1. **API-first Approach**
   - Everything is driven through APIs. Whether it’s using NSX UI or using automation tools, APIs and SDKs provide the interface into all product functions and control.

2. **Network Infrastructure as Code**
   - Create complex network topologies and address complex security requirements programmatically.
   - Message the source scripts in any version control system and revisions can be made easier.
   - Integrate the entire process with CI/CD pipeline, enabling network and security infrastructure to be managed as code.

3. **Many Automation Tools in the Chest**
   - Supports various tools such as software-defined automation, PowerShell, and third-party tools such as Terracode and Ansible. It puts flexibility into the hands of the network engineer.

4. **Hierarchical APIs = API Simplicity**
   - Designed to simplify with hierarchical structure allowing for create/edit/delete objects with a single API call.

5. **OpenAPI standards-based API**
   - Standards and standard schema development and export to various programming language SDKs enable organizations to develop third-party software.

6. **Active Community (Samples on GitHub)**
   - Sample code and fully automated end-to-end use-cases are available in GitHub for easy consumption: https://github.com/vmware-samples/nsx-t

7. **Wide Variety of Users**
   - VMware tools such as vRealize Automation, PowerCLI, and third-party tools such as Terraform and Ansible provide flexibility to the network engineer.

8. **Remote Access with NSX**
   - Supports VMware tools such as vRealize Automation, PowerCLI, and third-party tools such as Terraform and Ansible. Puts flexibility into the hands of the network engineer.

9. **Operational Efficiency**
   - Reduce human errors and ensure consistency which translates to lower risk of inefficiencies, equipment failure, data breaches and regulatory compliance violations.

10. **Risk Mitigation**
    - Reduce human errors and ensure consistency which translates to lower risk of inefficiencies, equipment failure, data breaches and regulatory compliance violations.