2007

ESS is a Certified ODDS© Master Channel Partner

MASTER CHANNEL PARTNER

ODDS

ON DEMAND DEFENSE SERVICES

ESS Channel Partner Proposal

Become a Certified ODDS© Partner by integrating ODDS into your business services. Customize the collateral in this content paper to solicit customers or to develop channel sales partners of your own. Let us help to assimilate the ODDS© marketing content into your business website and sales material. Use our marketing strategies to build a high margin recurring monthly profit center for your business….

Marketing Collateral Provided by ESS Marketing & are solely useable solely under the approval of Email Sorting Solutions.

Table of Contents

ESS Introduces ODDS® Partnering Opportunities

ODDS ON DEMAND DEFENSE SERVICES

If you could negotiate deep discounted volume pricing from “best of breed” top brand messaging security software companies, with your millions of direct customers, “cherry pick” from only the best application within each bundled line of security brand software offerings, and deliver each specialized top software as a service from your own carrier grade data center facilities… you would have ***ODDS®…*** On Demand Defense Services.

What we do with ***ODDS®*** is compliment or supplement the existing messaging security offerings for technology providers, within hours, one application at time, allowing customers to pay one month at a time. What is ***ODDS®***? ***ODDS®*** Manages internet messaging and data security threats…

- IM Security
- Email Filtering
- Web Content Filtering
- Archiving
- Basic Message Care (Webmail, Personal, or Business Class Email Hosting)
- Total Message Care (Hosted Email, IM, Web, & Email Filtering, Archiving, Office Collaboration-Calendar Share, Remote Device Synchronization)
- Managed Intrusion, Detection, & Prevention Services

ODDS® “On Demand Defense Services” gives message security customers a brand identity and the “buy in” confidence for a complicated multitude of messaging securities solutions, all under one umbrella services line, focused on internet data security. The true benefit of becoming an ***ODDS®*** provider, you have access to top brand “SaaS” security technologies, with very high margins, can offer one service or all services, can private label services, can use these top brand software names for market recognition, and take virtual ownership of the world class infrastructure dedicated to delivering your ***ODDS®*** program.

Through ESS's Master Channel Partners, ***ODDS***® providers have the opportunity to become;

CERTIFIED VENDING PARTNER ODDS ON DEMAND DEFENSE SERVICES	There are two avenues to becoming a **Certified Vending Partner** for ***ODDS®;*** by joining an IT purchasing consortium like the American Alliance of Service Providers or by contacting other ***ODDS***® Master Channel Partners like ESS. Credentialed IT companies can provide ***ODDS***® through simple pricing agreements, service level agreements, with credit authorization, and a token annual sales minimum.
MASTER VENDING PARTNER ODDS ON DEMAND DEFENSE SERVICES	There are two avenues to becoming a **Master Vending Partner** for ***ODDS®;*** by joining an IT purchasing consortium like the American Alliance of Service Providers or by contacting other ***ODDS***® Master Channel Partners like ESS. Credentialed IT companies can provide ***ODDS®*** through volume pricing agreements, service level agreements, with credit authorization, billing agreements, and a volume annual sales minimum.
MASTER DELIVERY PARTNER ODDS ON DEMAND DEFENSE SERVICES	There is only one way to become a **Master Delivery Partner** for ***ODDS®;*** by soliciting an IT purchasing consortium like the American Alliance of Service Providers through ESS. Credentialed IT "SaaS" companies providing month to month messaging security technology with guaranteed uptime, private label or co-branding, volume pricing agreements, 24/7/365 service level agreements, will be considered for ***ODDS®.***
MASTER CHANNEL PARTNER ODDS ON DEMAND DEFENSE SERVICES	There is only one way to become a **Master Channel Partner** for ***ODDS®;*** by contacting an IT purchasing consortium like the American Alliance of Service Providers through ESS. Credentialed IT channel sales companies can provide ***ODDS***® through volume pricing agreements, service level agreements, with credit authorization, billing agreements, and a volume annual sales minimum.

