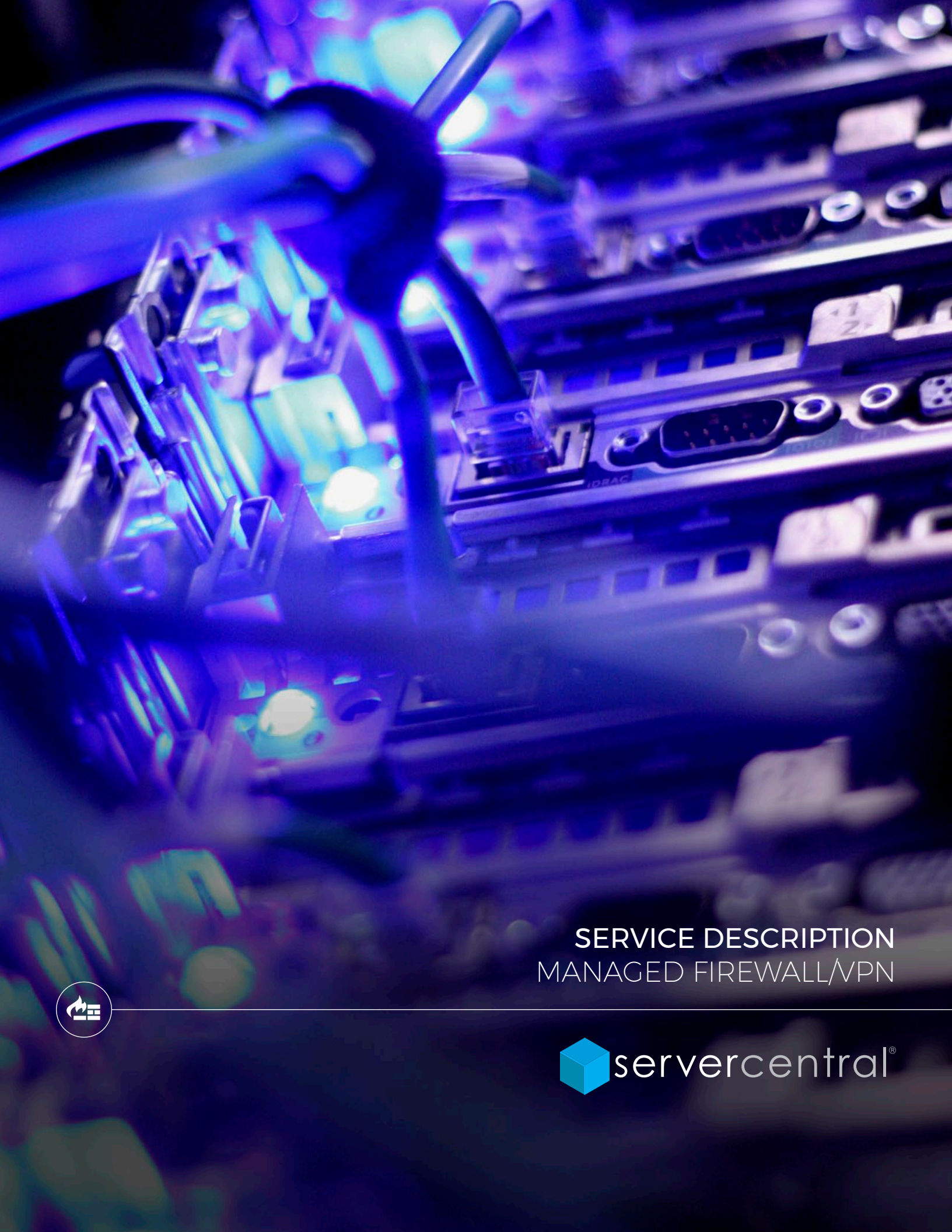


SERVICE DESCRIPTION
MANAGED FIREWALL/VPN

servercentral®

Contents

Service Overview

ServerCentral's Managed Firewall/VPN Service is a fully managed service providing dedicated virtual or hardware-based firewalls and VPN concentrators. This provides a barrier between the ServerCentral-provided uplink to the public Internet and Customer's equipment, permitting only designated traffic to pass between the networks. The Service includes configuration management, firmware patching and updates, on-site hardware sparing, and full maintenance & support, all monitored 24 x 7 by ServerCentral's Network Operations Center (NOC). Reporting and documentation are provided through ServerCentral's secure Customer Portal.

