



Effective May 27, 2025. These Service Descriptions supersede and replace all prior versions.

Schedule of Services

MANAGED SERVICES

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

Provider, through its Third-Party Services Providers will make its best effort to ensure the security of Client's information through third-party security software ("Security Software"). Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this Service is subject to the applicable Third-party Service Providers agreements regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client acknowledges that Third-Party Service Providers and their licensors own all intellectual property rights in and to the Security Software. Client will not engage in or authorize any activity that is inconsistent with such ownership. Client acknowledges and agrees to be bound by any applicable Third-Party Service Provider agreements regarding terms or use or end user licensing terms, and Client understands that any applicable agreement regarding terms of use or end user licensing is subject to change without notice.

Support

- **Remote Support**

Fortify Core Package Only

During designated Support Hours, provider will provide Remote Support for monitored client infrastructure which includes all managed business users, computers, servers, sites, mobile devices, tablets, and network infrastructure at the client's premises as deemed necessary by Provider. Support is available from Monday to Friday, 8:00 a.m. to 5:00 p.m. Local Time, with the exception of designated holidays. Onsite Support time **is not** part of your managed services addendum but is offered separately and billed hourly, in 15-minute increments.

Fortify Edge & 360 Packages Only

During designated Support Hours, provider will provide Remote Support for monitored client infrastructure which includes all managed business users, computers, servers, sites, mobile devices, tablets, and network infrastructure at the client's premises as deemed necessary by Provider. Support is available from Monday to Friday, 8:00 a.m. to 5:00 p.m. Local Time, with the exception of designated holidays.

- **Onsite Support**

Fortify Core & Edge Packages Only

During designated Support Hours, Provider will provide Onsite Support for monitored client infrastructure which includes all managed business users, computers, servers, sites, mobile devices, tablets, and network infrastructure at the client's premises as deemed necessary by Provider. Support is available from Monday to Friday, 8:00 a.m. to 5:00 p.m. Local Time, with the exception of designated holidays. Onsite Support time **is not** part of your managed services addendum but is offered separately and billed hourly, in 15-minute increments (with an 2-hour minimum).

Fortify 360 Package Only

During designated Support Hours, provider will provide Onsite Support for monitored client infrastructure which includes all managed business users, computers, servers, sites, mobile devices, tablets, and network infrastructure at the client's premises as deemed necessary by Provider. Support is available from Monday to Friday, 8:00 a.m. to 5:00 p.m. Local Time, with the exception of designated holidays.

- **After-Hours & Weekend Support**

Fortify Core & Edge Packages Only

After-hours & Weekend Support time **is not** part of your managed services addendum but is offered separately and billed hourly, in 15-minute increments (with an 4-hour minimum for on-site and a 2-hour minimum for remote). After-hours is considered 5:01 p.m. to 7:59 a.m. Local Time, with the exception of designated holidays.

Fortify 360 Package Only

After-hours & Weekend Support time **is not** part of your managed services addendum but is offered separately and billed hourly, in 15-minute increments (with an 2-hour minimum for on-site and a 1-hour minimum for remote). After-hours is considered 5:01 p.m. to 7:59 a.m. Local Time, with the exception of designated holidays.

- **Holiday Support**

Fortify Core & Edge Packages Only

Holiday Support time **is not** part of your managed services addendum but is offered separately and billed hourly, in 15-minute increments (with an 8-hour minimum for on-site and a 4-hour minimum for remote). After-hours is considered 5:01 p.m. to 7:59 a.m. Local Time any time during the 24-hour span of the designated holidays.

Fortify 360 Package Only

Holiday Support time **is not** part of your managed services addendum but is offered separately and billed hourly, in 15-minute increments (with an 4-hour minimum for on-site and a 2-hour minimum for remote). After-hours is considered 5:01 p.m. to 7:59 a.m. Local Time any time during the 24-hour span of the designated holidays.

- **Emergency - Remote Response Time**

Fortify Core & Edge Packages Only

The Emergency Initial Response Time is 2 Hours or less from the time the issue is reported via the Support Phone Number. The Emergency Severity Level is described as the whole company or department not being able to function due to a production system outage.

