WHITE PAPER

The Apstra Zero Lock-in Guarantee

How to Free Yourself From Hardware Vendor Lock-In

apstra®

Table of Contents

Apstra is committed to eliminating hardware vendor lock-in forever. This is a cause customers have recognized Apstra for, and one Apstra believes is mandatory if organizations are serious about digitally transforming and delivering on the goals of the business.

Hardware vendor lock-in has a long history.

Years ago, there were proprietary networking solutions like IBM Token Ring. Every new PO had to go to the same vendor if customers wanted to ensure connectivity.

Then came Ethernet which promised to be an open interoperable standard. However, vendors recreated lock-in by implementing proprietary VLAN extensions such as private VLANs.

Internet Protocol (IP) was another open standard, but hardware vendors came out with proprietary routing protocols such as IGRP which were designed to lock customers into the hardware vendor's equipment exclusively.

Today, with the emergence of whitebox switches and open source switch operating systems, vendor lock-in has become more critical than ever for the hardware vendors to defend themselves from the competition using vendor lock in. This also makes it more important than ever for businesses who want the freedom to defend themselves from lock in while having the flexibility to be vendor agnostic.

With white box switches, open source device operating systems, and commoditization on the rise what is the new hardware vendor lock-in strategy? Hardware vendors are coming out with proprietary management APIs which lock their hardware to their management systems. This is arguably the uber form of lock-in! These proprietary network management solutions are the ultimate form of lock-in - not the SNMP add-ons of the past, but sophisticated network monitoring, configuration and trouble-shooting solutions that only work with that one vendor's equipment.

Yes, the vendor may claim that the customer can use their management system with another vendor's equipment, but do customers really believe they are going to enable a competitor's hardware and software solution? Imagine the finger pointing when there is a problem!

Apstra gives IT freedom from endless vendor lock-in.

We're not alone in recommending against vendor lock-in. Quoting leading industry analyst Gartner, "I&O leaders should never rely on a single vendor for the architecture and products of their network, as it can lead to vendor lock-in, higher acquisition costs and technical constraints that limit agility." We agree.

So how does Apstra free IT from vendor lock-in?
We use the following three pronged approach:

1 Abstracting Away Hardware (and Offering Hardware Vendor Choice) Through Intent

Leveraging Apstra's intent-based approach, Apstra Intent-Based Data Center Automation starts at the system level, rather than the device level, and defines the services and requirements that need to be delivered and met by the system. These requirements are defined by the end user and incorporate all the capabilities that the customer needs from their infrastructure. These capabilities include underlay connectivity, overlay, security, compliance, policy, performance, traffic engineering, application performance, SLAs, etc. Requirement and services definition is done at the system level without any dependency or selection of a specific hardware platform or device operating system. Once the user's intent is specified, the user has the flexibility to choose specific hardware devices and operating systems. It is only at this point that these requirements are translated into specific vendor decisions, configurations, and telemetry gathering. This translation is done by AOS (Apstra Operating System) which knows how to control the device through configuration commands and how to extract telemetry from the device.

If a hardware vendor neglects to or inadvertently fails to maintain consistency with any of their prior APIs, Apstra Intent-Based Data Center Automation simply modifies the interface to that API to take advantage of the latest APIs. In doing so Apstra takes on the role of the expert on the differences between vendors (even between the same vendor's own products) ensuring our customers make best use of each vendor's equipment and features, while avoiding any pitfalls.

This enables Apstra to provide the widest range of hardware and software vendor choices that has ever existed in the industry. Apstra supports established vendors (Cisco, Arista, Juniper), as well as open alternatives (Cumulus, OpenSwitch, SONiC).

This unique approach allows Apstra to support, develop, update, configure, and test hardware platforms and device operating systems faster than end users would even need to deploy new versions of these platforms. This applies to the latest version of a device OS and new vendor platforms that an end user is deploying in their infrastructure.

Whether a business is building a new data center, refreshing an existing data center, or upgrading a few devices in the data center, the IT team is able to accelerate qualification of the hardware platforms and operating systems by leveraging the testing, qualifications, and support that Apstra has already done. IT benefits from Apstra's testing of devices and Switch OS's in their infrastructure and with their configuration before they consider going ahead and deploying it.

Apstra Intent-Based Data Center Automation also translates user requirements and services across multi-vendor implementations which ensures interoperability between different vendors.

2 One throat to choke without Lock-in

When a customer automates their infrastructure using Apstra Intent-Based Data Center Automation Apstra stands behind the entire system and services delivered by the infrastructure, including the hardware devices that make up this infrastructure. In other words, Apstra acts as the “one throat to choke” without forcing hardware lock-in. Customers get the benefit of choice without the risk of going it alone. This commitment includes the following:

If issues are observed in the infrastructure, the customer calls Apstra. No questions asked. Apstra is on the side of the customer.