Managed Firewall/VPN Services include high bandwidth devices, offering speeds up to 25 Gigabits per second. The Service is designed around the customer's requirements for throughput, traffic filtering, threat detection and prevention, remote access, and scalability. The standard configuration for the Service includes a pair of customer-facing devices configured for high availability. These devices are connected to ServerCentral's scalable, redundant data center network and core routing infrastructure. Full administration of any device is performed by ServerCentral's team of network experts. If needed, customers request changes to the Service through ServerCentral's Customer Portal.

This Service is available to all ServerCentral customers located in a ServerCentral-managed data center, including Colocation, Enterprise Cloud, Dedicated Servers, or Infrastructure-as-a-Service.

Key Features

- Configuration designed around customer needs
- High performance firewalls connected to scalable, low-latency backbone
- Complete configuration and administration by ServerCentral's network experts
- Creation and management of firewall ruleset, IPSEC tunnels, and SSL VPN user administration
- Advanced Monitoring, including traffic, capacity, performance, and more
- 24x7 continuous device health, performance metrics, up/down monitoring, and alerting
- Firmware updates and vendor feature analysis
- Periodic tuning to reassess and adjust performance and effectiveness of the device
- Secure customer portal for monitoring, documentation, ticketing, and other deliverables

Service Features

FEATURE	MANAGED FIREWALL	MANAGED FIREWALL W/ THREAT PREVENTION
Firewall	Included	Included
IPSEC VPN	Included	Included
SSL Mobile VPN	5 Users (additional available)	5 Users (additional available)
IPS	Included	Included
Application Control	Included	Included
Content Awareness	Included	Included
URL Filtering		Included
Antivirus		Included
Anti-Spam		Included
Anti-Bot		Included

ACCOUNT MANAGEMENT SERVICES	
Dedicated Client Relationship Manager	Included
IMPLEMENTATION SERVICES	
Hardware Procurement & Assembly	Included
Data Center Provisioning (Generator-backed Redundant Power, Cooling, Cables, Rack)	Included
Resilient Facility (24x7 Physical Security, Video Surveillance, Fire Suppression, Monitored Access)	Included
Network Provisioning (IP addressing, VLAN Configuration, Physical Cabling)	Included
Feature Validation for Firmware	Included
Device Configuration	Included
Configuration conversion from customer-owned devices	SOW Based
24 X 7 MONITORING SERVICES	
Network Traffic Analysis & Volumetric DDoS monitoring on IP Transit Service	Included
Hardware Health Monitors	Included
Hardware Availability Monitors	Included
Hardware Performance Monitors	Included
Capacity Monitors	Optional
Custom Runbook coordinated with Customer	Optional
Complex Custom Monitor Development	SOW Based
NETWORK DEVICE ADMINISTRATION (PROACTIVE SERVICES)	
Device Administration	Included
Configuration changes per customer requests	Included
Device Configuration backup & monitor for changes	Included
Change Management leveraging the ServerCentral change control process	Included
Change Management coordination with Customer	Included
Firmware Patching & Updates	Included
24 X 7 SUPPORT (RETURN TO SERVICE & VENDOR ESCALATION)	
Onsite sparing of identical hardware in US locations	Included
Hardware Troubleshooting	Included
Hardware Replacement	Included
Hardware Maintenance	Included
Access to 24x7 Network Operations Center (telephone, web, and email)	Included
Access to Customer Portal w/ Customer-defined roles	Included
Ticket Response time - Promised	15 minutes

Responsibilities

The following section outlines the scope and limitation of support that ServerCentral offers for this Service.

