cloudfactory SHIELD SECURITY

CloudFactory takes data security very seriously and has made protecting client data a top priority. Our Shield security options offer a layered approach to prevent unauthorized access and ensure compliance with regulatory, best practice, and customer requirements.

Shield Essentials, included in every client engagement, establishes baseline security controls and features that protect our clients' data, regardless of where our teams complete the work. For clients with heightened requirements, our Shield Network and Endpoint upgrades enforce additional layers of workforce, IT, and network security.

SHIELD SECURITY COMPARISON

ESSENTIALS | NETWORK | ENDPOINT

PEOPLE: WORKFORCE SECURITY

Client data will only be accessed by CloudFactory's employees, contractors, subcontractors, agents, or affiliates who adhere to our comprehensive security standards.

	ESSENTIALS	NETWORK	ENDPOINT
Full background screening, training and other evaluative measures conducted by CloudFactory, including a personal interview and resume validation	✓	✓	✓
Signed NDAs and remote work policy extending to all Client work	✓	✓	✓
Activity monitoring via desktop and webcam captures at random intervals to support security and performance monitoring	✓	✓	✓
Team activity digitally monitored during all shifts by staff trained on data security guidelines	✓	✓	✓
Industry-specific compliance training and adherence (e.g., HIPAA)			✓

SHIELD SECURITY COMPARISON

ESSENTIALS | NETWORK | ENDPOINT

TECHNOLOGY: IT AND NETWORK SECURITY

Client data will only be accessed through secured networks and devices adhering to our enterprise and data compliance standards.

	ESSENTIALS	NETWORK	ENDPOINT
Antivirus installed on all workstations	✓	✓	✓
Automatic Operating System Patching		✓	✓
Multi-factor Authentication (MFA) enforced on all user accounts		✓	✓
Access restricted by a secured virtual private network (VPN)		✓	✓
Ingress/egress firewall filtering and IDS/IPS with deep packet inspection, advanced behavioral analysis, and traffic anomaly detection to determine zero day attacks		✓	✓
Limited access into client systems via IP Whitelisting, backed by segregated network access		✓	✓
All work is performed on CloudFactory provided workstations that:			
Are centrally managed to run antivirus software and actively scan for known and zero day threats			✓
Are equipped with Vulnerability Management			✓
Use customized Host Level Firewall Policies			✓
Are equipped with full AES256 Host Level disk encryption using Bitlocker and managed through Endpoint protection			✓
Use Application Control to prevent launch and execution of certain applications			✓
Use Device Based Authentication that restricts remote access based on specific certificates			✓
Are equipped with hardware and software that completely restrict the physical and non-physical removal of data			✓

We're here to help. Contact us today.

contact@cloudfactory.com
UK • USA • Nepal • Kenya

cloudfactory