Achieving FedRAMP Compliance on Azure

Trend Micro™ Deep Security™ makes it easier to meet many of the key security controls required for federal information systems moving to Azure

The Federal Risk and Authorization Management Program (FedRAMP) requires all federal organizations that use, or plan to transition to, a cloud environment to implement the FedRAMP program for cloud security controls based on NIST Special Publication 800-53, rev 4, which details all security controls required for federal information systems under the Federal Information Security Management Act (FISMA).

Azure already supports a large number of these controls—those dealing with physical access to data storage facilities, network security, and the security of servers. Under the shared responsibility security model, departments and agencies are required to implement measures to satisfy the remaining controls relevant to data and application security.

Trend Micro Deep Security—a leading solution for securing physical, virtual, and hybrid data centers—includes host-based capabilities that support compliance with many of these controls. Some of these core capabilities include:

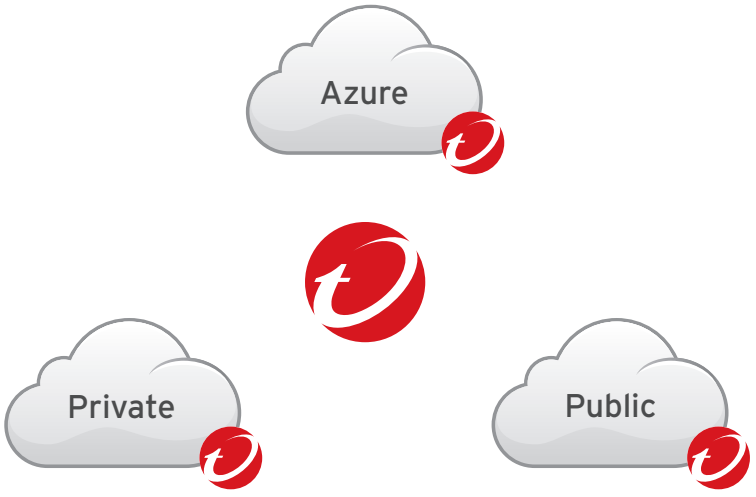
- **Real-time vulnerability scanning and protection**
- **Intrusion prevention and malware protection**
- **Continuous monitoring, logging, and reporting**
- **Automated firewall and access-control rules**
- **Advanced malware and incident handling**
- **Centralized management with multi-tenant support**

Microsoft Azure

FedRAMP
Federal Risk Authorization Management Program

Common Criteria

Trend Micro™ Deep Security™ 9.5 SP1 has achieved Common Criteria EAL 2 certification



✓ ***Choice***
✓ ***Flexibility***
✓ ***Certification***
✓ ***Security***
✓ ***Savings***

The following is a brief summary of the ways in which Deep Security supports the key categories of security controls required by FedRAMP:

Control Category	Supported Controls
Access Control Deep Security allows administrators to define fine-grained firewall rules/filters on specific servers to create separate processing domains/zones.	AC-6 Least Privilege
Audit and Accountability Deep Security logs all security-related events and shares logs seamlessly with syslog and/or SIEM products. Centrally managed reporting and auditing capabilities help administrators identify critical events. Packet-level data can be analyzed for further audit data.	AU-2 Auditable Events AU-3 Content of Audit Records AU-6 Audit Review, Analysis and Reporting
Security Assessment and Authorization Deep Security allows administrators to automate the scanning of systems and patch levels against the latest Critical Vulnerability and Exposure database, and to automatically apply predefined rules or filters to prevent exploitation. Findings and activities are logged for audit and continuous monitoring.	CA-2 Security Assessments CA-7 Continuous Monitoring
Configuration Management Deep Security automatically scans critical files, folders, and registries for changes against baseline configurations, and can automatically assign minimum recommended security configurations tailored for specific hosts.	CM-2 Baseline Configuration CM-6 Configuration Settings
Contingency Planning Deep Security links policies, rules, and filters to specific virtual machines, and maintains them when the virtual machine is moved to a different site or host. In addition, it automatically assigns recommended security configurations to new virtual machines as they are created.	CP-2 Contingency Plan
Incident Response Deep Security automatically alerts in response to security incidents. It continuously monitors systems for unpatched vulnerabilities, and shields these vulnerabilities until a patch can be installed. Infected virtual machines can be tagged and quarantined automatically.	IR-4 Incident Handling IR-5 Monitoring IR-6 Reporting
Risk Assessment Deep Security scans for vulnerabilities and patch levels, to ensure that all unpatched vulnerabilities are identified, reported, and shielded automatically, using the latest policies. It detects suspicious activities including reconnaissance activity by intruders, and correlates all suspicious activities against global threat data to identify and alert administrators to potentially malicious trends.	RA-5 Vulnerability Scanning
System and Communications Protection Deep Security's stateful firewall uses whitelisting to deny all traffic not specifically allowed. Rules can be specified for each host and virtual machine. Application control rules are applied to all outbound traffic, providing the ability to detect unusual or unexpected protocols and port usage.	SC-7 Boundary Protection SC-32 Information System Partitioning SC-36 Distributed Processing and Storage
System and Information Integrity In addition to identifying, reporting, and shielding vulnerabilities, Deep Security detects viruses and other malware, and may be configured to automatically clean, quarantine, or delete infected files. Intrusion detection and prevention capabilities guard against known and zero-day exploits, SQL injection attacks, and other web application attacks.	SI-2 Flaw Remediation SI-3 Malicious Code Protection SI-4 Information System Monitoring SI-5 Security Alerts, Advisories and Directives SI-7 Software, Firmware and Information Integrity

To learn more about how Trend Micro Deep Security can help you to create Azure-hosted offerings that comply with federal procurement regulations, please email USFed@trendmicro.com or go to azure.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud