CDO JOURNEY

Schneider Electric

SaaS as the catalyst for energy management leader's cloud transformation journey

Company:	Schneider Electric	**Revenue:**	$32 billion
Sector:	Listed Company	**Employees:**	144,000
Driver:	Hervé Coureil	**Countries:**	100+
Role:	Chief Digital Officer	**Locations:**	290

Company IT Footprint: Schneider Electric is a French multinational corporation that specializes in energy management and automation solutions, spanning hardware, software, and services. Schneider's IT footprint spans over 100,000 connected users in 100 countries.

> *"Many companies look at 'cloud-first' without assessing the network changes this entails. When we started to adopt cloud-delivered applications, we had to understand how our network architecture would be impacted by the cloud. There is a pretty significant network transformation required."*

Hervé Coureil, Chief Digital Officer, Schneider Electric

Excerpt from: Stiennon, Richard "Moving Applications to the Cloud," *Secure Cloud Transformation: The CIO's Journey*. IT-Harvest Press, 2019, pp. 41-50.

Schneider Electric Journey Overview

Business Objectives

- Move to the cloud
- Simplify infrastructure complexity
- Improve security
- Enable global app, network, resource, mobile access
- Improve scalability

The Solution

- Create a digital transformation team
- Integrate customer experience, user experience, business priorities
- Transform in three stages:
  - Adopt SaaS apps
  - Migrate internal apps
  - Develop IoT, mobile capabilities
  - Classify and protect critical data
- Improve security: Sandboxing, DLP
- Plan for growth

Impact

- Support for internet usage growth
- Reduced costs
- Improved service quality with local internet breakouts
- Improved security
- Support for network voice and mobile access
- Cloud adoption across the global organization
- Improved measurement, utilization reporting

Schneider Electric is one of the largest industrial equipment manufacturers in the world. For Schneider, the move to cloud was precipitated by SaaS as an early customer of Salesforce, and it became a global initiative. Schneider characterizes digital transformation as an initiative that goes beyond technology to encompass its customer experience, user experience, and business in general. Here, Hervé Coureil, Chief Digital Officer of Schneider Electric, describes his organization's cloud transformation journey.

In the words of Hervé Coureil:

> At Schneider Electric, our cloud journey began with the move to Salesforce. It became a global initiative that succeeded, and we leveraged that success for everything that came after.

I have been with the company for quite a long time. I started in finance and did a lot of M&A work. When we acquired APC in 2007, I was sent there to drive the merger integration with the title CFO. It was an opportunity to see what happens after the M&A, instead of just orchestrating the deal.

During that time, I realized that information technology was on the critical path to drive business convergence and integration. I also developed a keen interest in security. Schneider at that time had started a program to integrate IT across all of its businesses. The company decided to invest in technology and created the position of global CIO, which fell to me. The CIOs from all of the countries would report to this position. Soon after that, digital transformation became a super-hot topic.

Digital transformation goes well beyond technology to our customer experience, our user experience, and business in general. Last year, we created a digital team that would help us in that digital transformation journey. We took into account sales support, automation, and other projects.

That's why I moved to the role of Chief Digital Officer. It's quite a large team, including a new global CIO who reports directly to me.

The three stages of cloud transformation

The cloud is an enabler from a number of perspectives. It was not completely linear, but there were three distinct stages.

Stage 1: Started with software as a service. Schneider was an early customer of Salesforce. We saw SaaS as a way to enable our transformation. Leveraging SaaS also made a lot of sense for bringing together organizations as a result of many acquisitions. One of the gains was in speed of deployment.

Stage 2: We looked at cloud as a way to transform our infrastructure. Transforming the network is required to take advantage of the cloud.

Stage 3: Involved the cloud and the internet of things to provide new services to our customers. We could not do that without the cloud and mobility—the two mega-trends.

Wide-usage of SaaS applications

We just finalized a major undertaking to move to Office 365 backed by Box for file sharing and storage.

It's difficult to quantify how many sanctioned SaaS applications we have. I would estimate somewhere between 50 and 100. Counting the number of applications is a very common problem. We also took another look at our toolsets for monitoring the applications used in our network. Now we use Zscaler to monitor and notify us of application usage.

Our SaaS applications are segmented into three categories:

1. Internal applications that are connected to single sign-on and managed by us.
2. Applications that we might get alerts on—things like who is using them and how much.
3. Applications that we ban and block.

The migration of internal applications

We used to be a Lotus Notes user. Over the years, we had developed thousands of custom applications for Lotus. One of the big things we are doing in migrating to Office 365 is that we are working on moving as many of those Lotus functions as possible. We had a governance issue at one point, and it was impossible to know how all those applications were being used and what data they were using, and we tried to retire any application that was not needed anymore. We also looked at every application that was developed that could be used in the existing landscape. We had quite a few applications that had been developed on Lotus Notes that would be better served by Salesforce, so we migrated them. In the case of no

existing application, we are developing them natively in the cloud. Our partners are instrumental in making that happen.

We do a little bit of both internal and external application development. We are relying on partners but some applications are developed in-house. One of the big challenges is that many of our applications were deployed ten years ago, and the people who developed them are no longer with the organization. Some of the applications had been developed by citizen developers—people who were not even part of the IT organization. There is very limited tribal knowledge remaining for some of the things that were in use. That meant we had to engage in a little digital archeology exercise to reverse engineer the applications and re-develop them for the cloud.

Framework and controls to build right applications for the cloud

We are aware that without careful planning moving to the cloud can pose new challenges. Our goal is to create local environments, so people can develop workflows and simple applications. Rather than slow things down by banning these quick and effective developments, we want to create an environment that is supportive of them.