From more information on becoming an ***ODDS***® Master Delivery Partner email us at **odds@emailsorting.com**

E-MAIL SORTING SOLUTIONS

ODDS
ON DEMAND DEFENSE SERVICES

Protected by **ODDS®**

On Demand Defense Services

Employing internet communication platforms are necessary to compete in the global era of immediacy. Customers, clients, partners, co-workers, suppliers, etc… want instantaneous reply to their inquiry at “break neck” speed, or they can become hard to approach or offended. Even with “best of breed” firewalls our networks are continually bombarded with hackers searching for identity and intellectual property assets.

To succeed, we accept these connectivity risks by offering our email address, IM address, web addresses, cell numbers, because we have to. Unfortunately, being first in service also means more threats, more IT expense, less record of messages inbound, outbound, or internal, and unexpected risks beyond the firewall.

To communicate productively, every enterprise large and small has the overwhelming task to address multiple messaging and internet security risks;

- *Technical Protocols*
- *Message Born Threats*
- *Acceptable Use Policies*
- *Legal Record Obligations*
- *Network Intrusion Management*

Regardless of size, most enterprises have protections in place. Implementing solutions that address online risk ***does not*** have to be a holistic… a dump everything or do-over approach. The **ODDS®** advantage is to affordably compliment or supplement your existing securities within hours, one step at a time, and pay one month at a time.

ODDS® is SaaS & MSP

All enterprises require top brand mature technologies to be secure and productive. **ODDS®** provides trusted “Software as a Service” through proven Managed Service Providers to meet your technology needs.

ODDS® Gives you the flexibility to…

- *Address IM risks and IM Policy while allowing the usage for productivity.*
- *Implement internet access (Web Content) policy for blocking objectionable material and blocking website based threats.*
- *Focus on SOX (Sarbanes Oxley) or FRCP (Federal Rules of Civil Procedure) archive issues, affordably, without bundling.*
- *Re-evaluate email security, higher spam capture rates, enhanced protection with encryption, or block intellectual property theft, add user collaboration.*
- *Assess network threats past the firewall with live analysts detecting nefarious traffic patterns, blocking suspicious threat activity, and live consulting until a threat is diffused.*

With a perimeter based messaging security host, industry experts argue the comprehensive approach of a SaaS may be the best way for organizations of all sizes to protect their employees and networks from Internet-based communication threats.

To make your **ODDS®** solution perform at the highest comprehensive level… we deliver our Managed Intrusion, Detection, and Prevention Service (MIDPS). **ODDS®** MIDPS is a SAS 70 (Statement on Auditing Standard 70) certified, 24/7/365 human analyst reviewed threat diffusion service for a "best of breed" in achievable perimeter security protections.

With MIDPS, a 24/7/365 fully managed intrusion security service provider, there's no need to rely on artificial intelligence or an overburdened internal IT staff to block threats reactively from traffic monitoring logs.

Why ODDS®?

Let Us Do All The Heavy Lifting

ODDS® is a mature delivery model with trusted brand software that allows enterprise-level services without the cost, complexity, or threat ingestion associated with on-premise messaging solutions. Because all **ODDS®** services are hosted "in the cloud," outsource managed, they are rapidly deployed, and externally maintained. With **ODDS®** your messages are auditable, recoverable, searchable, and disaster recovery protected.

ODDS® certified providers have the technical resources and core focus to stay ahead of emerging threats.

All **ODDS®** Delivery Partners are highly scalable, bonded and insured to protect our Solution Partners and their clients.

Easy To Provision & Simple To Manage

ODDS® is a hosted service that can be deployed immediately, within minutes of signing up. Our private label web portals are conveniently accessible from any browser and allow credentialed administrators and sub-administrators to manage your security settings, your users, under your own brand name, intuitively and easily.

Isolate Your Enterprise From Message Threats

ODDS® delivers the brand name security your business requires for email, IM, Web, and Network;

- CA Message Manager™
- **BlueTie**™
- ST Bernard iGuard™
- ***VircoM*** Modus™
- **ProtectPoint**™

Providing enterprise class services to monitor filter and stop threats is our core competency… doing it before they can infect your internal systems or blocking the threat while it's happening, makes **ODDS®** your best security option.

Securing Business Continuity & Disaster Recovery Mechanisms

ODDS® maintains secure off-site storage for all your communications so that you never lose an email or IM message. With **ODDS®** we spool email when your email server is down, re-delivering email when you're back up and running. Rest assured your data is secure and easily accessible, and redundant to internal continuity plans.

