CISO JOURNEY

AutoNation

Embracing a New Security Architecture for Access to Internet and SaaS Applications

Company:	AutoNation	**Revenue**:	$22 billion
Sector:	Retail	**Employees:**	28,000
Driver:	Ken Athanasiou	**Countries:**	1
Role:	CISO	**Locations:**	300

Company IT Footprint: AutoNation has approximately 28,000 employees. It is the largest seller of cars in the United States. It has 300+ locations with internet points of presence.

"When ransomware attacks happen to other companies, thousands of systems in their environment are crippled, in addition to having serious impacts with having to pay a ransom. When this kind of event hits the news, I get worried calls from executives, and it warms my heart to be able to tell them, 'We're fine.'"

Ken Athanasiou, VP and Chief Information Security Officer, AutoNation

Excerpt from: Stiennon, Richard "Security Transformation," *Secure Cloud Transformation: The CIO's Journey*. IT-Harvest Press, 2019, pp. 101-113.

AutoNation Journey Overview

Business Objectives

- Closing the digital divide — seamless user experience online and in stores
- Enable new functional capabilities
- Connect 360+ retail locations via the cloud
- Reduce infrastructure, MPLS costs
- Improve security, reporting, visibility, management

The Solution

- Protect customer PII data
- Prioritize cloud vs. data center app migration
- Embrace cloud security, particularly SSL inspection
- Address security debt, processes for inline security
- Create local internet breakouts
- Optimize for Office 365

Impact

- Improved user experience: Less latency, fast Office 365
- Better protection against threats
- Easier to bring new locations, capabilities online
- Greater traffic visibility, better policy management
- Reduced security appliance costs
- Protection against zero-day threats with Cloud Sandbox behavioral analysis

AutoNation is a retail organization with 300 locations selling and servicing automobiles. Ken Athanasiou, Chief Information Security Officer at AutoNation, describes how cloud transformation saved AutoNation money while enabling new capabilities. He stresses the importance of timing and careful planning when embarking on a major strategic initiative such as cloud transformation. He further expands on the importance of being adaptable organizationally, and the willingness to make modifications to plans along the way, and approaching it with more of an agile methodology to prevent false starts and failures.

In the words of Ken Athanasiou:

Flexibility, repeatability, and security through cloud transformation

I've been at AutoNation for a little over three and a half years, as its first CISO. AutoNation has about 28,000 employees and we are the largest seller of cars in the United States. Prior to joining AutoNation, I was at American Eagle Outfitters as its CISO for about seven years. Previously I was at JPMorgan Chase, as the retail line-of-business information security officer, or BISO, for five years.

Journey begins with a breach

AutoNation experienced a small breach with a third-party vendor in 2014 that exposed about 1,800 customer records. That was enough for our general counsel to start asking questions about ways to improve security. He and a few other executives brought in a couple of different firms to do some assessments and make some recommendations, and one of those recommendations was to build out an independent cyber security team that could help them reduce the risks.

Closing the digital divide

At the same time, there was beginning to be a digital divide, especially for the customers. There is also a digital divide between the brick-and-mortar stores where vehicles are sold and our online presence. The intent is to close that divide and present to our customers a comprehensive user experience, where they can begin the shopping, selection, and credit application process online. They can wander into a store, access what they did online, and move the process forward a few steps; they can then go home, make a few decisions, sleep on it, whatever, and then either complete the purchase process online or come into the store the next day.

Closing that digital gap and giving our customers the opportunity to participate in a unique buying experience has become a driver for this organization.

Protecting customer data

There are unique security challenges to being an online auto dealer. We take credit applications every day, and credit applications are obviously about the most

“We’re extremely paranoid about how we handle our customers’ data.”

sensitive personally identifiable information (PII) that you can handle. We also process credit card transactions, so we deal with PCI requirements.

