

Managed Security Patching for secure, high-performance trading infrastructure



Keeping operating systems up to date is critical for maintaining security, stability and compliance. But in trading environments, applying patches isn't always straightforward. Updates must be carefully managed to avoid disruption to latency-sensitive applications and critical market connectivity.

Beeks provides managed OS patching services designed specifically for financial markets infrastructure. We apply security and stability updates across your environments in a controlled, scheduled and fully monitored way, helping you stay protected without impacting trading performance.

Key features

Automated OS patch management

- Regular application of security and stability updates across supported operating systems.

Controlled deployment processes

- Patching aligned to defined maintenance windows to minimise operational impact.

Latency-aware execution

- Designed to protect performance of trading systems, market data and connectivity services.

Pre-deployment validation

- Testing and staged rollout to ensure updates are applied safely and predictably.

Centralised monitoring and reporting

- Full visibility of patch status across infrastructure environments.

Security vulnerability mitigation

- Timely application of patches to reduce exposure to known threats.

Standardised patching framework

- Consistent processes applied across all environments to support operational stability.

Multi-environment coverage

- Delivered across private cloud, colocation and dedicated infrastructure.

Fully managed service

- Removes the need for internal teams to manage patching cycles and coordination.

Benefits

Lower operational overhead

- Removes the need for internal teams to manage patch cycles, testing and deployment.

Improved security posture

- Reduces exposure to known vulnerabilities through timely and consistent patching.

No impact on trading performance

- Updates are applied within controlled maintenance windows, protecting latency-sensitive environments.

Reduced operational risk

- Structured processes minimise the risk of failed updates or unplanned disruption.

Consistent and repeatable processes

- Standardised approach ensures patching is applied reliably across all environments.

Enhanced compliance readiness

- Supports alignment with regulatory and security standards including DORA, ISO 27001 and SOC 2.

Full visibility and control

- Centralised monitoring and reporting provide clear insight into patch status and activity.

Greater infrastructure stability

- Regular updates improve system reliability and reduce the likelihood of incidents.

Confidence in operational continuity

- Ensures systems remain secure and up to date without compromising availability.



Managed as part of your infrastructure

OS patching is delivered as part of Beeks' managed infrastructure services, supporting environments across private cloud, colocation and dedicated infrastructure.

Our platform ensures updates are applied efficiently while maintaining the performance and reliability required for financial markets operations.



Client use case

A global bank operating out of various sites would typically employ 20 – 50 infrastructure engineers, spending around 750 hours per month on security patching.

By using **Beeks Managed Security Patching**, the bank removes this operational burden and reallocates skilled resources to other strategic priorities such as platform performance, resilience and trading support, while maintaining a secure and compliant infrastructure.

Contact us

sales@beekgroup.com
Beeksgroup.com/security