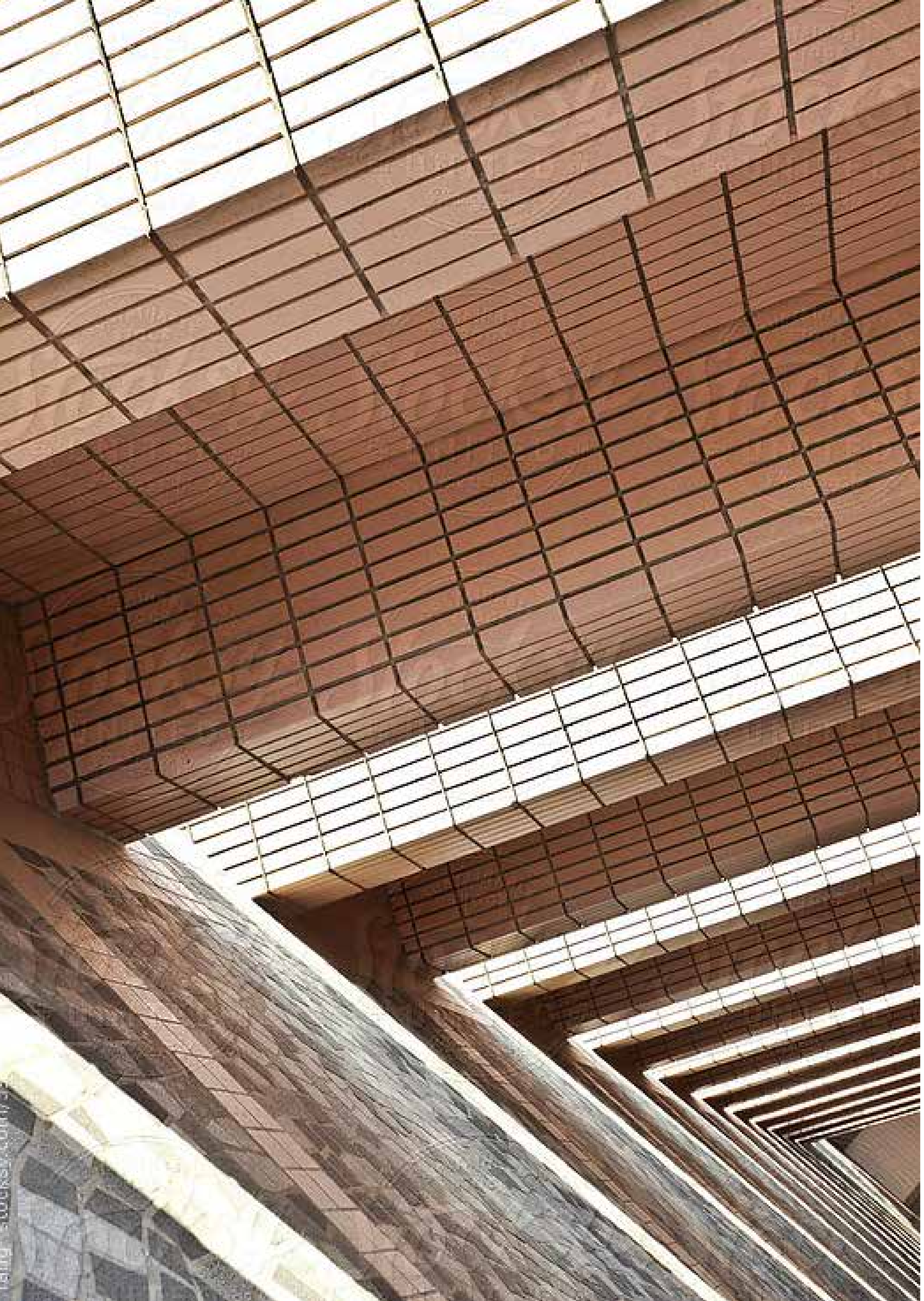
guardtime

Use of a globally distributed blockchain to secure SDN

www.guardtime.com



Introduction

Due to environmental constraints, budget cutbacks, and increased requirements to streamline data centers and systems, departments and agencies in the federal, DOD and Intel communities are looking to adopt industry best practices such as Cloud, Managed Services and Software Defined Networks (SDN). While all three are valuable strategies to increase efficiencies while cutting cost, SDNs enable cloud infrastructure and Managed or Shared services to extend virtualization into the network plane. SDNs allows enterprises to promote modernization and increased command and control over assets via:

1. Increased cloud enablement and effectiveness via virtualization across all network planes
2. Increased governance and control over large, enterprise networks
3. Increased mission readiness and agility to react and remediate network issues or breaches
4. Increased visibility and transparency into enterprise and geographically dispersed networks.

With all progressive technology, the very tenets that allow for increased capabilities will change the necessary security posture to adequately protect the enterprise. SDNs are similar to the adoption of previous architectures such as SOA or Web Services, where new security mechanisms and mitigations were required. With SDNs, the new architecture changes the paradigm from a decentralized aggregation of network assets to a more centralized and streamlined model.

Traditionally, most large networks consist of a multitude of routers, switches, gateways etc. that were managed almost independently. As illustrated in Figure 1 below, requirements are gathered, aggregated, and executed in a mostly manual method. Each Network Asset requires a configuration that is updated manually via an authorized user. While this provides some security through dissociation of assets, it does not allow for an agile enterprise that provides real time scaling, remediation and configuration.

Newest cyber threat will be data manipulation, US intelligence chief says.
US intelligence chiefs are warning Congress that the next phase of escalating online data theft is likely to involve the manipulation of digital information.

http://www.iacpcybercenter.org/news/newest-cyber-threat-will-be-datamanipulation-us-intelligence-chief-says/

NSA Chief on data manipulation:
“Historically, we’ve largely been focused on stopping the extraction of data and insights, whether for intellectual property for commercial or criminal advantage, but what happens when suddenly our data is manipulated and you no longer can believe what you’re physically seeing?” he said.

