

Feature	Standard Edition	Enterprise Edition
Functionality and Security		
AES 256 encryption	✓	✓
Endpoint floating license support	✓	✓
Protection against modification or termination of a Client	✓	✓
Password hiding during monitoring	✓	✓
Audit trail for system users	✓	✓
VDI golden images	✓	✓
Non-persistent VDI monitoring	✓	✓
SIEM Integration	—	✓
Offline Client detection ("Lost" Clients)	✓	✓
Deployment & Maintenance		
On-premises deployment	✓	✓
Remote installation/uninstallation/update of Clients	✓	✓
Update of endpoint Clients from the Server	✓	✓
MS SQL and PostgreSQL database support	✓	✓
Database cleanup	✓	✓
High availability and disaster recovery	—	✓
Multi-tenant mode	—	✓
System health monitoring	✓	✓
Database archiving	—	✓
Basic Functionality		
Integration with Active Directory	✓	✓
Access to the Management Tool via Smart Cards	✓	✓
Offline mode support for Clients	✓	✓
Product customization	✓	✓
Register logs to the Windows Event Log	—	✓

Activity Monitoring		
Session recording in video format	✓	✓
Live session view	✓	✓
Multi-monitor recording	✓	✓
Web pages and applications	✓	✓
Clipboard (copy and paste)	✓	✓
Keystroke logging	✓	✓
Keyword-triggered monitoring	✓	✓
USB storage monitoring	✓	✓
Linux console commands and parameters	✓	✓
Audio recording	—	✓
File monitoring	—	✓
Monitoring only during specified time intervals (working hours)	—	✓
SWIFT username monitoring	—	✓
Filtering during Monitoring		
Application filtering	✓	✓
User filtering	✓	✓
IP address filtering	—	✓
Incident Response Functionality		
Proactive real-time alerts and notifications	✓	✓
Out-of-the-box alert templates	✓	✓
Blocking restricted USB devices	✓	✓
User blocking	✓	✓
Behavior analytics and anomaly detection	—	✓

Password Management		
Password management to access Windows servers	—	✓
Secrets management to access Linux/Unix servers (passwords and SSH keys)	—	✓
Password management to access MS SQL	—	✓
Password management to access web applications	—	✓
RDP/PuTTY support	—	✓
Role-based access control	—	✓
Remote Password Rotation (Active Directory and Windows Accounts)	—	✓
Access Management		
Secondary authentication to identify users of shared accounts with built-in accounts	✓	✓
Multi-factor authentication	✓	✓
Time-based user access restrictions	—	✓
Approval Workflow		
Request access	✓	✓
Require comment	✓	✓
Request access to USB mass storage or mobile device	—	✓
One-time passwords (OTP)	—	✓
Ticketing system integration	—	✓
Enhanced Auditing and Reporting		
Multi-parameter search in monitoring results	✓	✓
Search by metadata	✓	✓
Search inside Linux session output	✓	✓
Responsive and actionable dashboards	✓	✓
Scheduled and ad-hoc reports	✓	✓
Export session	✓	✓