

# DIGIBEE SECURES IT INFRASTRUCTURE & REDUCES COMPLEXITY OF CUSTOMER INTEGRATIONS WITH CLOUDZITI

## SOFTWARE



COMPANY Digibee

LOCATION Fort Lauderdale, Florida

## CLOUDZITI ARCHITECTURE



Digibee is an enterprise integration Platform-as-a-Service (iPaaS) which enables organizations to build flexible, highly scalable integration architectures. Digibee iPaaS enables software engineers to build and maintain even the most complex data and systems integrations with unprecedented speed and simplicity. It serves some of the world's largest banks, and is the preferred iPaaS solution for 250-plus businesses, including Assai, B3, Barkley, Bauducco, GoPro, Oobe, and Payless.

## STORY HIGHLIGHTS:

### Accelerate innovation with faster deployments

Integrations between the iPaaS and customer infrastructure are days to weeks faster, because they are no longer dependent on nailing up VPNs, managing IP address overlap problems, or deploying bastion hosts.

### Provide customers with the strongest API security

APIs are unreachable from the Internet, only accessible from Digibee's private CloudZiti zero trust overlay, while also making the APIs just as simple to consume.

### Better customer results without security tradeoffs

Customers no longer need to open up inbound ports, VPNs or bastions in order to consume Digibee services. Digibee uses the CloudZiti platform for all networking, including APIs and remote management.

“Integrating CloudZiti into our platform helps us obtain a competitive advantage in our ability to digitally transform our customers' business with a faster time to market, a future-proofed IT infrastructure, the strongest security, and a reduced investment in operational costs.”

— RODRIGO BERNARDINELLI, CEO & Co-Founder, Digibee

## CHALLENGE

### Overcoming operational complexities and security concerns

Digibee's integration architecture is designed to enable enterprise integrations of any scale and size, unlocking organizational agility and supporting exponential growth. The platform offered a built-in API gateway, protected by cloud provider security features to avoid attacks such as DDoS. In this model, Digibee utilized a bespoke solution for point-to-point, device-centric tunnels and a trust model with coarse-grained access controls, resulting in a highly manual and configuration heavy architecture.

Due to the attack surface created by open ports required by VPNs, Digibee's leadership and technology teams began exploring alternatives to mitigate issues with IP overlap and reduce management time to simplify the connection between their infrastructure and their customers' pipeline. The existing architecture simply had too many limitations to scale faster, safer, or more cost-effectively. Given the fact the company had different customers utilizing the same internal and overlapping IPs, the use of site-to-site VPNs made it hard to increase the customer base easily. And multiple providers further complicated VPN management and increased the cost of doing business.

Removing these interdependencies required the company to build a more robust infrastructure as its existing architecture was operationally burdensome to administer and difficult to scale. Customers scrutinized the security threat of open inbound ports required to access local interfaces and shift data to the Digibee platform in real-time. As a result, costs continued to rise due to ongoing operations and management of multiple types of customer endpoints, leaving Digibee struggling to optimize for performance and cost.

When integrating CloudZiti into its iPaaS architecture, Digibee experienced the following gains:

