

# The Milestone Review

**milestone**  
systems, inc.



**M**ilestone Systems provides specialized technical consulting services and Internet management/security solutions. *The Milestone Review* is designed inform you about industry trends and ideas, as well as Milestone's products and services. If you have any suggestions or comments, please e-mail us at [newsletter@milestonesystems.com](mailto:newsletter@milestonesystems.com).

## **Stories in this issue:**

### **Application Delivery in a Box**

F5's new BIG-IP platform enables organizations to consolidate their data center infrastructures, reducing costs and carbon footprint while increasing IT agility.

### **Virtualization Going Mainstream**

A majority of companies have adopted server virtualization.

### **Oversights Expose Network Gear**

Nearly three-quarters of all networking devices have known security vulnerabilities that may expose organizations to external and internal security attacks.

### **Controlling Access**

Identity management helps organizations meet security and regulatory compliance requirements.

### **Once and For All**

Data de-duplication streamlines backup.

### **Effective E-mail Management**

An e-mail retention policy and archival solution helps protect against legal, regulatory and business risks.



---

## Application Delivery in a Box

**F5's new BIG-IP platform** enables organizations to consolidate their data center infrastructures, reducing costs and carbon footprint while increasing IT agility.

“Consolidation” is one of the biggest buzzwords in the IT industry — and with good reason. Many data centers are filled to capacity with legacy equipment as a result of the “scale-out” strategies of the past decade, coupled with the deployment of numerous single-function appliances, creating an IT infrastructure that is inflexible and difficult to manage. By consolidating that equipment onto advanced, scalable platforms organizations can reduce costs dramatically while improving IT agility.

When it comes to optimizing application delivery, F5's BIG-IP product family allows organizations to consolidate multiple single-function devices onto one highly scalable and flexible platform. BIG-IP provides high availability, improved performance, application security and access control, all in one unit that is adaptable and easier to manage.

The new F5 BIG-IP 8900 hardware platform takes those capabilities to the next level. With 12Gbps of L7 throughput, 58,000 SSL transactions per second and 8Gbps of hardware compression, the 8900 enables the functional and physical consolidation of

application delivery infrastructures, reducing management expenses and TCO. The new platform also comes standard with Fast Cache, IPv6 Gateway, Rate Shaping, SSL Offload and Intelligent Compression features to help organizations maximize the value of their investment without adding more appliances. Combined with F5's unified TMOS architecture, which gives BIG-IP platforms total visibility, scalability and control across all services, the new 8900 system provides customers with more options to meet their changing needs.

“The new BIG-IP 8900 platform helps reduce power, space and cooling requirements, and the associated costs,” said Terry Shidla, CISSP, Milestone Systems. “With this new platform, organizations can support extremely high levels of application traffic and integrate advanced optimization and security capabilities. In addition, the 8900 hardware supports the new BIG-IP version 10 software, providing an ideal platform to unify application and data delivery services.”

### *Boosting Efficiency*

BIG-IP version 10 software helps organizations align IT and business by streamlining application delivery, reducing capital and operating costs, and improving workforce efficiency. BIG-IP v10 unifies application security, optimization and acceleration onto a single device, paving the way for organizations to establish a more dynamic IT infrastructure.

“BIG-IP v10 redefines how application, server, storage and network resources are aligned and managed to deliver services that fluidly adapt to changing business requirements,” said Shidla. “These services provide an agile framework of simple and efficient mechanisms to integrate emerging dynamic computing models, such as virtualization, cloud computing and software as a service, without having to completely re-architect existing systems.”

F5's unified and integrated approach to application delivery offers as much as a threefold improvement in IT staff efficiency through rapid deployment, on-demand services and tools that reduce training and administrative time. In addition, by unifying, consolidating, virtualizing and optimizing the application delivery infrastructure, customers can save more than 50 percent on hardware, power, space and cooling costs.

“A dynamic infrastructure is able to understand the context of an application, its deployment environment and its users, and thus apply relevant policies to optimize the delivery of that application,” Shidla said. “By unifying application services — such as optimization, security, acceleration and more — across a dynamic infrastructure, F5 solutions enable organizations to implement a comprehensive solution that is intelligent, consolidated and resource-efficient. BIG-IP v10 builds on F5's existing context-aware capabilities with its



---

unique iSessions framework, which creates a secure site-to-site connection between two symmetrically deployed BIG-IP devices.”