SERVERCENTRAL RESPONSIBILITIES
ServerCentral will monitor the Managed Firewall/VPN for uptime and availability, including hardware systems, networking, and operating systems.
ServerCentral will manage, operate, and maintain the Managed Firewall/VPN based on accepted industry best practices.
ServerCentral will retain exclusive administrative access to the Managed Firewall/VPN for the duration of the agreement.
ServerCentral will use a standard configuration for the Managed Firewall.
ServerCentral will be responsible for system infrastructure support, including return-to-service and vendor escalation.
ServerCentral will not provide device SNMP & Syslog forwarding to Customers.
ServerCentral will perform firmware updates, including security updates, per the manufacturers recommendations and industry best practices. Updates will occur during declared maintenance windows that will be agreed upon in advance with the Customer.
CUSTOMER RESPONSIBILITIES
Customer is responsible for installing, configuring, and maintaining all infrastructure and applications connected to the Service.
Customer will work with ServerCentral to verify Managed Firewall/VPN is delivering the expected services to the Customer owned equipment attached to the Managed Firewall.
Customer will provide IP addresses for Customer-owned equipment attached to the Managed Firewall.
Customer will designate and maintain a Customer Contact who can be made available to ServerCentral for troubleshooting or questions.

Requests that are out of ServerCentral's support scope or responsibilities can be performed for a fee or on a time-and-materials basis. Please contact sales@servercentral.com for additional pricing information.

Additional Services

Many times, the Service will be integrated with additional Services provided by ServerCentral. Some examples include Colocation, Managed Switch/Router, Managed Storage, Enterprise Cloud and Managed Backup. All services and products necessary to complete the deployment will be completed either in tandem or in a phased approach during this post-implementation configuration period.

Backup: Customers are responsible for maintaining current backups of data on Customer-owned devices. ServerCentral offers a Managed Backup Service for physical or virtual servers, including Private Clouds. Please contact sales@servercentral.com for more information.

Monitoring: Customers are responsible for monitoring Customer-owned infrastructure or applications. If desired, ServerCentral can perform that monitoring though the Advanced Monitoring Service. For details and pricing information, please contact sales@servercentral.com.

For any of the other Managed Services associated with your Managed Firewall/VPN Service , please refer to the appropriate Service Description for further information regarding those services.

Implementation

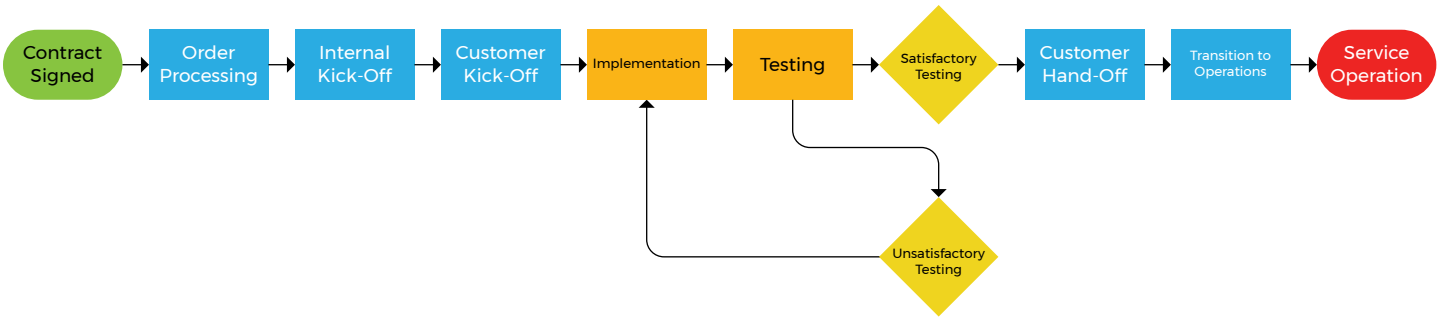
Validation

The Validation process begins with a comprehensive review of the information collected by Sales or Professional Services during the Assessment phase. The information usually includes applications and devices designated to be used with the Service, usual bandwidth requirements, relevant topology information, remote access requirements, customer-deployed hardware/software tools, firmware versions, application types, and initial configuration details. Other client-specific requirements, such as traffic filtering policies, threat prevention requirements, or third-party requirements, will also be reviewed. This information is documented and stored in the Technical Design Workbook. The Technical Design Workbook is used to create a Customer Workbook that is shared with the Customer after Implementation.