Fortify 360 Package Only

The Emergency Initial Response Time is 1 Hour or less from the time the issue is reported via the Support Phone Number. The Emergency Severity Level is described as the whole company or department not being able to function due to a production system outage.

- **Emergency - Onsite Response Time**

Fortify Core & Edge Packages Only

Emergency Onsite Response Time for this package is available from the time the issue is determined to require onsite support. Our goal is the same business day. An Emergency Severity Level describes the whole company or department not being able to function due to a production system outage and requires an onsite visit to resolve the issue during normal business hours.

Fortify 360 Package Only

Emergency Onsite Response Time for this package is available from the time the issue is determined to require onsite support. Our guarantee is the same calendar day. An Emergency Severity Level describes the whole company or department not being able to function due to a production system outage and requires an onsite visit to resolve the issue during normal business hours.

- **What Constitutes As An Emergency?**

An Emergency is when the whole company or department is unable to function due to a production system outage.

Data Breach Or Security Incident:

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Major Software Failure:

When a core business application or software system used by the client experiences a critical failure, rendering it inoperable and affecting business processes.

Network Infrastructure Failure:

If there's a significant disruption or failure in the client's network infrastructure, leading to loss of connectivity, inability to access resources, or communication breakdown.

Loss Of Business-Critical Services:

If services or processes that are crucial for the client's daily operations, such as email, file sharing, or customer support systems become unavailable.

Hardware Failure:

In the case of a critical hardware component failure (e.g. server, storage device) that impacts the client's ability to function properly.

Data Loss:

If the client experiences significant data loss due to hardware failure or software corruption, resulting in potential loss of revenue, compliance violations, or reputational damage.

Severe Performance Degradation:

When the client's systems or applications experience severe slowdowns or performance issues that hinder their ability to deliver services effectively.

Cybersecurity Event

A Cybersecurity Event is described as an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies with evidence of a security breach, unauthorized access, or any form of cyber-attack that compromises sensitive data, systems, or networks by a third-party actor, whereas the client's or client employee's negligence allowed the compromise.

Small Projects**Fortify Core & Edge Packages Only**

Small Projects **are not** included in the Core and Edge Packages.

Fortify 360 Package Only

If CNG determines a ticket request is a separate Project (as described in the Client's Addendum), CNG will obtain the Client's approval before moving forward. As a rule of thumb, we follow the "3 5's rule" when deciphering what is or isn't a project. If it is anticipated to take more than five (5) hours, includes more than five (5) steps, or affects more than five (5) users, it is a Project. The "3 5's rule" excludes onboarding and structured cabling. All onboarding fees are due before work can commence. CNG will include three (3) new computer setups per month at no additional charge for 360 managed services clients. 360 Clients will receive 10 free hours per year to be used toward small projects.

Block Hours

Block Hours are a **flexible, prepaid option** for clients who want coverage for services **not included** in their base plan. Block Hours require a minimum \$1,000-time block budget and must be pre-paid. We will bill our time against the \$1,000 based on the fee structure of remote, onsite, after-hours/weekend, and holiday support. Once the time block is used and drops under \$200, an additional \$1,000 time block will be billed. The time block will expire if not used within 24 months of receiving payment.

Dedicated Onsite Resource

All Managed Services Support Packages

A dedicated onsite resource **is not** part of the Managed Services Support Package but is an option to purchase separately in 4-hour increments.

Proactive Account Management

- **Proactive Account Management (For All Managed Service Packages)**

Weekly Cybersecurity & Tech Tips

We send out Cybersecurity & Tech Tips to all end users for educational and Cybersecurity purposes.

Payment & Invoice Portal

We provide a convenient and easy-to-use payment portal where we accept credit card and ACH payments.

Self-Service Portal

We provide a fully functional portal where you can pull reports, review tickets and where we provide custom ticket templates for your convenience.

Email Report

We send out a Monthly Email Security Report along with notifying you by creating a ticket of any breaches that we find about your company's email activity.

Dark Web Report

We send out a Monthly Dark Web Monitoring Report along with notifying you by creating a ticket of any breaches that we find about your company's data on the Dark Web.