### **Unified Solution**

BIG-IP v10 helps customers unify individual devices onto a single solution, consolidating the application delivery infrastructure three to one. BIG-IP Local Traffic Manager, BIG-IP WebAccelerator and BIG-IP Application Security Manager modules now all run natively on F5’s TMOS plug-in architecture, giving customers the means to secure and accelerate Web applications on a single BIG-IP device. IT staff can now efficiently support multiple customers, applications, and business units — on the same device — through the BIG-IP device’s network virtualization capability.

BIG-IP v10 offers enhancements and new features designed to simplify management and improve the productivity of those managing BIG-IP devices. Highlights include integration with existing authentication systems, at-a-glance dashboard monitoring capabilities, and a rich library of Application Ready Templates. The templates are designed to simplify the creation of profiles, policies and other pertinent configuration parameters needed to optimize a BIG-IP deployment with specific applications, such as Microsoft SharePoint

2007, Exchange Web Access 2007, VMware View, Oracle Application Server 10g and SAP ERP. By using these templates, setup time can be reduced from several hours to a few minutes.

“Today’s IT departments are being asked to scale back their budgets and, at the same time, deploy new applications that will drive revenue and increase workforce efficiency,” said Zeus Kerravala, SVP of Enterprise Research at Yankee Group. “IT is under tremendous pressure to lower operating costs while demonstrating immediate value for capital expenses. To succeed, IT organizations require flexible solutions that can consolidate legacy equipment and establish a forward-looking application delivery environment that can be aligned to business goals. Advanced Application Delivery Controllers like F5’s BIG-IP solutions help support the changing demands of the business by optimizing the IT infrastructure. ##

## **Virtualization Going Mainstream**

A majority of companies have adopted server virtualization, and a small but growing number of firms are piloting cloud computing initiatives, according to a survey by Forrester Research. The survey of 2,600 technology decision-makers in the U.S. and Europe is Forrester’s largest annual survey of emerging hardware trends for both enterprises and small and medium-size businesses (SMBs).

The survey found that 54 percent of enterprises and 53 percent of SMBs have implemented x86 server virtualization or are doing so within the next 12 months. In addition, enterprises report virtualizing 31 percent of their operating system (OS) instances today, and SMBs have virtualized about 36 percent of their OS instances. In two years, enterprise respondents expect to virtualize an average of 54 percent of all OS instances, while SMB respondents expect to virtualize 61 percent of all OS instances.

Firms surveyed showed growing interest in pay-per-use hosting of virtual servers, one of many types of cloud service offerings in the market. Five percent of enterprises and 2 percent of SMBs have already implemented pay-per-use hosting of virtual servers.

“These survey results demonstrate that firms large and small are in the midst of rethinking



---

and overhauling IT infrastructure and client systems, with new approaches for greater flexibility, efficiency and performance,” said Frank E. Gillett, vice president and principal analyst at Forrester. ##

## Oversights Expose Network Gear

Nearly 3/4 of all networking devices have known security vulnerabilities that may expose organizations to external and internal security attacks, global IT solutions and services provider Dimension Data claims. In its recent “Network Barometer Report,” the firm also says that each device deployed — such as a router, gateway, switch, etc. — has an average of 30 configuration errors, despite the fact that there are widely published and recommended standards to safeguard against these problems.

“While the implications are alarming, the problems we uncovered can often be easily addressed,” said Rich Schofield, global business development manager, Network Integration, Dimension Data. “The most basic protection measures against threats that could harm an organization, such as having proper access and password configurations, are simply not in place. It’s the functional equivalent of leaving the doors and windows unlocked when you leave home. Organizations must take action now, working to shore up their networks before they incur reputational or shareholder damage.”

Other major issues reported include expiring support and aging equipment. The report says that 43 percent of all network equipment reviewed was found to be at least at end-of-sale status, signifying increased difficulty in purchasing spare parts. Of that equipment, 56 percent was beyond either end of software maintenance or last day of support. ##

## Controlling Access

Identity management helps organizations meet security and regulatory compliance requirements.

