# What's next: Software-defined infrastructure and cyber security

**Achieving SDI  implementation that mitigates cyber risk**

April 2019

kpmg.com

# About the authors

**Yen Hoe Lee**
Director, Cyber Security Services
KPMG LLP

Yen Hoe Lee has more than 15 years of cyber defense solution and security operations experience. He has a strong background in designing solutions to protect digital properties both on-premise and cloud based, and he has led operation teams in highly secured and regulated environments. Yen Hoe has guided leading entities in the financial services and healthcare industries, using his substantial experience leading architects and engineers on piloting and deploying security controls capabilities. He has spoken on his specialist knowledge for organizations and events including the Information Systems Audit & Control Association and the Enterprise Risk Management Conference.

**Anish Mitra**
Associate, Risk Consulting – IT Advisory
KPMG in India

Anish Mitra is an information security professional with experience in information security design, reviews, and implementation across multiple industries, including banking, telecommunications, pharmaceuticals and e-commerce. In particular, he is experienced in enterprise architecture and design, red teaming, vulnerability assessment, and threat management. Anish's recent engagements include a network security audit, a cyber security review, red teaming for multiple clients, and an ATM security audit.

Not all cyber threats are malicious, but rather the result of human error combined with vulnerable network security architecture.

— On August 2017, a misconfigured cloud-based file repository at a third-party vendor exposed the names, addresses, account details, and account personal identification numbers (PINs) of as many as 14 million customers of a major U.S. telecommunications company.[1]

— Hundreds of mistakenly unprotected Kubernetes administration consoles for managing containerized workloads and services were cryptojacked at a car manufacturer, and the hackers began running cryptomining scripts in the company's cloud environment.[2]

— An unsecured, open S3 server at an international package-forwarding service led to the exposure of 116,000 scanned documents, including passports, driver's licenses, security IDs, and more. The company had not configured their user permissions and access control privileges correctly.[3]

Exposures like this are increasingly common due to misconfigurations to cloud-based data stores and improper permissions. Given the frequency of such incidents, organizations are searching for solutions that can help them reduce their cyber-attack surface.

At the same time, the use of a software-defined infrastructure (SDI) is on the rise. When implemented and managed properly, cloud-based architectures can offer even greater security, in addition to the scalability and efficiency companies require for digital enablement. But implementation mistakes and poor management can leave organizations exposed.

> “In a dynamic and rapidly expanding ecosystem, organizations need to maintain safe and manageable cloud-based environments. Network security and technology leaders have the opportunity to make sure their SDI architecture enhances their cyber security, rather than risks it.
>
> **Tony Buffomante, Principal,**
> **Cyber Security Services – U.S. Leader**”

[1] Data Leaks, Cyber Risk, and CSTAR, UpGuard, 2017.

[2] Lessons from the Cryptojacking Attack at Tesla, RedLock, February 20, 2018.

[3] Leaked FedEx customer data was stored on Amazon S3 server with no password, TechRepublic, February 15, 2018.

## The advantages of software-defined infrastructure

### The growing need for SDI in the digital age

SDI-related solutions are not new, but previous iterations were limited in scope and flexibility. Citrix, for example, determined user access to particular applications based on their authorization and authentication, requiring manual reconfiguration every time users changed groups.

Today's SDI-related solutions are more dynamic and easily configurable, allowing organizations across all sectors to automate a number of processes in order to better meet the demands of digital transformation.

With SDI, users can efficiently connect to critical resources remotely, both within and outside the organization. SDI also allows hybrid organizations to manage access to both cloud and on-premise environments effectively. Organizations can then eliminate the use of multiple solutions such as virtual private networks (VPN), firewalls, and Citrix to connect to the network remotely.

Additionally, the isolation of critical enterprise applications—especially in the manufacturing sector—allows isolation of critical supervisory control and data acquisition (SCADA)/distributed control system (DCS) applications from the IT environment while still continuing to integrate with key enterprise applications.

> “SDI supports a growing trend of faster software service delivery. If implementation is done with thoughtful and proper planning, SDI could also provide stronger security controls.
>
> **Tony Buffomante, Principal, Cyber Security Services – U.S. Leader**”

**The four components of standard SDI networks**

**Controller**

Controls access to the SDI resources based on policies and identity. Needs integration to an identity management solution.

**Client**

A client which initiates the connection from the end device.

**Gateway**

Gateways broker access to protected resources. Traffic from the client is sent through an encrypted tunnel to each gateway, where it is decrypted and sent to the appropriate application.

**Resources**

Applications to which access is established.

