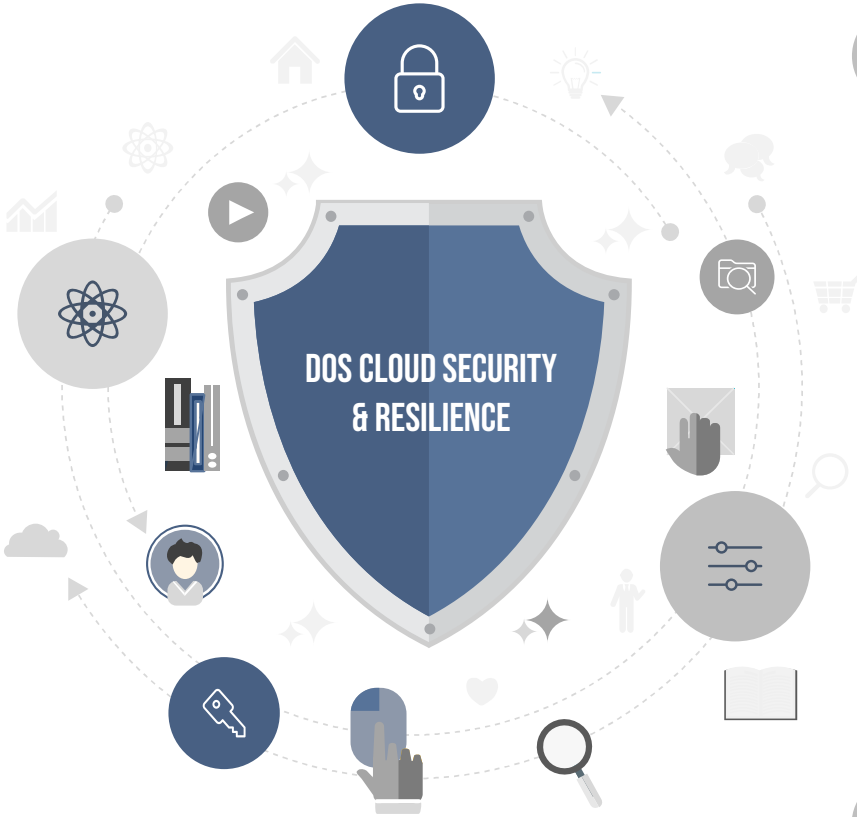
# SECURING THE CLOUD

## *Overview of Security Operations*

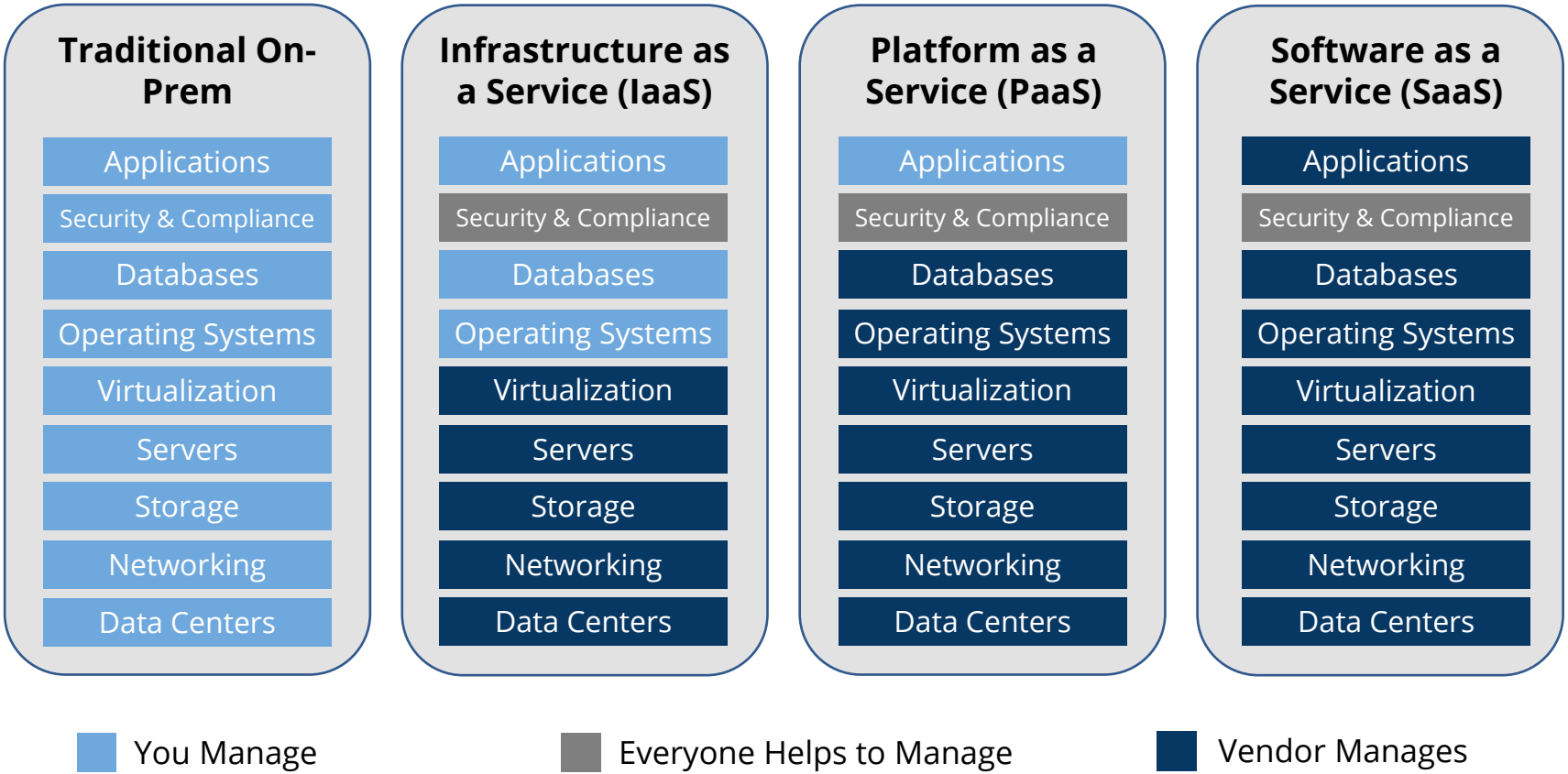
SEPTEMBER 2021

# CLOUD SECURITY CONSIDERATIONS




1. Security & Compliance
2. Zero-Trust Architecture
3. Cloud Security Posture Management
4. Data Sovereignty

# SECURITY AND COMPLIANCE



# IaaS Control Breakdown

- *Agency Authority To Operate (ATO) for FISMA Moderate Impact, SBU and PII*
- *Common controls for enterprise IaaS inherited by customer*
- *Significantly reduced security control responsibility via enterprise platform*

| **CUSTOMER WORKLOAD** CHARACTERISTICS | **PROFILE #1 FISMA Moderate** | **PROFILE #2 FISMA Low** |
|---|---|---|
| **Workload/System Categorization** | M, M, M | L, L, L |
| **Customer Requires Services Available in enterprise IaaS platform** | Yes | Yes |
| **Customer Processes PII (Requires Privacy Controls)** | Yes | No |

