Newsletter

CONTINENT 8 technologies
reliable innovation

In this issue, we focus on one of the key features of Continent 8 Technologies' recently launched Cloud Backup solution. We take a closer look at DDoS attacks and highlight the growing importance of protecting your business from these threats. There's also an overview of our latest facility in New Jersey, but first here's a roundup of various Continent 8 developments around the globe.

Issue 6 Spring 2014

In this issue

Global growth, local focus

Isle of Man expansion

To support our growth and success in the Isle of Man, we have just completed the build of a new data hall, adding 40 additional high-density racks to the footprint. The new expansion is the most efficient on the island, utilising the island's first adiabatic cooling architecture and advanced contained hot aisles.

Gibraltar electrical upgrade and data hall expansion

To cater for increased demand, and to stabilise future infrastructure in Gibraltar, Continent 8 is in the final stages of replacing all electrical infrastructure representing significant investment to support expansion. The facility upgrade will also coincide with the addition of two new data halls offering an additional 70 rack availability.

New Jersey launch

One of the most significant milestones in Continent 8's ongoing global expansion was the recent launch of the New Jersey data centre. The facility, which is located in Atlantic City, opened in January and offers the full suite of Continent 8 services to licensed gaming operators and providers in this newly regulated market. Continent 8 will continue to add services and locations to support the gaming community, with several projects currently under consideration. You can read more about the New Jersey facility on page 4.

New bigger London office

At ICE last year we announced the opening of our London office. It made perfect sense to open an office in London with so many eGaming companies based out of the city. London being an international gateway meant the team is only a flight away from our international customer base. We have quickly outgrown this and have recently moved to a new bigger office in North Row, W1.

In addition to the existing London team, Andy Davies joined Continent 8 in the position of Solutions Architect early in January. Andy's addition bolsters our pre-sales function supporting the sales and marketing team. Andy has previously been a pre-sales consultant at Symantec.Cloud, and led the Business Application Team at HP UK.

An additional account manager has been appointed and will be joining the London office soon.

These additions to the team will allow the company to continue to build on the existing relationships within the industry and further develop solutions to meet our customers' future business objectives.

Dublin expansion

Continent 8's EMEA Service Operations Centre in Dublin has continued to grow. Now a dedicated 10-strong team is providing first and second line global support services alongside our existing centre in Montreal.

Recent recruitment includes Systems Administrators, Security Specialists and dedicated Project Management resources. These appointments are all key to ensuring the continued smooth delivery of our managed services portfolio and to support the rollout of new products and services planned for 2014.

Continent 8's latest Data Centre opens in New Jersey

See full story on page 4.

Cloud Backup

Critical, Connected, Convenient

IT departments are under a constant and growing pressure to meet evolving regulation, provide effective disaster recovery procedures and meet the challenge of unprecedented data growth. At the same time, many departments are expected to save or limit costs, but is it possible to become more effective on reduced budgets? We think so...

What is "Agentless Backup" and why is it so good?

Continent 8's Head of Product, **Stephen Trimble** takes a look at just one of the key features of Continent 8's recently launched Cloud Backup solution…

Backup and recovery software typically requires an 'agent', a small piece of software to be installed and running on every server that an enterprise needs to backup.

Even in a modest-sized environment, agent management can become extremely complex when a systems administrator is forced to deal with different operating systems and revision levels. The complexity of agent management is further complicated by the growing number of applications that also require agents running on the same servers.

In addition, dealing with backup software agents is a cumbersome and mundane task that can be extremely time consuming. Matching agent revisions with operating system levels, researching compatibility issues, negotiating with security issues and other labour-intensive tasks are commonplace, and a frustration for any technical resource.

Additionally, many problems that occur while managing backup software in complex environments are due to compatibility issues with agents that's before they are running when they notoriously reduce the amount of processing power available to the core applications of every machine on which they're installed.