22%

Increase in customer revenue

18%

Reduction in infrastructure costs

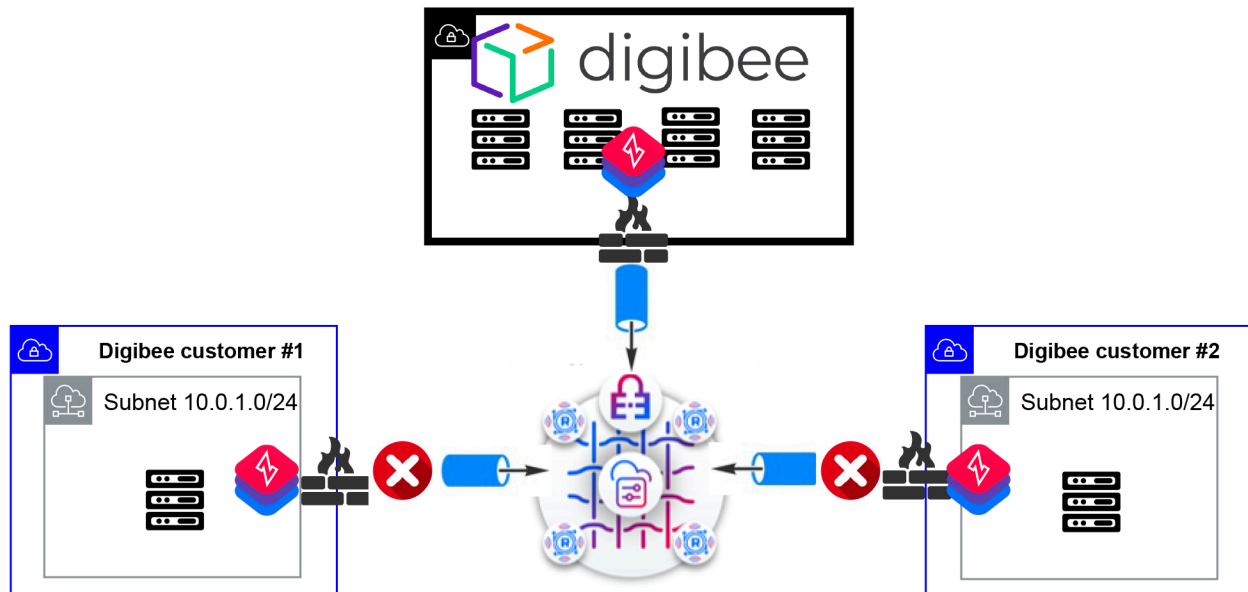
15%


Expansion of global footprint


32%

Decrease in maintenance hours

## CLOUDZITI ZERO TRUST ARCHITECTURE



 Digibee's customer servers make authorized, outbound connects to Digibee's zero trust, mTLS overlay. These connects secure all data flows, including APIs, RDP, SSH, server-initiated and bidirectional.

 Digibee customers close their firewalls to all inbound, and limit egress to Digibee's private overlay. Digibee customer servers private IPs are no longer exposed to the Internet, and CloudZiti identities replace the IPs for routing.



Digibee's multi-tenant, mTLS overlay is deployed anywhere as software, providing network optimization, central control, and rich telemetry. Overlay routers are deployed in minutes in any public or private cloud as Digibee expands. Only authorized Ziti SDK endpoints, Ziti agents, and Ziti routers can access the overlay.



Ziti SDKs enable Digibee to build Ziti zero trust networking into the IPaaS, as code. This embeds zero trust network overlays in proxies, gateways, APIs, and apps. Ziti SDK based endpoints are used for non app embedded use cases.

### Inherent strengths:

- 1 Secure by default private, zero trust fabric overlay renders all APIs and customer-side assets invisible to the Internet, closing all open inbound firewall ports
- 2 SDKs enhance the ability to build zero trust access directly into apps or any edge instantly extending anywhere, instead of a host device or gateway
- 3 Communication is outbound only requiring no overlapping IPs, no port-forwarding, and no firewall holes. Service binding via reverse communication is only permitted by AppWAN association
- 4 Least privileged micro-segmented app connections for data collection from APIs and admin access to networks for each individual customer session
- 5 Exceeds US federal government zero trust mandates with mutual TLS (mTLS), encryption and bi-directional X.509 certificate-based identity and authentication
- 6 Authenticate before connect: If a registered endpoint is not permitted to access a resource, it will never communicate to, or have awareness of, the provider of the resource unless provisioned to it



## SOLUTION:

### Achieving critical security at scale

The integration of CloudZiti into Digibee's infrastructure and customer pipeline allowed the company to immediately remove its complex dependencies on VPNs, mitigate issues with overlapping IPs, and scale the onboarding of new clients and workloads (UVP) with little to no friction. Reliant upon secure and efficient customer data transport, the ability to embed zero trust networking as code enabled the company to achieve unparalleled protection and security.