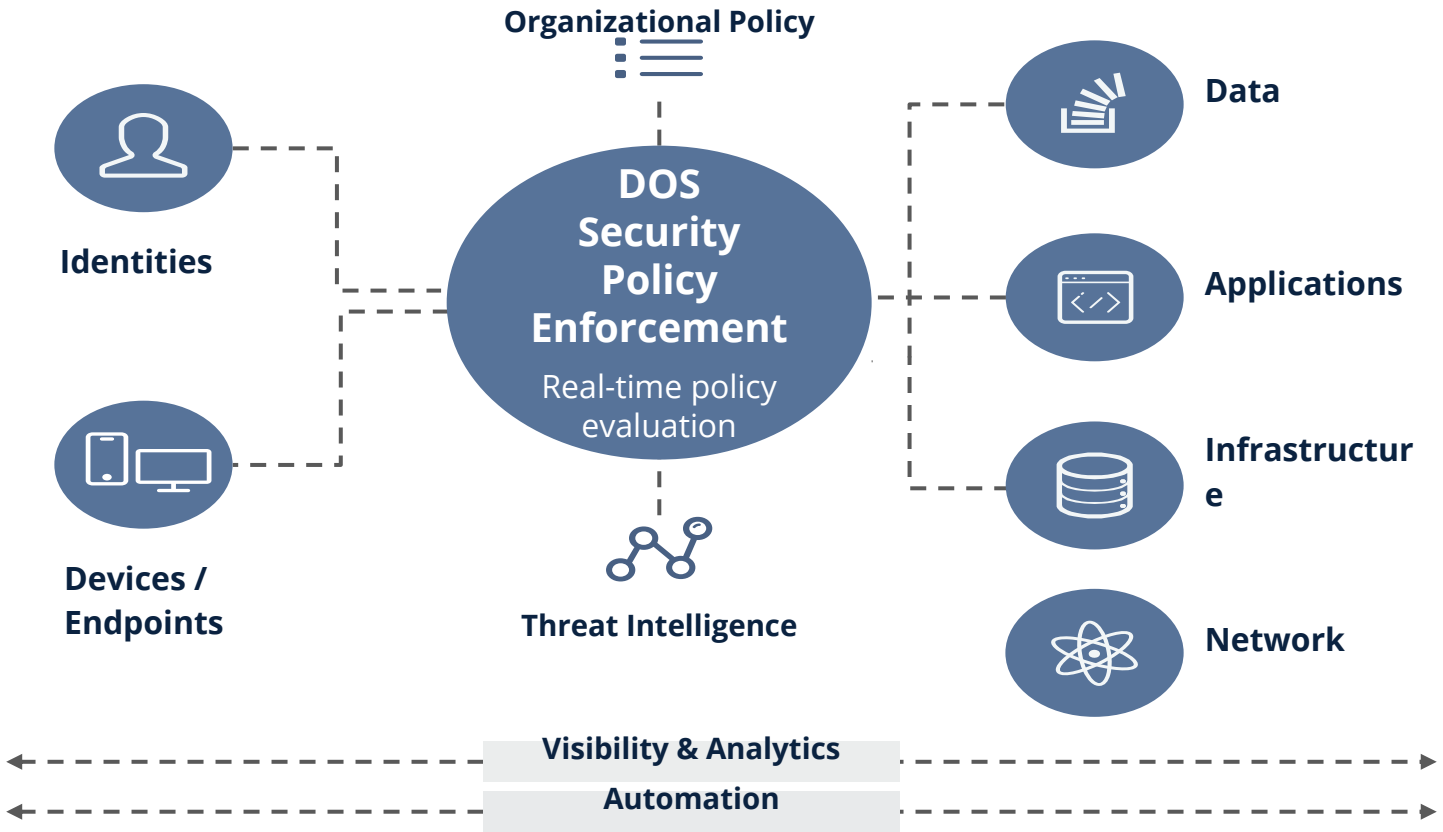
| **CUSTOMER SECURITY CONTROL** RESPONSIBILITIES | **PROFILE #1 FISMA Moderate** | **PROFILE #2 FISMA Low** |
|---|---|---|
| **Control Baseline** | 800-53 R4, FedRAMP Moderate + Privacy | 800-53 R4, FedRAMP LoW |
| **Total Control Baseline Count** | 378 | 164 |
| **Inherited Controls** *Provided by vendor, enterprise platforms* | 126 | 74 |
| **Remaining Controls** *Required of agency customer* | 252 | 90 |