The problems with Agents

- ✗ Compromised security.
- ✗ More pieces of software to manage and to fail.
- ✗ High Licensing fees.
- ✗ Mounting administrative costs.
- ✗ Application disruption.

The benefits of Agentless Backup

- ✓ Significant savings.
- ✓ Simple licencing.
- ✓ One piece of software to install, manage, and diagnose.
- ✓ WAN/LAN/CPU resource conservation.
- ✓ Robust, hardcoded security.
- ✓ Elegant scaling.
- ✓ Backup consistency, improved recoverability.

So, how does it work?

Continent 8's Cloud Backup solution does not require any agents to be installed, but instead reaches out over the network to backup operating systems, file systems, and applications, using industry-standard programming interfaces, which inherently makes it easier to install and support than other backup and recovery solutions.

Our software eliminates the requirement for locally installed agents because it leverages the protocols, APIs, methods and functionalities that platform, operating system, database, and other application vendors utilise for remotely managing their own systems.

Other backup and restore solutions require a unique backup agent (installed on every target machine) for each type of system and application. We, however, support all major platforms and applications with a software system composed of just two major components: the DS-Client (one installed at each site) and the DS-System (installed within a secure Continent 8 Data Centre).

Another advantage of Cloud Backup is that it enables multi-level access controls. At installation, the DS-Client is assigned privileges to establish access rights that meet the requirements of the site or organisation.

The software has also been highly optimised to conserve both LAN and target-system CPU resources, any customers who also have systems in a Continent 8 data centre can leverage the private network for backup traffic – reducing overhead on the network. Therefore, Implementing Cloud Backup can produce immediate and dramatic benefits.

Agentless Backup is just one of the many features which make Continent 8's Cloud Backup service 'revolutionary'. When coupled with compression, de-duplication and encryption the overall solution is truly, a new way of thinking about backup.

Keeping the Lights On

The Importance of DDoS Defence in Business Continuity Planning

Today's enterprises are increasingly motivated to formalise IT security and place it firmly within the context of enterprise risk management and business continuity planning. Current financial realities require that companies incorporate IT security into their operational and financial planning to control escalating costs. At the same time, they must provide adequate resources to address their financially, regulatory and reputation-driven security priorities and incorporate all pertinent risk factors into their organisational security model.

The abstract nature of risk management and business continuity planning can often make these processes daunting to planners and IT security professionals alike. In most cases, business continuity plans include detailed policies and procedures for keeping operations running in the wake of natural disasters such as fire, floods and earthquakes. But rarely do they incorporate contingencies for IT security incidents. This is a major oversight. Security incidents often have a negative impact on business operations resulting in significant operational expenditure costs, lost revenues, customer satisfaction challenges and an erosion in brand reputation. As a result, IT security issues constitute significant business risks, which place them squarely within the realm of business continuity planning and disaster recovery.

The most important aspect of enterprise security, availability, is the most easily understood and quantifiable aspect of security today. This means that organisations can readily establish the economic and reputational necessity of maintaining availability in the face of attack and the costs of failing to do so.

DDoS Attacks: Background and Context

Distributed denial-of-service (DDoS) attacks are attempts to consume finite resources, exploit weaknesses in software design or implementation, or exploit lack of infrastructure capacity.

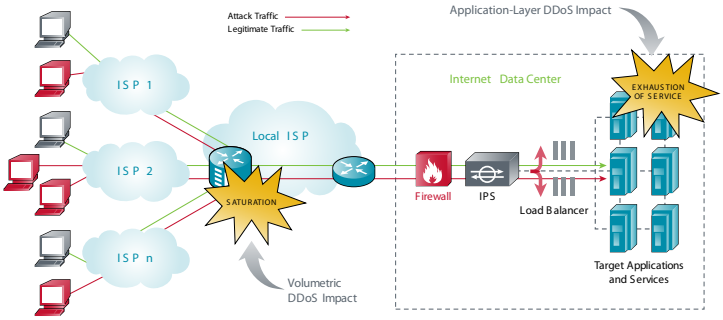
DDoS attacks target the availability and utility of computing and network resources; if a DDoS attack against a Web server, DNS server, email server, application server or other online property is successful, the availability of the target of the attack is negatively impacted.

