AXIM™

5 tips to extend the lifetime value of Nortel CS1000

By maintaining Nortel CS1000 after end-of-service-life many organizations will have to wrestle some massive security, resiliency and customer experience challenges. These could make the big cost savings from not migrating seem a false economy. Here are five tips that might just help improve CS1000 end-of-lifecycle management.

5 big Nortel CS1000 management challenges

1. Maintaining the security of the voice environment

2. Safeguarding the growing threat to resilience

3. Navigating the rise in operational risk

4. Maximizing the customer experience

5. Optimizing an ultimate migration to the cloud

All change

Many organizations don't recognize end-of-service-life (EoSL) as a reason to replace their Nortel CS1000. They see a dependable workhorse. They see big cost savings. What they don't all see is a constant stream of new security threats, business demands and customer expectations that could throw the low-cost argument out of the boardroom.

These challenges could redefine CS1000 lifecycle management, from passive to active. From a 'just gets on with it' voice technology that needs no attention, to a voice technology that needs time and attention to wring out more lifetime value. How will organizations continue to maximize the operating efficiency of their CS1000 system? This short paper headlines five simple tips that should help.

The dependable workhorse

For decades Nortel CS1000 has proved robust and reliable. And for many voice teams the risk of ripping and replacing it is greater than the risk of maintaining it post end-of-life. The logic makes sense: it isn't broken, it is saving big money by not migrating and there are a ton of support and maintenance providers stepping up to replace Avaya with commercially attractive SLAs.

This whitepaper is not intended to derail this status quo. Its purpose is to help those that have made the decision to stick with their CS1000 to better manage this legacy voice technology through EoSL. At its heart is a brutally simple observation: the big lifecycle management challenges won't center on the CS1000 technology itself, but the environment that surrounds it. The logic goes that by recognizing the big challenges the voice environment will impose on CS1000, voice teams can better husband it post-EoSL.

Better manage 5 big lifecycle management challenges

We see some big lifecycle management challenges hitting CS1000. Here we expand on some of them: security, resilience, performance management, customer experience and the cloud. We also provide some tips on how to manage to maximize the effectiveness of CS1000 after end-of-life. We also acknowledge that all good things will come to an end, and cloud will be the next state. The last tip focuses on a migration plan that optimizes CS1000 during a transition to the cloud.

1.

Constantly advancing security threats

Voice, IT and security teams are constantly battling with the accelerating cyberthreat.

The hard fact is that contact centers are in danger of becoming a fraud Achilles' heel, and voice services are in the front line. Increasingly sophisticated attackers are launching interactive voice response attacks to gather data, enabling account takeover, fraudulent transactions, shipment reroutes and fraudulent exfiltration of funds.

The threat doesn't lie with Nortel CS1000 but the aging end-of-support legacy that surrounds it in the voice environment – those technologies that lack the security patches to deal with the advanced nature of today's cyberthreats.

The demands on voice, IT and security teams mean that many organizations are not regularly identifying the security concerns and the depth of unsupported legacy products in their environments, so the security attack surface is expanded not reduced. Compounding this is the silo that often exists between voice and IT teams, especially when legacy environments are in use – meaning IT frequently lacks a view of the existing risks. Then there's the challenge of integrating new security technologies into the voice environment, like multifactor voice recognition capabilities and central fraud analytics.

So, in maintaining their Nortel CS1000 post end-of-support-life, how do organizations ensure that it is a safe bet not a security threat, and integrate new security technologies into a heavily legacy based voice environment.

Tip

Undertake an independent risk assessment of the voice environment.

How to best de-risk the voice environment? Here's a simple step-by-step guide:

Look to an independent and agnostic partner with extensive Nortel and voice experience.

Ensure they have a complete visibility of the entire voice environment, and they document it – along with lifecycles.

Focus on identifying the biggest areas of risk, not just security but the critical operational risks too.

Go deeper on the risk assessment to the potential ripple effects, e.g. service disruption, business continuity, disaster recovery and CX.

Isolate the short term improvements, and, the longer term risks inherent in consolidation, migration or transformation strategies.

2. Partially sighted support providers

Better manage the increasing danger of outages and slower remediation speeds.

Why? you ask. An army of support and maintenance providers has strengthened the business case to extend the lifetime of a Nortel CS1000 system. At face value the logic seems compelling; the SLAs offset the absence of Avaya, the cost is minimal compared to a rip and replace, and the business risk is negligible compared to the risk of a migration.

But are they really safeguarding resilience? It's tempting to point to problems around sourcing stock when a failure occurs, but whilst this does happen it isn't the biggest challenge surrounding resiliency - the greatest threat to Nortel CS1000 support and maintenance is visibility and transparency.

The growing reality is that a perfect storm is brewing. CS1000 is part of a voice environment that 3rd parties only partly support. By outsourcing, organizations lose visibility of the current environment, (and parts of it are already out of support and invisible). Wind forward to a voice outage and maintenance providers could fix part of it, the rest is down to the knowledge and skills base that exist in the organization. The result? It takes longer to find and fix voice outages and the impact is deeper on the business and its customers.

By extending Nortel CS1000 post end-of-support-life, organizations cannot take an out of sight and out of mind attitude to this voice technology. Voice teams must ask the killer question: how does Nortel CS1000 continue to be a strong point and not become a single point of failure?

Tip

Create total visibility of the ecosystem that surrounds Nortel CS1000.