1. **If Apstra determines that the issue is caused by the hardware vendor or device operating system,** Apstra determines if there is a way to mitigate the issue using Apstra Intent-Based Data Center Automation. There are many situations such as memory leaks in processes on the devices which can be mitigated using technologies like Apstra Intent-Based Analytics coupled with Apstra self-healing capabilities.
2. **If Apstra determines that the issues are beyond the scope of what Apstra can mitigate**, then Apstra commits to help the customer swap the hardware platform or operating system for one that Apstra knows works.
3. **If the customer is not interested or able to swap out the hardware platform**, then Apstra recommends involving the hardware vendor and will join in on initial and on-going calls at the request of the customer. Aprtra will leverage its infrastructure and partners to help debug the issue and get it to the fastest resolution.

Five millions of tests a day

How is Apstra able to provide this level of support? The simple answer is that we operate the most powerful automated test bed in the industry.

> Apstra runs tens of thousands of continuous tests per commit, per branch, across hundreds of devices from multiple vendors including a range of switch operating systems, chipsets, and models, and thousands of virtual appliances from multiple vendors. This amounts to more than five million tests a day.

Apstra is also able to automatically run these tests at our customers’ sites for new hardware platforms which may not be part of the Apstra testbed. If those tests pass, Apstra commits to supporting those devices, also. If those tests fail, then our customers are empowered with this information so they can decide which hardware platforms and operating systems to deploy in their infrastructure.

3 Uniquely Open and Extensible Architecture

Apstra believes in being part of a horizontally layered architecture, whereby layers are loosely coupled through APIs to avoid lock-in. Apstra Intent-Based Data Center Automation operates at the management plane. Apstra Intent-Based Data Center Automation supports data planes from various hardware vendors and does not replace the data plane. Apstra Intent-Based Data Center Automation supports various control plane protocols from various hardware vendors and device OS vendors and does not replace the control plane.

The network will operate without Apstra. Customers can even turn off the Apstra solution completely and the devices, operating systems, and network will continue operating. Customers can then continue controlling them using any other method they wish. Whether manual, or using other automation solutions, or software developed using a DIY model. With Apstra there is absolutely zero lock in.

Apstra stands committed to never break the Apstra APIs or threaten to do so in order to prevent customers from using other solutions. Apstra Intent-Based Data Center Automation is driven by open APIs; these open APIs drive the Apstra web UI; they are used to integrate with other systems such as ServiceNow, Slack, Infoblox, etc.. Apstra uses protocol buffers to stream out all telemetry. Apstra uses graph queries to manipulate the graph datastore representation that is at the core of our system. Zero lock-in.

The Apstra solution is fully extensible and customizable to meet customers' specific needs. Contrary to other solutions, Apstra doesn't expect customers to change their requirements to meet Apstra's solution - rather, the Apstra solution can be uniquely customized to the user's requirements. Zero lock-in.

Does your vendor really practice what it preaches about being open?

A situation that has happened to Apstra customers more than once illustrates the importance of the Apstra commitment to its core mission.

Apstra would be in the last stage of closing a deal and in a last ditch effort to lock-in their "customer" the sales team from a hardware vendor tries to dissuade the infrastructure team from going with Apstra by positioning their own management software solution instead. Apstra is always very respectful of fair competition, but often come out baffled by one of the arguments that this hardware vendor throws at their customer. They tell them that since the hardware vendor controls the hardware devices they could, if they wanted to, change their presumably open, and public APIs to disrupt Apstra's ability to interface with their devices. This effectively hurts their own customers that rely on these APIs, as well as their large community of ecosystems and partners that are dependent on these APIs.

The intent is to FUD (fear, uncertainty, and doubt) the customer into locking themselves into the hardware vendor's solution and only use the management/analytics software offered by that hardware vendor. It's the archetype of "the offer that they can't refuse" from the movie "The Godfather".

This is baffling for more than one reason:

1. The hardware vendor, in an attempt to lock their customers into their solutions, is essentially threatening them that they'll act against their interest - that is, the interest of their own customers by sabotaging their own hardware, so it doesn't work with other elements in their customers' infrastructure!

2. These hardware vendors, compelled by the agility and business needs of their customers, have gone to great lengths developing and advertising open APIs. Some even committing their full support for open networking and open source systems such as SONiC. And they've built large ecosystems and partnerships around these APIs. Yet behind closed doors, not only are they not supporting these open systems, they're going one step further by threatening their loyal customers that use these open APIs.

