THE TIME IS NOW FOR BLOCKCHAIN ENABLED-CLOUD DELIVERED NETWORK SECURITY

Networks are the nerve system of successful companies that are able to deliver on the ever-changing demands of a global marketplace. Although there are varied solutions that enable cloud-based orchestration of networks, they walk a tight rope due to the pros and cons they carry. While these solutions leverage concepts such as 'intent based networking' to provide immense flexibility and simplicity in managing networks, they also bring with them the challenges of multi-layer security and integrity.

Although there are many ways to skin the proverbial cat, few, if any are more effective than embracing the underlying principles of Blockchain. We at Happiest Minds would like to provide a deep dive into how Blockchain can be used to provide cloud-based network security. We also have showcased a list of use-cases that can be used in the context of Software Defined Networking and proposed a solution that would be agnostic to network automation frameworks.

EMERGENCE OF CLOUD ORCHESTRATION AND INTENT DRIVEN NETWORK CONFIGURATION AND MANAGEMENT

Cloud based management platforms are crucial in managing important elements of the infrastructure that typically includes compute, storage and networking. An evolved version of this is 'cloud orchestration' that includes multiple cloud management platforms and other tools to provide a holistic view and manage a complex and interlinked cloud infrastructure.

Concurrently, 'Intent based Networking' is the next big thing in the constantly busy networking world that was until recently smacking its lips over SDN and SD-WAN. The goal of intent-driven networking is to scale network management and add real intelligence to the infrastructure. A process that is intent driven allows for the management of networks with a single interface and effectively provisions orchestration. Engineers now benefit from a preconfigured network application that interprets intent and translates it to the various languages, protocols and syntax necessary to configure any type of network device.

CHALLENGES OF MULTILAYER NETWORK SECURITY

SDN and NFV have captured the imagination of several enthusiasts and businesses alike with a plethora of benefits like agility, openness, cost optimization and remote programmability. But they also bring with them pertinent security concerns that need to be addressed to maximize their business upside. Let us explore some of the most important challenges in ensuring security of multi-layered networks.

INSIDER THREAT

As is often the case, the biggest threat to a security operation being compromised is from the inside. It isn't uncommon for a disgruntled employee or business associate to engage in nefarious activities like releasing viruses, worms, trojan horses or manipulating network configurations. Although the popular perception with insider threats is that they are caused with malicious intent, a lot of such data breaches and leaks are accidental and the result of a system with poor checks and balances.

INTEGRATION

We live in a world that is driven by collaboration and integration and the same holds true for ensuring network security as well. While this collaboration and integration allows for unparalleled efficiency of deploying and managing network security in a heterogeneous environment, it also poses a significant risk as the lack of a shared identity roster could allow a partner to tamper with the sanctity of an entire network's configuration.

CONSISTENCY

Ensuring consistent configurations across each layer like network automation platform, the SDN controller and the network elements is key in addressing today's rapidly escalating security threats. Additionally, organizations need to be on top of all the latest upgrades and revisions that have been brought about by vendors of anti-virus systems, firewalls and intrusion detection systems. Falling behind this curve means exposing yourself to providing inconsistent configuration and compromised network security, which businesses of today can ill afford.

AVAILABILITY

The definition of 'Availability' has changed drastically in recent times and the bar has been set higher with each iteration. Although availability in an absolute sense would entail "100% availability", a more popularly accepted yet difficult target is the "five 9s" or 99.999% availability. There are mechanisms for High Availability which can ensure the "five 9s", however, a lack of secure, reliable and instantaneous rollback from misconfigurations makes it an arduous task to recover from outages and ensure business continuity.

SILVER BULLETS TO ADDRESS THE CHALLENGES OF MULTI-LAYER NETWORK SECURITY

SOFTWARE DEFINED SECURITY

SDSec offers a new way to design, deploy and manage networking services by decoupling the network function, such as firewalling and intrusion detection, from proprietary hardware appliances, so they can run in software mode. The result is a dynamic and distributed system that virtualizes the network security enforcement function, scales like VMs and is managed as a single, logical system.