“As a military guy, who’s used to the idea that, ‘I can look at a display, I can look at a set of data, and I can very quickly draw conclusions and start to make risk-based decisions quickly,’ what happens if that gets called into question? I believe that’s going to happen.

http://www.businessinsider.com/nsa-chief-describes-3-biggest-cyber-threats-2015-10

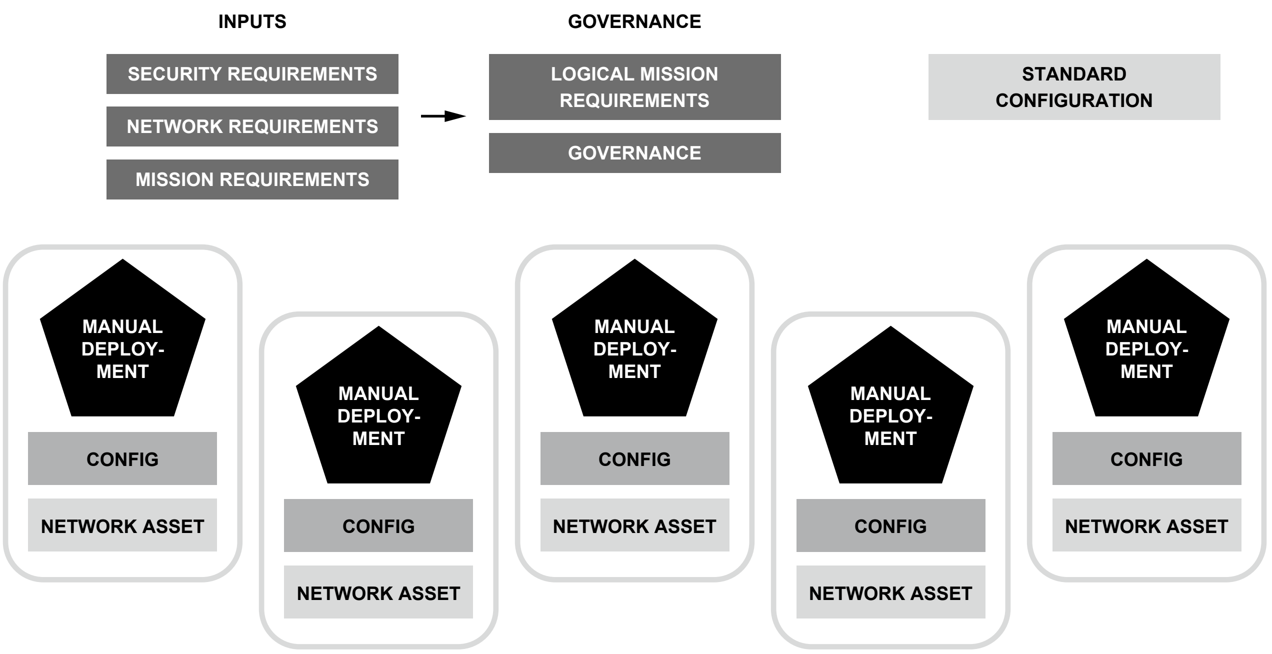


Figure 1 Traditional Network Configuration

With a SDN, the network is abstracted from hardware appliances and bare metal assets. By abstracting the control of these configurations and creating virtual network assets, the applications, VMs and other components can connect to these assets as they would on a traditional network, but provides the enterprise with the ability to add, remove and update the network assets in a dynamic and centrally controlled model. Thus SDNs provides a robust and agile network allowing for additional nodes and assets to be created and removed with the same agility as creating a VM or other virtualized or cloud asset.

With the centralization and aggregation of the control of these virtual network assets, the security posture of the enterprise shifts from a segregated, dissociated attack plane to a more centralized and abstracted surface. By the tenets of SDNs, the control mechanisms are managed by a centralized control application that will logically store all configurations for the network assets. Integrity and access to these configurations is paramount for the system to function correctly and defend against malicious behavior. In order to provide accurate and protected configurations, Keyless Signature Infrastructure (KSI) provides the required security posture to monitor and verify that assets are accurate and accessible.

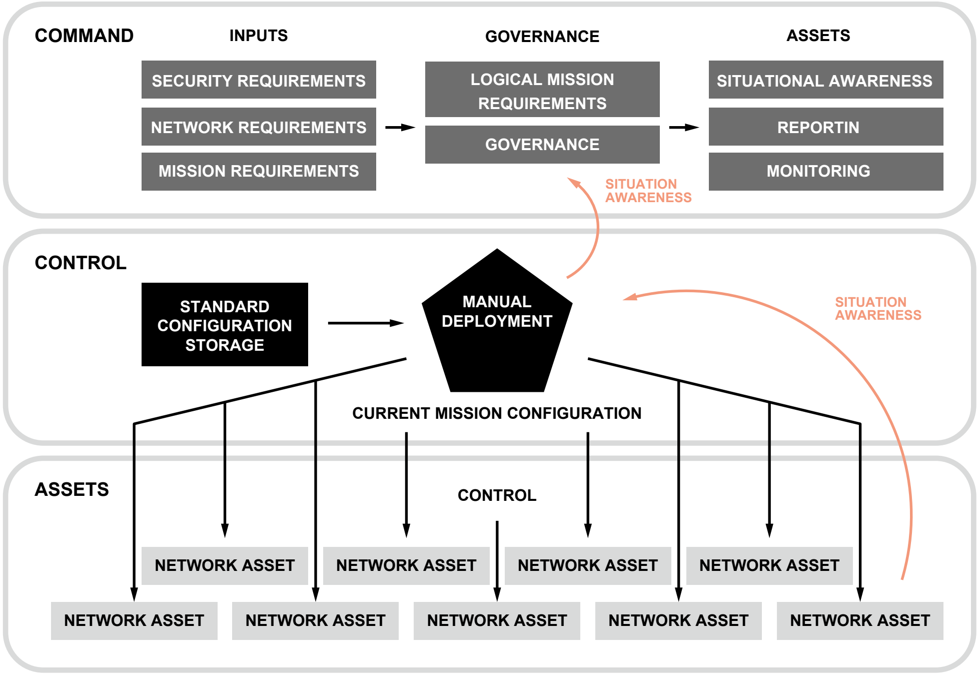


Figure 2 SDN Configuration

KSI is a data-centric security technology based on cryptographic hash functions, requiring only the use of hash-values and binary trees. By integrating KSI into networks, irrespective of where an asset is transmitted or stored, every component, configuration, and digital asset generated by humans or machines can be tagged, tracked and located with real-time verification independent of trusted administrators. KSI provides a truth-based system wherein the need for trust can be completely eliminated. KSI provides the capability to create a signature of the configuration or control data upon creation and verification of that data upon use by the network nodes or other assets.

By leveraging KSI technology, the components of a SDN will have the ability to sign and verify data as it moves between components. This provides the enterprise with a data integrity infrastructure in which data can be signed and verified in near-real time. The data residing in the configuration storage is monitored and verified against the associated signatures that were created upon the creation of the configuration data. This allows for near-real time enterprise data integrity checks before the network nodes request to use a configuration. By monitoring the current true configurations and verifying the configurations upon network asset creation or change, the enterprise can assure each network asset uses the correct configuration.

