



# Novis builds scalable and secure networking infrastructure with NetFoundry

CASE STUDY



**NOVIS**

Novis has been a leading company in managed services for the entire life cycle of SAP systems since 2001. They service over 150 companies, 1000+ SAP systems and 100,000 users. Their staff comprises more than 200 consultants and SAP managers, providing services to major companies across the Americas - making them one of the region's leading providers of SAP outsourcing services.

Novis optimizes SAP operations through proactive and innovative management, enhanced with the integration of SAP with cloud analytic tools. Following various SAP and cloud certifications, they ensure the services they offer meet the best level of global standards for SAP applications management and operation.

Enterprises migrating SAP to the cloud have much to gain in terms of agility, productivity and access to innovation. Novis Cloud Manager platform, along with their operations team, help customers automate SAP operations in public clouds like Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) to ensure an imperceptible transition so that customers can harness all the cloud's potential.



## Challenges with secure multi-cloud connectivity

With networks scaling across wired, wireless, and virtual IT environments, network management has become increasingly complex. As customers start running SAP applications on the cloud, they need secure connectivity which allows different systems to be accessed by different people - including developers, DevOps, sales, partners and customers - located in different offices, with different access permissions, and connect using a variety of desktop or mobile devices. This needs to be a proactive, secure-by-design approach that mandates Novis and their customer's SAP environments are not exposed to exploitation of vulnerabilities common to solutions that use the public internet while ensuring the ubiquity and connect-from-anywhere approach the internet allows.

Initially, Novis tried to meet these requirements by using VPC Peerings or/and Virtual Private Networks (VPN) to provide users with access credentials. Novis soon encountered the following challenges:

- No option to create VPC peering connections between VPCs in different regions to support remote working.
- Limitations of VPC also extends to public cloud services, like internet gateway, where it is not accessible via peering connection.
- Managing peering at scale can become very difficult and operationally, it can be complex to troubleshoot issues
- Weak VPN protocols, ill-managed VPC peering, public IPs and lack of application microsegmentation or least privileged access become an easy target to malicious hackers.
- Difficulty managing access across so many environments, access policies for individuals and teams.

To preserve their high standards of security, agility and efficiency, Novis needed an effective, secure, yet affordable network management solution to streamline communications between instances.

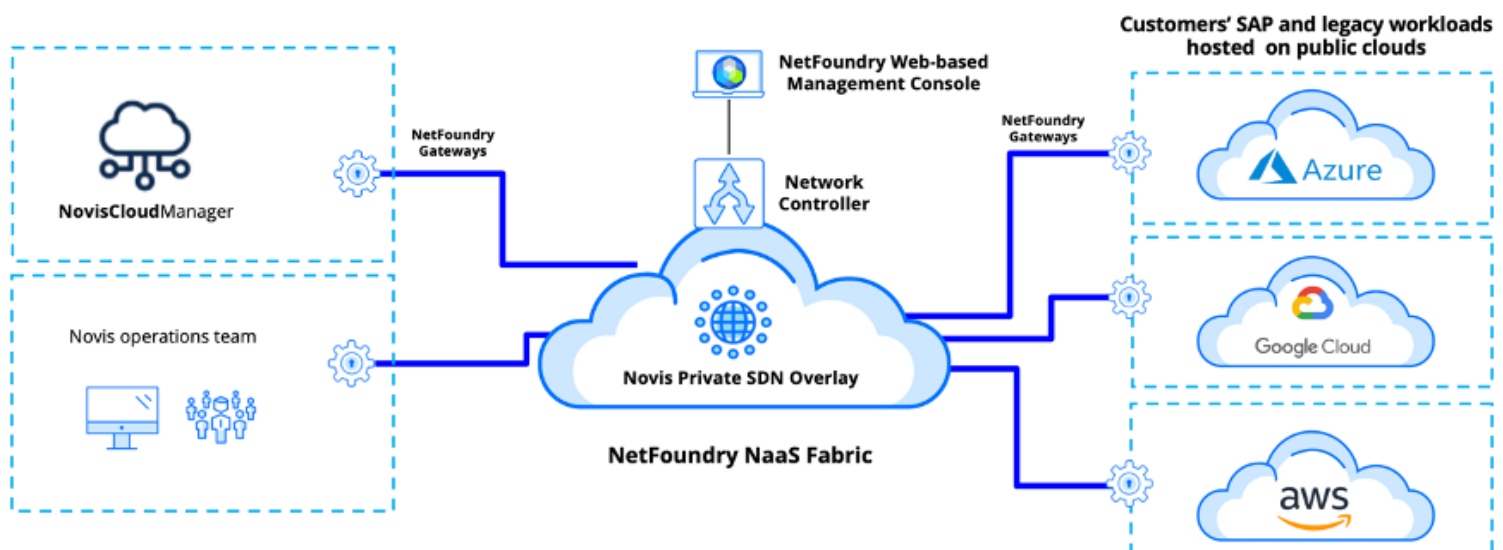
## NetFoundry - Right partner, right solution and the right price