Monthly Quality Assurance Touchbase Email

Your Account Manager will reach out to you via email or phone call monthly to see if you need any assistance from us and to make sure all is well in our partnership.

Custom Employee Onboarding / Offboarding Form

At client's request, we will provide you with the ability to create customized onboarding and offboarding forms for your users and computers. Our team will work with you to help set those up.

- **Proactive Account Management (For Fortify Edge and 360 Packages Only)**

DNS Filter Report

We send out a Monthly DNS Filter Report along with notifying you by creating a ticket of any breaches that we find about your company's DNS activity.

IT Documentation Portal

We offer a centralized portal for comprehensive documentation of your IT infrastructure, ensuring easy access to critical information, streamlined management, and improved operational efficiency.

Monthly Executive Report

We provide a report of the health of your network along with ticket trends and SLE reporting.

Asset & Inventory Management Report

We deliver a detailed report on the status and lifecycle of your IT assets, helping you track inventory, optimize resource allocation, and plan for future upgrades.

IT Budget Preparation

We assist in the creation of a comprehensive IT budget, offering insights into cost management, forecasting, and strategic planning to align your technology investments with business goals.

Strategic Business Reviews

CNG Account Manager will collaborate with client's key stakeholders on a regular basis to develop an IT strategy in alignment with the short- and long-term objectives of the client's organization. A detailed roadmap and predictable budget will be provided to ensure major projects and expenses are planned for well in advance.

User Management

- **User Management (For All Managed Services Packages)**

User Management

Provide troubleshooting and support for managed user related issues, including access permissions and group memberships.

Email Spam Filtering

As part of a layered security approach, robust spam / malware filtering services are included to help protect you from email threats.

Phishing Simulation

Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

Cybersecurity Awareness Training

We provide access to Award-Winning eLearning Courses for cyber security awareness training sessions available with certificate of completion. This is a self-paced training course for your employees.

Access Permissions Violation Monitoring

Access controls and User Behavior Analytics (UBA) will be implemented to monitor and alert for failed logins, unapproved region-based logins, and logins outside of the users learned working habits.

*Requires appropriate Microsoft licensing and client-defined parameters.

M365 Suspected Attacks Monitoring

Managed M365 accounts will be monitored for known and suspected threat actor attacks.

*Requires appropriate Microsoft licensing and client-defined parameters.

Mass Data Deletion / Download Monitoring

Managed cloud-connected accounts will be monitored for mass data deletion and downloading indicative of insider threats and threat actor access.

*Requires appropriate Microsoft licensing and client-defined parameters.

M365 User Account Monitoring

M365 Defense provides around-the-clock M365 security monitoring and policy enforcement.

With M365 Defense, cyber analysts will monitor and harden your M365 environment and user accounts.

*Requires appropriate Microsoft licensing and client-defined parameters.

White and Blacklist in Spam Filter

We can allow or disallow certain mail flows based on different categories/preferences.

- **User Management (For Fortify Edge and 360 Packages Only)**

2FA / MFA

Multi-factor authentication provides an additional layer of security when logging into supported systems. It's the concept of something you know (password) plus something you have (phone).

M365 Or Google Workspace Support And License Management

We facilitate the purchase and maintenance of licenses for M365 and Google Workspace. We provide support and troubleshooting for managed M365 and Google Workspace accounts. No development is included in support of these products.

M365 or Google Workspace Backup

Provide industry-leading 256-bit encryption at rest and 128-bit in transit. Provide multiple snapshots at regular intervals throughout the day. This ensures that the backups keep up with your demands and provide you with peace of mind.

Password Manager

A password manager is used to store passwords in a central location and protect them with encryption. This simplifies password management by eliminating the need to memorize multiple passwords for different accounts.

- **User Management (For Fortify 360 Package Only)**

User Training

We provide your company with live virtual training for your users when it comes to your technology needs. We will provide up to 1 hour of training per company per quarter.

Data Loss Prevention

CNG will build policies to control who and what devices can access managed M365 infrastructure and data. *Requires appropriate Microsoft licensing, Mobile Device Management (MDM), and client defined parameters.