SOFTWARE DEFINED PERIMETER

SDP solution ensures that all endpoints attempting to access a given infrastructure are authenticated and authorized prior to being able to access any resources on the network. All unauthorized network resources are made inaccessible.

SEGMENTING

Simply put, network segmentation is the act of splitting a network into many "sub networks" known as segments. With network segmentation, organizations can enhance network security by controlling access to sensitive data in the form of enabling or denying network access.

LEVERAGING THE PRINCIPLES OF BLOCKCHAIN

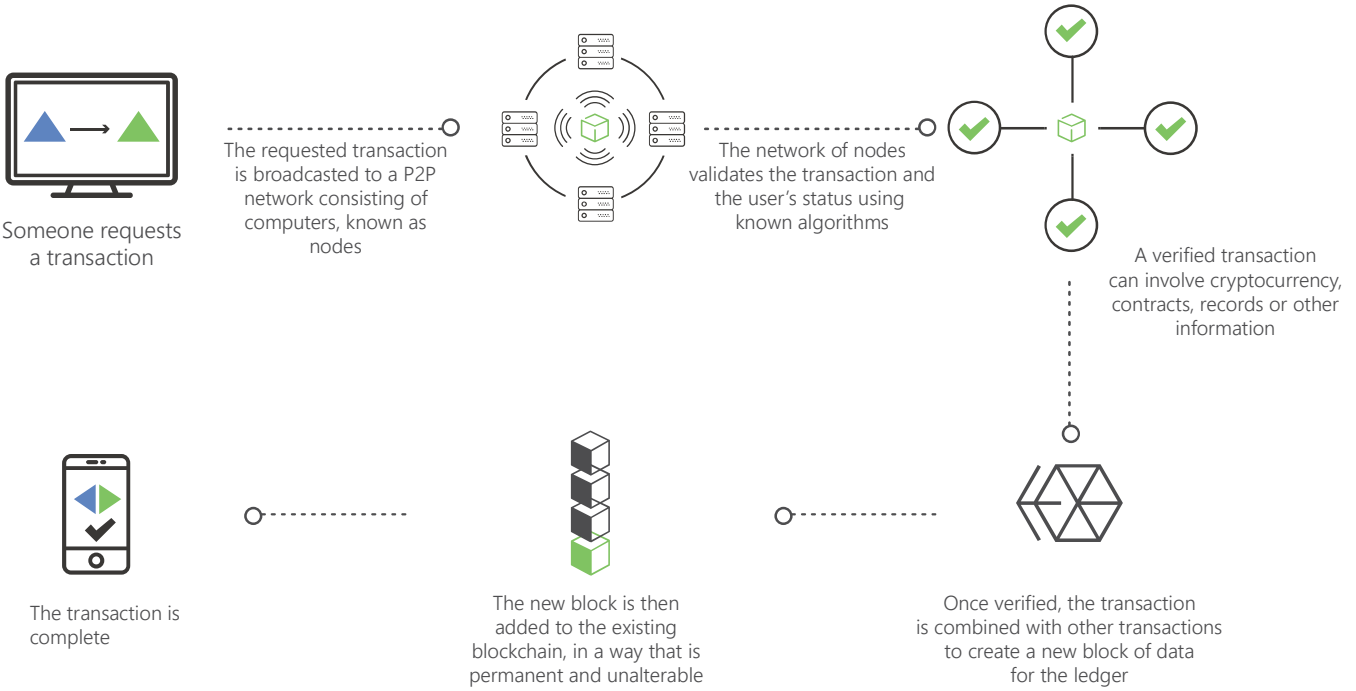
The technology world is never short of new ideas that carry with them the smell of disruption and few ideas have captured the imagination of visionaries and pundits alike, as has 'Blockchain'. Although the underlying technological components, processes and standards are still far away from reaching maturity, it hasn't stopped a swathe of interested observers from imagining the unending possibilities.