Reallocate Your IT Assets
Because we are hosted security solutions, we eliminate wasted IT resources on procuring, installing and maintaining complex internal security solutions.

Our affordable trusted services are implemented within minutes allowing your IT assets to monitor security reports and focus on the critical projects that grow your enterprise.

As technologies get more sophisticated and require specific IT dedication the old adage of internal is better isn't always the smart choice in today's network.

ODDS®… What We Do

Email Funneling

Email Filtering

Basic Message Care

Total Message Care

IM Security (Requires Bundling)

Web Filtering

Archiving

Managed Intrusion, Detection & Prevention

Email Funneling

Email Funneling is a "first pass" email processing strategy for businesses managing their own email servers and utilizing internal software for Spam and virus solutions.

Our strategy offers companies multiple methods of user authentication to verify that only legitimate mail is passed from our world class email data center to your email servers. DNS attacks, directory harvesting, and email bombs are defended at our data centers forwarding only user verified email, which can reduce your own email processing loads from up to 50%

Email Filtering

ODDS® Email Filter protects your enterprise from email attacks, spam, phishing, viruses, other malware and inappropriate messages before they reach your network. Within the minutes it takes to deploy **ODDS®** email filter, your perimeter spam and virus quarantine begins to build.

Email Filtering Details

Premium Spam & Virus Protection
Your email is filtered at world class NOC (Network Operating Centers) data centers using brand name proven processes that isolate threats. Millions of emails contribute to our honey pot evaluation process. We are able to detect email-borne threats and spam within milliseconds and forward threat free email on to you. Our 98.6% spam capture rate and .01% low false positive rates mean only legitimate email is delivered to your internal servers.

Quarantined Email

What are your **ODDS®** for never losing an email? Our uptime guarantees your email is delivered to your email server and in your "inbox" or safe and secure in your web quarantine 99.99%. Our filters do not use RBL's or blatantly block email. All email is quarantined or delivered. Administrators can block email into quarantine for oversize attachments, global blacklisting, or by IP address. The ability to adjust setting strengths, add to a white list or black list. Permissions are granular, even settings can be granted all the way to the end user by your administrator.

Reporting

Reports are accessible via the administration portal and consist of statistics which help with what you need to analyze ROI, plan for security upgrades or enhancements, or show a real-time snapshot of your email activity.

Custom Policy Settings

ODDS® email filtering employs many AUP controls. With comprehensive Spam categories to ensure scanning and content approval of all emails (inbound and if selected, outbound) based on your settings:

- ***Attachment Filter***
  This filter allows you to restrict and quarantine dangerous files by rejecting messages with certain types of file attachments.
- ***Content Filter***
  The content filter scans the email metadata, bodies, and imagery giving you quarantining messages based on AUP.
- ***Policy Filter***
  This filter blocks messages based on their size.
- ***Black/White Listing***
  Designations by domain or by user… form web console or emailed quarantine report.
- ***Custom Notifications***
  You can include headers and footers, notifications to administrators, senders or recipients to alert them of various filter actions.

Basic Message Care

Targeting massive volumes for hosted email options. **ODDS®** offers;

WebMail

- Private Label or Co-branded Web client
- SSL Option
- Email
  - i) Anti-Virus & Anti-Spam
  - ii) Attachments up to 25MB
  - iii) Retrieve external POP3 accounts
  - iv) Multiple aliases & email forwarding
- Custom domain support
- Personal Contacts
- Personal Calendar
- Tasks
- My Day At a Glance
- 5GB Universal Storage

Personal Email

- Private Label or Co-branded Web client
- POP3/IMAP4/SMTP support
- SSL Option
- Email
  - i) Anti-Virus & Anti-Spam
  - ii) Attachments up to 25MB

iii) Retrieve external POP3 accounts
iv) Multiple aliases & email
forwarding

- Custom domain support
- Personal Contacts
- Personal Calendar
- Tasks
- My Day at A Glance

5GB Universal Storage

Business Message Care

Business Class Email & Messaging

- Private Label or Co-branded Web client
- POP3/IMAP4/SMTP support
- SSL Option
- Web Mail
- Email
    - i) Anti-Virus & Anti-Spam
    - ii) Attachments up to 25MB
    - iii) Retrieve external POP3 accounts
    - iv) Multiple aliases & email forwarding
- Custom domain support
- Personal Contacts
- Personal & Shared Calendars
- Personal & Shared Files
- Tasks
- Mobile Device Synchronization
- Outlook® Synchronization
- My Day at A Glance
- Enterprise Manager
- Instant Messaging
- SecureSend encrypted file transfer
- Archiving & Discovery

10GB Universal Storage

****With the option to add Premium Email Filtering & Web Content Filtering*

Total Message Care

ODDS® Total Message Care is the complete bundling solution for **ODDS®**. We host your email; provide the complete security filtering services, give you work collaborative tools, remote device synchronization, and employ archiving.

