices like smart thermostats that are used occasionally. Right at the bottom, we have smart electronic locks, employee badges, and HVAC technologies.

All these IoT devices by themselves don't present much of a problem, but when you connect all of these disparate technologies to a single network, it will be difficult to ensure IoT security.

This is because we don't have a one-size-fits-all solution to secure a variety of smart devices with multiple end-points to a single network.

Before anyone even heard of IoT, enterprises were struggling to keep their IT infrastructure secure. Now they're tasked with securing their IT infrastructure with thousands of smart devices that you don't always see.

If that wasn't difficult enough, IT leaders also have to develop a robust strategy to leverage these devices to collect critical that can be useful in helping the organization streamline operations.

The Real Threat of an IoT Security Breach

Since the emergence of smart devices, hackers have been working to compromise them. You don't have to look far to find examples of enterprises that experienced major network breaches due to IoT endpoint device vulnerabilities. The Mirai botnet attack remains as the worst example to date but Brickerbot and the Chrysler Jeep attacks also rank highly.

While all these vulnerabilities pose an immediate risk to privacy, some of these exposed devices can also allow access to internal networks. As IoT can act as a potential gateway that leads right into enterprise networks, it can have serious consequences.

Vendors of IoT devices know security is a problem, but many of them pay more attention to shoring up security in certain devices and not others. That puts the responsibility to ensure all endpoint devices are secure in the hands of the enterprise's IT leadership.

The question leaders in enterprise technology must ask, "Are IoT-enabled devices delivering enough value to the enterprise to justify the time, energy, and resources necessary to secure them and protect the company's network?" This will remain a key question for CIOs because security vulnerabilities are often baked into IoT endpoints.

The good news is technology does exist to provide an orderly, focused, and iron-clad barrier around IoT-enabled endpoints to give enterprises the freedom to introduce them to the network at will.

SDN for Network Protection Ensures Adaptability, Programmability, and Visibility

While software-defined networking (SDN) can't secure the IoT devices themselves, it can help control the network and leverage segmentation to mitigate a potential network intrusion. This means that by taking a cloud-based approach, enterprises can use SDN to optimize, route, and automate IoT security.

When smart devices and sensors are added to the network, it will make a note of each device that's added to the network.

This approach will allow for the network to react differently to each endpoint depending on the nature of the device, the potential risk of a malicious attack, and the resources required to secure the device. SDN enables firms to:

- **provision or de-provision the network to actively monitor and divert suspicious activity until it's cleared for access**. Network admins can program rules to make this happen automatically, making for fast, worry-free additions of endpoints to the network.
- **build multiple firewalls at various network distances to effectively respond to IoT breaches**. This is a much better approach to security than building a single firewall at the edge of the network.
- **virtualize network components and services to apply access rules, reroute traffic, and program automatic adaptive responses to IoT devices**. This means that you can segregate the network path where a potential intrusion has been detected and then investigate it from a central point.

By using SDN for network protection, you can significantly reduce the amount of time and resources needed to investigate each potential security issue. In the long run, this will save your company a lot of money.

SDN is also a highly affordable solution that can be adapted to meet the future technology needs of the business while remaining key to shoring up exposed networks.

3 INSURANCE AND FINANCIAL FIRMS THAT ARE GROWING THEIR BUSINESSES WITH IOT SOLUTIONS

Financial institutions rely heavily on gathering and analyzing data. As a result, IoT and related automation technologies provide financial firms with high-value information that influences business decisions.

In the financial sector, retail banks have invested heavily to develop both internal infrastructure and consumer-facing technologies. According to IDC Financial Insights, retail banks are predicted to spend more than $16 billion on digital information technology initiatives by 2019.

However, this is not something that is only going to be realized in the future, it's already happening. So let's take a look at some examples of financial firms utilizing IoT solutions to adapt and grow their business.