Arising from the emergence of 'Bit Coin', the idea of Blockchain has taken on a life of its own because of its potential to create an evolutionary 'shift of trust' from centralized to decentralized record keeping models in complex, interlinked and distributed business environments.

While there are plenty of academic definitions of Blockchain, in its most practical sense it is a highly secure digital ledger that allows for information to be distributed but not copied so that businesses can use it as a single source of truth to track critical activities and create cost and operational efficiencies.

For the purposes of this paper, we attempt to use the underlying philosophy of Blockchain to provide cloud-based network security, ensure adequate security at multiple layers while efficiently addressing complex integrity requirements.

HOW IT WORKS?

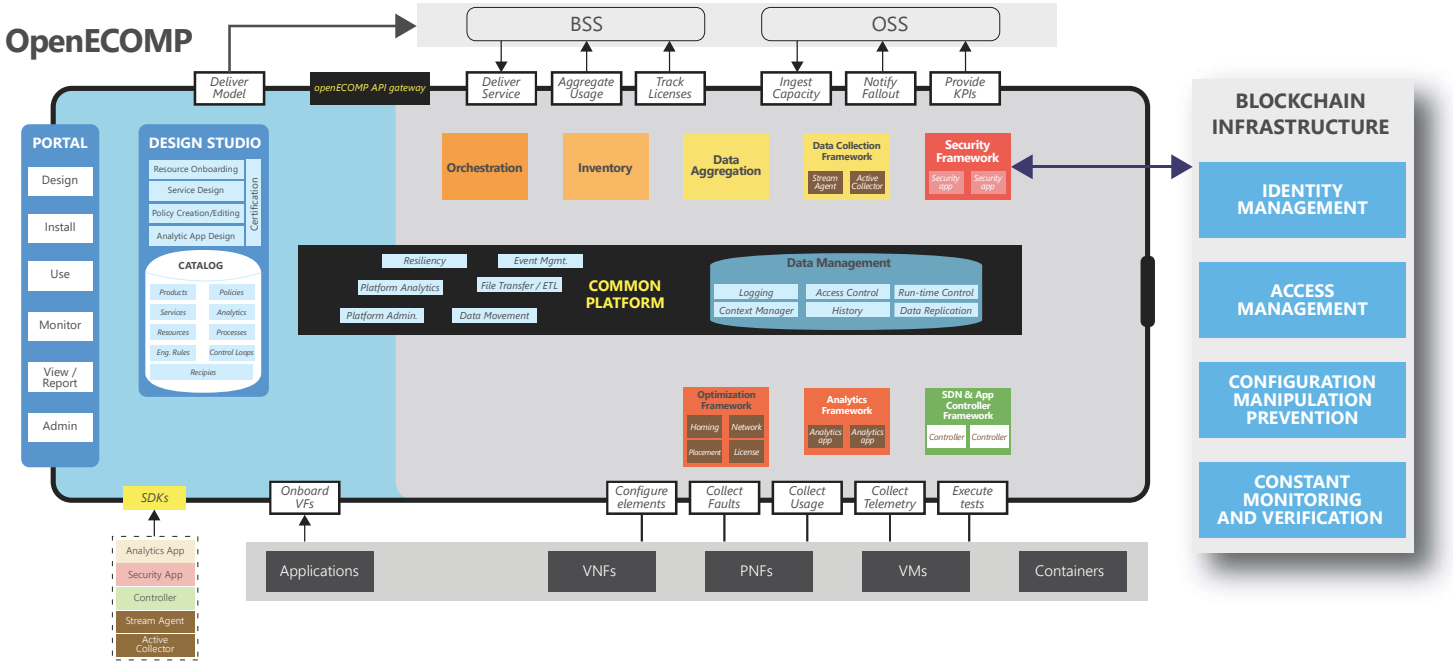


ONAP

ONAP (Open Network Automation Platform) is an open source software platform that delivers capabilities for the design, creation, orchestration, monitoring, and life cycle management of:

Virtual Network Functions (VNFs)	Carrier-scale Software Defined Networks (SDNs) that contain them	Higher-level services that combine VNFs and SDNs

A high level Solution Architecture with ONAP integration



IDENTITY AND ACCESS MANAGEMENT

Blockchain based identity management systems can ensure that user identification data, after appropriate consensus in a distributed environment is shared amongst the domains. In addition, appropriate provisioning privileges are granted based on the information stored in the latest node of the ledger. Further, the system can be linked to a biometric based authentication system – which would find further acceptance as compared to password based with emerging finger sensing capabilities in mobiles.

