Breaking The Mold: How Zoho's Stance on Privacy and Security Benefits Customers

An Enterprise Applications Consulting Focus Report

Joshua Greenbaum, Principal

Fall 2021

This is the third in a series of reports on the different ways in which Zoho breaks the mold in the enterprise software space and how that benefits its customers. This first report looked at Zoho's customer-friendly licensing and pricing model, while the second report explored how Zoho supports its customers' heterogeneous software environments. This report highlights how Zoho's longstanding policies regarding privacy and security help to safeguards its customers, and their customers too.

Introduction: Security and Privacy as Core Values

The issues surrounding the privacy and security of data in the enterprise have never been more important than they are today. Regulators around the globe are questioning the tools and technologies that have created an increasingly invasive surveillance economy that is encroaching on civil liberties and personal privacy. Simultaneously, companies are facing the threat of ransomware and illicit access to corporate IP as well as customers' personally identifiable information (PII) at an alarming rate.

A lot of vendors have only recently woken up to the threat these twin problems pose, and not always with the same reactions. For some enterprise and consumer software vendors, the surveillance economy and its endless tracking and accumulation of personal data are important parts of those vendors' business models. So while all agree that ransomware and IP and PII theft are important problems to solve, the issue of whether a vendor should be enabling or blocking the underlying tools of the surveillance economy are still up for debate in some companies.

At Zoho, the security issues relating to ransomware has been on the front burners for many years, and when it comes to the surveillance economy, the company has consistently backed away from playing a role in enabling these capabilities. Importantly, for Zoho the two issues are deeply intertwined and

indicative of a culture of security and privacy that has been a core value, instead of an afterthought, for years. An important moment in that history took place in 2002, when Zoho acquired what became its Managed Engine IT services division. Managed Engine has had a focus on enterprise-level security for decades, and the acquisition helped reinforce a strong focus on security and privacy that had been imbued in the company long before it became a "popular" concept, according to Vijay Sundaram, chief strategy officer at Zoho. "We took a stance on privacy many years ago," Sundaram said. "We now find ourselves ahead of the regulations and we have people who have been doing this for 15 years."

"A lot of this goes back to core convictions we've held from our origins," Sundaram added.

Those convictions are at play in three fundamental ways. The first is that Zoho limits how much tracking occurs on its own websites, trying to strike a balance between automation, personalization, and privacy while erring on the side of privacy at every opportunity, Raju Vegesna, chief evangelist at Zoho, told Enterprise Applications Consulting. The second factor is that Zoho runs its own datacenters, and its software is built organically, not acquired. This is a huge advantage over vendors that have to manage security and privacy in products that run on multiple cloud platforms and were built on different code bases and with vastly different security and privacy regimes. "When you own all the individual components, security can be tightly integrated into the system itself," Sundaram pointed out. "When you own everything, you can secure better."

The third factor is that this focus on privacy and security and the control that Zoho has over the development and deployment of its applications means that the apps themselves have an exceptionally high degree of built-in security and privacy. The organic development model that Zoho was built on, combined with the fact that its CRM and Zoho One apps run exclusively on Zoho's own cloud, means that the company is able to provide levels of security and privacy that other companies could do only at great expense, expenses that are then passed on to their customers.

Zoho's model is much more efficient while delivering an equivalent level of security and privacy, Sundaram explained. "A lot of it doesn't take massive capital investment," Sundaram said. "It takes know-how."

Security and Privacy that Meet the Customer's Needs

The fact that the Zoho has built top-level security and privacy into its applications as well as its cloud backend is a hugely important issue for customers like Call Center Sales Pro, a provider of outsourced call center services based in Seymour, TN.

The company operates call centers for a wide variety of customers, many of which are in industries, like healthcare, that have strict privacy regulations that mandate significant penalties for organizations that violate that privacy. "For a call center, data privacy is paramount to our existence," explained Marc Fishman, director of Sales and Marketing at Call Center Sales Pro. "We would run ourselves out of business without it."

In addition to the security and privacy provided by the Zoho cloud, Zoho's applications allow the company to manage these issues at the individual employee level as well. Call centers can have relatively high rates of employee turnover, and it's important to make sure that a former employee's system access is rapidly and thoroughly deactivated, just as it is equally important to be able to quickly

on-board a new employee at the appropriate level of access. “Zoho makes it easy to manage accounts,” Fishman said. “Reassignments can happen very quickly without worry.”

That trust extends to the cloud backend too. “If there is anything wrong with our site, chances are they’re the first ones to know it,” Fishman added. “Our data is very secure.”

For customer Artic Spas, a spa manufacturer and distributor based in Thorsby, Alberta, its unique business and global footprint means that ensuring data privacy, particularly with respect to customer data, isn’t something that every CRM application can do and still meet the company’s requirements, according to Mike Sigvaldason, corporate Zoho administrator at Arctic Spas.

The company’s websites – there are over 160 localized websites worldwide – are used to channel customer leads to its network of dealers. Sigvaldason has added a geo-coding capability to Zoho CRM that sends customer information to the appropriate dealership based on the location of the prospective customer. Nonetheless, ensuring that dealers don’t poach each other’s leads was something the company struggled with before implementing Zoho.

“One of our biggest problems with different systems was maintaining customer privacy between dealers,” Sigvaldason explained. “I was able to use role of admin in Zoho to do this.”

The company also has to navigate a complex set of regulatory regimes relating to the customer data it acquires and uses in its CRM and fulfillment processes. As a Canadian company, Artic Spas has to comply with a Canadian anti-spam law, called CASL, which came into effect in 2014, as well as Europe’s GDPR data protection regulations. And because its products can be used for medically therapeutic purposes, Artic Spas has to comply with Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA) as well as the Health Insurance Portability and Accountability Act (HIPAA) in the United States.

Zoho was already compliant with GDPR, HIPAA and PIPEDA out-of-the box, and Sigvaldason was able to implement the fundamental protections required by CASL using his admin functionality. As this is a relatively new and less well-understood law than the others, Zoho is currently in the process of adding full CASL compliance directly to its products, Sigvaldason said.

On the backend, Zoho’s ability to protect its customers from hacking recently helped prevent a serious data breach at Arctic Spas, one that could have exposed sensitive customer and financial data. Knowing that Zoho’s security team was on the job was important, Sigvaldason said. “We take our customers’ needs for security seriously, and I’m happy with how Zoho takes their security seriously too.”

It’s Not Just About the Bottom Line

The focus on privacy is of course a requirement for selling software, and there’s no getting around the issue for Zoho or any enterprise software company. But unlike many vendors, Zoho’s decision to forgo monetizing the data in its cloud as part of a more typical vendor business model is a choice that Zoho makes willingly, despite the potential loss of revenue and opportunity it faces from this decision, Sundaram explained.

“We don’t want to make money by selling people’s data. It’s driven by ethical considerations,” said Sundaram. “We know we may be giving up some advantages. I can live with that.”

Judging by the company’s success, its customers feel they don’t just have to live with these policies, they can actually thrive within the context of Zoho’s security and privacy practices. “I like having a better

experience for the customer and the end user," Sigvaldason explained. And it's one that is safe and secure. As it should be.