Each of us has multiple identities — personal, consumer, business. To his family a man might simply be “Sam,” but to his employer Sam is a complex array of user IDs, passwords and access privileges across numerous network resources and applications. When you consider that Sam’s is just one of hundreds or thousands of identities within an organization, you begin to understand the challenge of identity management.

Faced with growing numbers of end-users who require access to IT resources, many organizations devote significant time and effort to the task of adding, changing and deleting user information and permissions. In many cases, user identities must be manually

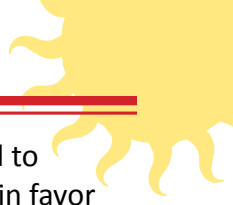
updated across disparate applications and resources, leading to data entry mistakes and delays that impact end-user productivity and increase the risk of internal security breaches.

Worse, delays in terminating access privileges when an employee leaves or changes positions can trigger red flags in a compliance audit. Auditors also look for instances where password policies and access controls aren’t uniformly enforced — such as when rights to access the purchasing system enables access to accounts payable.

## Granting Permission

A growing number of regulations are forcing organizations to more tightly restrict information access and to document the internal processes and IT controls in place to prevent unauthorized access to sensitive information. What’s more, organizations affected by these regulations have to generate an audit trail that proves compliance to internal or external auditors.

These kinds of regulatory pressures are compelling investment in identity and access management (IAM) solutions. IAM systems can help relieve these problems and improve the integrity of business processes by providing a framework for managing users and their access privileges across the enterprise.



---

IAM tools include user provisioning, password management, strong authentication, single sign-on and other technologies, which are increasingly bundled into comprehensive platforms. They are designed to streamline the creation, maintenance and use of digital identities, integrating business processes with the supporting technology needed to effectively manage end-user attributes, credentials and entitlements.

IAM solutions help organizations assure that users — employees, customers, distributors or partners — have secure and seamless access to the applications and other resources that correspond to their profiles. Such solutions not only aid enterprise security and regulatory compliance but also make it easier to assign privileges to large groups of users and to manage those groups more easily.

### *Many Benefits*

Effective identity management can help organizations automate user management and roll out self-service solutions, potentially saving millions of dollars per year in help desk-related costs. According to Gartner, a 10,000-person enterprise can achieve savings of about \$3.5 million in a three-year period by implementing an automated end-user identity provisioning system, primarily by cutting thousands of hours of IT and help desk time.

IAM solutions can also improve security by ensuring the confidentiality, integrity and availability of IT resources. Given that employees are responsible for more than 70 percent of unauthorized access to information systems — and more than 95 percent of intrusions that result in significant financial losses — organizations are rightfully concerned about controlling access privileges.

Growing numbers of remote and mobile users, as well as contractors, suppliers and others who need access to enterprises systems, have complicated identity management. As access needs extend beyond the trusted network, organizations must utilize federated identity solutions to control which internal resources the external identities can access.

### *Comprehensive Approach*

The ultimate goal of secure identity management is the application of corporate policies onto enterprise systems to ensure that users have appropriate access to the right resources at the right times. But that goal can't be realized without a comprehensive, strategic approach that considers all aspects of the identity infrastructure.

Identity information across an organization must first be integrated — but with respect for authoritative sources of identity. For example,

it's not realistic to force HR personnel to stop using their internal applications in favor of a centralized identity repository and its associated interfaces. Standards are slowly being adopted within the identity management space, but most implementations still require substantial application integration efforts.

The prospect of implementing a secure identity management solution can be an imposing challenge for many enterprise customers. Not only are there significant technological and political considerations but many identity management offerings are limited-purpose, addressing only provisioning or single sign-on, instead of the greater problem. Deploying these “silos” of identity often only makes the situation worse.

On the other hand, a comprehensive approach to identity management ultimately makes the entire network infrastructure more secure and easier to manage. Whether contained internally or spreading across the extended supply chain, identity management is becoming a near necessity for organizations with ever-increasing numbers of end-users, applications and information resources. Many organizations are adopting IAM solutions because of regulatory compliance demands, but quickly realize the benefits of efficiency, security, flexibility and scalability. ##



---

## Data De-duplication Streamlines Backup

The face of business continuity planning has changed over the years. As recently as the 1990s, most organizations focused on “disaster recovery,” which typically involved shipping nightly backup tapes to a remote site for safekeeping. In the event of a disaster, IT personnel retrieved the tapes and took them to a remote data center to restore operations. Recovery time was measured in days.

