Island

How the Enterprise Browser Has Reshaped the Modern Workplace

Island CEO Mike Fey on How Enterprise Browsers Streamline Operations, Fuel Security and Enhance the End User Experience

ISMG
INFORMATION SECURITY
MEDIA GROUP

Digital transformation has permanently altered the way in which organizations manage their network, infrastructure and end users. Still, the most commonly used application within enterprises—the browser itself—remains exactly the same. The problem? The traditional consumer browser isn't an enterprise application.

MIKE FEY

CO-FOUNDER AND CEO, ISLAND

Island co-founder and CEO **Mike Fey** compared having a consumer browser in the modern workplace to using Microsoft Excel or writing a long research paper without a functioning copy-and-paste feature. In contrast, he said, enterprise browsers facilitate efficient business processes through cloud integrations, safeguard sensitive data effectively and deliver a user experience tailored to the needs of business environments *(see: Enterprise Browser Is More Than Just Security)*.

"We've shifted our applications in the cloud; we've shifted our own data centers in the cloud," Fey said. "Now our networks are managed and run from those same locations. The only thing we saw that wasn't changing were the endpoints themselves. We were still acting and behaving in the exact same manner as we were pre-cloud."

In this video interview with Information Security Media Group, Fey also discussed:

- How the enterprise browser streamlines operations and improves efficiency;
- Key benefits including enhanced security and reduced complexity;
- Strategic business insights enabled by the enterprise browser.

Prior to founding Island, Fey served as president and COO at Symantec and before joining Symantec, he served as president and COO of Blue Coat, leading all product and go-to-market functions at both organizations. Before that, Fey was executive vice president and general manager for enterprise products at McAfee and chief technology officer of Intel Security, where he drove the company's vision around network, endpoint and analytics security.

“Every time we’ve been met with a challenge relative to this cloud transition, the answer has been stacking on tech outside of the browser. We’ve been forcing the browser to behave, and not treating the browser like a collaborative member in this journey.”

Benefits of Moving to the Cloud

NOVINSON: How have businesses benefited from moving workloads, applications and data to the cloud? What have been the biggest gains?

FEY: We’ve been on this journey to the cloud so long now, we probably forget all the wonderful things that have happened. When we kicked this off, implementing an ERP system was a massive on-premises project involving thousands of consultants. It was an outrageous expense.

Then a couple of progressive ERP applications show up and they’re in the cloud. All of a sudden, we can just configure them; we don’t have to implement them. We can just engage with them and start to work our way through that. That was our first taste of: What if we don’t own our infrastructure?

Then the Amazons and Google Cloud Platforms and Azures of the world stepped up, and now we can run a data center not only more cost-effectively, but with a more functional path, as well. The networks behind Amazon, Azure and GPC are some of the best networks in the world, so we no longer have to think about how we get to the traffic. We literally are there when we publish into those environments. As we progress, we’ve shifted our applications in the cloud. We’ve shifted to our own data centers in the cloud. Now our networks are managed and run from those same locations.

The only things that hadn’t changed were the endpoints themselves. We were still behaving in the exact same manner as we had pre-cloud. But everything else has made that journey; and it’s driven huge ROI, and a better end-user experience. It’s also improved availability and security. The cloud has delivered on a lot of its promises that led us to believe, “Let’s all move to the cloud.” It took some of us longer to get there, and some of us were dragged there kicking and screaming. But at this point, the world is there.

The Evolution of the Web Browser

NOVINSON: How has the shift to the cloud changed what customers need from their web browser?

FEY: Your first interactions with a web browser 20 years ago involved a flat file reader. Then we realized it might visit sites that we don’t think are that safe or are unsavory, so we started to do web filtering. Then we realized we needed some malware scanning. Now that we’re putting important applications on the web, the data that we interact with might dump onto the desktop, so we then had to govern that desktop. Every time we’ve been met with a challenge relative to this cloud transition, the answer has been stacking on tech outside of the browser. We’ve been forcing the browser to behave, and not treating the browser like a collaborative member in this journey.

"What the Chrome browser does today is no different than 10 years ago. The network's different. The infrastructure's different. The end user is different. The tools are different. But we've continued to use the same consumer browser. We saw the opportunity to modernize that browser for business."

What the Chrome browser does today is no different than 10 years ago. The network's different. The infrastructure's different. The end user is different. The tools are different. But we've continued to use the same consumer browser. We saw the opportunity to modernize that browser for business, for people that are interacting with these important properties in the cloud. Not: How do we shop better? Not: How do we make it easier to watch Netflix? But: How do we engage critical applications in a more mature way and start answering those challenges in the browser itself? Not, how do we keep layering on these additive technologies.