Introduction to KSI

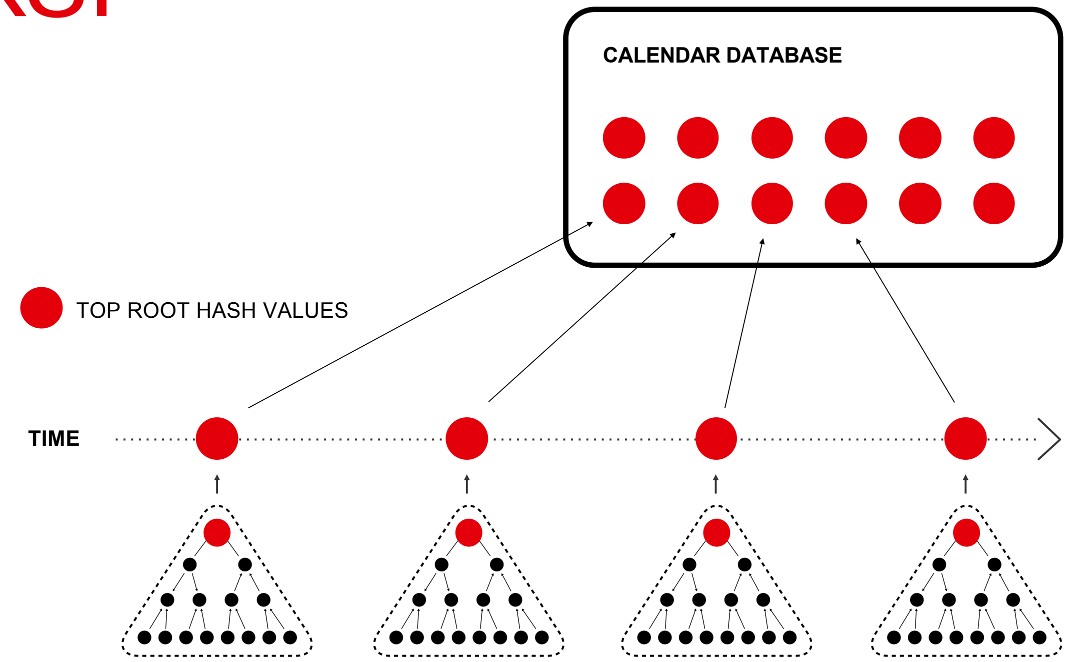


Figure 3 *Calendar hash block chain*

Every second, a federated and distributed binary tree is generated using hash-values of data generated around the globe within that second. A hash tree is essentially a binary tree of hash values. Two input values, along with any other desired parameters, are concatenated and run through a hash function. This process is iterated, resulting in a single root hash value.

The word “keyless” means that signatures can be verified without assuming continued secrecy of any keys. While shared secrets may still be used for authenticating clients during the signature creation process, no keys are needed for the signature verification itself. The integrity of the signatures is protected using one-way, collision-free hash functions.

In the use of KSI, the root hash is calculated and “published” in a distributed “calendar” database that every customer (or subscriber) has a copy of. For every hash value entered into the tree, there is a unique hash-chain, or series of hash-values that allows the root hash-value to be recreated. This hash chain is returned and stored as the signature. A signature for a given digital asset identifies the computation path, through the hash tree, from the asset’s own hash value, up to the root calendar value. The signature also includes “sibling” values that were concatenated at every step in the hash tree, which are necessary to recreate the root hash. With access to the public “calendar” database, anyone, anywhere, can receive data and verify the signature, which includes indications of time, identity and integrity, without reliance on a central trust authority.

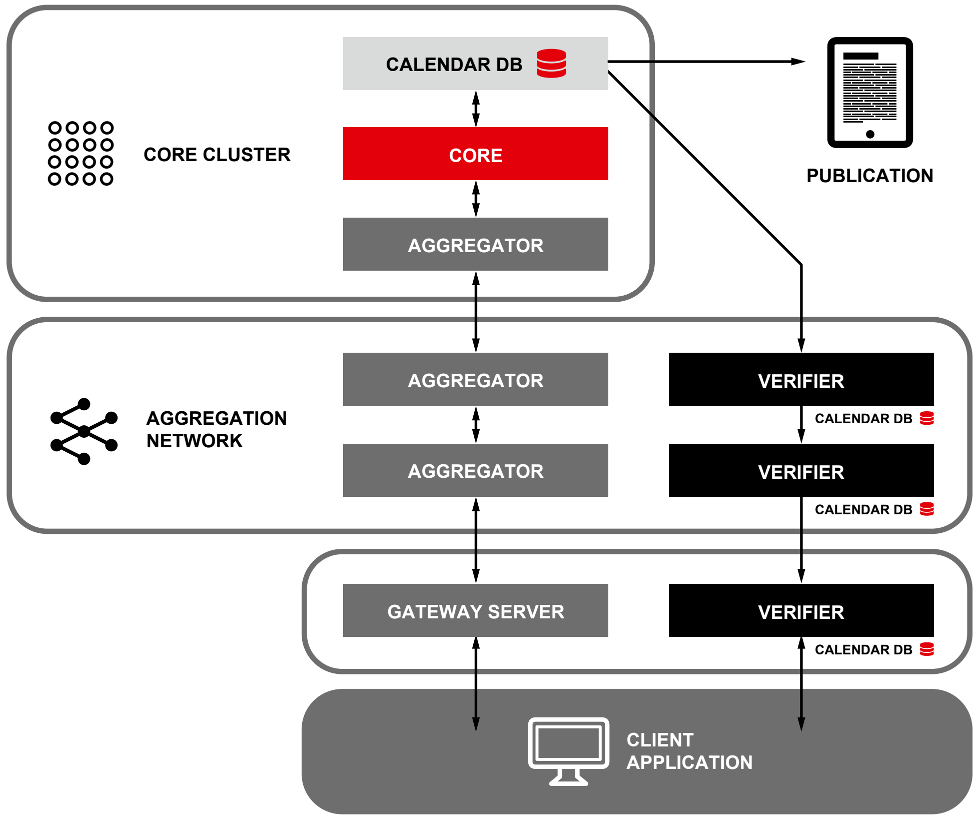


Figure 4 *KSI Infrastructure*

The KSI infrastructure comprises four main components - Cores, Aggregators, Verifiers and Gateways. The core cluster manages the calendar and selects the top root hash for each second. The aggregation network aggregates the hash values and distributes the signatures. The verification network provides widely witnessed access to the state of the calendar. KSI signatures provide proof of signing entities, since parent aggregators accept requests only from authenticated child aggregators.