The Technical Design Workbook provides all necessary information to ServerCentral engineers to ensure that information-gathering is complete and the Service will be able to address the Customer's needs. This may include network diagrams, configuration details and requirements, special security considerations, and more. The Technical Design Workbook will serve as a basis for configuration detail and will be utilized in the long-term planning and execution of the Service.

Implementation Process

All provisioning activities at ServerCentral follow our Implementation Process summarized in the Graphic below:



After the customer's order for the Service is processed, ServerCentral holds an Internal Kick-Off meeting to assign the ServerCentral resources necessary to provision the service. Sales attends this meeting to provide information from the pre-sales process. A Project Manager or Project Lead will be assigned to coordinate and own the remainder of the Implementation Process from this point forward and act as the main point of contact with the Customer.

Customer Kick-Off

The Customer Kick-Off Call includes an overview of the provisioning process, a review of the information collected to date, and validation of the Customer's desired outcomes for the Service. The projected time line of the deployment will be established and the customer will be informed of any information they must provide for ServerCentral to complete the build. Generally, the Project Manager will also create a schedule for regular updates during the implementation process. The Customer should be prepared to designate at least one technical contact for ServerCentral to work with during the process.

Initial Configuration

Using the baseline information in the Technical Design Workbook, the ServerCentral Engineering team will configure the baseline parameters for initial operation. The variables include:

- Port Configuration
  - Descriptions to match hardware for inventory purposes
  - Logical setup to match network requirements
- Traffic Filtering Configuration
  - IP Addresses and Ports to open
  - Network and Port Address Translation as required
  - Higher-level URL and application rulesets
- VLAN Configuration
  - Includes switch local private VLANs
  - Includes Trunked (802.1Q) connections to other Customer-owned devices
- IP Addressing
  - Public addresses whether provided by ServerCentral or the Customer
  - Private (RFC1918) addresses
- IP Routing
  - Includes simple connectivity to ServerCentral network
  - Includes complex routing to Third Party Providers for both Public (BGP) and private (L3VPN) connections
- Cable Management
  - All physical cables will be deployed by ServerCentral personnel
  - With prior approval, cabling may be deployed by the customer, however, ServerCentral personnel will be required to enable ports.

Provisioning & Testing

Implementation includes the activities necessary to provision the service. ServerCentral engineers will configure, deploy, and test the various hardware and software tools used to deliver the service. ServerCentral records all of the configurations used to implement the Service in a Customer Workbook, which is provided to the Customer after Implementation.

ServerCentral technical teams will perform testing on the environment prior to customer hand off. This usually includes, but is not limited to cable pull testing, system redundancy verification, verifying network connectivity, monitoring and alerting configurations, and activation of the Service in the Customer Portal. Any deficiencies found will be corrected and re-tested until the system functionality is verified. Requests for customer-specific test criteria will be reviewed by ServerCentral and evaluated on a case-by-case basis.

Billing

After a successful Test phase, Implementation will be considered complete and the Service Delivery phase begins. In general, billing for the service begins immediately after ports are up and able to forward traffic.

Fees will be inclusive of a non-recurring charge for setup and configuration and a monthly recurring charge for ongoing Managed Firewall Services. Additional fees may be incurred by the Customer for completion of services provided by ServerCentral outside the scope of the Managed Firewall Service. All additional fees will be agreed upon, in writing, by both parties prior to the service being performed.

Service Level Agreements

Service Level Agreements (SLA's) are posted for each service at https://www.servercentral.com/legal-information. For questions regarding SLA's, please contact your account representative.

Service Delivery

Customer Hand-Off

The Project Manager or Provisioning staff will schedule a Customer Hand-Off Meeting, either in person or via conference bridge. The Meeting is designed to advise the Customer of the state of the service, the current configuration, and answer any general questions about the Service. The Meeting will usually include training on using the ServerCentral Customer Portal, including providing any access credentials to the Customer, walking the Customer through support engagement procedures, and general interaction with the Portal. The Project Manager will also share the final/completed Customer Workbook, which takes the data from the Technical Design Workbook and Implementation process and acts as a the "as-built" documentation of the Service.

Steady State Configuration

Once the Managed Firewall/VPN Service has been deployed, any configuration changes will be performed by ServerCentral. Copies of firewall rules, port and VLAN configurations, IPSEC tunnel, and SSL VPN configurations will be available in the Customer Workbook or by submitting a service request.