Total Message Care Details

ODDS® Total Message Care allows you to easily host all of your data messaging needs from the same convenient Web interface. Targeted for small business like independent contractors, 5-20 users' offices, TMC is…

Hosted Email- POP3, IMAP, MAPI, & Web Mail

IM Filtering

Email Filtering

Web Filtering

Archiving

Shared Calendar, Contacts, Tasks

Mobile Device Synchronization

Outlook Compatibility

The most affordable comprehensive messaging security solution on the planet; **ODDS®** Total Message Care sets your entire messaging security solution "in the cloud"… you're enterprise computing requirements can be reduced to a PC, Microsoft Outlook software, and a high speed internet connection.

IM Security

ODDS® IM services secures IM activities. reducing unproductive chat is a bonus compared to capturing intellectual property losses, stopping unsecure file sharing, and managing libelous human behaviors. With

ODDS® IM you monitor, filter, block and can log* IM activities across your enterprise.

IM Filtering Details

Platform Compatibility

ODDS® IM Security can be an internal enterprise wide private IM solution or can support all the widely used IM platforms including AIM, Yahoo, and MSN Messenger. The ability to secure internal IM or public IM protocols are not break out solution but part of our Total Message Care Service.

Authenticated User Control

ODDS® Public IM Security requires registered user credentialing and matching anonymous screen names. This identification process allows you to cross reference IM users and their email addresses, giving you complete oversight of your network IM traffic users.

AUP (Acceptable Use Policy) Disclaimers

With custom definitions, you can automatically intervene chat sessions with a unique disclaimer messages when AUP policies are being abused. Enforcing AUP with active intervention enhances your policy enforcement efforts by notifying IM participants inside and outside your organization that the conversation is being monitored.

Content Filtering

Creating flexible enforcement is another way our **ODDS®** IM Filtering helps you structure your AUP. By allowing you to block specific words and phrases before they can be communicated, and by not blocking, you're in control. Because IM is a less formal way to communicate, enterprises may choose to loosen the guidelines they would normally apply to workplace language.

ODDS® IM Security manages inappropriate words and phrases and lets you add your own objectionable words list (OBL), formulas, letters, etc… to the blocked list.

AUP Abuse Notifications

When IM policy violations are detected, you can be notified automatically or have notifications sent to others in your organization.

File Share Block

Secure use of IM means protecting both your network and user by blocking all file transfers via IM, or selectively choosing files over a certain size and by type. **ODDS®** allows you customize and to meet your enterprises requirements.

Web Filtering

ODDS® Web Filtering is the world's best balance of protection and productivity. At default our web filtering service enforces common website viewing policies and allow for custom blocking, unblocking, with individual and grouping permissions. Powered by the world class award winning iGuard™ 100% human-reviewed database for unrivalled accuracy, objectionable website visits are censored within the minutes it takes to implement our service. Blocking undesirable websites is only a piece of the web filtering puzzle. **ODDS®** "in the cloud" Web Filtering secures your web viewing activities from damaging malware delivered via web browsers such as java script and other executables buried in click on pictures, links to other pages, etc… All browsing attacks are diffused and managed outsider your network perimeter.

Web Filtering Details

iGuard™ - World's Leading URL Database

ODDS® Web filtering is based on the award-winning iGuard URL database, giving you the power to accurately block sites by individual, group, or across your entire organization. Internet analysts continuously update the iGuard 100% human-reviewed database so that emerging sites can be added, categorized and blocked. You choose from the list of 11 categories allowing you to customize filtering to match your acceptable use and security policies.

