NETFOUNDRY

Ramco Systems future proof cloud, network and security strategy with NetFoundry's Zero Trust Network Access platform

CASE STUDY

ramco

Ramco Systems is a fast-growing enterprise software player disrupting the market with its multi-tenant cloud and mobile-based enterprise software. Ramco offers comprehensive ERP covering, Asset Management, Financials, Manufacturing, Project Management, Aviation MRO (Maintenance, Repair and Overhaul), M&E (Maintenance & Engineering), SCM (Supply Chain Management), Logistics, HR & Global Payroll on the most appropriate cloud model – public and private.

One of the first IP-led companies in APAC, Ramco has 24 offices, globally, and a client presence in more than 50 countries. Ramco builds applications that drive enterprise-wide business transformation – creating an intelligent ecosystem of customers, partners, and employees.

Ramco's network and security challenges

As Ramco embarked on its cloud journey towards digitizing existing processes, it faced a few of these challenges:

• Simplifying and accelerating application-cloud migration and data replication.

• Mitigating cyber-security risk.

• Automating and streamlining secured access provisioning to workers/remote workers.

Blazeclan Technologies, NetFoundry's strategic partner for cloud solutions, aided Ramco in their cloud migration and network security efforts. Blazeclan designed and implemented a disaster recovery solution for Ramco's workloads deployed on-premises with NetFoundry providing secure connectivity solution via Network-as-a-Service (NaaS) model.

Ramco was already on the verge of implementing a disaster recovery solution for their on-premise deployments and needed a solution that would provide secure connectivity while accelerating the process of data replication to AWS. Any IT disasters during cloud migration impacting service delivery, delays, server corruptions and data centre failures could cause data loss, further impacting revenue.

Along with the growing popularity of cyber-attacks, Ramco was looking for options in managing their cyber risk, especially with their hybrid cloud environment. As applications and data are spread across their private data centres in Chennai as well as on Amazon Web Services™ (AWS) and Azure® Cloud, improving security posture and strengthening their IT security was a crucial pain point to protect most critical databases.

Ramco also wanted to empower their workforce, especially their software development team. As their developers constantly change teams as per project requirements, any access to tools, systems or servers, would take days as access could only be granted by their central IT team. With the constraints of these ineffective processes, Ramco realized there is a need to enable developers to securely connect and easily access corporate databases and tools from anywhere to ensure business continuity.

NETFOUNDRY

Ramco implements ZTNA with NetFoundry

Blazeclan recommended the implementation of NetFoundry as they knew NetFoundry's Zero Trust Network-as-a-service (ZTNaaS) platform was the best solution in addressing Ramco's challenges. As cloud migration and demand for secure remote access accelerated, and with new and constant data privacy regulations changes, Ramco chose to implement Zero Trust Network Access (ZTNA), replacing their existing VPN. Blazeclan lead and managed the project with NetFoundry architects and delivered a network infrastructure that is designed to provide secure access, high-performance and granular traffic control across multiple applications, devices and clouds.

Comprising of both the core and the edge, Blazeclan successfully deployed Netfoundry onto Ramco's environment. At the core is a management orchestration platform consisting of the NetFoundry web console through which Ramco's business units' leaders or administrators can easily provision and manage networks. The edge consists of endpoints, such as NetFoundry Windows desktop edge that is installed on the laptops of Ramco's employees and the Net-Foundry edge routers which are installed on virtual machines (VMs) across Ramco's private data centre in Chennai and in public clouds.

Along with the seamless acceleration of cloud traffic, the NetFoundry platform extends global networking and security capabilities down to each Ramco user's devices. These are key features of ZTNA implementation in Ramco:

• Digital token-based enrollments which is a better option making authentication quicker and safer for authorized users.

• Endpoint multi-factor authentication

• Link security achieved with mTLS and end-to-end security achieved with end-to-end encryption.

• Two-way trust between endpoints and controller, ensuring controls and policies can be pushed to the endpoints and enforced even before the connection.

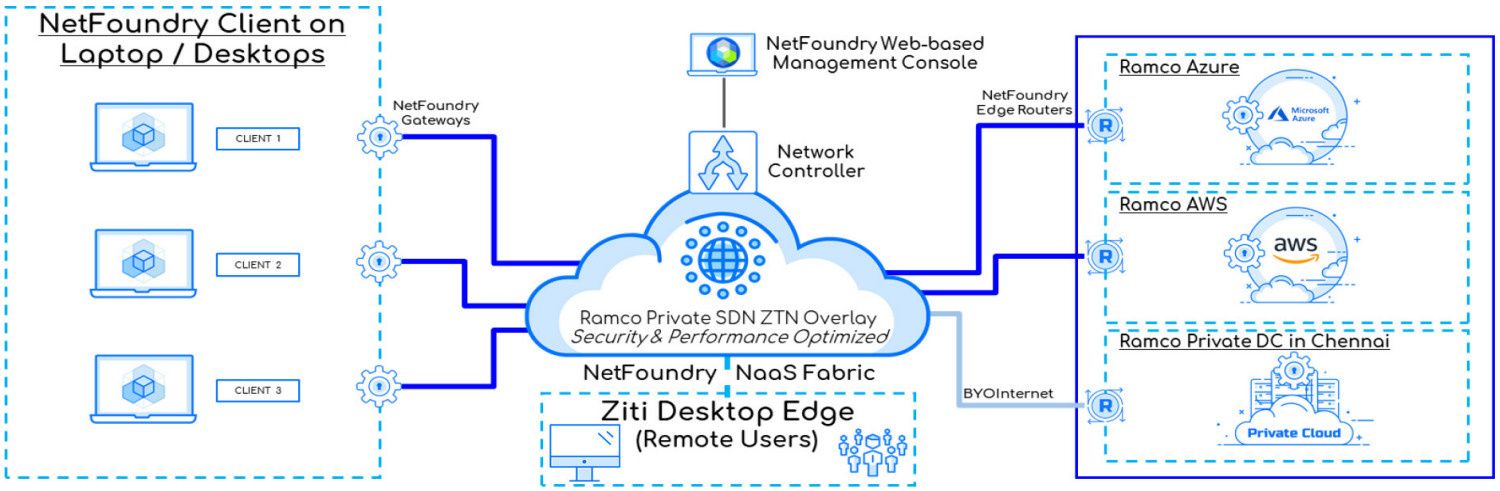
• Microsegmented AppWANs for each business unit to secure each data flow and to prevent collateral damage if a specific flow is breached.