USAA Embraces Voice Technology for Future Customer Interactions

It's no secret that retail banks are taking note. In early August, USAA announced its pilot project to leverage Amazon's Alexa technology to offer USAA members access to information about spending patterns, account balances and transaction histories.

USAA customers who already have an Alexa-based device (like Echo or Echo Dot), now have the option of turning on the feature through the device's application and linking it to their bank account.

According to the bank, this new skill for Amazon's Alexa will leverage Clinc's artificial intelligence conversation management technology to enable a more human-like interaction from Amazon Alexa. This can be achieved as the skill remembers the context, follow-up questions, and complex human language.

The technology will keep learning through interactions with members and will tell users if they're going over their monthly budget for a certain spending category. This initiative is expected to help the bank better engage with their customers and grow the bank's market share.

Progressive Turns Safe Driving into Savings

The rise of connected cars and data analytics has created a new dimension to the auto insurance space. As connected cars can be used to collect data on an individual's driving history, it now provides an opportunity to assess exactly how responsible a person is to balance the costs and risks involved (instead of looking at traditional factors like where they live or the type of car they drive).

By using telematics and machine learning, you can now track the speed, breaking patterns, the overall condition of the vehicle, and a range of other data points. This innovation didn't go unnoticed, as Progressive with its tiny Snapshot program, now allows safe drivers to access real savings by providing their personal data to reduce their premiums.

This enables the insurance company to reduce risk and cut costs by pricing more accurately on an individual basis.

Progressive's agreements with Zubie (the maker of the "thing" that plugs into your car) also lets Zubie customers know how much the insurance company would charge them based on the driving data collected by Zubie.

Royal Bank of Canada Enables Bill Payments Using Apple's Siri

Beam Dental, when compared to the examples above, is unique in that it wouldn't even exist without IoT technology. The Beam Brush is an innovative approach that companies both large and small can extend to their employees to ensure good dental hygiene.

Underwritten by National Guardian Life Insurance Company (NGL) and marketed by Beam Insurance Services LLC (and administered by Beam Insurance Administrators LLC), it's uniquely positioned to disrupt the dental insurance space.

All the plans are offered with perks that include beam's smart connected toothbrush and a quarterly shipment of the following:

- Toothpaste
- Floss
- Replacement toothbrush heads

As IoT continues to offer profound opportunities for the financial sector, financial firms are now driven to differentiate their offerings in an increasingly competitive marketplace. As a result, you can expect IoT to continue to transform the industry for years to come.

DIGITAL SIGNAGE AND RETAIL IOT SOLUTIONS FOR STADIUM MONETIZATION

When stadiums and arenas leverage digital signage in their retail environments correctly, they create greater opportunities to enhance the customer experience and increase retail outlet monetization.

For a digital signage system to be effective, it must reflect the way fans interact with each other, the stadium and the event by first meeting four criteria:

- Deliver customized design and implementation to meet a particular stadium's needs
- Target patrons based on every stadium zone
- Provide dynamic response to user needs in real time through central control
- Integrate holistically with high-density WiFi, IoT and network virtualization for targeted and easily changeable interactive retail opportunities

Collectively, these factors influence placement, numbers, configuration and monetization flexibility through opportunities such as display ads, partnerships, branded content and vendor offerings.

To realize the dynamic digital signage opportunities with retail in your stadium requires accommodating the retail needs of fans at a sporting event versus a concert or trade show, and the different ways they move and through and interact with the venue and digital signage.

Dynamic Digital Signage for Stadium Retail Opportunities

For stadiums, implementing digital signage represents an extra revenue stream by facilitating content delivery for marketing and vendor partnerships through delivery of unique and targeted digital content. This also opens up the possibility of completely “rebranding” a stadium for different events and vendor needs.

