Juniper Software Security Features

Juniper uses a **Microsoft Azure** platform, a set of cloud services that allow us to offer a secure, expandable network. Security is integrated into every aspect of Azure, protecting applications and data and supporting compliance efforts. These are the key security features offered by Juniper.

Access Control

- Access Control Policy
- Role-based access control where applicable
- Principle of least privilege
- Remote Access policy
- Network Access Controls
- Automated account locking and intrusion detection
- Physical Access Controls

Third Party Assurance

- Third Party Service Provider Management policy
- Vendor Security Risk Assessments completed for new vendors that handle sensitive information
- NDA, MSA, standard for new vendors that handle sensitive information

> *Source*: Microsoft Azure. Learn more about Azure security features at http://bit.ly/2Wyu5rB

Password Management

- Strong password enforcement
- Password history and age restrictions
- Increased protections for privileged accounts
- Password Management policy

Audit Logging and Monitoring

- Segregation of duties
- Administrator activity logs
- Automated security log alerting
- Access monitoring
- Network monitoring
- Email monitoring
- File integrity monitoring
- Error logging

Business Continuity and Disaster Recovery

- Continuity of Operations plan
- Documentation of critical business technologies and solutions
- Back-up and Recovery capability
- Annual plan review
- Periodic testing of disaster recovery solutions

1-855-215-2174 | trellisconnects.org

TRELLIS™