Why MSPs Should Care About Autonomic Computing & the 4 Steps to More Profitable Remote Service Delivery

by: Bill Whitney with Tara Flynn Condon

Driven by an increase in the complexity, convergence, and mission criticality of IT and voice systems, companies of all sizes now seek to outsource the management of these critical systems to Managed Service Providers (MSPs). As such, many companies now view service providers as extensions of their own IT and operations departments. For service providers, this means the time is right and the market is ripe for success in the services business.

Even as a potential recession looms, opportunity only increases for service providers, as they may be called upon to compensate for shrinking enterprise IT departments. However, the pressure is on. To remain competitive, service providers must offer increasingly sophisticated services that provide higher value to customers. Paradoxically, at the same time, the very same service providers must also reduce the cost of delivering these services. Thriving in the managed services marketplace requires that service providers evolve to meet these changing demands. This evolution will require service providers to shift to an autonomic computing model by deploying technologies that leverage automation and facilitate the delivery of next generation services.

What is Autonomic Computing?

A term first coined by IBM in 2001, autonomic computing refers to the creation of computer systems capable of self-management. For service providers, autonomic computing would mean that high levels of automation could be applied to both problem identification and resolution.

With autonomic computing, policies and tools are applied to basic troubleshooting and problem resolution, freeing technicians to focus on the delivery of more advanced services.

Service Levels & Workflows

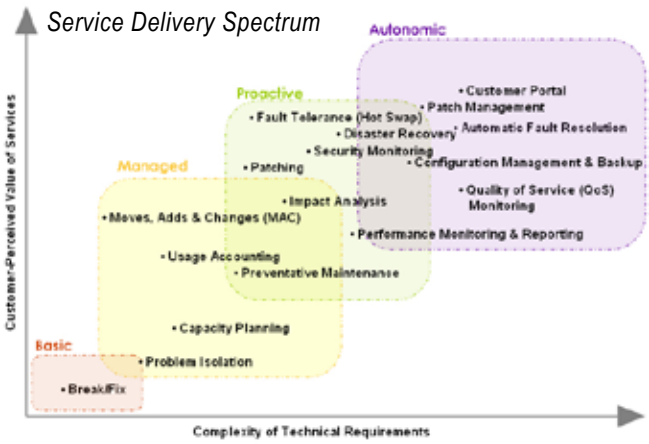
Service Level	Workflow
1 Basic	Complaint → Receive → Assign → Resolve
2 Managed	Complaint → Gather Data → Triage → Assign → Resolve
3 Proactive	Gather Data → Analyze → Notify → Triage → Assign → Resolve
4 Autonomic	Gather Data → Analyze → Resolve → Notify / Assign → Resolve → Gather Knowledge

Why Should MSPs Care About Autonomic Computing?

To differentiate themselves from the competition and continue to provide outstanding value to enterprise customers, service providers must constantly offer a wider, increasingly sophisticated range of services. Because computers can process data far faster than a human in a given period of time, analysis and response is almost instantaneous, which insures maximum uptime for managed systems. In the autonomic computing model, domain experts generate the policies used to govern automated processes, rather than resolve individual problems.

Continued Next Page >

This allows service providers to greatly reduce the cost of service delivery, as well as deliver more high-margin services.



Today, many service providers already use NOC-based tools to gather, analyze, and correlate data to provide the most effective levels of service. Leveraging those tools to deliver autonomic services require service providers to treat Customer Premise Equipment (CPE) as an extension of their own network. Traditionally, barriers such as security and network virtualization have made service providers reluctant to ask for this access and enterprises even more reluctant to grant it. However, there are steps service providers can take today to deliver revenue-generating autonomic services, while leveraging their existing infrastructure and meeting enterprise customers' security and compliance requirements.

The Top 4 Steps to More Profitable Service Delivery

Step #1: Phase out customer-supplied access methods

When preparing to deploy a remote management solution, service providers often hear from customers, "Use my VPN" or "Just use my Citrix system." To many service providers, this appears to be the path of least resistance – at least at first. However, service providers soon feel the pain when a customer wishes to add a new service (necessitating yet another negotiation with the customer's security team), or the service provider wishes to centrally manage the solution (and lacks the scalability to do so), or wants to deliver next generation services (and can not connect remotely managed systems to NOC tools).

