

Celestix Cloud Edge Security: Why an appliance?

Whitepaper

June 2014

Overview

This white paper discusses the benefits of security appliances for IT remote access and cloud infrastructure.

Introduction

Infrastructure

Areas to consider for remote access and cloud connectivity expansion.

Deployment

A dedicated appliance solution addresses hardware and functionality issues for connectivity options.

Solution

A more secure, cost-efficient deployment strategy.

Conclusion

Introduction

Connectivity to IT resources is a key component to empower workers and drive productivity. Microsoft® is innovating the adoption of remote access and cloud computing for every level of network infrastructure with Windows Server® 2012 R2. Server 2012 has taken leaps forward to incorporate networking and security functionality that once required multiple solutions to achieve.

IT managers must consider the most efficient solution to successfully meet the deployment goals for transitioning access options to external users and services. The following topics discuss infrastructure considerations and deployment options to inform strategic connectivity planning.

Infrastructure

The technology to diversify the IT environment through cloud services and remote access has two main areas to consider: functionality and hardware.

Functionality

- Server 2012 is packed with features to manage initiatives that help organizations extend the work environment for greater resource access.
- External access to the network is now a core service for many organizations.
- Many organizations can benefit from the opportunities offered by cloud scalability, but most want or require some level of on-premises infrastructure. Establishing secure connectivity with off-premises services can require extra IT resources.
- Secure implementation requires a broad range of expertise because configuration can be complex. This sometimes makes connectivity initiatives costly to deploy.
- Feature deployment requires thorough preparation to maintain best security practices.

Hardware

- The deployment process for a server often includes several steps: obtaining the necessary hardware, assembling the server, installing and hardening the operating system, then installing and configuring the application software.
- Generic hardware can serve many purposes, but has to be configured to do any one thing well. Expertise is paramount for secure remote access integration.

- Generic hardware exposes a larger attack surface in the IT infrastructure because it contains unnecessary components and services that open up threat vectors.
- Common component extras on industry standard servers, like high-performance graphics cards, CD/DVD drives, and expansion slots do not serve networking or security functions, but introduce additional points of failure.

Deployment

Functionality and hardware issues for connectivity expansion can be addressed through a dedicated appliance solution.

Functionality

- Software hardening is based on informed best practices that mitigate threats like intrusion or malevolent behavior.
- Appliances that include tools for headless integration to the network make the initial configuration during installation far more efficient.
- Application management tools and wizards save time and reduce complexity. They can also prevent configuration conflicts that adversely affect security and usability.
- A dedicated appliance simplifies the connection between internal resources and the variable resources that the cloud can host.
- Easy remote access to resources allows organizations to capitalize on worker productivity and creativity.

Hardware

- Appliances simplify the procurement process.
- Specialized appliances are engineered to offer efficient configuration for server settings and feature deployment. This reduces demands on IT resources.
- Appliances feature tuned hardware that is purpose built. Components like memory speed, memory size, memory latency, CPU, and cooling are designed to optimize performance and longevity. Tuned hardware also means that you don't pay for unnecessary components.
- Software drivers and firmware are tested against engineering standards to curtail threat vectors for the appliance application.

Solution

Deploying complex connectivity customizations without specific experience or with limited time actually increases organizational risk for information security. The Celestix E Series appliance provides a more secure, cost-efficient deployment option.

Setup Simplicity

Our appliances offer onboard setup tools using an LED screen and Jog Dial. Administrators can configure the IP address, subnet mask, default gateway, and static routes in minutes, without the need for a keyboard, mouse, or monitor. The platform also features a compact appliance form factor, allowing our devices to be mounted in any standard 19" equipment rack. Hardware-integrated disaster recovery is also included.

Centralized Administration

The E Series includes the new Comet 2.0 web user interface (web UI). The web UI centralizes general Windows Server administration and Remote Access (RA) configuration, so administrators can go to one place to customize the deployment. One-click installation for several RA features relieves the tedious task of installing features one by one. Administrative efficiency can offset appliance costs by saving IT staff hours.

Tuned Hardware

Our hardware has undergone extensive testing, and minimizes the attack surface by engineering just the services and applications that are necessary for security and connectivity. Hardware is hardened based on expertise gained through years of experience in networking security.

Access Multiplicity

Every organization is different, there is no 'one size fits all' scheme for remote access. The E Series provides for multiple access scenarios and the supporting functions they require. Secure access strategies can include managed/unmanaged devices, application publishing, and facilitation for public and private cloud connectivity.

Expanded Functionality

The E Series improves upon current Server 2012 functionality with exclusive features. Reporting, alerting, and monitoring tools both simplify daily management and support compliance

requirements. Real-time connection management provides greater control over user access to resources.

Future Ready

Future enhancements can be added through updates to both Remote Access and the Comet platform. Examples include virtualization, SSO enhancements, and forms-based authentication. By allowing organizations to leverage new features, the E Series continues to provide value for the investment.

Celestix Brand

Our appliances have a proven track record in the security industry. Celestix has over 15 years of experience providing 24x7 support for tens of thousands of appliances to thousands of customers worldwide – all backed with comprehensive SLAs.

Conclusion

Organizations may wonder whether an appliance provides worthwhile advantages over deploying a generic Windows Server 2012 R2 white box. While Server 2012 offers a host of connectivity features, most companies don't have specialized or in-depth knowledge regarding best configuration practices for the features that are now included. To help IT departments handle an ever-increasing scope of services, reducing complexity while maintaining security is essential to advance organizational goals.

Celestix strives to deliver high value to our customers. Our appliances save installation time, ease configuration tasks, and reduce licensing costs. They are hardened for security and undergo extensive, purpose-specific testing. Celestix also adds functionality not available in standard Server 2012 deployments. Imminent product releases will provide a wealth of additional features that will continue to return on connectivity investments.

Contact

Celestix Networks, Inc.

3215 Skyway Ct.

Fremont, California 94539

www.celestix.com

sales@celestix.com

510.668.0700

facebook.com/celestixnetworks

twitter.com/CelestixNetwork