One of our customer's apps didn't work in anybody's browser. It didn't work in Chrome, Edge or Island. But they had a support contract with Island. We were able to actually fix it for them. When that becomes a primary operating system and there's no one to call and nowhere to get help or make a change, it sets a customer up to be at the mercy of these tech giants instead of owning their destiny, which they've owned in every other part of their compute landscape.

The Problems With VDI

NOVINSON: One of the compromises that's often come up is virtual desktop infrastructure or VDI. Why is that not effective when it comes to the interest of the business as well as security interest?

FEY: End users hate VDI. They hate the experience, and it makes sense. They're clicking on their desktop to interact with a server far away, which then backhauls the traffic to a scanning location, which then steers it back to the application. Those are the steps if they're lucky. There could be significantly more bumps in the road. The whole reason that these technologies showed up originally was to take fat apps and push them to the edge, to give us capabilities we didn't have. But now they're being used to create a data barrier. To take that BPO – that business process outsourcer, that call center worker, that BYOD worker – and somehow deliver a format that we can trust as a business.

People are using VDI as a data barrier, and it's very expensive and a poor security approach. The end-user experience is fundamentally flawed. We've moved past the day where our endpoints were undersized. If you go back five or 10 years ago, that Dell you had would be hot at the end of a Zoom session.

But this Mac next to me, I shudder to think at how little I'm challenging it daily. It is so overscoped from the little bit I use of it. As a result, we can do more on the endpoint to enable a better end-user experience that's more cost-effective and more secure.

We started to realize we've asked VDI to do things that it doesn't need to do for reasons it wasn't built for, and we can get back to using it for what it is needed for. It's not about removing it; it's about reducing its usage and delivering a native experience. I love Salesforce. But Salesforce was not designed for us to not work directly in it, and instead go through a multilayer of abstraction to get there.

"An enterprise browser allows beautiful separation of church and state. You can use your browser to shop, surf, enjoy and be that great consumer that we all love to be. When it's time to go to work, you bring up your company's browser."

That's not how the end user experience was expected to be. It is an expensive, painful process to put all these speed bumps in the road. Most of our clientele are looking to change that.

To make matters worse, the VDI market space is raising its prices dramatically at a time when they're not offering new innovations. It is a fork in the road. What does the future look like? What does modernization look like? The answer isn't a hosted OS far away. The answer is let web properties be web properties, and use alternate solutions to deliver fat apps to the edge as needed. But don't build the entire infrastructure for the lowest common denominator.

Benefits of the Enterprise Browser

NOVINSON: Shifting to the enterprise browser, what are the key benefits to the line of business, security, and the end user?

FEY: The definition of enterprise browser is to deliver for those three constituencies. That's what makes it an enterprise browser, not a secure browser or an automation tool. That's the community the product is built for. By embedding a lot of the security controls and then integrating into the existing controls, it's a collaborative member of the estate. It has dexterity in terms of which policy and controls it runs. Collaboration and dexterity are key words.

Take something as simple as governing copy and paste. That can be very helpful, but you don't want to turn that off. Imagine using Excel without copy and paste. Imagine writing a long document without the ability to cut from your email and paste in or to grab something from your research. You want that. You just want to govern how it is done, so you want that dexterity. Think of the cybersecurity portion of that three-pronged approach: It's about simplification and the ability to run a policy simply and effectively with dexterity.

Then we go to the business. How do they understand the digital experience? How do they enable AI? How do they enable contract workers and BYOD and call center workers in the best, most efficient way possible? That's where we see the value start to show up. You'll see companies implement entire real user monitoring strategies where they implement all their apps. They augment them to try to get timings back so they can understand the end-user experience. Meanwhile, the browser has always known that experience, so that data can be shared back now.

When we think about enabling the business and the end user – the third constituency – it's something as simple as giving them multi-copy/paste. Give them 50 copy/paste buffers, but don't just leave them there. Connect to an API that autofills them. If I'm a call center worker, read the VoIP name of the customer, fill in those items, and see where your users cut and paste those. Then automate that for them. If I bring up my browser and try to buy something as a consumer and it doesn't know my address or my credit card, I go to a different site or bring up a different browser. I'm not typing that stuff in.

With just a little bit of awareness, a massive amount of automation can be done and a massive amount of efficiency can be brought to bear. Those are the types of things that an enterprise-focused solution offers but a consumer-based solution has little regard for. The focus on those three constituencies is what drives the enterprise browser at a 30,000-foot level.