Customers do not have access to the devices, which are wholly administered by ServerCentral. Should any ongoing changes be necessary, such as new firewall rule creation, IPSEC tunnel creation, VPN user management, port configurations, adds/moves/changes, or any other type of work, Customers can open a support case with ServerCentral to request the work. Requests for non-standard changes will be reviewed by ServerCentral and evaluated on a case-by-case basis.

During the Service Delivery, the ServerCentral Provisioning and Managed Services teams will review the configuration documents in the Technical Design Workbook and discuss any changes to scope. These changes, if any, will be documented in the Customer Workbook described above.

Service Operations

General Operations

The Managed Firewall/VPN Service , including all associated hardware and software, are monitored by ServerCentral's Network Operations Center. Should any issues or anomalies be detected with the Services, a member of the ServerCentral NOC or Network team will take corrective action as planned and notify the customer.

In the event of hardware failure, ServerCentral personnel will proactively replace any failed hardware and restore the Service to normal operations. If the Service is configured for high availability, ServerCentral's network team will attempt to coordinate the replacement to fit with the Customer's normal change schedule.

From time to time, ServerCentral will perform scheduled maintenance activities on the infrastructure supporting the service. Customers will be notified in advance for all scheduled maintenance. Emergency maintenance may be required and performed without advance notice. Should a service-impacting emergency maintenance be required, ServerCentral will use commercially reasonable efforts to notify Customer upon execution of the maintenance.

Customers may also view real time and historical graphs of the Service via the ServerCentral Customer Portal located at https://portal.servercentral.com.

Service Interaction

ServerCentral provides customers with an online Customer Portal, allowing access to view and update account information and to open and review tickets. The portal can be accessed at https://portal.servercentral.com.

For any issues, Customers should contact the ServerCentral NOC. Support requests are monitored 24x7x365 by on-site and off-site personnel. There are three ways to contact the NOC:

- Customer Portal: Preferred method for Customers to open tickets, as well as monitor ticket status
- Email: Customers can email a request for ticket to support@servercentral.com
- Phone: (888) 875-7775 or (312) 829-1111, ext2 or +1 (312) 895-3005

For billing inquiries or to contact Sales, please call +1 (312) 829-1111.

Support Requests

Time is applicable prior to executing the support request. Additional support can be purchased at a one-time rate or through a pre-reserved set of hours. Please contact your account representative for additional details and pricing.

ServerCentral personnel are generally available to accommodate end user prescheduled maintenance requests. All requests for scheduled maintenance must be submitted as a support request with, at a minimum, 48-hour advance notice of the requested date and time. Please note that submission of the request does not guarantee the requested date and time until ServerCentral personnel confirm availability for the date and time requested. This is necessary to ensure scheduling of all required ServerCentral personnel and to allow sufficient time for ServerCentral Change Review processes to occur. Please refer to section 4 (Change Review) in the Managed Services Handbook for additional information regarding ServerCentral Change Review procedures.

If you have any questions, comments, or concerns, please notify the Sales team via email to sales@servercentral.com.

Access Management

Customers are responsible for maintaining the list of authorized personnel in the ServerCentral Customer Portal. The access list can be self-maintained by Customers and can be reached at https://portal.servercentral.com. ServerCentral is not responsible for any unauthorized access or modifications to any Service due to out of date access list information.

For ServerCentral Managed Service deployments, Customers will need to designate contacts that can have the following access levels:

ROLE	ACCESS
Administrator	Full access to all account functions, including user management and all other functions listed below.
Manage Users	Access to remove non-Administrator users or add users with permissions at or below the current level
Physical	Full access to physical infrastructure via escort
Unescorted	Full access to physical infrastructure without escort
Technical	Able to open support requests
Billing	Able to make billing inquiries related to the Services for the account
Sales	Able to order additional Managed Services via ServerCentral Sales

ServerCentral does not provide forensic analysis of application exploits as part of any managed service. If a Customer suspects that a customer-owned application or device has been compromised or exploited, the Customer is fully responsible for determining the attack vector and any compromise that may exist.