Neustar and NetFoundry Deliver World's First Identity-Secured IoT Networking Solution

Oct 4, 2017

End-to-end, network-independent security, compliance and reliability

Neustar, Inc., a trusted, neutral provider of real-time information services, and NetFoundry™, a Tata Communications business incubated in Tata Communications' 'Shape the Future' program, announced an integration between the Neustar Trusted Device Identity (TDI) solution and NetFoundry's Application Specific Networking (ASN) platform, which provides customers with superior security, extending trusted identity based solutions across multiple networks and clouds.

The Neustar Trusted Device Identity (TDI) solution, built-on-top of the NetFoundry Application-Specific platform, reduces the time, cost and risk of implementing secure end-to-end solutions.

"Creating a secure end-to-end environment based on identity for devices and secure core transport to the edge is necessary for IoT to gain adoption," said Hank Skorny, SVP of IoT, Neustar. "Neustar and NetFoundry together provide a highly secure, highly manageable and recoverable environment to secure communications between any and all parties."

"Traditional networking with the use of PKI and firewalls has been manageable to date, but the digitally transformed applications landscape requires the app contexts, such as identity, to programmatically define the network," said Galeal Zino, Founder of NetFoundry. "Our platform enables leading solutions from innovative partners such as Neustar to program the network to enforce each application's identity, access and security policies, rather than trying to manually manage a separate set of policies on the network."

PKI-based identity management solutions are leaving IoT enterprises exposed and overburdened with the need for certificate management of thousands of devices. Neustar TDI delivers a next-generation approach to trusted identity management, offering the scale and security required for the Internet of

Things. By applying this new approach to traditional PKI with multi-factor device authentication, Neustar TDI can authenticate and revoke identities in real-time, monitor and detect behavior anomalies, as well as enable organizations to quickly isolate and recover from breaches. This way the IT Network Operations Center (NOC) can take back control of revocation and restoration.

The NetFoundry platform enables leading solution providers like Neustar to integrate application specific networking into their solutions ("AppWANs") with no restrictions on network providers, VPNs or custom CPE. Each AppWAN is driven by the context of the application, such as identity, compliance and performance needs, enforcing application level micro-segmentation across any set of networks and clouds, with superior performance and security results, while enabling complete, centralized control and visibility of each AppWAN.

The Neustar and NetFoundry implementation is ideal for microservices-based architectures, such as the one developed by the open source EdgeX Foundry project of the Linux Foundation, of which both Neustar and NetFoundry are founding members.

Customers using a TDI and NetFoundry end-to-end solution benefit from:

- Real-time activation and revocation
- Route validation
- Secure remote management
- Anomaly detection
- Multi-factor authentication
- Recovery without the need to re-key
- Endpoint and identity management
- The security and efficiency of end-to-end identity driven networking
- Enhanced application performance with dynamic path optimization and remediation
- Application level micro-segmentation with data-in-motion encryption and isolation

A secure end-to-end Networking Platform as a Service (NPaaS) solution will be demonstrated by Neustar and NetFoundry at the Linux Foundation/EdgeX Foundry booth at IoT Solutions World Congress in Barcelona, Spain from October 3-5.

For more information about Neustar TDI and EdgeX Foundry, read our blog.