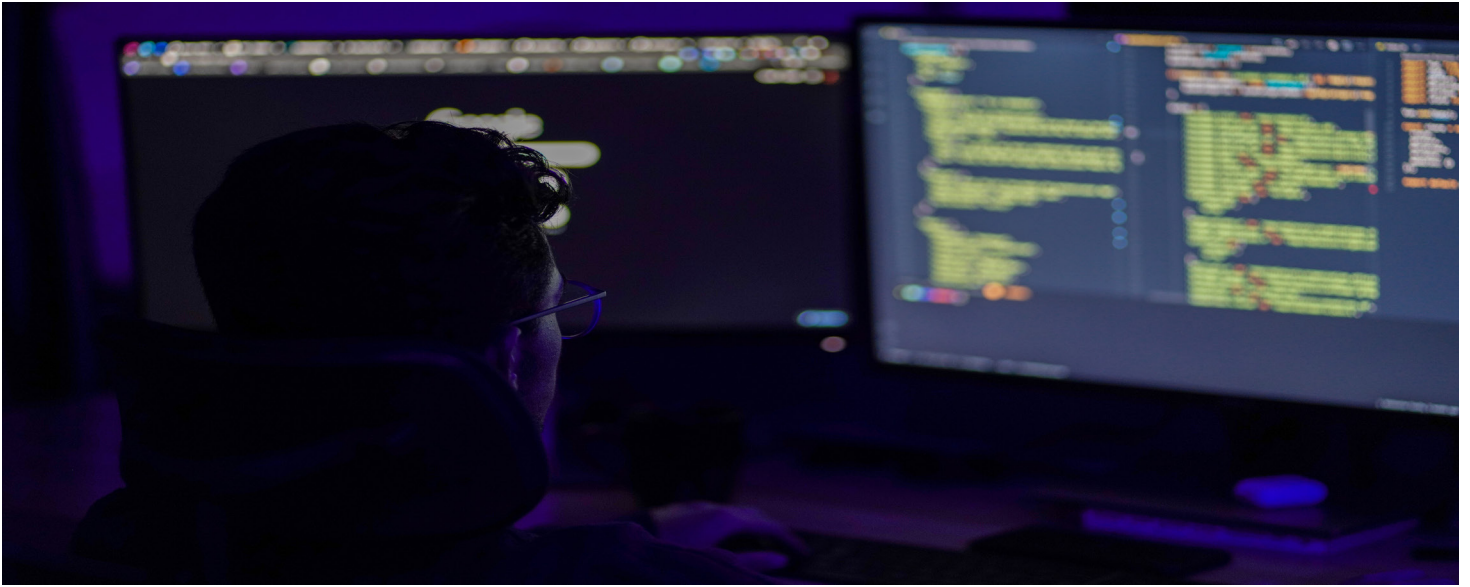
Novis was introduced to NetFoundry Zero Trust platform, and it solved all the challenges they were experiencing. The NetFoundry cloud-native platform enables Novis to spin up global, secure, high-performance networking within minutes which are proactively secure-by-design. Novis first started doing rollouts by using the NetFoundry Console. With infinite customization and scalability, the console serves as a centralized, web-based dashboard for creating and managing networks. After the first couple of scenarios were implemented, Novis adopted an automated integration with their own cloud management solution, Novis Cloud Manager.