On the one hand, we want to enable the development of applications, but at the same time, we do not want to create more technical debt. We strive for an empowerment framework. We want everyone to be able to build what they need. So we have two control points:

1. Go through the main portal to determine if we already have a suitable application. It's a very simple process to search and discover apps. The internal customer should make sure the application was not developed somewhere else. In one case, we had a request come through and quickly determined that a team in Italy had already developed something that met the need.

2. Downstream, the second control is an internal privacy and security certification. We want to make sure that we are dotting the i's and crossing the t's when it

“When we started to adopt cloud-delivered applications, we had to understand how our network architecture would be impacted by the cloud.“

> comes to security. So we vet the applications to ensure they do not introduce a privacy issue, perhaps by collecting data, or open up a security issue.

While it is not written in stone, we have a high-level philosophy of all new applications being built for the cloud.

Our network transformation: MPLS to direct connection to cloud

Many companies look at “cloud-first” without assessing the network changes this entails. When we started to adopt cloud-delivered applications, we had to understand how our network architecture would be impacted by the cloud. There is a pretty significant network transformation required. First, we looked at the architecture: MPLS and the number of network access points versus direct connections to cloud providers.

The second thing that’s relevant from a network standpoint is the security of local internet breakouts from each office. That is where we invested in Zscaler.

We have more local breakouts than we used to have. Before the cloud, internet access was a second-class citizen. After the cloud, it becomes a critical element of our network usage.

We used to have firewalls and numerous other hardware appliances, but now we have a cloud-first strategy that Zscaler has allowed us to do.

While local breakouts provide one benefit—cost savings—another has been quality of service. Schneider is a global company with over 100,000 connected users. Many countries don’t necessarily have the best local network architecture, and one of the things we were trying achieve was a good response time globally.

On top of that, we have a mobile strategy. We try to give people voice access to the network, and we enable BYOD (bring your own device) in every country where possible.

> *“Our security strategy focuses on protecting the crown jewels.”*

Classifying and protecting critical data

Our security strategy focuses on protecting the crown jewels, the most significant intellectual property in the company. This approach means that we have to be good at data classification. When identifying those crown jewels to protect, the natural tendency is to be super conservative; everything is a crown jewel. To instill discipline in the process, we designated one person whose role is to look at the identification of those crown jewels: our confidential information, sensitive IP, and of course, privacy data. We try to keep the crown jewel category very limited.

When we certify each internal application, we look at both security and privacy criteria. We have a Data Protection Officer running our EU General Data Protection Regulation (GDPR) program. When we certify a new application, we do a privacy assessment at the same time as security to ensure that we are only collecting the data we need, that we properly notify the end users when we collect it, and we take precautions to protect it.

Security: the key to cloud transformation

Security is an obvious priority. Without it, the rest of cloud transformation cannot happen. We have been thinking a lot about the security model and considering how to look at the cloud security we wanted to adapt.

Security is never over. Incident response is a big topic, as is network segmentation, network monitoring, and endpoint protection. We have eight or nine security initiatives currently.

While data loss prevention (DLP) is one of the things we looked at, we decided it is a very heavy burden to take on. There are so many ways to exfiltrate data. So, to begin, we have taken a very light approach. Applications should be DLP-secure at the application level. Since we are inspecting traffic in both directions, it is a simple matter of looking for common things like personally identifiable information (PII) and set an alert or block them.

We’re using sandboxing technology to stay on top of advanced malware. We have deployed the Zscaler sandbox in the cloud to identify malware in files and internet sites our users may visit. We also believe that having a centralized identity

management system is important to a successful cloud strategy. We use Active Directory and another product for single sign-on.

It is not very original, but you can feel very safe inside of a castle—but you don't see the known unknowns on your extended perimeter. Our cloud strategy allows us to have a much more global approach.

Legacy approaches to security are complicated, requiring isolated mini-castles in every office. You have to replicate your headquarters security stack in every location. The cloud allows us to be much better at managing multiple sites in multiple countries with one control plane.

Challenges along the way

There was a bit of resistance to our cloud transformation, but it wasn't massive. For us, the defining point was the global move to Salesforce, which was a great success. We managed to embrace it relatively quickly. From there, we had created our first success story. We had deployed it faster than we would have deployed a traditional on-premises solution.

We had a couple of issues in our journey to the cloud. The main problem we had was quality of service in certain places. The experience in the United States with Salesforce was not replicated everywhere, and we learned the hard way that some countries do not have the best infrastructure. We had to rethink the network globally.

While measuring results is important, we are not looking at one golden metric that will summarize all the good things we achieved through cloud transformation. But every time we launch a project, we do monitor its success. When we deployed the custom application environment, we looked at how we are modernizing the application base. For every application we are decommissioning, we have a gain we can chalk up. Cloud is now so pervasive in everything we do that we look at the metrics of utilization.

How is internet usage growing? Since our initial move to Salesforce, we have seen cloud usage grow steadily. That first step started us on this journey.

What not to do:

- I would advise against going too broad. Don't try to boil the ocean and do everything at one time. Deploy a pilot, have a success story, and build on that.
- Do not ignore the network implications. Look at the network architecture at the beginning of the cloud adoption. Try to get ahead of the problems.

What to do:

- Cloud is a means to an end. You want to create customer and business value. Cloud enables machine learning, which enables voice. Voice has its own benefits that lead to collaboration opportunities.
- Cloud allows you to connect sites together more quickly. Just point all the users at the apps.
- When talking to my peers in the industry, a lot of the conversations I have revolved around big questions. What's next? What is the next wave? How do we prepare for the new trends? We are forward-looking, while keeping security concerns front and center.

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.

© 2019 Zscaler, Inc. All rights reserved. Zscaler™ is either (i) a registered trademark or service mark or (ii) a trademark or service mark of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.