DDoS attacks are typically launched by botnets, which are collections of compromised computers utilised by attackers without the knowledge of their legitimate owners. Hundreds of millions of botted computers are on the Internet and enterprise networks today. They represent a major threat to organisations with an online presence due to the near-infinite computing power and bandwidth available to attackers who leverage botnets to launch DDoS attacks
DDoS can be thought of as man-made disasters, the threat to availability represented by DDoS attacks cannot be overstated.

No business continuity plan is complete without taking into account the need to maintain the availability of critical online properties, even in the face of a concerted attack.

Traditional security solutions such as firewalls and intrusion prevention systems (IPS) do not provide a DDoS mitigation capability. These devices are focused on maintaining confidentiality and integrity of organisational systems and, by their very nature, do not provide availability protection.

However, companies can successfully detect, classify, trace back and mitigate DDoS attacks with appropriate operational best practices and dedicated anti-DDoS solutions. Any enterprise risk management model and business continuity plan must account for DDoS attacks.



Continent 8 can help mitigate your operational risk from DDoS attacks

Retaining the risk, or simply absorbing DDoS attacks and their negative impact on availability, is not a viable strategy due to the overwhelming resources controlled by determined attackers. In an era of 100 Gigibit/sec-plus DDoS, attackers can potentially overwhelm any organization. Therefore, more proactive measures are required.

Helping to reduce the operational risk of DDoS attacks is enabled by the DDoS attack detection, classification and mitigation solution from Continent 8. By providing carrier level 24×7 monitoring, full help desk support and escalation, backed up by comprehensive online portal access for analysis and reporting, you have full visibility and transparency.

Our DDoS prevention is a transparent, fixed fee service, uniquely – your financial commitment is known and budgetable, not a "blank cheque" service where the organisation is exposed to potentially unlimited costs during or after an attack.

In summary, risk reduction is the single most important strategy for mitigating the operational risk represented by DDoS attacks. It should be a key part of business continuity planning for maintaining availability in the face of determined DDoS attacks.

CONTINENT 8 technologies

reliable innovation

continent8.com

New Jersey

Continent 8 has announced the launch of its suite of hosting and managed service offerings to the New Jersey market, bringing to 10 our data centre offerings worldwide. Prior to the introduction of the recently introduced online gaming regulations, Continent 8 has been working with all facets of the industry in New Jersey to bring a neutral co-location and managed services offering to the market. Continent 8 has established a hosting centre in one of the licensed premises in Atlantic City and this offers the benefit of allowing operators and providers to serve multiple locations and brands from one independent location into the newly regulated market.

From our hosting location in Atlantic City, Continent 8 will bring our full range of offerings to the market. As with our other offerings around the world, Atlantic City is being incorporated into our global private backbone with diverse links into Northern New Jersey and New York thus allowing our customers to link back into other markets and locations from which they operate.

In addition to the standard co-location and managed service offerings, Continent 8 is offering customers its DDoS Prevention and Cloud Backup services. Continent 8 has been offering DDoS prevention services to our customer base for many years and this is a very important offering to a new and evolving online gaming market. In contrast, our new Cloud Backup service is based upon Asigra, a leading cloud backup, recovery and restore software provider and it allows for flexible data recovery options and the ability to support rigorous data compliance requirements for the online gaming sector.

Secure Networks

Reliable, Fast, Secure

Contacting Continent 8

Sales

Europe
+44 1624 694625
North America
+1-514-461-5120
Asia
+65 6505-9795
sales@continent8.com

Technical

Europe
+44 1624 694611
North America
+1 514 461 5111
Asia
+65 6505 9791
support@continent8.com

Headquarters

Continent 8 House
Pulrose Road, Douglas
IM2 1AL
Isle of Man

Tel. +44 1624 678 888
info@continent8.com