# Critical Components for AI Security in Your Organization

netskope

As organizations seek to adopt AI at speed and drive their innovation forward, it's important for security teams to keep up regular inspection and maintenance so that AI systems run safely. Here's a checklist of the critical components you should consider.

### Engine—core infrastructure

Secure data pipelines through Netskope One Zero Trust Engine. Put critical diagnostics—such as model monitoring—in place. Configure access controls.

### Brakes—risk controls

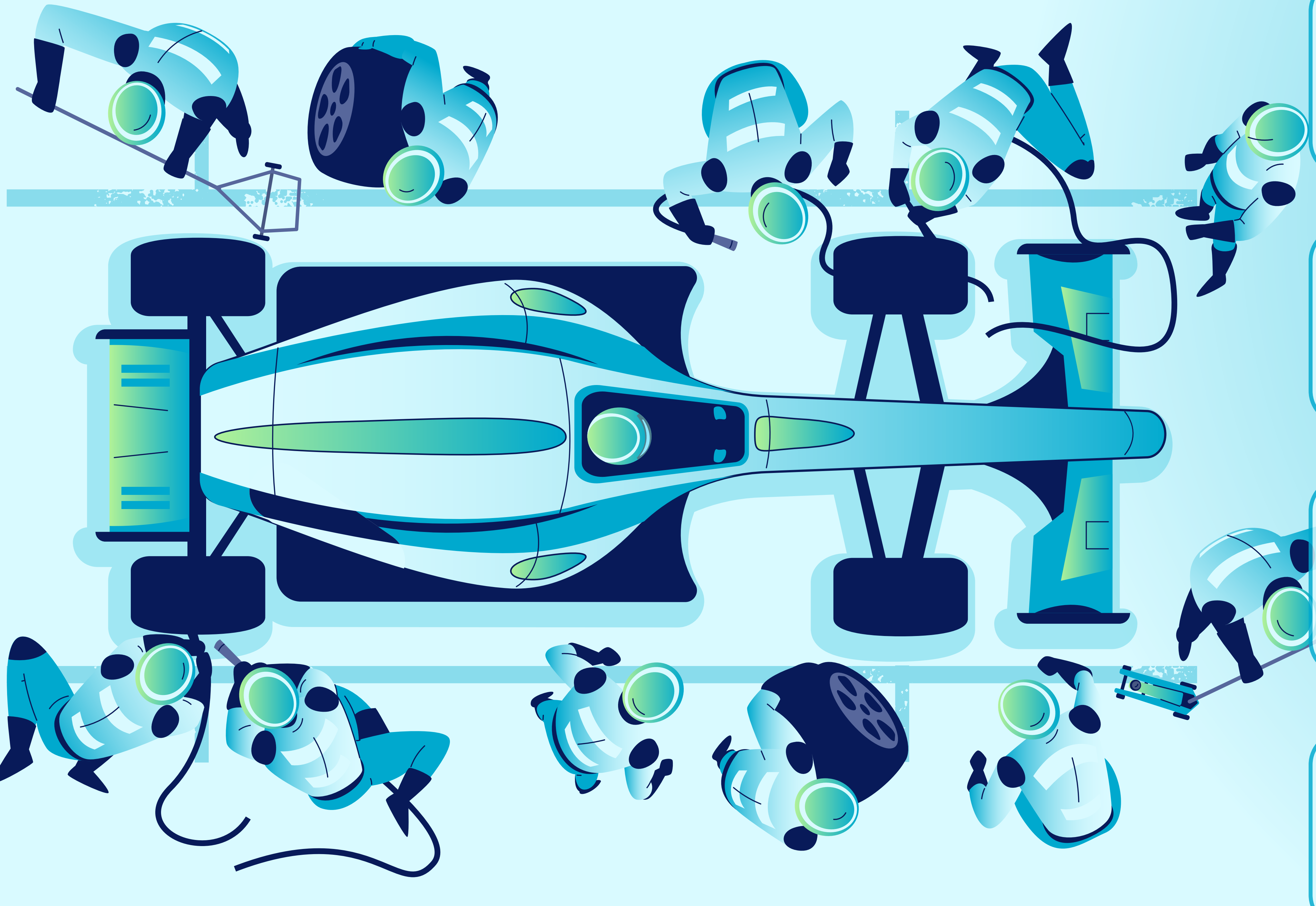
Install data loss prevention barriers and mitigate against prompt injection. Implement output validation checks and deploy data masking tools.

### Dashboard—real-time analytics

Deploy Netskope One Advanced Analytics to provide real-time threat detection. Regularly refine anomaly detection. Utilize ongoing compliance monitoring.

### Wheels—model deployment

Track model versioning and actively monitor performance. Secure the production environment and test capabilities.



### Fuel—data quality

Verify the data sources fueling your AI systems. Run data clean-up processes and active contamination detection. Regularly assess data quality.

### Driver—human oversight

Establish a clear chain of command, with decision authority mapped and security team roles defined. Ensure that override controls are in place.

### Rules of the road—governance

Establish AI usage policies across the organization. Map regulatory compliance and configure audit trails.

### Pit crew—your team

Provide real-time coaching on data loss risks to help users stay on track. Set up an active training program to keep skills updated.

netskope

Learn more about how Netskope One secures the use of AI to enable innovation while maintaining robust data protection.

Read full eBook