Software Development Kits (SDKs) are required to integrate KSI into end-user applications. Clients who wish to digitally sign objects using KSI use the client side KSI SDKs to communicate with a KSI gateway. The application presents the data hash to the gateway, receives and must then store the signature, and performs verification calls.

KSI and SDN Security

There are several known attack vectors on SDN:

- Malicious SDN applications
- Malicious controller that creates entries in the flow tables of the network elements, thus gaining complete control of the network.
- Malicious network element, admin
- Unauthorized access to an SDN controller, network element or host connected to the SDN
- Unauthorized modification of data – network policies, configuration files, network topology
- Destruction of essential SDN function/data – loss of integrity and service disruption

The Open Networking Foundation (ONF) has recommendations for securing SDNs (Reference #1). A subset of these issues is addressed in the sections below.

Insider Threats

Breaches and a loss of trust (insider threat) are inevitable in any networked environment and with that implicit trust is gone. External, independently verifiable indicators of tamper are required, to establish ground truth. Insider threat is a case of who watches the watcher.

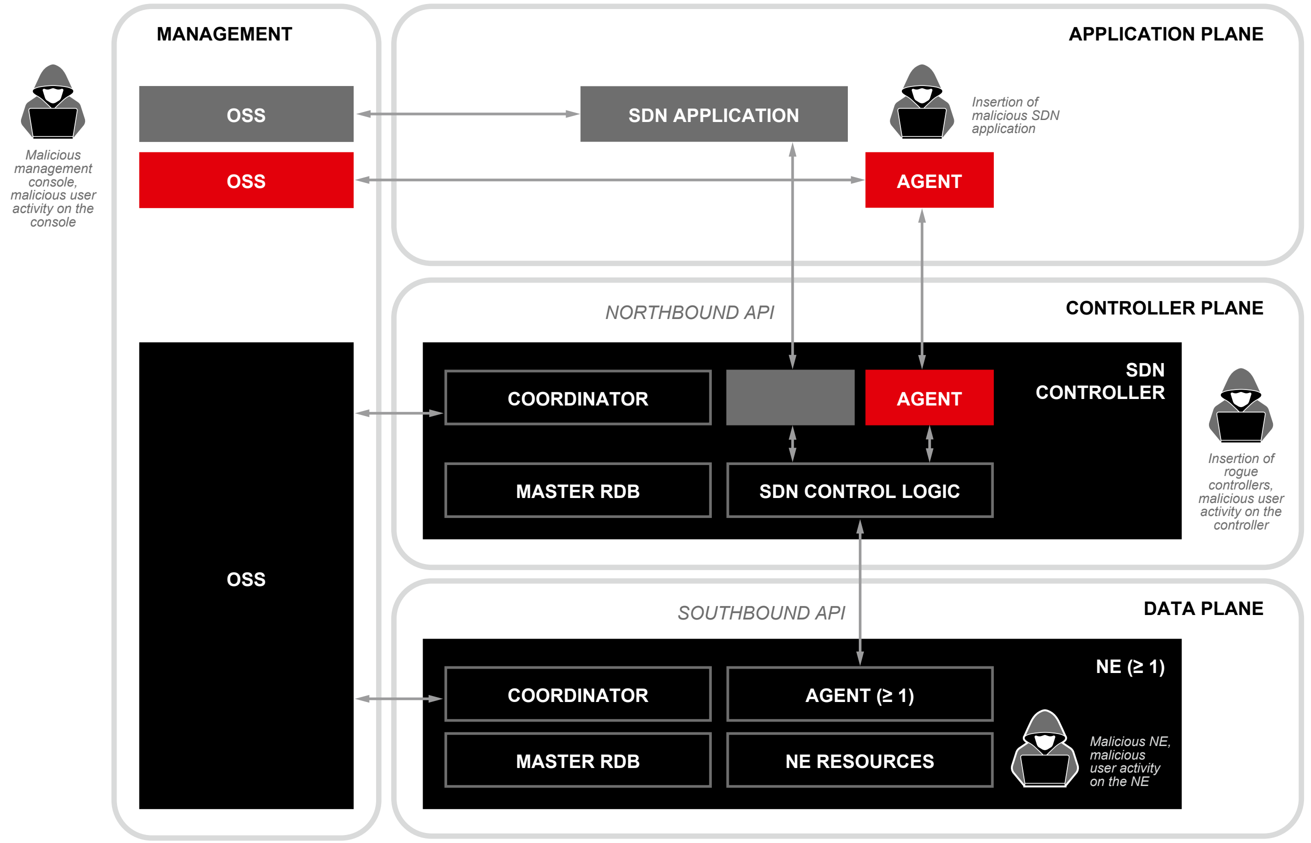

MANAGEMENT
APPLICATION PLANE
Malicious management console, malicious user activity on the console
OSS
OSS
SDN APPLICATION
Insertion of malicious SDN application
AGENT
NORTHBOUND API
CONTROLLER PLANE
COORDINATOR
AGENT
SDN CONTROLLER
MASTER RDB
SDN CONTROL LOGIC
Insertion of rogue controllers, malicious user activity on the controller
OSS
SOUTHBOUND API
DATA PLANE
NE (≥ 1)
COORDINATOR
AGENT (≥ 1)
MASTER RDB
NE RESOURCES
Malicious NE, malicious user activity on the NE

Figure 5 SDN Architecture and Threat Vectors Overview

KSI can watch the watcher (an insider with access or a hacker with stolen credentials or elevated privileges) by providing, external, immutable proof that the data supporting the SDN is valid and unchanged from a point in time forward. It can alert to an unanticipated modification in moments. Additionally, KSI could enforce a two-person protection to the underlying SDN data, further reducing the ability for a single rogue administrator or hacker to do damage. These steps mitigate the threat created by SDN's centralization of control - a key security concern with the model.

- Trust - Traditional SDN security solutions deploy white lists to enforce trust between devices and controllers in an SDN. KSI can be used to offer integrity protection on these white lists.

- Mishandling of secrets - Unlike traditional public key infrastructure (PKI) signatures, KSI does not require the use of secrets to sign objects or assets. Hence a malicious insider cannot misuse any secrets to hide their tracks.