INSIDER ATTACK PREVENTION & SECURITY EVENTS

ONAP has a component DCAE – Data Collection and Analytics Engine that gathers VNF data, network data, logs and events and runs analytics for determining security events while responding to actions like modifying firewall rules or updating IPS signatures. By using Blockchain, tampering of information can be prevented thus ensuring that the analytics engine processes the right logs, in the right order resulting in prevention of any security event.

CONFIGURATION MANIPULATION PREVENTION

This is an important attack vector and some well-known techniques in this area are:

1. Insertion of malicious flow entries in network elements.
2. Modification of network policies or configuration at the orchestrator or element layer

With Blockchain infrastructure, we can get immutable and independent proof of time and order of configuration events like policy change configurations, topology change configurations, introduction of new services and changes in existing services. This property can be used to prevent any tampering of the configuration across the components of the configuration work flow.

Consider the typical work flow of service configuration:

STEP 1

Typical flow:
As depicted in the diagram above, when a configuration order request is received from the portal, the service creation component generates the service request and appropriate policies are then assigned in the design framework component.

Blockchain Flow:
When a new service order is received, the design component and policy creation engine stores the order information as well as the appropriate rules / policies into the blockchain

STEP 2

Typical flow:
The Policies and Rules created in Step 1 are then sent to the Run Time framework of the Controller Function.

Blockchain Flow:
When the Run-Time environment receives the rules and policies to be applied, it would query the blockchain infrastructure to ensure that the rules and policies stored in the last node of the Blockchain are same.

STEP 3

Typical flow:
The controller component would register the rules and update the inventory, topology info and push these rules as updates to nodes through south bound adaptors.

Blockchain follow:
The controller component would register the Blockchain validated rules

STEP 4

Typical flow:
The configurations are received and the node level is updated with the new configuration request.

Blockchain follow:
The nodes are updated with the Blockchain validated configurations. Similarly, at each subsequent step of the work flow, such pre-application validation can be performed.

CONSTANT MONITORING AND VERIFICATION
AN ADDITIONAL SAFE GUARD

While due safeguards can be put in place at each stage of the configuration work-flow, there might still be a blind spot, which can provide a window of opportunity for the intruder to manipulate the network. We can use the signage property of the Blockchain to ensure that configuration is consistent and on detection of any failure, an appropriate roll-back is initiated. This can be achieved by deploying a monitoring agent at each element of the work-flow which would trigger an event for validation of the signed configuration data.

CONCLUSION

Undoubtedly, there are many solutions that can prevent security breaches. However, none of them are powerful enough to deter an insider from circumventing these solutions and removing their trails. Further any incorrect information of the events, logs and configuration changes can result in unexpected system behavior with disastrous consequences.

Using blockchain ensures an immutable & signed record of events and configuration updates thus creating an independent validation system that is tamper proof and immune from external and internal attacks.

Write to us at:
sdnnfv@happiestminds.com

ABOUT HAPPIEST MINDS

Happiest Minds enables Digital Transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights through an integrated set of disruptive technologies: NFV & SDN, Big Data analytics, Internet of Things, mobility, cloud, security, unified communications, etc. Happiest Minds offers domain-centric solutions-applying skills, IPs and functional expertise in IT Services, Product Engineering, Infrastructure Management and Security. These services have applicability across industry sectors such as retail, consumer packaged goods, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India, Happiest Minds has operations in the US, UK, Singapore, Australia and has secured $52.5 million Series-A funding. Its investors are JPMorgan Private Equity Group, Intel Capital and Ashok Soota.