Auditing the entire voice environment will highlight the big resilience threats and help reduce downtime from outages. Here are some pointers on how:

Ensure the audit is done by those who subject matter expertise across all the technologies in the voice environment.

Don't focus on specific technologies, target full knowledge of the current architecture of the voice environment.

Fully analyze and document the complete voice ecosystem.

Understand what is nearing and what is past end-of-life or end-of-service, to optimize the management of aging legacy.

Deliver total visibility of the greatest potential single points of failure across the voice environment.

3.

An ever-more demanding customer

Look to the impact on customer experience not just the impact on the bottom line.

It is understandable. The cost/benefit equation is still stacked in favor of Nortel CS1000: performance continues unabated and the lifetime value is only getting stronger the longer the technology endures in the voice environment. Add the fact that maintenance is low, continued support is acceptable and a big investment cost is unnecessary, then CS1000 could be seen as the definitive cash cow.

But is this a genuine corporate upside or a false economy? There are many elements to bake into any cost/benefit, from security and operational risks to business agility, but one critical business metric to factor into the financials is the impact of aging legacy technology on customer service experience and revenues.

The truth is that CS1000 can't support the latest CX technologies that organizations must increasingly adopt to satisfy the constantly changing demands of their customers, like self-service and personalization. Another customer demand is seamless service, yet CS1000 is a disparate system that can't contribute to a single truth. Then there is the impact of the increased outages and slower remediation speeds referenced earlier on the quality of customer delivery.

The chances are the CX limitations of CS1000 could cost businesses in lost customers and revenues, which could massively outweigh any technology cost savings. Add to this the fact that the importance of voice to the contact center refuses to die to new technologies, then voice teams face a profound question: can they enable Nortel CS1000 to save money and not lose customers?

Tip

See Nortel CS1000 through the customer's eyes and not just a technology lens.

Go beyond security and operational risks, look at the risks to the customer experience and the business impact. Here are some thoughts on a CX audit:

Look at all the customer touchpoints and customer impacts of the voice environment, where possible measure and quantify.

Expand the voice environment to the voice of the environment. Talk to management, operations staff and front line agents.

Overlay insights from voice of the customer and journey mapping.

Prioritize the critical risks the voice environment poses to customer delivery, and unearth the critical single points of failure.

Combine the operational, security and business risks with the CX risks and see the full picture on the CS1000's commercial viability.

4.

Deal with the reality that the cloud is the natural home for the voice environment.

The inevitability that is the cloud

Maintaining Nortel CS1000 through EoSL is not a long term strategy but a commercially prudent shorter term fix. Managing cost with the big security, operational, business and customer risks will help organizations today, but won't obscure the fact that tomorrow belongs to the cloud.

This brings a ton of new risks into play. It starts with a brutally simple question: how long is it realistic to maintain a low-risk and stable on-premise solution? Then there's the risk of limited visibility: if organizations have lost sight of the totality of their voice environment how can they deliver the right cloud applications, and, can any of the legacy technologies be lifted and loaded? There are also architectural risks: what is already in cloud and can there be consolidation or is this a full migration? And probably most critically, there is the need to mitigate the performance risks in a protracted migration - from optimizing CS1000 to the management of the big operational and customer risks in the voice environment pre- and during the migration.

The question becomes this: how long can Nortel CS1000 remain a workhorse before it becomes a white elephant? Conventional logic would say that a blind focus on Nortel CS1000 lifecycle management can only be a jam today strategy. Jam tomorrow demands voice teams look to the lifecycle management of the entire voice environment and how Nortel CS1000 and cloud migration naturally co-exist in the most commercially effective way.

Tip

Create a roadmap to transition from Nortel CS1000 to the cloud.

Extend the life of CS1000 and plan for a cloud migration. Here are some thoughts on roadmapping an operationally more impactful migration:

Analyze more deeply: fully audit the voice architecture and take a holistic view of the entire voice environment.

Phase a migration plan that manages lifting and loading and targeted application migration.

Codify the business-critical outcomes of the migration, and ceaselessly reference them in the planning process.

Identify, target and mitigate the big failure points so the cloud migration is lower risk and more seamless and frictionless.

Understand and mitigate the main security and operational risks of maintaining Nortel CS1000 during a protracted migration.

Look beyond the planning and migration to cloud governance: identify metrics and KPIs that define short and longer term success.

A parting thought

Nortel CS1000 is continuing to deliver a great investment return, but how soon will it become a money pit?

The argument case goes like this: security risks (it will no longer be actively patched) + operational risks (a paucity of spares) + less business agility (custom integrations and yesterday's features) = business cost not lifetime value.

But many organizations are for now sticking with their CS1000 system and not twisting. Hopefully these four tips will help them improve lifecycle management. The challenges we outline are not intended to undermine this strategy. The real issues surround the landscape that surrounds Nortel CS1000, from an aging environment to selective support and maintenance, to constantly changing cyberthreats, to the full CX ecosystem. Which leads to our fifth tip: identify a partner who can help you see the complete picture.

About Axim

Axim is an international enterprise consultancy that focuses on enterprise communications, customer experience and the cloud. We are subject matter experts on Nortel and Avaya yet independent and vendor agnostic. Our architects audit and document voice architectures and risk assess and manage voice environments from security through to operational risk. Our CX teams evaluate and optimize the performance of voice within complete customer experience ecosystems. And our cloud specialists plan and phase cloud migrations that end in operational excellence. Learn more, visit **aximglobal/nortelcs1000**