

Benefits

- **Reduce capital outlays and operating expenses**—since you no longer have to buy, install and manage premise-based firewall devices and appliances at individual locations
- **Centralize control and management of data security policies**—with consistent, company-wide firewall and security rules that you design
- **Help shield your network infrastructure and applications**—from being compromised, with up-to-the-minute information about security threats and compliance

Enterprise Cloud Security

Quickly and efficiently deliver uniform, network-based security across your enterprise.

Enterprise Cloud Security is a robust suite of network-based security capabilities that can be easily and cost-effectively deployed to protect your enterprise network. As part of your organization's overall risk management strategy, XO Enterprise Cloud Security helps you prevent unauthorized access to your network infrastructure, block access to inappropriate web content, inhibit downloads of infected files, and ensure secure use of your organization's corporate IP-VPN network. XO Communications integrates the fully managed, Security-as-a-Service with your XO private data network service so that you can easily centralize network security controls and policies across your enterprise.

Network Security in the Cloud

With XO Enterprise Cloud Security, your organization eliminates the need to buy and manage premise-based, security devices and appliances. Instead, you control company-wide data security standards across all of your locations—and XO Communications security experts monitor and manage the authorized use of your network security policies.

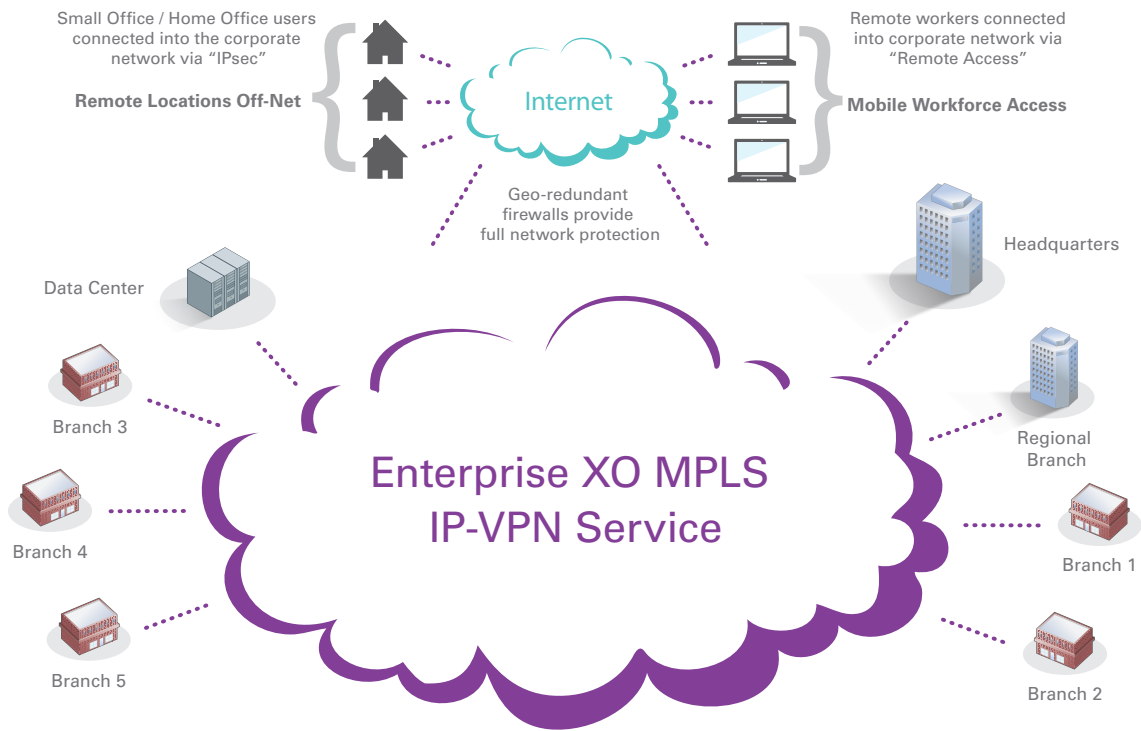
Using the security rules that your organization custom designs, XO Enterprise Cloud Security helps you to:

- Identify and deflect Internet-based attacks to your company's network
- Block employees from accessing unauthorized websites or downloading content that could be harmful to their computers or your company's network

- Provide employees with secured access to your company's intranet environments
- Mitigate the risk of Internet hackers, malware or other malicious programs from compromising your company's intellectual property or critical business applications
- Maintain highly secure connections to your enterprise by providing the ongoing maintenance of security-related software updates and patches.

By integrating Next-Generation Network Firewalls and other security tools with your XO MPLS IP-VPN or IP Flex with VPN service, XO Communications makes it easier for you to mitigate the risks of cyber security threats that could disrupt your business operations and damage your business reputation.