New User Setup

We provide up to 3 new user and/or computer setups per month included in this CNG 360 package. Any additional users and/or computers will be billed at a flat fee of \$375.

Computer Management

- **Computer Management (For All Managed Services Packages)**

Endpoint Protection

An end-to-end approach to cybersecurity deeply rooted in artificial intelligence (AI) and machine learning (ML). Helps detect and prevent attacks from malware.

24 / 7 / 365 Device Management And Alerting

We provide 24/7/365 Management and Alerting for all supported devices under this addendum.

MDR / SOC

A team of cyber security experts actively identifying and remediating security threats. Takes in huge amounts of security / behavioral data from PCs and servers to identify suspicious patterns or actions. These behaviors are then reviewed by our security Edges. Another team of "threat hunters" are proactively looking for signs of compromise.

Scheduled Preventative Maintenance

We provide scheduled maintenance for all supported computers under this addendum.

Patch Management - Microsoft

Our Network Operations Center team identifies, approves, and automates the installation of necessary security patches. The installation is scheduled for pre-determined times to ensure security vulnerabilities are minimized.

*Additional patch management may be supported as requested by client and approved by CNG.

Automatic Escalation and Resolution Of Alerts

Our remote monitoring and management system provides the ability for us to escalate alerts to the appropriate engineers for resolution.

Service Auto-Healing

We have the ability to create auto-healing functions in our system if we find there are reoccurring issues that we can solve through automation.

Firmware Updates

We provide firmware updates for all managed computers.

Computer Encryption Management

CNG will manage computer encryption on managed devices that support encryption.

- **Computer Management (For Fortify Edge and 360 Packages Only)**

M365 / Azure / InTune Support

We will provide support and changes to the Azure and InTune environments to optimize performance and security. With the client's guidance, we will also manage the appropriate licenses for Azure and InTune.

*Requires appropriate Microsoft licensing, Mobile Device Management (MDM), and client-defined parameters.

- **Computer Management (For Fortify 360 Package Only)**

Support & Fix Computer Issues

CNG will provide computer break fix and managed software troubleshooting. Unmanaged software will receive best effort support or act as technical liaison with product support.

*Remote support will be performed unless the technician determines onsite repair is necessary.

Custom Alerts

We provide the ability to setup custom alerts for service and applications as requested by client.

Data Loss Prevention

CNG will build policies to control who and what devices can access managed M365 infrastructure and data.

*Requires appropriate Microsoft licensing, Mobile Device Management (MDM), and client defined parameters.

Cyber Attack Remediation

CNG will provide or facilitate the first five (5) hours of cyber incident triage per calendar year. Cyber Attack/Hack due to client's or client employee's negligence are not covered.

*Incident Response (IR) is billed hourly beyond the included hours at a rate of \$375/hour per security engineer required.

Automated Software Deployment

CNG will deploy managed software automatically on all managed devices.

*CNG can help deploy unmanaged software at scale for an additional cost or block of hours.

Provision Computer

CNG will configure managed computers to match the clients approved desired state for new hires. These devices will be required to meet the CNG minimum baseline requirements (i.e. Hardware, system specifications [CPU, RAM, storage space, etc. and current operating system). We provide up to 3 computer setups per month included in this package. Any additional computers will be billed at a flat fee of \$495 per new computer setup.

*Labor Only; All Hardware and Software Costs Will Be Additional

Installation Of New Software

Labor Only; All Hardware and Software Costs Will Be Additional. CNG will provide managed software troubleshooting and support. Unmanaged software will receive best effort support or act as technical liaison with product support.

Web Gateway / Content Filtering Security

We will build and maintain web content filters based on client-defined website categories.

All The Time VPN For Laptops

CNG provides VPN for your remote users, so they always have secure connections.

- **Computer Management (Add-On / Additional Billing)**

SIEM

SIEM logs nearly every bit of under-the-hood activity on a computer, network access, security changes, permissions changes, etc. Those behaviors are then used to trigger alerts when an unusual or potentially malicious string of behaviors is detected. SIEMs also provide CNG with a means of tracing a security incident back to its source which is traditionally a blind spot for IT Edges. 30-Day Retention is included, additional retention available for purchase by request.