# SaaS/aPaaS Control Breakdown

- *Agency Authority To Operate (ATO) for Moderate Impact, SBU & PII*
- *Common controls available on enterprise platforms for inheritance (Profile 3)*
- *Significantly reduced security control responsibility; potential elimination of separate ATO*

| | **PROFILE #1**<br>**End User** | **PROFILE #2**<br>**Standard Application** | **PROFILE #3**<br>**Complex Application** |
|---|---|---|---|
| | Standard end-user of platform all security control responsibilities are addressed in Rules of Behavior. | Customer app on platform with only minor security-related factors.<br>*e.g. Apps processing PII* | Customer app on platform with significant security-related factors.<br>*e.g. Apps tied to non-DOS systems* |
| **Deployment Model** | SaaS | SaaS/PaaS | PaaS |
| **Total Control Baseline** | 361 | 361 | 361 |
| **Inherited Controls**<br>*Enterprise platform and Vendor* | 361 | 303 | 303 |
| **Shared Controls**<br>*Enterprise platform, Vendor, Agency Customer* | 0 | 43 - 53 | 5 - 53 |
| **Remaining Controls**<br>*Required of Customer* | 0 | 5 - 15 | 5- 58 |
| **Security Responsibilities** | – Inherits all controls from platform<br>– No security responsibility beyond Rules of Behavior<br>– Falls under existing platform ATO<br>– No entry to compliance tool required | – Inherits majority of controls<br>– Modest security responsibilities<br>– Self-assessment of control responsibilities<br>– No entry to compliance tool required | – Inherits majority of controls<br>– Customer has additional security responsibility<br>– Requires A&A + ATO<br>– Enter into compliance tool |

# ZERO TRUST ARCHITECTURE



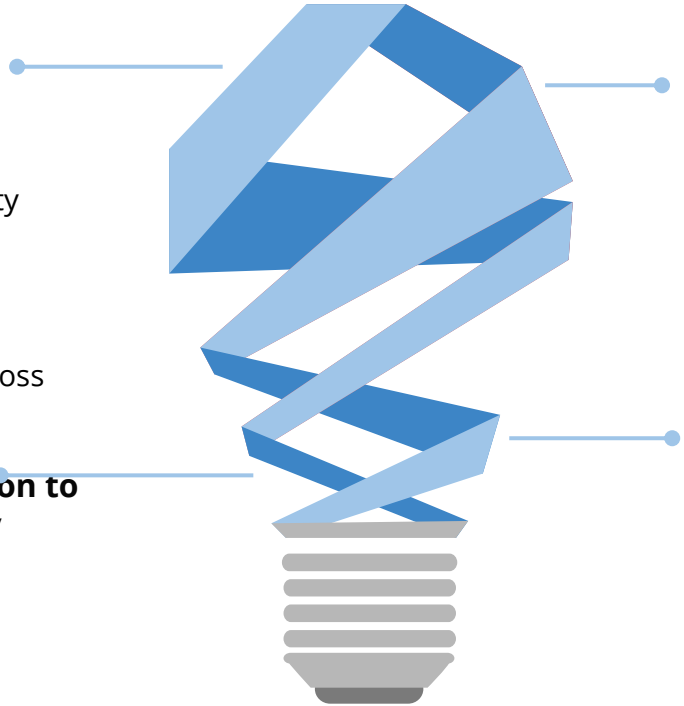
# Cloud Security Posture Management

**Identity is the new perimeter**

- Essential to have single enterprise cloud-based identity solution
- Leverage MFA, RBAC, multiple IDPs
- Normalize access controls across disparate platforms

**DevSecOps - drive automation to increase consistent security**

- Reduce risk of poor configurations and deliver at scale
- Automated code review and testing - reduce risk of bad code upfront



**CASB**

- Granular environmental controls based on business rules
- Account for platform differences - combine effort of CASB, Identity and native controls

**Monitoring**

- Integrate threat intelligence into tailored and actionable platform mitigations
- Access to monitoring data across multiple platforms

# DATA SOVEREIGNTY

## DEFINITION

Concept that digital data is subject to the laws of country where processed

## OVERSEAS CLOUD PROCESSING

Most nations leverage cloud, blurring boundaries and creating complex data sharing environments

## POLICY

Rely on existing diplomatic relations policy - must be regularly reviewed in light of disruptive innovations and policies

## COMPLIANCE

Must meet NIST standards regardless of data locations