Stadiums are finding success with dynamic digital signage that is centrally connected for easy management, targeted offers /sponsorships, and concession routing/wayfinding. This can include a number of monetization opportunities including the following:

- Advertising networks with vendor partnerships to display their ads and directing fans to in-stadium as well as after-game sales opportunities at key points in the stadium as part of a full content model and business strategy
- Vendor menu changes, availability, and selection as well as routing to relieve line congestion.
- Branding based on location in a per-zone basis that can range from individual luxury suites clubs and bars to individual designated vendor retail operations along the concourse.
- Delivering interactive content is based on real-time events such as game scoring, half-time activities, limited sales opportunities, interactive games and more.
- Digital menu boards capable of real-time changes based on item availability, and vendor changes per event and direction to alternate vendor locations to improve menu presentations and increase concession sales.
- Outdoor schedules for upcoming games and events that boast game times and ticket specials to increase ticket sales.

The power of digital signage monetization can be seen in a Cisco Case Study on digital signage implementation at Denver Broncos Stadium that showed a 50 percent increase in concourse signage revenue. That being said, the true power of digital signage technology is its ability to connect to the fans through high-density WiFi networks. This connectivity through smartphones and IoT sensors provides an additional level of monetization and connectivity approaches that boost the fan experience and the bottom line.

Digital signage can alert fans to numerous opportunities that can change during an event. These monetization opportunities include:

- in-game seat upgrades for unsold stock
- in-seat food delivery
- limited-time offers on merchandise sales, among others.

The first step is to alert fans to these opportunities via digital signage. Simultaneously these opportunities are made available via targeted messages prompted by Wifi and retail IoT sensors to smartphones via apps. The result is that stadiums can increase sales and fan fulfillment experiences at the same time.

Stadium Retail Opportunities with High-Density WiFi

While digital signage displaying paid advertisements is common, high-density WiFi can take the interaction and monetization to the next level by displaying relevant, engaging content during an event based on fan location at specified times. WiFi network integration with digital signage enables the mobile interaction such as in-event trivia games, sales, and short-term offers. This lets your vendors, advertisers, and sponsors extend their advertising reach beyond the big screen and the concourse TVs to smartphone users.

WiFi is integral to the fan experience by augmenting digital signage of game and event action with smartphone access to HD video replays and access to real-time statistics and additional content from their mobile devices during live events. App functionality also makes it easier to share content on social networks to allow the amateur commentator to come alive. But the further integration of IoT can deliver fan user data via their smartphones that can shape real-time and long-term monetization and marketing in profound ways.

Retail IoT for Stadium Connectivity

The concept of the smart stadium can become more of a reality with digital signage and retail IoT for stadiums through the use of sensors that track individual actions by fans.

The fan data from smartphones with customized apps for POS captures what they're buying, where they're moving, and how they're travelling to and from a venue.

To enable data tracking, sensors and beacons can be deployed. Analytics then provides insights for future marketing campaigns, sponsorships and more. Sponsors and event management companies can track fans' behavioral patterns, monitor their location or decision-based data and push appropriate offers accordingly.

Retail IoT for Stadium Connectivity

The WiFi network, transport of IoT sensor data, and the content transmission to digital signage all require highly proactive network virtualization to accommodate bandwidth and routing needs as well security data monitoring. Without this network connectivity, targeted monetization, messaging and security content cannot happen in real time.

By using an intent-based networking approach your IT team can easily configure the network based on real-world needs. This enables understanding of usage and demands while also facilitating real-time reconfiguration in preparation for future event loads, services, and activities that are added to the network.

While the possibilities of this level of connectivity and monetization from digital signage, WiFi, IoT, and network virtualization in stadiums can be a reality, it requires a level of system integration that can only come from a unified design. By having an integration partner like Acadia Technology Group, your stadium can choose the technology solutions that are designed to work together holistically for increased retail profitability and user experience.

RESOURCES

Connected Solutions in IoT

The Current State of IoT by Industry

Retail's Digital Revolution: Real-World Retail IoT Use Cases

Click below to continue the conversation with Acadia Technology Group.

CONTACT US

CISCO™

ACADIA TECHNOLOGY GROUP