Finally, the most critical factor of SDI specification is single-packet authorization (SPA). With this technique, clients generate a hash-based message authentication code (HMAC) to create a one-time password based on a shared secret (seed) and submit this to the SDI controller and gateway to "negotiate" the connection between the gateway and clients during the initial connection setup. Unauthorized packets without the SPA are dropped, thereby guaranteeing higher security of the negotiated connection.

With these benefits, it's no surprise that the software-defined infrastructure market, including consulting, integration, implementation and maintenance services, is expected to produce a 25 percent compounded annual growth rate between 2016 and 2022. While the increase is expected across all industries, the retail and banking, financial services, and insurance sectors are projected to contribute to the most growth to date.[4]

## SDI's positive impact on cyber security

With increasing complexity comes increased risk—risk that SDI has effectively countered.

The SDI model combining device authentication, identity-based access and dynamically provisioned connectivity, has been shown to be capable of stopping all forms of network attacks including distributed denial of service (DDoS), man-in-the-middle and server query (OWASP10), as well as advanced persistent threat (APT), according to the Cloud Security Alliance, a nonprofit organization promoting security leading practices in cloud computing. SDI helps manage risk by doing the following:

- Masks the IP addresses of the ultimate target and makes them nonroutable, hence protecting the infrastructure from traditional network attacks
- Allows organizations to have air gap between systems, while reducing costs for the implementation of multiple solutions such as network access control (NAC), firewalls, VPN, and demilitarized zone (DMZ)
- Eliminates the need for solutions such as virtual desktop infrastructure (VDI), a solution that can't meet the same scale, mobility, and access management challenges
- Reduces compliance and audit costs, particularly in public cloud infrastructures
- Eliminates the need for systems such as jump boxes, which do not allow separate policies for multiple users or access to multiple systems based on user roles, thereby opening up all other systems connected to the jump box to compromise.

The use cases below highlight the kinds of personas, access patterns, and scenarios that can be secured using SDI:

- Secure access by developers into infrastructure as a service (IaaS) environment
- Secure business user access to internal corporate application services
- Secure admin access to public-facing services
- Updates to user access when new server instances are created
- Hardware management plane access for service provider
- Controlled access across multiple enterprise accounts.

[4] Software Defined Infrastructure Market Analysis, Market Research Engine, January 2017.

**By its nature, SDI helps protect organizations against the following issues:**

### Data breaches

By adding a layer of preauthentication and preauthorization, SDI helps by reducing the attack surface of publicly exposed hosts. This ensures a "least-privileged access" model of security for servers and networks, thereby reducing many attack vectors that could lead to data breaches.

### Weak identity, credential, and access management

Because VPNs typically grant users broad access to an entire network, it is one of the most significant points of failure in the case of weak credential management. In contrast, SDI does not allow broad network access but rather limits access to only those hosts explicitly allowed. This limits the overall blast radius in case of credential theft and makes the security architecture much more resilient against weak identity, credential, and access management. SDI also can enforce strong authentication before users can access resources.

### Insecure interfaces and APIs

Protection against unauthorized users is a core SDI capability. SDI also can protect APIs if they're being invoked by processes running on user devices.

### System and application vulnerabilities

SDI significantly reduces the attack surface area, hiding system and application vulnerabilities from unauthorized users.

### Account hijacking

The session cookie-based account hijacking is mitigated by SDI. The application server simply rejects incoming requests from malicious end points if they are not preauthenticated and preauthorized and carry the appropriate SPA packets. Thus, even if the request carries a hijacked session cookie, it will not be allowed by the SDI gateway.

### Malicious insiders

SDI will limit the ability of insiders intent on causing damage. A properly configured SDI system has access policies that limit users to only those resources required to perform their specific business function and hides all other resources from them.

### Advanced persistent threats (APTs)

SDI can certainly reduce the likelihood and spread of an APT by reducing the attack surface, limiting the capability of an infected end point to find network targets, and more easily enforcing multifactor authentication throughout an organization.

### Denial-of-service attacks

The SPA scheme in the SDI architecture makes SDI controllers and gateways much more resilient toward thwarting a DoS attack. Processing an SPA takes significantly less resources than a typical handshake, making it possible for servers to process and drop unsolicited network packets at scale.