Now, however, organizations of all sizes are coming to the conclusion that disaster recovery is not sufficient. Even a few hours of downtime can be incredibly costly. As a result, more and more organizations require disaster-tolerant solutions that not only protect critical data but enable operations to continue without a blip.

The good news is that the cost of business continuity solutions has dropped dramatically. Not so long ago, only the very largest organizations could afford to replicate data to a secondary data center. Today, many midsize and large organizations have two or even three data centers, with data and applications mirrored to remote sites in real time. And now virtualization technology is allowing even small businesses to set up remote recovery sites.

Unfortunately, even the most sophisticated backup solutions cannot keep pace with the vast amounts of data to be protected in today’s environment. That’s why organizations need a data de-duplication solution as part of their backup strategy.

### *One Out of Many*

Also known as global compression, commonality factoring and referential integrity, data de-duplication eliminates redundant copies of data to reduce storage costs and shrink backup and recovery times. It also makes wide-area backup an operational reality. Since only de-duplicated data moves across the WAN, organizations can securely replicate vital data without high bandwidth costs or physical transportation risks.

Data de-duplication solutions can be used in-line as the data is backed up or after the backup has been completed. Although computationally intensive, in-line data de-duplication dramatically reduces the amount of storage space required for backups because only globally unique blocks of data are saved on the backup disk. Also known as storage-based data de-duplication or single-instance store, it makes disk-based backup more cost-effective, enabling organizations to eliminate backup tapes and mitigating the risk associated with shipping tapes offsite.

Source-based data de-duplication further optimizes the backup environment. Data is “fingerprinted” at the source before it is backed up to disk so that only data that has changed is sent across the wire, reducing the load on the network up to 95 percent.

Data de-duplication can play a major role in a broad range of applications for protecting and retaining data, including long-term archiving, continuous data protection and secure retention for compliance. It offers significant advantages for applications that benefit from efficient data transmission, including remote replication and WAN optimization. With data de-duplication, organizations can take full advantage of the latest data protection solutions for disaster tolerance.

### *Virtual Solution*

Data de-duplication is also essential for the virtual server environment, which further increases the complexities of data backup even as it facilitates disaster recovery. Traditional backup products are simply not designed for servers that may support as many as 128 virtual machines (VMs).

All VMs share a single physical host with finite resources that generally are fully allocated to maximize application performance. As a result, I/O- and network-intensive backup processes place a strain on the minimal system resources



---

that are available. Backups need to be reengineered with these constraints in mind.

Storage-based and source-based data de-duplication technologies combine to create the VM-optimized backup environment. First, only unique data segments are backed up, with 20-byte identifiers pointing to duplicate instances. Then new data segments are identified and backed up.

Data de-duplication has come to the forefront as a way to reduce the amount of disk space required for backups and to support bandwidth-constrained branch office backup. Virtualization is the next frontier for this technology. Minimizing the amount of data to be backed up minimizes the load on virtualized systems. As an added benefit, data de-duplication supports green IT initiatives by reducing space and power requirements within the storage infrastructure. ##

## Effective E-mail Management

An e-mail retention policy and archival solution helps protect against legal, regulatory and business risks.

If your organization were the target of litigation or a regulatory investigation, you'd likely be required to produce financials, customer records, contracts and related documentation, right?

Not so fast.

All of those e-mails zipping through your messaging system would also be subject to scrutiny. That's right: you would be forced to sift through all of the forwarded jokes, gossip, lunch invitations and other purely social messages to find those relating to the legal or regulatory issue in question. Worse yet, this process could yield messages that might prove damaging to your organization.

A comprehensive e-mail retention policy coupled with an effective e-mail archival solution can help mitigate these risks. By establishing best practices and implementing the right technology tools, organizations can ensure the successful management of e-mail business records, reduce e-discovery costs, improve productivity and enhance security.