When we have a credit application, we have every piece of information that a bad guy needs to do some pretty robust identity-theft activities, so we’re extremely paranoid about how we handle our customers’ data. A critical element of this process is the ability to protect that type of data, while allowing customers to access it.

Transitioning the CIO

I was hired by a new CIO who had joined the organization just a few months before I did. He was brought in to do some transformational activity and had inherited a significant amount of technology debt within the organization. We made some progress under that CIO and did an enormous amount of work around solving some of that technology debt and getting security in place—and closing some of the most critical gaps that the organization had.

Over the last year and a half or so, we’ve made some dramatic changes within the technology organization. We’ve been able to advance the maturity of the process, get completeness, and instill some robust frameworks.

Backing off on cloud backups

The decision to move to the cloud was made by the technology operations team with our disaster recovery (DR) capability. The misstep we made was to take legacy applications that were heavily dependent upon very large hulking boxes of iron that run very hot and heavy and putting them into a cloud environment without actually refactoring those applications.

The transition didn’t go well. We were about four months late exiting the data center and six months late in actually executing a test against the new cloud DR environment. As predicted, that test failed miserably. We had transactions that had been sub-second go to 60+ seconds from the physical colocation to the cloud environment. It was an abject failure.

One of the first conversations I had with the new technology lead was about fixing our DR environment. We needed to fix it fast, and we had a discussion about what’s the right thing to do. Do we refactor these applications so that they can play well

in the cloud? After some discussions with the application development teams, we determined it would take us approximately two to three years to fully refactor the applications, based on the available resources, the workload, and the business requirements.

We made a decision as a team at that stage that the organization could not suffer that type of risk for such an extended period of time. The executives agreed with us and we built a new colo data center. Brand new hardware, all sorts of beautiful, shiny new toys in that data center, and we moved all those applications out of the cloud, back into the traditional data center.

Timing is everything

Although the decision to go to the cloud was a wonderful idea, the problem was that the time frame associated with doing that transition and the requirements of actually executing that transition weren't fully understood.

As with anything, if you don't truly understand what you need to do, you're likely to fail at it. Unless you are adaptable, and you are willing to make modifications to your plans along the way, and approach it with more of an agile methodology, you will fail.

Embracing cloud security

On the client application side, one of the other things that I did when I first got to AutoNation was to install UTM (unified threat management) devices; these are basically SOHO, small home office types of appliances, that combine all the features and functionality of the next-gen firewall on a very small platform.

We had 300+ locations with internet points of presence. The networking team was intending to deploy more than 300 little boxes across the entire country and that's when I decided it was time for us to learn more about this cool cloud-based network firewall solution that I'd heard of called Zscaler. That's when I called up Jay and his team and asked to meet with them.

Instead of doing the little boxes of iron across the entire country and rolling trucks all over the place and having to manage that nightmare architecture, we went down the Zscaler route, which was intense. I didn't sleep for probably six months. I was worried

about our exposure. Every time I went to bed, I expected to wake up to a major breach until we got Zscaler rolled out across the environment.

Addressing the security debt

There were quite a few issues that we uncovered as soon as we wrapped Zscaler as a prophylactic around the environment—lack of robust patching and IT hygiene, the ineffectiveness of the McAfee antivirus that we were running, broken update processes across the board, very old systems, middleware that wasn't being patched.

We looked at various engines that were out there, including hardware based. Three years ago, there really wasn't any other cloud-based solution that was even comparable to the capabilities that Zscaler had. They were the only true, full-protocol firewall in the cloud. They had the most robust capabilities. Everything else was pretty much just a web proxy. You can pump your traffic through that, but it's definitely not the same thing.

The rollout decision was a no-brainer

Zscaler was just a completely different architecture, so we made the decision to pilot Zscaler and see how it looked and felt. We rolled out Zscaler to a couple of stores and our corporate headquarters and we let that run for a little bit. Again, the visibility we got into outbound bot traffic, and obvious infections and those sorts of things very quickly upped the urgency of getting a solution deployed across the entire environment.