Browsing Malware Defenses

ODDS® uses real time virus and spyware scanning engines to give you complete protection from malware entering via ports 80 and 443, the default ports for HTTP and HTTPS requests. This web filtering application is an overlooked value and much needed layer of Internet security.

Web Activity Reports and Logs

ODDS® logs all Internet activity on your network and makes the individual histories available in the easy-to-use Web interface. You can review Internet events across your organization or drill down to obtain information on groups or individual users.

Archiving

ODDS® Archive Solutions are differentiated by;

- Provisioning Choice- Hosted or Journalled
- Compliance Level; Litigation Support or full SEC/NASD Financial
- E-discovery Methods- granular versus generic search and report capability

Archiving Details

Message Storing (Provisioning)

Message volume can be stored with **ODDS®** via server journaling and storing on SAN server media, or performed on a fully hosted certified exchange platform and stored on Centera media for compliance. Either platform securely stores your data with perimeter safety, redundancy and adds efficiency by freeing your own network storage of duplicate or unnecessary files.

Compliance or Litigation Support

Whether journalled or hosted, our storage platforms assist with FRCP an exceed SEC/NASD mandates for compliance. The decision to enable your enterprise to affordably cope with legal requirements, HIPPA, SOX, FRCP, SEC is what **ODDS®** Archiving solutions are built for.

E-Discovery

Protecting your most important enterprise assets, your data, can be simple and often misunderstood as highly unaffordable. For most enterprises large and small, email, IM, and attachments files are at best recoverable from several devices PC, Laptops, PDA's, thumb drives, burned to disc or found on shared folders in servers at different locations.

With **ODDS®** Archiving your data communications are stored, organized, categorized, indexed, labeled, and fully "web base" recoverable, printable, exportable and usable. The reduction in Legal e-discovery expenses alone justifies **ODDS®** archiving over and over again.

ODDS® Archiving is all about choices and needs fulfillment. Our Archiving solution is a standalone email or a bundled email and IM offering with flexible retention strategies.

Managed Intrusion Detection & Prevention

Irrespective of your firewall capabilities, **ODDS®** MIDPS performs a multitude of necessities. From an IT resource perspective, **ODDS®** saves time, money, and reduces risk. Internal IT personnel cannot watch network traffic 24/7/365. An artificial intelligence (AI) solution can flag attacks, notify IT personnel, but can't "**in real time**" block all questionable traffic without excessive false positives.

Human analysis of the intrusion is the only way to properly assess and disarm all intrusions. When your IT staff is notified by AI, or they find an active intrusion via logs, they may not have seen the attack before thus know of a patterned solution to quickly diffuse the threat.

ODDS® MIDPS becomes your network eyes, ears and "live" traffic police.

Managed Intrusion, Detection and Prevention Details

- Detect a hack/intrusion in progress
- Provides the ability to block attacks in Real-Time
- Helps protect the network against mis-configured firewalls.
- Detects attacks that firewalls legitimately allow through (such as attacks against web servers).
- Protects systems with known vulnerabilities until the necessary patch can be installed.
- Managed compliance with corporate policies for network and protocol use by restricting protocols such as instant messaging and peer to peer networks.

PCI Compliance with MIDPS

ODDS® MIDPS meets requirements in the Payment Card Industry Data Security Standard focus on the ability to monitor and report on changes made across the IT environment. The standard requires not only that you achieve a secure state for you cardholder data, but that you be able to prove that state doesn't change over time.

Configuration Auditing meets these PCI requirements by:

- Confirming access to computing resources and cardholder data is limited to the proper individuals
- Validating that patches are deployed properly
- Alerting you to unauthorized changes to firewall rules
- Ensuring wireless network security policies are not circumvented
- Detecting new, modified, or deleted user IDs
- Maintaining file integrity across the entire enterprise

ODDS® MIDPS is responsible for detecting anomalous, inappropriate, or other data that may be considered unauthorized on your network. A regular firewall is configured to allow or deny access to a particular service or host based on a set of rules. If the traffic matches an acceptable rule, it is permitted regardless of what the packet contains. **ODDS®** MIDPS captures and inspects all traffic regardless of whether it's permitted or not. Based on the content of each packet, ODDS determines if it is safe or not. If it is dangerous, an alert is generated.