Needless to say, this attempt at control does not go over well with customers who are fed up with vendor lock in. In an age where customers must profoundly transform their infrastructures to meet the needs being driven by business transformation, the techniques used by hardware vendors over the past 30 years are backfiring and confirming the great dangers of hardware vendor lock-in to customers.

Indeed hardware vendor lock-in is very dangerous. Apstra's experience with Fortune 500 and Global 2000 enterprise customers is that vendor lock-in is the reason they find themselves with suboptimal solutions that don't meet the rapidly growing needs of the business. Lock-in has become the principal reason enterprises have lost their price negotiation advantage and all of their vendor leverage. It is also the reason they experience outages and SLA violations at an alarmingly unacceptable rate. All while spending an order of magnitude more money than they should.

Definition of hardware vendor lock-in

Since vendors which deliberately devise ways to lock their customers into their single solutions are very creative in their ability to confuse the market, defining hardware vendor lock-in is important.

Hardware vendor lock-in is when IT chooses one and only one hardware vendor for all the devices in the infrastructure that serve one specific function; AND use software tooling that locks IT into that hardware.

An example of this would mean using one hardware vendor for all the switches along with the management software from this same hardware vendor. It means that not only is the customer forced to use one hardware vendor today, but the customer is guaranteed, through lock-in, to be forced to use that same hardware vendor in the future, without a path to have the ability to bring in other hardware vendors.

Be aware of confusing statements by hardware vendors

Incumbent hardware vendors would like customers to believe that they have a multiple vendor environment, and that customers are not locked into only their hardware even if customers actually are.

For example, if a customer chooses switches from vendor X and firewalls from vendor Y, while having implemented the management software for vendor X as well as the management software for vendor Y, then the switch vendor will try to convince the customer that this is a multi-vendor infrastructure. This is incorrect because the customer is still locked into both vendor X for switching and vendor Y for security. The customer is essentially totally at the mercy of Vendor X and Vendor Y. The customer does not have a multi-vendor management design to allow another choice for that critical function in their infrastructure - and that is because the customer has used their management software.

Hardware vendor lock-in is when IT chooses one and only one hardware vendor for all the devices in the infrastructure that serve one specific function; AND use software tooling that locks IT into that hardware.

Dangers of hardware vendor lock-in

The dangers of hardware vendor lock-in are real, consequential, and affect every aspect of IT business operation. It starts with the fact that IT is completely at that vendor's mercy, which has profound consequences.

Extremely high costs

When an organization locks itself into their hardware vendor, two things happen:

1. IT loses control over the pricing of hardware:

How can IT have any leverage when there is only one vendor to talk to? IT may have negotiated an initial deal for the first batch of hardware, or for the first year. But when IT is locked-in, nothing prevents the hardware vendor from coming back with higher prices as soon as they are able.

Hardware vendors aggressively promote and position their own management software because they know once deployed they gain account control, become deeply entrenched, and make it difficult to replace them. At that point, IT has all but guaranteed the highest prices and TCO (total cost of ownership).

If IT had one hardware vendor and leveraged the ecosystem to bring in a management software that works across hardware vendors, then they would at least have the optionality to bring in hardware from other vendors at a later time.

In this report, Gartner comments that "By introducing competition in this thoughtful manner, Gartner has seen clients typically achieve sustained savings of between 10% and 30% and of as much as 300% on specific components like optical transceivers". In another report, Gartner analysts Mark Fabbi and Debra Curtis find that "Sole-sourcing with any vendor will cost a minimum 20% premium, with potential savings generally reaching 30% to 50% or more of capital budgets when dealing with premium-priced vendors".

2. IT loses control over operational expenses

With vendor lock-in, IT loses control over the ability to reduce operational expenses. This happens for many reasons:

a. Reducing operational expenses is achieved by using the automation tools that meet IT's business needs. Those automation tools are generally built by specialized best-of-breed companies which are 100% focused on solving those problems. It is highly unlikely that the management software built by the hardware vendor, and designed to lock the customer into that hardware vendor will meet all the customer's requirements for automation.

b. Apstra has observed that in many cases, the hardware vendor positions extremely expensive and highly profitable "professional services" that build spaghetti code to remediate this divergence between IT requirements and the capabilities of their software solution. With every new version of the management software, the spaghetti code has to be upgraded, at excessive cumulative expense. The result is massive costs, coupled with an innate inability to deliver on the needs of the business. This becomes the proverbial slippery slope.

c. The IT team becomes mired in hardware vendor minutia - from arcane commands to arcane workflows, or arcane vendor specific tools; this wastes resources and time, and keeps IT away from the tasks that are more aligned with the needs of the business. It is no wonder that according to ZK Research, businesses are now dedicating 82% of their IT budgets solely to keeping the lights on, leaving very little budget for innovation.