Partnering with NetFoundry complimented Novis' services with a comprehensive and compliant out-of-the-box offering for the most critical and security-sensitive customer scenarios. Inbound firewall ports are closed and IP addresses are no longer exposed - this is nearly impossible with a solution that doesn't have NetFoundry's architecture and components. This private, authenticate-before-connect architecture, enforced with strong identities and least privileged access to Private Fabric Routers, minimizes the attack surface against all external malicious network attacks. As a Service Provider, Novis was able to support multiple networks in several cloud providers, multiple customers and several management systems and operators, solving restrictions due to network design.

The solution is 100% software-defined, making it very fast and easy to deploy, with simple-to-manage least privileged connections. This further reduces overhead in the administration as a smaller team is needed to manage the network and provision access.

"NetFoundry helped us simplify complex connectivity scenarios. As a Service Provider, we managed to integrate customers' SAP workloads on three different clouds (AWS, Azure & GCP) and our on-premises services without impacting final users. NetFoundry's vision for automation and the highest and easiest security-by-design aligns with our own and they prove to be a reliable partner, addressing challenging scenarios," Patricio Renner, Chief Technology Officer, Novis.





## The benefits

Novis leveraged NetFoundry to solve and support very wide sets of use cases. Benefits include:

- **Improved service delivery.** 200% quicker delivery time, more efficiency and with fewer errors using NetFoundry's APIs; the time taken to set up and integrate end customers' systems to Novis' administration tools and operations was reduced greatly.
- **Zero Trust Networking.** Novis customers get completely dark cloud instances which are impervious to external network level attacks (DDoS, zero day and CVE exploit, bruteforce and more) as well as software-defined encrypted overlay AppWANs which microsegment traffic with least privileged access to reduce risks from lateral movement. This is all controlled via NetFoundry's web console and APIs integrated with Novis Cloud Manager to define and deploy these secure connections instantly and dynamically. AppWANs are completely service-provider agnostic, as an overlay it also adds layers of security and isolation when working over the Internet, in public clouds, or in shared environments.
- **Reduce cost.** Reduced administrative cost and total cost of ownership by 30% through NetFoundry network-as-a-service (NaaS) managing the infrastructure, Novis was able to eliminate the dependency on VPNs and VPC Peering each time they added a customer or an endpoint

NetFoundry proved to be a powerful platform for Novis and it only took a few weeks for Novis to do a complete rollout. After a successful POC, the NetFoundry support and development team worked side-by-side with Novis' development and operations team to provide frequent updates and bug fixes. Looking to the future, Novis is also exploring extended automation with further integration of Novis Cloud Manager.

## ABOUT NETFOUNDRY

NetFoundry is the leader in Cloud-Native Networking, enabling businesses to simply, securely and cost-effectively connect distributed applications across edges, clouds and service meshes. The NetFoundry platform, delivered as SaaS, enables businesses to connect applications without the costs and complexity of VPNs, custom hardware and private circuits.

NetFoundry's platform is accessed via APIs, SDKs and DevOps tools integrations, enabling practitioners, application developers, and network administrators to get the levels of automation and agility which are only possible with connectivity-as-code. NetFoundry is headquartered in Charlotte, North Carolina, with offices in California, Colorado, New York, London, Bangalore, and Singapore.



Address —  
101 South Tryon Street, Suite 2700  
Charlotte, NC 28280

Telephone —  
+1.704.762.1405

Contact us

Share



For more information, visit us at [www.netfoundry.io](http://www.netfoundry.io)

© 2022 NetFoundry, Inc.