We ***Detect***, ***Alert***, and ***Block*** security threats including buffer overflows, stealth port scans, CGI attacks, SMB probes and NetBIOS queries, NMAP and other port scanners, backdoors, Trojans, and Microsoft operating system and application vulnerabilities, Dos clients, and many more.

Customizing your intrusion security configurations can be a dead end with hardened internal solutions as well, not with **ODDS**® MIDPS.

Marketing Strategy

Let your customers and prospect to try it! Earn a trial with your prospects because if they try it they will buy it.

Gain footprints with your customers and prospects with email funneling, up-sell to email filtering, add content filtering, and then add office collaboration for calendars, tasks, and contacts. Multiple services within **ODDS**® allow our partners to cherry pick and target footprint opportunities.

Prepare a cost/benefit analysis sharing the difference between how it's being done and how you can do it for them.

Go to Market Kit

ESS will help our members to customize any marketing collateral available through documents like the one you're reading… or any content we provide within our website.

ESS will provide the custom content to add to your website or sales tool to succeed. Visit our website www.aaserviceproviders.org and see what services can be rebranded for you….

The ESS logo is interchangeable with your Company logo;

http://aaserviceproviders.org/images/pdf/basicfilter.pdf

ODDS® "The" Network

Introduction

In 2000, ESS set out to change the way ISP business' collaborates on sharing resources. From the very beginning, ESS vendor relationships with products and services were negotiated to provide carrier-class reliability, scalability, security and private labeling to our ISP's members' and their millions of users. The following outlines ESS's physical system design and architecture and provides a high-level overview to the ESS **ODDS**® Infrastructure.

Physical Security

ESS **ODDS**® currently works with Tier-1 data center providers in addition to a our Master Delivery Partners' fully-owned and operated facilities to provide the highest levels of physical security for our hosting and managed services infrastructure. Having secure servers is of paramount importance; however, ESS feels that the physical systems and subsystems designed to protect the infrastructure are equally important. Our **ODDS**® primary facility is operated by an industry-leading telecommunications provider and is located outside of the metropolitan New York City area (company and exact location not disclosed for security reasons). This facility, in addition to **ODDS®** hosting application infrastructure is responsible for several high profile Web-based companies as well as backbone infrastructure for one of the largest local, long distance and network service providers in the United States. The physical infrastructure of this facility was designed to withstand both natural and man-made assaults and is guarded by highly trained security personal at all times.

Facility Access
Authorization for access and entrance into the facility consists of multiple layers of verification. The perimeter of the facility is protected by security gates which can be controlled only by security personnel within the building after the first video-based and access control list verifications have been completed. Once within the perimeter of the facility, security personnel again unlock the main doors for entrance into the lobby and mantrap area. This stage of authorization requires visitors of the facility to surrender any personal items, including cellular phones, packages, laptops and bags for inspection as well as surrender personal, government-issued identification for further verification. All authorized individuals are provided security access cards which then can be used to access the main data center floor.

Man Traps
When visitors enter an **ODDS®** data center, they must first pass through a man-trap system. This system is designed to capture the individual on video surveillance systems while also detaining the individual until further security verification can be completed.

Security Personnel
Upon successful verification of identity while in the man-trap system, security personnel who control physical access to the data center floor then greet the visitor and provide temporary access cards and cabinet/cage keys for physical access to the equipment once on the data center floor.

Access Logs and Key Tracking
The security personnel keep access control logs which detail the entrance and exit times of all visitors to the facility, in addition to real time access logs of every successful or unauthorized attempt to access doors within the facility with the issued temporary access card. Keys for customer cabinets and cages are available only to those who are on the ESS access control list. These keys are stored in a Key-Trax vault, which monitors security personnel’s access to the vault as well as the physical location of the keys at all times. All access control logs are available to **ODDS®** Master Delivery Partners for review.

Biometric Access Control Systems
Portions of the **ODDS®** data centers utilize state-of-the-art biometric scanning equipment for access to highly sensitive and restricted areas. These thumbprint or hand identifications provide the highest level of security and report access attempts to the central access control logs and to ensure only authorized individuals can access these rooms, a minimal number of operations staff are enrolled into these systems.