Enterprises, overburdened by compliance-related requirements, may standardize on third-party access methods that are ill-suited to service providers. For example, the suggested method is often an extension of the same systems companies use for employee remote access. These methods are good for telecommuters but ill-suited to service providers' remote management needs. Rather than simply accept the customer-supplied method, service providers must think about their service delivery needs both today and tomorrow and offer their own solution to customers. Ideally this solution should marry both the service provider's need for access with the customer's need for security. Only by standardizing on a service delivery platform, can a service provider retain the scalability and flexibility needed to easily deliver revenue-generating services in the future.

Step #2: Insist on "always on" IP access

Despite significant improvements in service delivery technology, many service providers and their customers continue to view remote management as a convenience, something to be used in emergency situations and/or when an onsite technician visit is difficult or impossible to schedule. The more advanced the service, the more incumbent it is upon the service provider to receive real-time alarms from remotely managed systems located on customer sites. Without consistent IP access, the service provider can neither receive alarms, nor conduct necessary maintenance, thereby making it impossible for the service provider to deliver on Service Level Agreements (SLAs).

In order to deliver next generation managed services, consistent IP access is a necessity. Ideally service providers should seek out a solution that combines a high level of security with ease of access, such as SSL VPN. Initially some companies may be reluctant to grant IP access to service providers, often citing security risks. However, when presented with the ROI IP access can offer (for example, faster response times and proactive maintenance), companies are more likely to grant this access. This likelihood can increase significantly when a service provider presents a compelling security message.

Continued Next Page >

Step #3: Have an enterprise security message

When service providers hear the word "security," they think of lengthy sales and deployment cycles. This is typical reaction, as service providers often find themselves on the defensive when talking about security. As such, it behooves service providers to understand the enterprise security environment, as well as any compliance-related requirements that directly affect service providers (i.e. requirements related to remote network access by third parties). Then, the service provider should put technology and processes in place to address common enterprise security requirements. By proactively demonstrating this commitment to security and compliance, service providers can vastly speed the sales and deployment processes.

As an example, a common requirement is that service providers be able to produce an audit trail of access to, and activities on, the network. Service providers should have a way to meet this requirement – or partner with a company that can. As service providers continue to move towards autonomic service delivery, the audit requirement will become increasingly more important, as many system changes will become entirely transparent. Having this record of activity has two benefits to the service provider: (#1) It will help meet enterprise security and compliance requirements, and (#2) The service provider can leverage the audit trail to demonstrate the high levels of service it regularly provides its customers.

Step #4: Make plug-and-play deployment and scalability a priority

Traditionally, large enterprises have made up the bulk of managed services customers. However, small-to-medium size businesses (SMBs) have become the fastest-growing community of MSP adopters. To capitalize on this growing market, many service providers are targeting SMBs with new offerings. With this new audience, it is no longer economically feasible for service providers to invest hours of time negotiating remote access. As such, service providers must standardize on service delivery tools that snap into customer environments and allow for immediate service delivery.

Even if service providers do not wish to offer autonomic services today, laying the appropriate groundwork now will give them the flexibility and infrastructure to deliver a wide array of revenue-generating services in the future. Also, in moving towards the autonomic computing model, service providers can realize benefits today, including a lower cost of service delivery and speedy deployment cycles.

By following the steps outlined above, service providers can create a standardized service delivery platform that satisfies customers' security needs, simplifies device access, and facilitates the deployment of sophisticated tools and next generation services – all essential to the future success and growth of a service provider.

About the Author: Bill Whitney is Chief Technology Officer and co-founder of ION Networks, a leading manufacturer of remote administrative management and secure access technology. A recognized authority on security, Whitney has worked with some of the world's premier organizations to improve remote management and security, including Fortune 500® financial institutions, telecommunications firms, and government and military agencies. Bill can be reached at bw@ion-networks.com. For more information about the company, visit www.ion-networks.com.

About ION Networks: ION Networks, now part of Cryptek, Inc., is the world's leading provider of secure remote administration solutions, with over 60,000 devices deployed on six continents by the world's largest telecom firms. ION also offers purpose-built Vendor Access Control (VAC) products that enable Global 2000 companies and government agencies to manage and secure third party remote access to voice and IT systems. For more information, visit www.ion-networks.com or call +1 908.546.3900.