- Assured Identity - Authentication based on identity is paramount to security of an SDN system for impersonation prevention to ensure malicious entities don't tamper with the controller configuration. KSI offers a means to cryptographically assure robustness of endpoint identities by including the identity as part of the KSI signature. (Refer to #1 for further details on assured identity)

- Proof of participation - The KSI hash chain contains the information needed to regenerate the root hash value from a given leaf of the tree. The hash chain proves that the input value was part of the original set the tree was built upon. Thus, KSI provides proof of participation of each SDN node in any given hash chain, thus preventing malicious nodes from hiding their tracks.

Data manipulation is a real threat. If the insider copied sensitive company IP and then tried to delete/edit the log files to remove traces of their actions, any software tool that is monitoring the KSI-stamped logs would see a change alert resulting from a failed KSI signature verification. This event can be reported immediately so that the security operations team can take appropriate action quickly. In the absence of technology like KSI, the logs would typically need to be examined manually/visually to interpret changes/malicious events before any action taken, often far too late.

CIA Triad

- Confidentiality – Encryption is widely used to provide confidentiality. However, without integrity, encryption brings a false sense of security in cases where malware can be introduced into systems, compromising the integrity of the system securing sensitive data assets.

- Integrity - Protecting the network policies, configurations, and flow tables from intentional or unintentional tampering helps contain the threats in an SDN environment. There are more network-accessible interfaces and network control information is consolidated into a smaller number of locations instead of being spread over the entire network.

  - In the control plane, the logs and network topology are prone to attacks.
  - Southbound and Northbound APIs can be spoofed and the attacker could create 'rogue' controllers to control the entire network.
  - At the application plane, the SDN applications and logs need to be protected from application manipulation.

Former National Security Agency director and retired Gen. Keith Alexander told FCW on Oct. 22, 2015 – "The ability of an adversary to manipulate the content of data stored on networks is an "emerging art of war in cyberspace".

The phenomenon is on the radar of U.S. intelligence officials. Alexander's successor as leader of NSA and Cyber Command, Adm. Michael Rogers, and Director of National Intelligence James Clapper has warned that data manipulation is an emerging cyberthreat.

The future might include "more cyber operations that will change or manipulate electronic information in order to compromise its integrity...instead of deleting it or disrupting access to it," Clapper said in prepared testimony for a House Permanent Select Committee on Intelligence hearing in September, 2015.

https://fcw.com/articles/2015/10/22/alexander-datamanipulation.aspx?m=1

- Availability - Additionally, the centralized model of SDN heightens the impact on the third leg of security, availability. As with the OPM breach, the loss of trust in the central database wreaks havoc on their operation to this day. Imagine then the impact of a loss of trust in the SDN data assets. The campus, wide area or operational network would have to be brought down. The most massive denial of service imaginable. With KSI instrumenting and providing integrity of the policy, configuration and transport data, upon breach or notification of tamper, KSI would provide ground truth allowing near immediate restoration the network to a known and trusted state. Only with KSI is that known state externally verifiable with no reliance on trusting the credentials or intentions of a possibly compromised inside administrator.

KSI and SDN Use Case Overview

While KSI is a cornerstone of the overall enterprise security posture, KSI enables SDNs by adding a layer of integrity to the data and ultimately trust in the switch to logical and virtualized networking assets across the enterprise. While each actual deployment of KSI with the different technologies has specific design details, the overall use case for enabling SDNs with KSI has four key integration points in the reference architecture shown in Figure 6 below.

In the reference implementation diagram above, the numbers depicted below highlight the integration between a logical SDN stack and the enterprise KSI infrastructure. The reference implementation diagram can be explained by the following:

1. Sign Configuration Data – In this example, at data flow 1, the original configuration upload that comprises the configuration data to be stored or uploaded to the Control applications is created and uploaded to the Configuration Storage. This data is signed prior to upload, which creates the original KSI signature of that data. This signature can be stored with the original configuration data or stored in an external system (signature escrow).

2. Monitor Verification Data – Data flow 2 illustrates the periodic monitoring of the current configuration data. Since all data has been signed upon upload, each configuration document can be verified periodically against the signatures. The overall state of the configuration data storage is also signed and periodically verified against signatures related to logical blocks of the data. This allows for the configuration data storage to verify either all or subsets of the storage data to recognize any change to the storage environment.

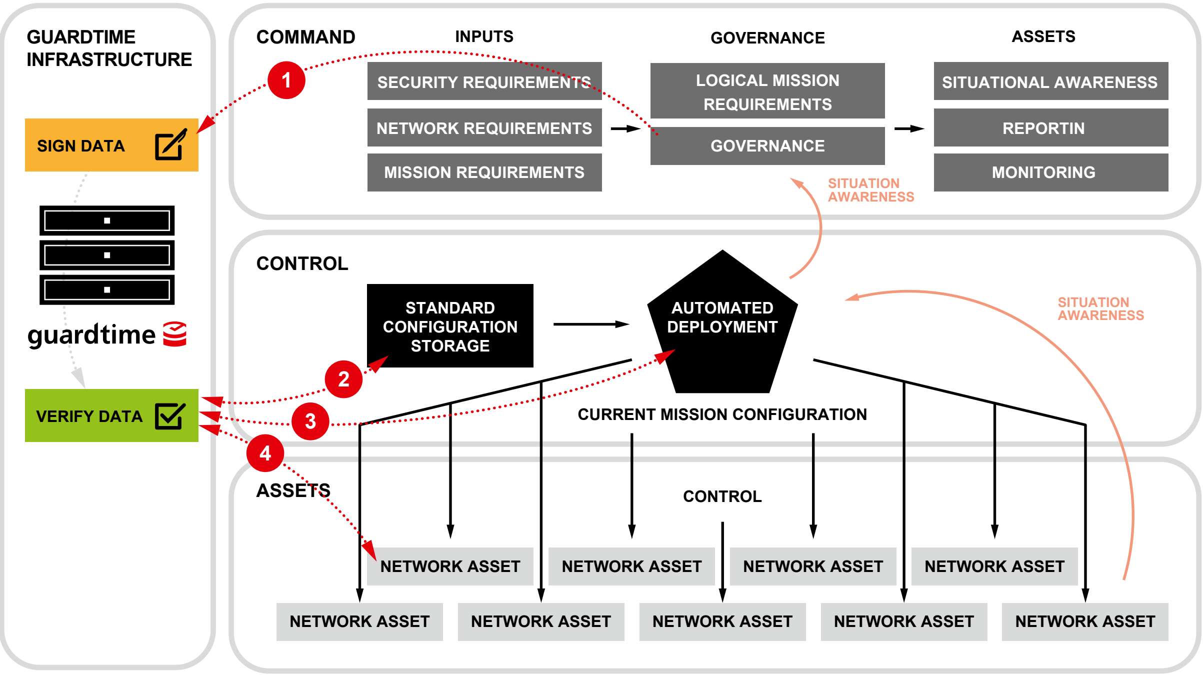


Figure 6 KSI instrumented SDN

3. Verify Deployment Inputs – Data flow 3 illustrates the near-real-time verification of the configuration stage to be deployed to network assets. For example, before the control application creates another node or network asset, the configuration of that asset will be pulled from the Configuration Storage Environment. The control application will then again verify the configuration pulled against the KSI infrastructure to assure the data about to be deployed is accurate and has not been altered.