The iPaaS platform now exceeds US federal government zero trust mandates with mutual TLS, X.509 identities, and a private DNS. CloudZiti authorizes each end-to-end encrypted session for least privileged access – creating micro-segmented networks for each individual customer session. Unlike the former complexities associated with the use of VPNs that exposed the vulnerabilities of the public facing edge, CloudZiti allowed Digibee to take edges off the Internet and available only to authorized endpoints without VPN clients or overlapping, whitelisted static IP addresses - and do it with code and control it all from the cloud.

Digibee's new cutting-edge zero-trust networking architecture enabled secure L3 access to IP: PORT/PROTO or internal DNS names through AppWANs. This allowed endpoints to exist in multiple environments, and with the help of SDKs, zero trust access could be seamlessly integrated into the iPaaS application with performant RDP and SSH. AppWANs offered outbound-only communication and service binding via reverse communication. Endpoints had to authenticate before connecting, and administrators could effortlessly provision access to new services and distribute them to other endpoints. Users could safely access high-performing services like live video with this private network's added security and performance.

CloudZiti eliminated Digibee's complex and expensive "bolted-on" infrastructure and processes that their public-facing endpoints traditionally required. The same platform secured remote management of the company's infrastructure, secured connections to its CI/CD and ops management and monitoring solutions, and secured networking between its servers and backend data stores with

certificate-based security applied to the network layers (not just applied to the user level).

### Operational simplifications, automation, and maintenance

CloudZiti enabled Digibee to embed secure provisioning, management, and networking into its platform as pure software, and its cloud-native integration with every major cloud allowed the company to build and run scalable applications. This greatly reduced the time to onboard new customers and deploy workloads, while improving and simplifying the security posture of the enterprise.

The new architecture eliminated VPN and private mobile APN backhaul and the dependencies on static IPs or port forwarding. It also enabled simple remote provisioning and management for authenticated administrators, using any network, even third party WiFi. Now with private app-specific networking, Digibee can limit bespoke IT systems and extend zero trust security across many use cases to be future-ready and solve new security challenges over time.

The cloud orchestrated software improved app performance and productivity of the company, increasing agility and automation, and decreasing support costs. CloudZiti's Smart Routing capabilities also ensured Digibee could automatically minimize latency as endpoints and routers dynamically choose the best path available on the private, zero trust fabric. The complete, integrated solution simplified customer deployments for the company and significantly reduced maintenance and support hours.

**“We have significantly reduced our VPN complexity and mitigated issues related to NAT and FTP with overlapping IPs, which has enabled us to onboard new clients and workloads with as little friction as possible. NetFoundry has allowed us to scale faster, safer, and more cost-effectively, while CloudZiti's zero trust overlay mesh network provides secure provisioning, management, and networking into our solutions as pure software.”**

— RRODRIGO BERNARDINELLI  
CEO & Co-Founder, Digibee

## ABOUT NETFOUNDRY

Networking was once a barrier to app innovation and automation with dependencies on after-the-fact security and performance engineering. NetFoundry is shifting the paradigm in cybersecurity by embedding zero trust networking and security as code. Our CloudZiti solution embeds zero trust as software into apps, APIs, IoT devices, and other valuable assets rendering critical infrastructure invisible to the Internet – and unreachable by potential attackers. It is the world's first programmable, cloud native, zero trust network with near unlimited scale, concurrency, and performance. CloudZiti represents a new art of the impossible by enabling developers, network engineers, DevOps, and cloud teams to programmatically control private, zero trust, high performance networking. CloudZiti is built on NetFoundry's OpenZiti solution, the world's most used and widely integrated open source secure networking platform.