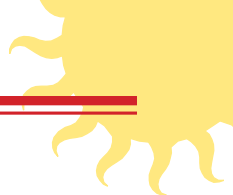
Unfortunately, too few organizations have such policies and procedures in place, waiting instead for an e-discovery or regulatory request before even thinking about e-mail retention and archival. This reactionary approach can prove very costly.

### *What Is a 'Business Record?'*

A recent study conducted by the Association of Record Managers and Administrators (ARMA) International reveals that a large majority of records management professionals feel unprepared when it comes to e-mail management (72 percent) and e-discovery (68 percent). The study also found that 62 percent of respondents lack an e-mail archiving system.

It's important to remember, however, that implementation of an e-mail archival solution is the final hurdle. An effective e-mail management strategy begins with the development of an e-mail retention policy. Given that only 34 percent of organizations have a formal e-mail retention policy in place, according to the ePolicy Institute, additional education is clearly needed.

The first step is to define, from a legal and regulatory perspective, what constitutes an electronic business record. This clearly written definition helps the organization distinguish messages involving business-related activities



---

and transactions from insignificant and purely personal e-mails.

Once this definition is in place, the organization should make sure that every employee knows what kinds of messages must be retained, and understands his or her role in the organization's overall e-mail retention strategy. Because e-mail is generated throughout the organization, e-mail retention practices cannot focus on the IT department. All employees must take part in the archival of business-related e-mails and the purging of extraneous messages.

### ***Processes, Training and Automation***

Next, organizations should establish the policies and procedures necessary to ensure compliance with legal and regulatory e-mail retention rules. The e-mail retention policy should also address business requirements and risks, and be updated regularly as laws change and new technologies are adopted. In addition to establishing e-mail retention processes, organizations should define electronic business record lifecycles and delete messages as they become outdated.

Employees throughout the organization should receive training on how to comply with the formal e-mail retention policy. This training should stress that policy compliance is mandatory. Enforcement through disciplinary

action and technology tools not only helps ensure effective e-mail management but illustrates to courts and regulators that the organization is serious about its e-mail retention obligations. Demonstrated consistency increases the odds of a favorable ruling should the organization become embroiled in an e-discovery dispute.

E-mail archival solutions play two key roles. First, these technology tools reduce e-discovery costs and help ensure policy compliance by automating e-mail archival processes. E-mail business records are preserved in a way that enables structured searches for rapid compliance with e-discovery and regulatory requests as well as day-to-day business operations.

Second, e-mail archival tools help ensure that e-mail business records meet evidentiary requirements. Because e-mail must be authentic, trustworthy and tamperproof to be considered legally valid, e-mail archival solutions should encrypt messages and protect against the deletion or alteration of archived e-mail.

### ***Business Benefits***

E-discovery is typically touted as the primary reason for establishing an e-mail retention policy and archival solution. Without effective e-mail management, organizations face incredibly expensive and time-consuming e-discovery challenges as well as the potential for costly court sanctions if they fail to meet e-discovery deadlines.

Regulatory requirements also compel organizations to get a handle on e-mail. Sarbanes-Oxley, HIPAA and the Gramm-Leach-Bliley Act all require the preservation, protection and control of business records, with the potential for huge fines and civil and criminal liability for non-compliance. Other government and industry regulations may also come into play.

However, effective e-mail management can provide organizations with a number of key benefits. E-mail is not always a "smoking gun" — in fact, e-mail can often be used to protect the organization from legal liability. The ability to produce the right e-mail records at the right time helps win lawsuits, and may even compel an opponent to settle out of court. E-mail business records also help document transactions and personnel matters and aid in decision-making.

---

Given today's litigious environment and increased regulatory scrutiny, organizations face significant e-mail-related risks. Organizations of all sizes need an e-mail retention policy and automated e-mail archival solution to help speed the retrieval of e-mail records related to a legal claim. Effective e-mail management also helps ensure compliance with government and industry regulations and facilitates day-to-day business activities. E-mail is not a simple communication tool but rather a key component of any organization's business records. ##

**milestone**  
systems, inc.



8401 Golden Valley Road, Suite 300  
Minneapolis MN 55427 USA  
Toll-free phone: 866.646.9211  
Fax 888.215.5428  
email: [info@milestonesystems.com](mailto:info@milestonesystems.com)  
[www.milestonesystems.com](http://www.milestonesystems.com)