4. Network Asset Continuous Monitoring – Data flow 4 highlights the continuous monitoring of the actual network nodes or assets. After the network asset is deployed, each asset can periodically or continuously verify its current configuration via the signature.

KSI instrumented SDN environment

Figure 7 below depicts a sample SDN configuration and the potential threats.

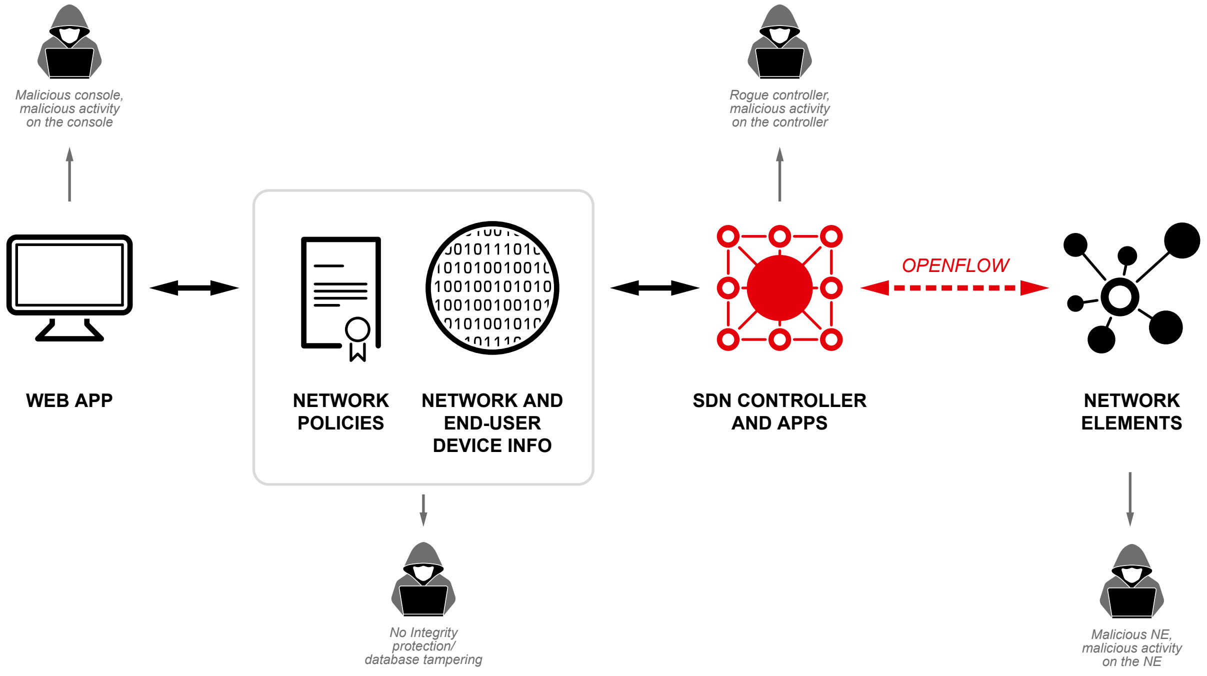

Malicious console, malicious activity on the console
Rogue controller, malicious activity on the controller
WEB APP
NETWORK POLICIES
NETWORK AND END-USER DEVICE INFO
SDN CONTROLLER AND APPS
OPENFLOW
NETWORK ELEMENTS
No Integrity protection/ database tampering
Malicious NE, malicious activity on the NE