Use Cases for the Enterprise Browser

NOVINSON: Let's talk about use cases. What are some of the ways that the enterprise browser is particularly helpful in the case of remote workers, BYOD or firms that are newly acquired?

FEY: BYOD is a macro problem. Everything else is easier. BYOD is the supreme problem because it's a device I don't own and legally can't do much to, and the worker has high trust. They have all the logins and accessibility on the device. In the past, we handled BYOD by saying, "I'm going to configure your device but call it your device. I'm going to push apps out to your device. I'll manipulate the data on that device. You'll have to figure out when you're going to work and when you're not, and you need to own that."

We'd open a VPN that would backhaul all our traffic to work. But why is all my personal traffic going back to work? That doesn't make sense. So, we start turning the VPN on and off. Then you want to control the configuration of the device, so you need an agent that runs all the time. So MDMs show up. A lot of governments have said, "If you put an MDM on that device, you own that device now. If you own that device, you got to pay for that device." The whole BYOD thought process falls apart.

An enterprise browser allows beautiful separation of church and state. You can use your browser to shop, surf, enjoy and be that great consumer that we all love to be. When it's time to go to work, you bring up your company's browser. It's powered by Island, but it's your company's browser. It's their portal, and it'll feel like a portal. You can click on a link and download it, and then it is only running when that person is working on that. You don't have a mix of church and state. You don't have your personal browsing showing up at work.

Because of dexterity control at the policy layer, we can decide what makes sense for the business. Your device may be well-configured. You may be in a geography I trust. You may be accessing applications that are low-risk. Let's play ball. You may be misconfigured, so I want to help you get right. You may be in a geography that doesn't make sense, or you may be trying to access applications that make me nervous, so I want to govern how you do that. I want to redact information or make sure where you can store that data and what you can do with it.

That flexibility allows us to not think of BYOD as a binary on or off. BYOD has always been treated as binary. Open up the VPN and get access to your stuff. Do I or don't I allow you? Those are our decisions. As a result, a lot of companies have either had to take the very risky path of allow or the very draconian path of block. There's a beautiful tapestry in the middle and we can be productive in that zone.

Now let's go to M&A scenarios. I'm a corporation. I just bought a company. I can't trust the IT environment of that company to merge into mine yet. I have to do due diligence and be prudent in how I work with them.

I could treat shared applications like BYOD on day one, but they're way better off than BYOD because they've got their own corporate controls and probably their own security. Adding this in allows both parties – the acquired and the acquirer – to operate and be effective early on.

“We give the end user the experience that the app makers designed. [The apps] were meant to be on-premises and delivered as they built it. We enable that experience to stay there, but we improve visibility, compliance and separation as a by-product of their natural existence.”

In some M&A cases, by taking a more creative approach to the BYOD thought process, we’ve been able to deliver messaging and key applications on day one that normally would’ve taken six months, a year or two years to get there. Contractors and business process outsourcers are just a little different on that gradient of BYOD to M&A, so with just a slight tweak we can enable those as well.

The Enterprise Browser and Business Success

NOVINSON: What are the biggest ways that an enterprise browser facilitates business success in a cloud-driven world?

FEY: One of the biggest ways is that we take the traffic where it needs to go and where it can be used. That’s a starting point. What does that really mean? Right now, in most organizations, all traffic gets routed back through some central scrubbing station somewhere, regardless if that station can do a darn thing with it. Right now, those stations can’t. They don’t do anything with Office or Salesforce or any modern application. Every firewall is bigger than it needs to be, and so is every VPN. Every scrub is bigger than it needs to be. Everything is oversized to add no value. We fix that.

Then it’s the control of the data: Where is the data going? Where can it go? What data should be kept safe? What data should be kept in the application?

Salesforce is a great example.

My reps are in Salesforce all the time. They don’t take data out; they put data in. If I have a sales rep running a report, it’s probably because they’re leaving and they’re taking their customer base with them. Control over that data flow allows me to protect my customer’s data and my company data in a nice, easy way that isn’t 5,000 rules trying to describe what important data looks like. Instead, it says: “Keep Salesforce data in Salesforce. Here’s how we allow for export. Here’s where export can be stored.” Those simple rules allow us to trust our data again.

Then finally, we give the end user the experience that the app makers designed. When these beautiful SaaS app makers built their product, they weren’t planning for it to be streamed over 75 hubs with 26 inspections and then hosted on a VDI infrastructure in another country. It was meant to be on-premises and delivered as they built it. We enable that experience to stay there, but we improve visibility, compliance and security as a by-product of their natural existence.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG INFORMATION SECURITY MEDIA GROUP