Computer File Backup

CNG will provide a file level backup with a retention of 30 days.

*Requires Storage Plan billed separately

Image-Based Backup

We can purchase bare metal backup for your entire computer.

BDR Backup

CNG will provide leased Backup and Disaster Recovery appliances housed at the client-owned office location to perform a bare metal backup and ongoing file and folder level backup of the managed servers and/or workstations.

*All BDR services are custom quoted based on the needs. It **is not** included in any of our packages by default.

Server Management

- **Server Management (For All Managed Services Packages)**

Endpoint Protection

An end-to-end approach to cybersecurity deeply rooted in artificial intelligence (AI) and machine learning (ML). Helps detect and prevent attacks from malware.

24 / 7 / 365 Server Management And Alerting

We provide 24 / 7 / 365 Management and Alerting for all supported devices under this addendum.

MDR / SOC

A team of cyber security experts actively identifying and remediating security threats. Takes in huge amounts of security / behavioral data from servers to identify suspicious patterns or actions. These behaviors are then reviewed by our security Edges. Another team of "threat hunters" are proactively looking for signs of compromise.

Scheduled Preventative Maintenance

We provide scheduled maintenance for all supported servers under this addendum.

Patch Management - Microsoft

Our Network Operations Center team identifies, approves, and automates the installation of necessary security patches. The installation is scheduled for pre-determined times to ensure security vulnerabilities are minimized.

*Additional patch management may be supported as requested by the client and approved by CNG.

Automatic Escalation And Resolution Of Alerts

Our remote monitoring and management system provides the ability for us to escalate alerts to the appropriate engineers for resolution.

Service Auto-Healing

We have the ability to create auto-healing functions in our system if we find there are reoccurring issues that we can solve through automation.

Firmware Updates

We provide firmware updates for all managed servers.

- **Server Management (For Fortify Edge & 360 Packages only)**

M365 / Azure / InTune Support

We will provide support and changes to the Azure and InTune environment to optimize best performance and security. We will also manage the appropriate licenses when it pertains to Azure and InTune with the guidance of the client.

*Requires appropriate Microsoft licensing, Mobile Device Management (MDM), and client defined parameters.

Server Disk Encryption Management

CNG will enable and maintain server disk encryption on managed servers.

Remote Support & Fix - Server Issues

CNG will provide server break fix and managed software troubleshooting. Unmanaged software will receive best effort support or act as technical liaison with product support.

*Remote support will be performed unless the technician determines onsite repair is necessary.

- **Server Management (For Fortify 360 Packages only)**

Custom Alerts

We provide the ability to setup custom alerts for service and applications as needed.

Automated Software Deployment

CNG will deploy managed software automatically on all managed devices.

*CNG can help deploy unmanaged software at scale for an additional cost or block of hours.

Data Loss Prevention

CNG will build policies to control who and what devices can access managed M365 infrastructure and data.

* Requires appropriate Microsoft licensing, Mobile Device Management (MDM), and client defined parameters.

Cyber Attack Remediation

CNG will provide or facilitate the first five (5) hours of cyber incident triage per calendar year. Cyber Attack/Hack due to client's or client employee's negligence are not covered.

*Incident Response (IR) is billed hourly beyond the included hours at a rate of \$375/hour per security engineer required.

Onsite Support & Fix - Server Issues

CNG will provide server break/fix and troubleshooting. End-of-Life hardware will receive best effort support or CNG will facilitate vendor support on the client's behalf.

*Remote support will be performed unless the technician determines onsite repair is necessary.

Web Gateway / Content Filtering Security

We will build and maintain web content filters based on client defined website categories.

- **Server Management (Add On / Additional Billing)**

SIEM

SIEM logs nearly every bit of under-the-hood activity on a server, network access, security changes, permissions changes, etc. Those behaviors are then used to trigger alerts when an unusual or potentially malicious string of behaviors is detected. SIEMs also provide CNG with a means of tracing a security incident back to its source which is traditionally a blind spot for IT Edges. 30-Day Retention is included, additional retention available for purchase by request.