Figure 7 *Traditional SDN – Sample configuration*

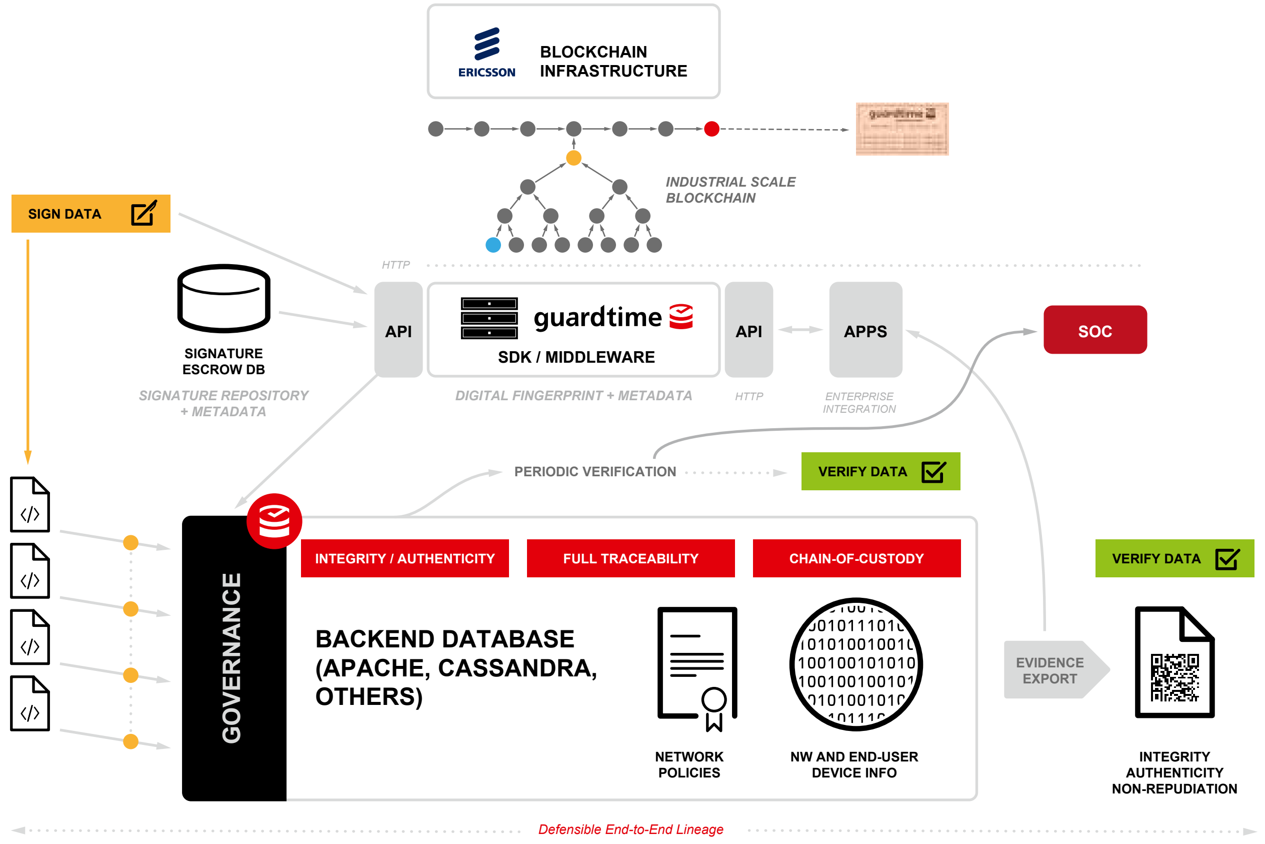
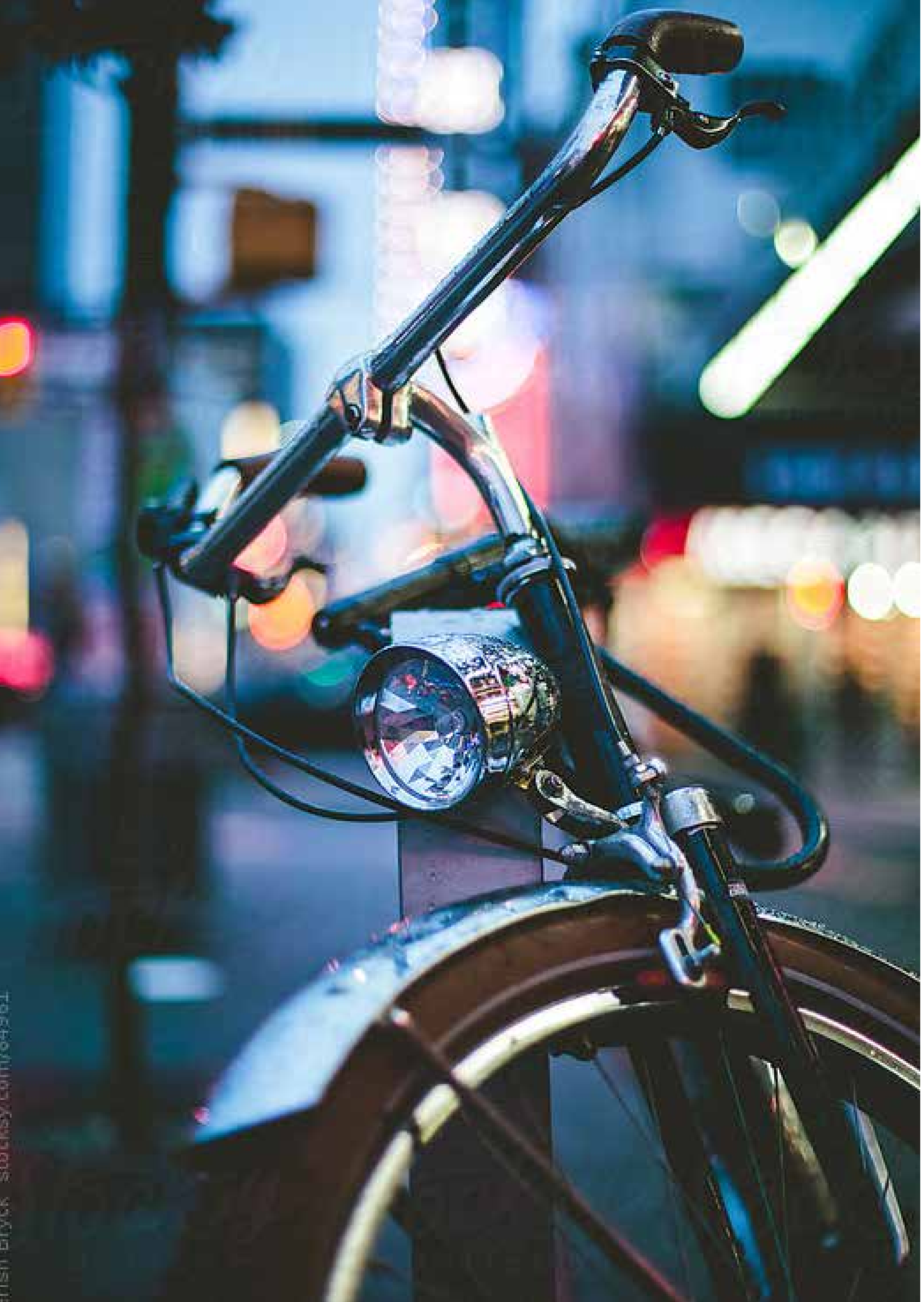

ERICSSON
BLOCKCHAIN INFRASTRUCTURE
INDUSTRIAL SCALE BLOCKCHAIN
SIGN DATA
HTTP
SIGNATURE ESCROW DB
SIGNATURE REPOSITORY + METADATA
API
guardtime
SDK / MIDDLEWARE
DIGITAL FINGERPRINT + METADATA
API
HTTP
APPS
ENTERPRISE INTEGRATION
SOC
PERIODIC VERIFICATION
VERIFY DATA
GOVERNANCE
INTEGRITY / AUTHENTICITY
FULL TRACEABILITY
CHAIN-OF-CUSTODY
BACKEND DATABASE (APACHE, CASSANDRA, OTHERS)
NETWORK POLICIES
NW AND END-USER DEVICE INFO
VERIFY DATA
EVIDENCE EXPORT
INTEGRITY AUTHENTICITY NON-REPUDIATION
Defensible End-to-End Lineage

Figure 8 *KSI Instrumented SDN – Sample configuration*

Currently, in the CIA triad, integrity has taken a back seat and the databases holding critical information for functioning of the SDN are not protected from data manipulation.