XO Enterprise Cloud Security helps you prevent unauthorized access to your network infrastructure, block access to inappropriate Internet websites, inhibit downloads of infected files, and ensure secure use of your organization's corporate IP-VPN network.

More Benefits

- **Add an extra layer of security protection**—to minimize the risk of unauthorized access to your company data, applications and XO MPLS IP-VPN or XO IP Flex with VPN service
- **Gain utilization reporting**—on your Internet resources
- **Focus on your core business**—and rely on an experienced service provider to monitor and maintain your security policies
- **Control who can access what**—from any location or user accessing your network using encryption and authentication standards
- **Help free up bandwidth**—for legitimate business traffic across your network
- **Be able to quickly grant access to the company IP-VPN**—for new locations or employees

A Range of Security Options

XO Enterprise Cloud Security encompasses a range of Security-as-a-Service capabilities that are available on a subscription basis:

- **Network-based, Next Generation Firewall** allows or denies traffic based on the policies and rules you apply
- **Intrusion Detection and Prevention System (IDPS)** captures and inspects all traffic to safeguard against targeted attacks or other threats, and includes Distributed Denial of Service (DDoS) protection
- **Web and Content Filtering** to protect users from entering company-prohibited websites
- **Secure Remote Access** to your corporate IP-VPN for mobile workers
- **Off-Net Connectivity** allows off-net locations to cost-effectively connect to the corporate IP-VPN through IPsec tunnels.

These components are available with no set up charge. A monthly recurring

charge includes the set up of your virtual domain, set up and configuration of optional features, monitoring and management, and online custom reporting.

Great Flexibility and Scalability

The solution offers aggregated Internet bandwidth that can be shared by all of your IP-VPN locations. It's also highly scalable; you add the security options as your organization grows, and as you need them, to meet the ever-changing requirements of your distributed workforce.

Business Continuity Features

With XO Enterprise Cloud Security, you gain high-availability and failover among geographically diverse physical gateways, with network redundancy to ensure business continuity.

In addition, the Next Generation Network Firewalls that reside in the XO network divert unauthorized traffic from the public Internet away from your corporate network. An entire team of experienced, certified security professionals provide 24/7 monitoring and management of security events.

Easy Online Management

XO Enterprise Cloud Security is managed through an online management portal. The portal provides visibility to the Firewalls, and allows you to implement rule changes and configuration requests quickly. Use the secure portal to:

- Get on-demand reporting about the health and security configuration of your network including attack attempts, attack source severity, and targeted systems

- View incidence response tracking—such as event and incident details, actions taken, attack header and payload and more
- Capture transaction audit details—including device log-ins, rules updates, configuration changes, actions taken and alerts issued.

An End-to-End Solution

XO Enterprise Cloud Security delivers a high level of network and content security without degrading the availability or performance of your IP-VPN service. That’s because XO Communications integrates XO IP-VPN with XO Enterprise Cloud Security into an end-to-end networking and security management solution. You benefit from the economies of combining security solutions for all of your locations and users—through a single provider on one invoice.

About XO Communications

XO Communications is a leading nationwide provider of advanced communications services and solutions for businesses, enterprises, government, carriers and service providers.

XO customers include more than half of the Fortune 500, in addition to leading cable companies, carriers, content providers and mobile network operators. Utilizing its unique combination of high-capacity nationwide and metro networks and fixed wireless capabilities, XO offers customers a broad range of managed voice, data and IP services with proven performance, scalability and value in more than 85 metropolitan markets across the United States.



For more information, call your XO sales representative, visit www.xo.com or call: **866.349.0134**

Key Features:

Next Generation Firewall Protection

- ✓ Provides stateful packet inspection of network traffic and allows or denies traffic based on the IP header and ports involved in the connection
- ✓ Distinguishes legitimate packets for different types of connections

Intrusion Detection and Prevention System

- ✓ Safeguards your network from targeted attacks before the attacks can enter your corporate IP-VPN network
- ✓ Includes Distributed Denial of Service (DDoS) protection
- ✓ Looks for anomalous data and generates an alert when it finds unauthorized data packets

Web and Content Filtering

- ✓ Protects users from entering company-prohibited websites or from downloading content that may be harmful to computers or to the company network
- ✓ Is easily custom designed; you can set up lists to allow or deny access based on company policies and best-use practices

Secure Remote Access

- ✓ Allows users to connect to your corporate network while on-the-road or from an off-net, home office location
- ✓ Authenticates identification, grants access and maintains security privileges for the remote connections

Off-Net Connectivity

- ✓ Maintains an off-net connection between your location and the network firewall
- ✓ Encrypts each packet in the data stream to ensure data integrity