It became pretty much a no-brainer, and we made the decision to go forward with this even if we had to break a bunch of stuff in order to filter traffic and gain control. We invested capital to drive some maturity into our patching processes and to improve our anti-malware controls.

We took advantage of Zscaler's anti-malware. When I was first talking with the Zscaler team, I was adamant that I wanted full-blown next-gen firewall capabilities, which would include filtering network-based malware detection and sandboxing.

We are now pretty much fully deployed with Zscaler capabilities. We're currently not making extensive use of its Zscaler Private Access to access our internal

applications, although it's compelling. We just simply haven't had the opportunity to really push that out very far. But we've got pretty much everything else, like DLP, and all the obvious stuff around the URL filtering. We are now a heavy consumer of Zscaler capabilities and we've been very pleased with the controls that we got from them.

Penetration testing has become more difficult, and that's a good thing

We do aggressive penetration testing using third-party vendors. It's common for them to become stymied by the Zscaler layer when they're doing remote testing, because they simply can't penetrate the malware and sandboxing controls and get anything to work. That's also a result of the changes that we've made around patching. We're using Tanium for endpoint management across our entire environment, which I am just in love with—it's a fantastic piece of technology.

So, with all these additional controls in place and obviously driving mature patch processes throughout our environment, our resiliency—our hardness, so to speak—has just gone several levels above where we were previously.

Seeing is believing: The value of reporting

For reporting we don't often use the stock stuff that comes out of Zscaler, but we do pull numbers from it to include in board presentations. I show the board a bunch of gee-whiz numbers, and these gee-whiz numbers show for the most part how much we're under attack. The reason I call these gee-whiz numbers is because every single one of these attacks was blocked or prevented by one of the engines that we have in place. This particular set of numbers shows all the attacks or incidents that were blocked or prevented by our cloud-based firewall solution, Zscaler.

It's more of a validation that this is stuff that we would have to deal with if we didn't have these controls in place, but the fact is, we do have these controls and, therefore, we wouldn't consider these incidents or really anything all that important to deal with. We don't react to them because they're noise that is filtered out by the engines that we have in place.

“We’ve gotten down to a seven-day patch cycle, and that’s not even a critical or an urgent cycle. If we have a critical patch that needs to be pushed, we can do that in about 24-hours.”

The senior executive staff loves the numbers, because they look at them and they go, “Holy smokes, that’s a lot!” Every now and again, we do see spikes in attack activity and I usually end up having to explain the spikes. “What happened there where it jumped up so high?” they’ll ask, and then I’ll usually explain how there is a zero-day exploit or a critical vulnerability that was discovered and we see an enormous amount of traffic attacking that critical vulnerability because it was fresh and new.

“We’re fine”

When ransomware attacks happen to other companies, thousands of systems in their environment are crippled, in addition to having serious impacts with having to pay a ransom. When this kind of event hits the news, I get worried calls from executives, and it warms my heart to be able to tell them, “We’re fine.”

We’ve gotten down to a seven-day patch cycle, and that’s not even a critical or an urgent cycle. If we have a critical patch that needs to be pushed, we can do that in about 24-hours.

Piloting the types of engines that can give visibility into the state of your environment, like the level of botnet traffic and infections, is something that you can then use to drive further activity, spending, and resource implementation.

It’s important to really understand what is going on in your environment in terms of infections and risk levels in order to put something like Zscaler in place. For example, if you have 70 infections, you will find that maybe your patch processes are broken. Then, you could start piloting a couple of engines that look at EDR, response, and software distribution packages. Do a side-by-side comparison, and you’ll find that your Microsoft SCCM product says you’re fully patched—but then when you run something that’s independent of Microsoft against that, it says you’re only patched at about 50%. Well, in that case, you’ve got things in your environment that are missing patches, that are two years old, so something’s wrong there. Again, that would drive further activity to resolve.