Figure 8 depicts an example of an SDN deployment with KSI instrumentation. Any data - network policies, end-user device info, topology, configuration files etc that is written into a database will be KSI signed via a call to KSI SDK. The KSI signature that is returned is stored in the local signature database along with any pertinent metadata. Data from the SDN database is periodically verified against the previously stored KSI signature using the KSIverify API call. Any change/tamper of the KSI-stamped data results in a KSI verification failure. Thus all SDN critical data stored in the database is protected against data manipulation.

SDN system logs shall be KSI signed to ensure they are not tampered with, thus providing auditors with 'clean' data. A potentially malicious insider in a KSI controlled environment will quickly realize that they cannot cover their tracks, and that their activities will be detected and responded to swiftly.



Conclusion

There is no silver bullet for the threats that mire an SDN environment, but most current controls are woefully inadequate when it comes to integrity. “Trusted” entities are frequently able to circumvent the access controls and other security mechanisms in place, and remove evidence of their activities.

No security solution is effective unless the system can guarantee, irrefutably, that the logs or applications have not been tampered with, or there is a way to verify beyond doubt that your security measures are working. Incorrect information can lead to unexpected system behavior.

The application of KSI will materially improve enterprise environments for controlling insider threat and by providing a real deterrent. Advanced dashboards can be built to extract KSI attributed information from the system and promote custom integration with legacy SIEMs.

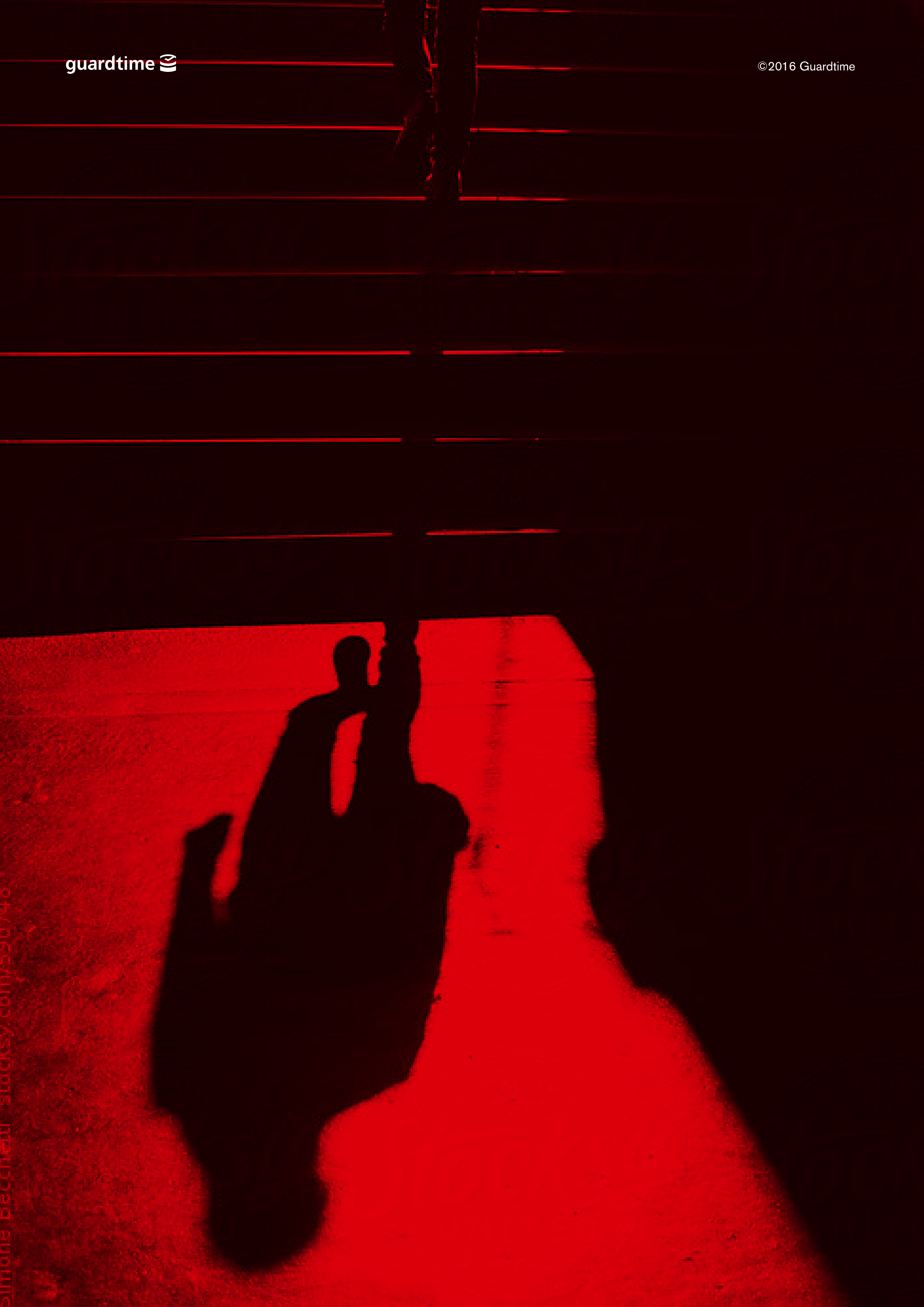
All critical components in an SDN network are essentially attributable, and the evidence of interactions between users and these assets immutable. With KSI, you can continue to trust your administrators and users, but more importantly you can now independently verify their actions.

Whilst an effective solution to the variety of threats faced by an SDN environment has so far proved elusive, KSI now offers a truly scalable solution based on mathematical certainty to offer 100% detection, accountability and auditability, and across highly complex systems.

Key differentiators provided by a KSI instrumented SDN environment are:

- Long-term integrity – KSI offers integrity protection on the contents ie on policies, configurations, topology that might be stored in any backend database including but not limited to Apache Cassandra. KSI provides an immutable chain of custody, with independent proof of time, integrity, and proof that events occurred in the correct order while ensuring no human interference.
- Inherent auditability and forensics - Logged data will help auditors uniquely identify the entities involved in a particular action and also the sequence of actions. KSI enables auditability and transparency of evidence that in turn offers provable compliance with regulatory and governance frameworks.
- Data lineage - All signature and verification operations in a KSI instrumented system can be tracked as changes are made to the SDN controllers/associated databases.
- Secure Provenance - KSI offers a means to cryptographically verify ownership of a file or digital asset in a way that it cannot be denied by the party modifying the object.
- Quantum Immunity - KSI is quantum immune i.e. keyless signatures are resistant to quantum computational attacks, unlike traditional public key cryptosystems like RSA - since they are purely based on cryptographic hash functions that are second pre-image resistant

guardtime



imone Becchetti stocksy.com/590746