• The dark network where only outbound connection request is permitted (endpoints towards the internet), blocking inbound requests, saving network from internet attacks.

• Security posture checks on the devices before allowing devices to connect to the network.

• Easier provisioning and management of endpoints via Azure Active Directory synchronization

"At Ramco Systems, we pride ourselves on providing world-class enterprise software to improve our customers' lives, with data security being a top priority. The experience of implementing NetFoundry's zero-trust Networking-as-a-Service (NaaS) platform has made me its strong advocate. One platform has enabled us to simply and effectively replace multiple bespoke solutions for multi- cloud, remote work and hybrid cloud while improving security and performance. With the NetFoundry platform and NaaS services enabling us to easily take care of simple, secure, high-performance networking, we are even more focused on providing our customers with innovation and excellence", Virender Aggarwal, CEO, Ramco Systems



Contact us

Share

For more information, visit us at www.netfoundry.io

NETFOUNDRY

Beyond security benefits

The implementation of the NetFoundry ZTNA NaaS platform by Blazeclan provided a resolution for Ramco's security and network complexity. The NetFoundry platform provided Ramco with agility, with seamless integration between appliances, users and cloud services. When migrating workloads, Ramco was able to establish an on-demand connection to any public cloud provider or any private data centre, without any hardware. This also reduced deployment time further reducing TCO, as the alternative options could have taken weeks to provision, impacting cost. NetFoundry gateways deployed on VMs enabled performant and secured network connectivity over the available internet.

The NetFoundry platform also provided Ramco with a more secured environment- Network security at the edge. The private overlay network generated by deploying the platform, connects all devices, edges and clouds, with zero trust network access security, and SASE framework security. This replaces Ramco's old model of network infrastructure, replacing VPNs, enabling them for today's modern workplace.

NetFoundry also simplifies the process of establishing networks where Ramco's business units or administrators can easily control access for users using the NetFoundry console. By bypassing central IT, employees do not need to wait for a long approval process. Ramco developers' team can now gain secured access to tools used to build software, such as their remote desktop servers (RDP), GitHub repository where coding is stored and some corporate systems over hybrid cloud development environments. Various endpoints are easily provisioned and managed via Azure Active Directory synchronization, eliminating the need to manually add or remove endpoints, providing a great level of automation.

"Ramco Systems wanted to transform its network architecture to align it with Zero Trust Network. They intended it to be designed based on the latest security practices which include performance throughput, availability and eliminating redundancy while supporting both their on-premise and cloud environments. Blazeclan, in partnership with NetFoundry, helped Ramco System implement Zero Trust Network Access (ZTNA), replacing the time-intensive and constrained; connectivity and access procedures", Varoon Rajani, Founder & CEO of Blazeclan Technologies.

Looking at future possibilities, Ramco and NetFoundry are partnering to embed zero trust networking into Ramco applications via NetFoundry's open SDKs. With this integration, Ramco customers would no longer need VPNs to access Ramco's private apps, instead, the apps will be provided with zero trust, high-performance networking over any Internet connection.

ABOUT BLAZECLAN

Blazeclan is amongst the world's leading providers of public cloud services with a proven history of helping enterprises unlock the value of cloud computing. Established in 2010, the company has been providing customers across the globe with cloud advisory services, cloud migration, DevOps and Automation, Big Data and Analytics, Cloud Native Application development, and cloud managed services.

Blazeclan has attained various accolades, including FT-500 High Growth Companies Asia Pacific, Apptio FinOps Partner of the Year 2020, Digital Skills Award (Nasscom Tech Innovation Conclave 2020), CRN Excellence Awards 2020, 2020 CRN Fast Growth 150, India's Growth Champion 2020, CRN Excellence 2019 - Big Data Analytics, AWS Country Partner of the Year 2019 Singapore, AWS Singapore Partner of the Year 2018, CRN Excellence Award. 2018, FT 100 High Growth Companies APAC 2018, Top 100 Public Cloud MSP 2018, AWS APN Excellence - Partner of the Year 2017 and many more.

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.

NETFOUNDRY

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