Continuous Video Surveillance

Our primary data center operates in excess of 100 high-resolution, 360 degree, pan, zoom and tilt cameras. More than 20 cameras of similar abilities are located in alternate **ODDS**® facilities. These cameras record all movement in the facility 24x7x365 and can be enabled for remote administration and surveillance purposes. Access to these video files can be granted at the request of authorized **ODDS**® Master Delivery Partners.

Motion Sensors

Motion sensing equipment in the data center is linked to the video surveillance system which in turn automatically alerts security personnel of movement within the facility and as well as repositions cameras in the direction of the motion to ensure this movement is captured.

Environmental & Power Controls

ODDS® data center facilities are fitted with industry-leading power and environmental controls to ensure proper operating temperatures, humidity, backup and clean power are available at all times. The primary facility operates on two independent power grids which supply utility service to the facility. This utility service is then conditioned and sent through UPS systems which then feed each of cabinets on A and B UPS systems. This design, also known as a “wet-power” infrastructure ensures that cutover to battery backup systems is instantaneous and eliminates any potential for failure during a cutover procedure from utility to backup power. **ODDS**® architecture requires that all systems housing customer data are cross connected to both the A and B power feeds provided in rack enclosures. This ensures that the unlikely event of loss of power on one half of the grid will not affect these systems. Clustered systems are dispersed amongst the grids to ensure that no single cluster of systems can fail as a result of a grid failure. In the event of a utility failure, the primary data center is fitted with 3 – 3 Megawatt diesel generators which are immediately engaged via transfer switch mechanisms in the event of a utility power outage. These generators supply power to the UPS system to restore depleted battery systems and provide constant power to cabinets and rack enclosures. Similar infrastructure exists at the alternate data center location, both of which maintain a diesel supply sufficient to provide power to the facility continuously for multiple days. Contracts and arrangements are in place with multiple diesel providers should a situation arise where a long haul outage is imminent. **ODDS**® primary data center facility utilizes Liebert 40-Ton air handling systems, positioned throughout the facility to provide cooling to servers. This glycol, chilling tower system is designed to utilize cold-northeast temperatures during winter months to chill the facility, while in the summer months utilizing the cooling tower systems. Cooled and dehumidified air is pumped throughout the facility in an intricate under-floor system which duct out of the floors directly in front of server equipment, allowing this equipment to pull cool air through the server chassis and exhaust through the rear of the cabinet. These systems are computer controlled to maintain a constant operating temperature of 69 – 71 degrees at all times, with relative humidity ranging from approx. 53 – 61%. In addition to data center monitoring systems of these environmental controls, additional sensors are installed throughout the facility and immediately notify operations personnel of any fluctuation in temperature so that appropriate actions may be taken.

Network Infrastructure
ODDS® network infrastructure has been designed with security and scalability in mind. Using industry-leading suppliers of routing, switching, load balancing and firewall equipment to ensure a secure, optimized and low latency network for internal server communication and connection to the backbone infrastructure, ultimately connecting to the Internet.

Peering Relationships
ODDS® Master Delivery Partners' contract with our primary data center provides us with access to several major ISP network gateways to the internet. A combination of multiple OC-192, OC-48 and OC-12 connections from multiple carriers, routed across both primary and secondary feeds to The perimeter routing equipment provides **ODDS®** with extremely high redundancy to the Internet. Our alternate data center facility is serviced by two major ISPs equipped with automatic failover mechanisms.

Routing Infrastructure
ODDS® utilizes Cisco carrier-class routing systems to connect our data centers to backbone networks which supply the Internet access to the services application. These routers are configured for automatic failure between primary and secondary networks, to ensure packets are routed efficiently and through the most readily-available network.

Firewalls
ODDS® uses a combination of Cisco PIX and SonicWall firewall technology to ensure our network infrastructure is secure from perimeter attacks to the **ODDS®** network. Our firewalls and security control mechanisms control access to specific ports, provide deep-packet inspection, DOS/DDOS prevention, IP filtering and more.

Switching Infrastructure
ODDS® utilizes Cisco carrier-class switching equipment to provide aggregate connectivity to our server infrastructure. These switches are equipped with fully-redundant processing modules and power supplies to provide high levels of availability. The switching infrastructure is fully-meshed with multiple, redundant pathways between switches to ensure a single failure does not compromise the entire infrastructure.