## Key challenges to widespread SDI adoption

While automation and the usage of SDI-based infrastructure leads to a reduction of overall costs from networking, data center, and operations perspectives, certain inherent challenges within SDI implementation provides challenges in widespread adoption of SDI:

- *Lack of expertise about SDI technology among industry peers.*
- *Risk of single point of failure of the SDI controller.* The controller in the network topology is responsible for managing the network traffic; therefore, the failure of the controller would lead to a collapse in the network.
- *Scalability of the overall network.* The SDI infrastructure is run primarily by a controller. In most scenarios, SDI implementation requires multiple dedicated controllers for multiple networks leading to scalability, cost, and operations overhead.
- *Lack of interoperability between SDI vendors.* While traditional networking equipment is standardized, SDI doesn't have a standard architecture, hardware, or protocols in place. Different vendors use different hardware and software, thereby making organizations wary of adopting one particular technology and ultimately serving as a major deterrent to SDI adoption altogether.
- *Need for evaluation.* The performance of SDI infrastructure needs review to ensure that flow rates are not constricted or limited to the bandwidth available to the controller.
- *SDI security is not foolproof.* While still being evaluated, SDI has a few weak points that need to be addressed, including the following:
  - A primary construct of SDIs is the containerization of data. Any vulnerabilities in implementation of the containers or at a kernel level could lead to the container becoming compromised, thereby compromising data.
  - SDI infrastructure also is still vulnerable to credential-based attacks, such as pass the hash or pass the key. And, SDI has a single point of compromise at the controller, which maintains the connections and access to various devices. Any compromise of the controller would lead to a compromise of the entire infrastructure.
  - Finally, the data is generally in an encrypted tunnel between the client and the gateway. But unencrypted communication between the gateway and the server could lead to a compromise of sensitive data and credentials, especially in sensitive environments such as banking and manufacturing.

### Take the following steps to evaluate your organization's readiness to move into SDI operation:

**Conduct an assessment to identify all possible cyber security "personas."**
A persona simply identifies types of users with certain roles and access patterns, such as roaming users, VIP users, and privileged users; their spread across the environment; and how they access the environment. Understanding these personas provides insight into access patterns and associated use cases. For example, personas can be used to understand how to best provision for business users or roaming users who need to access internal corporate application services.

**Conduct a cyber-maturity assessment to identify the cyber security posture of the organization.**
This assessment helps identify and understand the technology and processes supporting the personas who are accessing the environment. Additionally, it helps organizations understand the tools and technology spread for the five-step cyber security framework (identify, detect, protect, respond, and recover) that enables the personas and supports their access patterns.

**Conduct a risk assessment for "crown jewel" applications and how their access is managed.**
Organizations need to understand their crown jewel assets and prioritize protection for them from rogue and malicious elements. An assessment includes an estimate of the level of risk as well as the investment required to secure these assets.

**Evaluate how cloud instances are provisioned in the environment.**
Cloud instances are deployed dynamically and when the need arises, but provisioning of the access to these cloud instances, and developer access to the infrastructure, is often not regulated or over public channels. Additionally, the access to the hardware management plan needs to be monitored and regulated to ensure that access is not over public channels.

**Identify the administrators in the environment and the access they use.**
Evaluate administrator access to crown jewel applications. Administrators often access systems over public networks, and weak credentials and "access creep" can lead to insecure administrative access.

**Identify the remote access used in the environment and which applications are accessed.**
Remote access in the environment often requires access to be configured over multiple components, including VPN servers and application access, often leading to inaccurate access provisioning. As a result, controlling access lists and access to multiple applications becomes increasingly difficult.

## Summary

Network security and technology leaders are increasingly turning to software-defined infrastructure as part of their solution to limit access to critical network resources. However, organizations must still ensure that proper policies and procedures are in place to guard against risks ranging from data loss to the use of insecure cloud services. A proper assessment of the personas, provisioning and maturity of the existing cyber security framework will help limit risks while allowing companies to take full of advantage of SDI's strong cyber security attributes.

# How KPMG can help

We collaborate with companies across all industries to design and implement cyber security solutions aligned with business needs and strategy.

Our approach to enhancing cyber security for software-defined infrastructure is to help companies drive the value of their SDI framework by protecting their critical assets, enabling their business strategies, and providing resilience for sustainable growth. Working across all levels of the organization, from the board to the back office, we offer a spectrum of services including cyber security strategy and governance, transformation, cyber defense, and cyber response.

By instituting an effective cyber security function, companies can better manage their risks, take control of uncertainty, and increase agility. We look forward to helping you incorporate cyber security leading practices into your SDI projects and convert risk into opportunity.

# Contact us

**Tony Buffomante**
**Principal, Cyber Security Services – U.S. Leader**
**KPMG LLP**
**E:** abuffomante@kpmg.com

**Yen Hoe Lee**
**Director, Cyber Security Services**
**KPMG LLP**
**E:** yenhoelee@kpmg.com

**Anish Mitra**
**Associate, Risk Consulting – IT Advisory**
**KPMG India**
**E:** anishmitra@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

**kpmg.com/socialmedia**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.