Our Office 365 implementation needed more bandwidth at each point of presence

As we made the transition to Office 365, we had to learn how to implement the process. Originally, we were going to have everybody use the portal and not bother putting Office on individual machines. Also, we didn't have the required bandwidth. It didn't work, so we had to step back and change up how we do things as a process. Now we're doing local installs of Office 365, and we're executing the product differently. It works much better now.

At the time, every one of our locations had from a T-1 up to a multiple T-1 type of MPLS connection back to our data center, so very small pipes for the private circuit back to the data center.

Internet access was also not all that great. You're talking somewhere around ten megabits per second type of connections to the internet, which, obviously, if you're not careful with that type of an environment, you will easily clog those pipes and you will have very degraded performance.

Local internet breakouts helped reduce costs

After we got the new technology leadership in place, we renegotiated with our providers and we significantly reduced our network bandwidth cost and jacked up our bandwidth ten-fold. We went from very small MPLS circuits to ten and 20 megabits per second MPLS circuits back to our data center, and 150 megabits per second connections to the internet for the most part. We had very significant increases in performance and capability for internet bandwidth, and again, that was primarily due to a technology gap, lack of planning, and a lack of understanding of the bandwidth requirements involving our most used applications. We still do have MPLS circuits and we have internet circuits. The vast majority of our traffic goes direct to the internet, but we do have internal applications, like our CRM and some other systems, that we just simply backhaul across the MPLS circuit.

Today, we are still using a hybrid network. We have considered doing away with those MPLS circuits and going full internet, maybe using things like a ZPA, but we've not made that transition at this point.

“When we do acquisitions or divestitures, it’s very easy to enroll a new location in our environment.”

We don’t use Zscaler for mobile devices at this point. That’s another one of those things that’s on the list, but we have not actually executed against it. We’re transitioning from Intune over to AirWatch right now for MDM, and once we complete that, we’ll go back and look at what else we could do in that space.

Improving the user experience

One of the other advantages that we’ve gotten out of Zscaler for some of our other cloud-based applications is that the connection speeds through Zscaler are actually pretty robust. This goes back to the peering that Zscaler has done with a lot of the other larger providers out there, like with Microsoft and Office 365. Our number of hops—even though we have to do a tunnel from our external router into the nearest Zscaler cloud, and from Zscaler to Office 365—is only one or two hops, versus going directly from our dealership to the internet; it would actually take longer to get to the service than going through Zscaler.

Instead of inducing additional latency because of those pairing connections, we get all our controls in place and we see very minimal latency and, in some cases, our connections are actually even faster.

Taking advantage of cloud capabilities

There are multiple inherent advantages of moving to the cloud. You get better resiliency, you get better scalability, you get a lot of really cool abilities that you can’t get out of a standard colo environment, and as you re-architect your legacy applications, as you build new applications so that they’re actually cloud-focused and can natively take advantage of those capabilities, I expect that we will continue to see more and more of these applications move into this model.

Another advantage is in mergers and acquisitions. For M&A, Zscaler has been a big win for us. When we do acquisitions or divestitures, it’s very easy to enroll a new location in our environment. We don’t have to roll a piece of security hardware out there. For the acquired entity, we simply configure the tunnels for the internet bound traffic to Zscaler and we’re covered.

One of the things that we’ve found to be a little interesting is when we divest a dealership, the acquirer comes in, and they may ask us what we do for our network security.

They ask us where our firewall is located. Our response to that has been—we use Zscaler, so you don't have a physical firewall in there. You're going to have to figure something out. They don't like that answer because they're used to just taking whatever was there and making use of it.

When we do an acquisition, we do more of a rip-and-replace for the technology environment. We may purchase computers with an acquisition, but then we generally will rip them out. We'll resell them to someone else and put our stuff in.

Ready to transform your company?

Create business value with Zscaler today.

CONTACT US

REQUEST DEMO

https://www.zscaler.com/company/contact

https://www.zscaler.com/custom-product-demo

About Zscaler Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.