**Employee Security Concerns**

The following table lists the security concerns for various types of employees:

| **Employee Type** | **Job Role** | **Type of Work** | **Type of Host** | **Connection** | **Security Strategy** |
| --- | --- | --- | --- | --- | --- |
| On-site user | On-site staff; for example, accounting, marketing, finance, and human resources | Work hours are from 9am to 5pm. Employees are full-time and work primarily in an office. | A desktop or a stationary laptop. | The user is physically connection to a corporate office. | * Antivirus scanner * Firewall * Screen lockout * Physical lock |
| Field user | Staff that does fieldwork, supporting multiple locations; for example, auditors, investigators, and technical support | Employees travel between locations, performing audits, assessments, and installations, maintenance, and troubleshooting | A laptop, tablet, and a smart phone | The user is physically or wirelessly connected to remote offices. | * Multifactor authentication with a strong logon password and biometric logon * Antimalware software * A host firewall * Application and OS patches or updates * A password-protected screen saver with auto timeout * Location-aware antitheft software * Hard disk data encryption |
| Teleworker | Remote support staff, customer service staff, and inside sales staff | Employees work from a home office | A desktop or a laptop and an IP telephone | The user is connected from home to the office via a virtual private network (VPN). | * Multifactor authentication with a strong logon password and biometric logon * Antimalware software * A host firewall * Application and OS patches or updates * Hard disk data encryption * A VPN connection |
| Road warrior | Executives, outside sales, and consultants | Most work is done off-site by employees while traveling and at a customer location | A laptop and a smart phone | The user is remotely connected to a network via a VPN. | * Multifactor authentication with a strong logon password and biometric logon * Antimalware software * A host firewall * Application and OS patches or updates * A password-protected screen saver with auto timeout * Location-aware antitheft software * Hard disk data encryption * A VPN connection |
| Roaming user | Information technology (IT) staff, facilities staff, and security staff | Work is done primarily at one location, but not often from the same desk. | A laptop or a smart phone. | The user is physically or wirelessly connected to a corporate office. | * A laptop connected to a network and protected by the network firewall and perimeter defenses * A strong logon password * Antimalware software * A host firewall * Application and OS patches or updates * A password-protected screen saver with auto timeout |