**Compliance as a Service clients will get additional log retention.

Server Data Backup

CNG will provide file-level backup with a retention of 90 days retention of 90-days. Any

*Requires Storage Plan billed separately

**Client compliance requirements may dictate the length of data retention where applicable.

Image-Based Backup

We can purchase bare metal backup for your entire computer.

BDR Backup

CNG will provide leased Backup and Disaster Recovery appliances housed at the client-owned office location to perform a bare metal backup and ongoing file and folder level backup of the managed servers and/or workstations.

*All BDR services are custom quoted based on the needs. It is not included in any of our packages by default.

Site Management

- **Site Management (For All Managed Services Packages)**

Dark Web Monitoring

A combination of human and machine intelligence with powerful search capabilities to scour the dark web to identify, analyze and actively monitor for your organization's compromised credentials 24 / 7 / 365, alerting you to potential trouble, fast.

Power Management

In the case of internet service or power outage, the power management device automatically restarts your router / firewall / server in an attempt to automatically restore connectivity to your business.

- **Site Management (For Fortify Edge & 360 Packages only)**

Network Monitoring and Alerting for All Network Devices and Peripherals

Visibility into Network Traffic flow, helping to identify issues or inconsistencies causing slow-downs or interruptions in your network infrastructure.

Network Management

CNG will provide network management and support for all office infrastructure equipment. End-of-Life hardware will receive best effort support or CNG will facilitate vendor support on the client's behalf.

*Remote support will be performed unless the technician determines onsite repair is necessary.

- **Site Management (Add On / Additional Billing)**

SIEM

SIEM logs nearly every bit of under-the-hood activity on a computer, network access, security changes, permissions changes, etc. Those behaviors are then used to trigger alerts when an unusual or potentially malicious string of behaviors is detected. SIEMs also provide CNG with a means of tracing a security incident back to its source which is traditionally a blind spot for IT Edges. 30-Day Retention is included, additional retention available for purchase by request.

Firewall With IDS / IPS as-a-Service

We will provide a firewall equipped with IDS and IPS. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are security features found in industry leading firewalls. They monitor the events occurring in your network and analyzing them for signs of possible incidents or threats.

Managed Tablet

- **Managed Tablet (For Fortify 360 Packages only)**

Tablet Device Management (MDM)

Mobile Device Management software allows us to automate, control, and secure administrative policies on your employees' business-owned tablets.

* Requires appropriate Microsoft licensing, Mobile Device Management (MDM), and client defined parameters.

Support & Fix Tablet Issues (Remote Only)

We provide remote support for all business tablets. This does not include repairs to damaged or malfunctioning tablets.

- **Managed Tablet (Add On / Additional Billing)**

All The Time VPN For Tablets

CNG provides VPN for your remote users, so they always have secure connections.

Application Control

We can provide Application Control through MDM or InTune.

* Requires appropriate Microsoft licensing, Mobile Device Management (MDM), and client defined parameters.

Managed Mobile

- **Managed Mobile (For Fortify 360 Packages only)**

Mobile Device Management (MDM)

Mobile Device Management software allows us to automate, control, and secure administrative policies on your employees' business-owned mobile devices.

* Requires appropriate Microsoft licensing, Mobile Device Management (MDM), and client defined parameters.

Support & Fix Mobile Issues (Remote Only)

We provide remote support for all business-owned mobile devices. This does not include repairs to damaged or malfunctioning mobile devices.

- **Managed Mobile (Add On / Additional Billing)**

All The Time VPN For Mobile

CNG provides VPN for your remote users, so they always have secure connections.

Application Control

We can provide Application Control through MDM or InTune.

* Requires appropriate Microsoft licensing, Mobile Device Management (MDM), and client defined parameters.

Additional Notes

We bill labor for any discovery or audit requests related to lawsuits, compliance regulations, and third-party audits.

Anything not specifically mentioned above is excluded.

Provider does not provide internet connection. Client is responsible for providing internet connection to use the Service.

**THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY
TIME WITHOUT NOTICE.**