Brick Technology Group, LLC

Service Catalog – Ver. 2025-05-01

Brick Technology Group, LLC (BTG) offers three (3) tiers of Subscription: Essential, Secure & Complete. Each tier includes features defined below based on Client's selected subscription as indicated on the SOW. Reference the SOW to ensure that you have purchased the correct service tier that includes the features required for your company's needs.

Managed Services: During our normal business hours, BTG will attempt to resolve day-to-day IT support incidents via remote support tools for existing systems and software that we manage. This includes troubleshooting hardware, software, printing, network and other IT-related issues relevant to Client's corporate systems. BTG will attempt to resolve such technical problems in a professional, reasonable, and timely manner, taking into consideration the circumstances and nature of the technical problems. Managed Services does not assure that every request for technical support will be resolved to Client's satisfaction. BTG has limited proprietary information from vendors, manufacturers, and developers, and may not have the ability to obtain the proprietary information necessary to resolve Client's technical problem. Technical problems that arise may be a result of software or hardware errors or problems that may not be correctable or may be too difficult to resolve remotely, at which point BTG, at its own discretion, will determine if on-site support services are required. Business line application support is provided on a best effort basis and only if Client has a current manufacturer support contract and/or agreement allowing BTG to initiate a manufacturer service request for support on behalf of Client. Remediation does not include changes to the status quo such as the installation, implementation, instantiation or integration of devices or software to the environment. Changes to the status quo will be considered Out of Scope. Included with Managed Services:

- **Remote Monitoring & Management:** BTG will deploy software to oversee the Client's devices. Provide an inventory of devices and track various metrics like system performance to ensure smooth operations. This allows for BTG to identify potential issues and proactively work to correct them.

- **Patch Management:** BTG will monitor/deploy the patching of approved Operating Systems, firmware, and some third-party applications. Users will be prompted to reboot their computer systems as needed to apply patches.
  - *1. Windows Systems*: Windows systems are patched by default in a hybrid auto-approve and manual approval model. Based upon the categories and descriptions set by Microsoft in KB824684 (https://support.microsoft.com/en-us/kb/824684), manual exceptions can be made to the approval model based upon customer request and BTG Approval. All patches that fall into the manual approval category will be approved on a case-by-case basis by BTG. BTG will approve manual patches based on whether there are any security implications, and once the patch has been tested.
    - Important Patches:
      - Critical Updates: Automatic Approval
      - Regular Updates: Automatic Approval
      - Update Rollups: Automatic Approval
      - Service Packs: Automatic Approval
      - Feature Packs: Automatic Approval
      - Definition Packs: Automatic Approval
      - Drivers: Automatic Approval
      - Feature Updates: Automatic Approval
    - Optional Patches
      - Critical Updates: Manual Approval
      - Regular Updates: Manual Approval
      - Drivers: Manual Approval
  - *2. Mac Systems*: Check daily for all critical Apple OS Updates.
  - *3. Linux Systems:* Run all security updates available to the Operating System every week.
- **Remote Access:** BTG will deploy Remote Access software that will be used by the BTG for unattended access to machines. Client may request access to Remote Access software for devices within their company.
- **Vendor Management**: BTG shall interface with Client's contracted third-party technology vendors to the best of our ability and only if Client has a current vendor support contract and/or agreement allowing BTG to initiate a service request for support on behalf of Client. In some situations, vendors may be unsuccessful in their efforts to solve problems. BTG cannot be held responsible for the performance of third-party vendors. Additionally, vendors may require (or common sense may dictate) that Client's staff interact with vendors for specific issues that require demonstrations of specific failures or day-to-day use issues that BTG will be unable to perform and/or replicate.
- **User Account Management:** This includes creating and managing user accounts, assigning licenses, managing user access and permissions, and handling user onboarding and offboarding processes. BTG will provision new user accounts and assist new users with their initial logon to the system. This will include ensuring printers are mapped, Office 365 applications are mapped and configured, enrollment in MFA, etc. This does not displace the need for proper computer hardware and operating system configuration and assumes a computer that is already fully configured is ready for use.

- **Privileged Access Management:** BTG will deploy software to audit and track access to administrative accounts used by BTG.
- **User Verification:** BTG will deploy software and/or apply best efforts to confirm user identity prior to work being performed.
- **Unifi Network Hosting:** BTG will provide and manage a cloud site for any Ubiquiti Unifi Devices.
- **Antivirus:** BTG will provide, deploy and configure endpoint antivirus software product to Windows computer(s) that we manage. At our discretion, we may leverage multiple such products to meet our internal objectives. Deviation from BTG standard configurations and/or Client requested customizations may result in additional fees or out of scope charges. BTG may provide Web filtering at either the local device and/or in conjunction with DNS filtering at the firewall level.
- **Zero Trust Cyber & Auto Elevation - Workstation/Server:** BTG will provide and maintain software that creates a Zero Trust application environment on Client's machines. Client may request changes to the environment and BTG will approve on a case by case basis. This may include the ability to automatically elevate processes to the administrator level.
- **Zero Trust Cyber - Network:** BTG will provide and maintain software that creates a Zero Trust Network environment. All network requests will be restricted unless a need is documented and approved.
- **Network Management:** BTG will provide licensing and maintenance of the Client's firewall. These licenses may include features such as IPS, IDS, DNS Filtering, Geo IP Filtering, etc. BTG will make requested or needed configuration changes and perform software and/or firmware updates to the device(s) as needed following BTG best practices for the network firewall device that BTG manages (if any.) Unless otherwise noted, firmware updates require an ongoing maintenance/security subscription from the manufacturer of the device are included in this Service. If ongoing maintenance is not maintained or if a device is no longer supported by the manufacturer, updates may not be available, and your device may be at risk for security compromise. BTG will make every effort to notify you in such a situation.
- **Password Management:** BTG will provide a password management software: a software application or feature, often integrated into web browsers or offered as a standalone app, that helps users securely store, manage, and generate passwords for online accounts.
- **Security Awareness Training:** Security Awareness Training (SAT) is an educational program designed to help their clients' employees recognize and avoid cyber threats. It aims to make employees more aware of information security risks, encourage them to become a trusted first line of defense, and ultimately reduce the organization's vulnerability to data breaches and cyberattacks. BTG may utilize third-party software to deliver SAT. SAT will include monthly online training and phishing simulations. BTG will deploy SAT to all users within the Clients email environment, any new user will automatically be added to SAT. BTG will provide a monthly report to Client primary contact and/or other requested contacts, with data and reports on training completion, phishing click rates, and other relevant metrics.
- **Device Multi-Factor Authentication:** BTG will provide software that will lock down all covered end-user devices with Multi-Factor Authentication, requiring customers to use more than one form of identification to access devices.

- **Microsoft 365 Tenant Management:** BTG shall manage access to Client's Microsoft 365 environment including: Manage Exchange Online settings, including email routing, security settings, spam filtering, and other related tasks; Manage SharePoint and OneDrive such as storage quotas, sharing permissions, document security, and collaboration settings; Adding or removing Microsoft licenses and assisting with general billing questions. Client agrees that BTG shall have full administrative control of Client's Microsoft 365 tenant in order to effectively provide this service.
- **Google Workspace Tenant Management:** BTG shall manage access to Client's Google Workspace environment including: Manage Gmail settings, including email routing, security settings, spam filtering, and other related tasks; Manage Google Drive such as storage quotas, sharing permissions, document security, and sharing settings; Adding or removing Google Workspace licenses and assisting with general billing questions. Client agrees that BTG shall have full administrative control of Client's Google Workspace tenant and purchase one additional Google Workspace license for BTG in order to effectively provide this service.