Data Sheet

DTS SOLUTION
CYBER SECURITY REDEFINED

Blue Team
Cloud Security

At **DTS** we will help your organization make this informed decision and judgment through due care and diligence; working proactively with your cross-functional teams we will ensure that each key decision is technically assessed based on a business risk approach.

DTS Cloud Computing Security expertise can assist in the following areas;

- Cloud Service Model adoption – SaaS, PaaS and IaaS
- Cloud Computing Risk Management
- Compliance and Audit Control in Cloud Computing environments
- Information Lifecycle Management in the Cloud
- Data Portability and Interoperability between Cloud providers
- Virtualization and Multi-Tenancy environments
- Application and Hypervisor Security
- Encryption and Key Management
- Identity and Access Management
- Data Center operations and Disaster Recovery Planning

Virtualization Appliances for Multi-Tenant environments and offering Security as a Service on demand with rapid elasticity are some of **DTS** key specialized areas in the **Cloud Computing Security** domain.

Cloud computing is one of the next significant stage in the Internet's evolution, providing the means through which everything – from computing power to computing infrastructure, applications, business processes to personal collaboration – can be delivered to you as a service wherever and whenever you need.

The "cloud" in cloud computing can be defined as the set of hardware, networks, storage, services, and interfaces that combine to deliver aspects of computing as a service. Cloud service models are based on three categories; Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Services (SaaS).

Consumer Cloud Computing services has been well established eversince mainstream Internet. Well known examples are WebMail services and social networking platforms. However the adoption of Cloud Computing within the Enterprise sector has been slow. This slow uptake in Cloud services that promises so much has been primarily influenced by the numerous security risks, concerns and challenges posed within such an environment.

Governance, Risk and Compliance factors of Cloud Services need to be fully assessed by organizations to provide informed judgments. Data and Information lifecycle, source and origination, transfer, destination, validation and deletion all need to be understood. Transborder data flow of sensitive information resulting in litigation have to be approved by legal team. Periodic right for 3rd party audit clause, frequent reporting mechanisms of security violations and a clearly defined service level agreement. With Cloud providers utilizing shared pool of resources, virtualization and isolation capabilities need to be questioned along with identity access control and management frameworks. Encryption key lifecycle of virtualized environments, portability of information if your organization decides to move to another Cloud provider are just some critical factors to consider.

Cloud Security Framework

RISK MANAGEMENT
- Risk Ranking
- Service Modeling
- Data Security
- Data Portability
- Incident Response
- Service Level Agreement
- Docker Based Security
  - Kubernetes
- PaaS Security / IaaS Security

Virtualization Security

TECHNOLOGY
- Virtual Machine Security
- Hypervisor NG Firewall
- VDI Security
- Data Tokenization
- Security Automation
- CASB

Security as a Service

ON-DEMAND
- Security Service Chaining
- Web Application Security
- DDoS Mitigation in the Cloud
- Encryption
  - Data at Rest
  - Data in Motion

DTS SOLUTION
CYBER SECURITY REDEFINED

DUBAI: Office 4, Oasis Center, Sheikh Zayed Road, Dubai, United Arab Emirates
T: +971 4 338 3365 | **E:** info@dts-solution.com

800 HACKED

ABU DHABI: Office 253, Al Bateen C6 Tower - Bainunah, King Abdullah Bin Abdulaziz Al Saud Street | **T:** 971 2 2076777
LONDON: 160 Kemp House, City Road, London, EC1V 2NX, United Kingdom | **T:** +44 2081230 387 (DTS)
www.dts-solution.com