In fact Gartner finds that by breaking their lock-in from one single vendor, some organizations were able to reduce their opex costs by as much as 95%!

Outages and security risks

1. Substantially higher rate of outages

When IT is locked into one hardware vendor, the business is completely at the mercy of their bugs and quality problems (both hardware and software). When problems occur, customers have no recourse but to depend on their hardware vendor, and them alone, to solve these problems. Even if they are motivated to fix the issues, they are limited by development cycles, and it may take them a lot longer to solve a problem than what IT has written down in an SLA contract, or by what is acceptable by the business. Even if IT is able to hold them accountable for violating their SLA, it doesn't help the business, and frankly IT has very little recourse since they're locked in. Being locked into the management software and analytics that the hardware vendor has provided means not being able to take advantage of other tools on the market that may be more effective at preventing these outages in the first place.

2. Security vulnerabilities Exposure

Security vulnerabilities are common and are routinely discovered on devices in the infrastructure. When a hardware vendor discovers a security vulnerability in a customer's hardware and device OS that they are locked into, the customer must wait for the hardware vendor to provide a patch, which may take months; and then when this patch shows up, the customer will need to go through your qualification process for that security patch, which may take many more months. Skipping the qualification process is akin to rolling the dice on new potential unknown bugs (a very common occurrence with new device OS versions) that could potentially cause bigger problems, performance problems, or outages. Gartner analyst Andrew Lerner wrote a great blog about the pain involved in network upgrades, where he compares the process to going to the dentist!

In summary, when a customer is locked into a hardware vendor and faces a security vulnerability there is a risk of be exposed for months before it can be remediated.

Failing to deliver for the business and losing relevance as a result

1. Unable to meet the requirements of the business

When IT locks itself into hardware, a massive missed opportunity cost is incurred. As engineers are deployed to become experts on hardware and specific device OS versions, they are unable to focus on the initiatives that are most critical to the business: the cloudification of their infrastructure; improving their infrastructure to avoid outages and improve application availability; automation efforts in support of the business's digital transformation initiative, to name a few.

Indeed, it is common that Fortune 500 enterprises delay their critical automation initiatives because of their investment in becoming world experts at the vendor's latest hardware or latest device operating systems. This is often viewed as a "sunk cost" and results in dramatic consequences to the business, and also to the relevance of infrastructure teams. As businesses digitally transform and application teams grow impatient with their hardware first infrastructure teams' inability to deliver on their requirements, application teams turn elsewhere to make progress.

2. Shadow IT

What often happens is that application teams and devops teams start spinning up workloads in the cloud, hence bypassing the IT infrastructure teams completely! The phenomena, often referred to as "Shadow IT," is quite pervasive. For example, according to a 2014 PwC report, it was estimated that "80% of enterprises have used cloud platforms and SaaS applications that have not been approved by IT; and for those enterprises, the percentage of applications that were running on shadow IT was a whopping 35%."

Needless to say, shadow IT significantly increases the security risks for an organization; it also results in costs ballooning out of control.

Onwards!

This is an exciting time in the industry. Customers need to digitally transform. In order to do that, they need to change their ways. It is clear that the right solution involves a hybrid solution - anchored in the private cloud with the option to deploy a multi-vendor solution and an ability to leverage multiple public clouds as needed. With cloud services penetrating the private cloud - e.g. Microsoft with Azure Stack, and AWS with Outpost, customers can no longer afford to be hardware driven, and lock themselves into one hardware vendor.

Customers can certainly no longer operate under the threat of having hardware device vendors sabotage their devices as a way to compel them to abandon a multi-vendor approach and lock themselves into the hardware vendor's solution.

Apstra was founded with a mission to break hardware vendor lock-in forever and enable organizations to automate their infrastructures while embracing heterogeneity. Automation and support for multi-vendor and multi-cloud are key to slashing costs, and delivering on infrastructure reliability and agility that are required for the business to deliver on their goals.

Apstra breaks the vicious cycle of vendor lock-in by committing to loosely coupled architecture and powerfully open APIs; support for the widest array of hardware vendor choices; being the single throat to choke, thus providing choice without risk; And zero lock-in.

If you are committed to deliver on your goals, and get off your addiction to your current hardware vendor, please call us - we are delighted to help!

www.apstra.com

sales@apstra.com
1-844-9APSTRA
333 Middlefield Rd, Menlo Park, CA 94025

apstra®