Load Balancing
ODDS® application and network infrastructure relies on F5 Networks load balancing technology. This technology is specifically configured to constantly monitor all network and server services and actively remove equipment and reroute connections should a failure occur within the infrastructure. This equipment allows **ODDS®** Master Delivery Partners to failover stateful connections to alternate standby systems to ensure customers can continue working with the applications without interruption.

Inter Data Center Connectivity

ODDS® data centers are connected using virtual private network systems. These systems allow for the seamless, encrypted communication of servers and operators between facilities. Remote administrative access to **ODDS®** systems is also accomplished using the VPN system.

Systems Infrastructure

ODDS® Master Delivery Partner's systems infrastructure has been designed from the beginning to support high levels of customer utilization and large volumes of incoming and outgoing messaging. **ODDS®** approach to system architecture and high-availability includes the use of clusters of servers built on low-end commodity hardware, brought into and out of service by "smart" load balancing technology which can detect failures at the system and service level. This approach allows **ODDS®** Master Delivery Partners to operate substantially more servers, all performing the same action, thereby reducing the potential for a single server to cause noticeable application outages to the end user.

Front-End Application Servers

ODDS® front-end application servers, built on ultra-reliable Linux/Apache platforms are designed to deliver the browser based services. These stateless systems are responsible for service page and image content as well as assembling the presentation layer of the application interfaces. Each of these servers is monitored for uptime, performance and overall availability by our central monitoring systems which are responsible for notifying IT Operations personnel of outages or other server problems in addition to being monitored by our load balancing system which is responsible for automatically removing systems from service should they encounter any problems. Upon a server being removed from active service by the load balancing equipment, this equipment also seamlessly transfers the connections from the customer to an alternate node that is available thereby eliminating any noticeable outages or errors within the collaboration system.

Customer POP/IMAP and SMTP Servers

ODDS® operates a large cluster of POP/IMAP and SMTP servers which are responsible for providing these services to users who which to use more traditional desktop clients such as Thunderbird, Outlook or Outlook Express. Similar to the front-end application servers, these systems are also monitored for performance by our central monitoring system, in addition to our automated load balancing solution. Outages in these clusters are handled in a similar fashion as the Front-End Application Servers.

Inbound and Outbound SMTP Servers

ODDS® manages five clusters of servers responsible for the transit of messages between service providers. Our inbound SMTP cluster is responsible for accepting connections from other service providers on the Internet, applying perimeter level spam detection (RFC compliancy checks). Inbound servers then handoff email to our SPAM and Virus filtering systems for analysis before ultimately being delivered to the users INBOX. The outbound SMTP cluster is responsible for sending mail outbound to other service providers from **ODDS®** users. This cluster also performs some perimeter level SPAM detection to ensure **ODDS®** users are not violating TOS agreements.

Databases

ODDS® utilizes two primary database platforms to store user data and various information regarding user accounts, Oracle Enterprise 9i and PostGres. These systems are configured in redundant, fully-replicated pair clusters to ensure all data is available to users at all times. Data is committed to the primary "active" server and then committed on the secondary "standby" server. In both platforms, automated failover mechanisms allow the databases to switch between active and standby quickly and without operations personnel intervention to ensure systems are online and available at all times for customer access to data.

LDAP Directory Services

ODDS® core application, email, is designed around a complex directory system housed in LDAP. This directory is responsible for providing the necessary information to processing systems so that they may route email to the appropriate destination. **ODDS®** operates a large cluster of "read-only" LDAP servers which provide processing systems rapid access to data, and also operates a pair of "master" servers, which are responsible for storing changes or entries to LDAP data, and then replicating down to the "read-only" cluster.

Mail Storage Servers

ODDS® Mail Storage servers are custom built using enterprise class Red Hat operating systems. These systems are responsible for the storage of user email and attachments as well as the indexing of those emails for fast retrieval and display to customers using the web interface. The systems are built fully redundant and utilize RAID-5 disk arrays to ensure reliable storage of user data. The mail storage servers deliver user email to the web application as well as customer POP and IMAP servers. These units are backed up using enterprise class backup and restore technology to large scale disk arrays for recovery purposes.

Write us at ODDS®

ODDS
ON DEMAND DEFENSE SERVICES

For more information on any of our **ODDS®** services or to contact a certified **ODDS®** Delivery or Channel Partner write us at…

ODDS@emailsorting.com