

# The Trusted Enterprise as a Single, Secure Domain

**E**nterprise environments are composed of thousands of distributed IT systems that include various operating systems, business applications, and hardware devices. While the systems themselves are connected through the network and generally work as one, the security remains separate and unique. From the security perspective, each IT system remains an independent security domain that requires individual administration, reporting, management, and maintenance—with all the associated cost this requires. This approach creates security risks and exposures because it requires replication of control information on multiple disparate systems that

must be synchronized. With so many different technologies, it becomes extremely difficult, if not impossible, to be compliant.

Maintaining and administering a large number of security systems in a single enterprise is a daunting task. Each system must have user accounts added and managed and fine-grain access control lists created and administered. Managing these environments is further complicated because different vendor systems use proprietary schemes for control, administration, and reporting. The resulting complexity negatively impacts the level of security in the enterprise. The security actually achieved is directly related to the usability

of security controls more than the capabilities of the security systems themselves. More simply put: The more complex a system is to use, the less likely it will be used.

If those in the enterprise who have governance, fiduciary, and operational responsibilities are going to meet the demands of stakeholders, customers, partners and regulatory agencies, they must mitigate system complexities.

What if there's a completely different approach to enterprise security that solves the complexity issues and improves security at a lower cost? What if this solution is actually a proven methodology? That's what this article is about.



BY RONN H. BAILEY

### **Centralized Should Mean More Than a Dashboard**

Most enterprisewide security solutions attempt to address the problem of managing thousands of IT systems by creating additional layers of technology on top of each of the individual security systems. These layers replicate security control information from the individual servers to a centralized command and control center with an enterprise dashboard. While this enterprise repository of security policy appears to be integrated, it isn't. That's because individual systems continue to be separately maintained and administered.

The command center doesn't actually perform security functions; it simply

contains the rules and pushes them down to the individual systems. While this approach might be considered "centralized," it's by no means integrated, resulting in additional layers of software and replicated control data that need to be administered and maintained (see Figure 1). Each individual system can still be managed locally, outside the centralized command and control center, which often creates out-of-sync conditions between the enterprise dashboard view and the actual systems being controlled. This can create a false sense of security and compliance becomes impossible. As a result, increased efforts (resources) are required to correct, administer, and report on the

dashboard and the many individual systems it controls. The bottom line is that limited and costly resources are spent on managing the security systems themselves, instead of doing the actual security the systems were meant to perform.

Organizations need to find a better way to address the interactions between the security systems themselves. The answer is a new integrated enterprise security architecture that offers a simple design, ease-of-use, and security (application) automation tools.

A true integrated approach to enterprise security is one that treats the entire trusted enterprise as a single secure domain—resulting in one system to secure, not thousands. With this

approach, all enterprise systems (e.g., mainframe, Windows, Novell, HP, Sun, Unix, Linux, and others) are controlled by one security system that redirects all security processes to a single enterprise security server.

An integrated solution, as shown in Figure 2, solves many of the problems associated with enterprisewide security; it dramatically reduces security costs and complexity and decreases the number of people in the enterprise needed to manage security. If you add to this a suite of security application software tools that automate security processes, you can achieve the goal of autonomic security, and security can be delivered from a central point as a service. Such an integrated approach can be deployed on the IBM System z Security Server—(RACF)—a proven, robust security architecture, or other trusted operating systems.

This integrated, Service-Oriented Architecture (SOA) approach to security solves many problems. Use of the simpler architecture, by itself, eliminates many problems. It avoids the introduction of more complex layers that ultimately make the problem worse. Consider user sign-on and password management, for example.

Today, most enterprises are challenged with users having too many passwords to remember and maintain. Different security systems have dissimilar password management policy rules. Something as simple as password length, construction, aging, history, and other criteria can become impossible to implement. Different password rules on different systems make it quite difficult for users to remember which password belongs to which system. When that occurs, users frequently require help desk assistance with passwords. According to surveys performed by several vendors and analyst groups, each such call typically costs an enterprise \$20 to \$50, and 40 percent of all calls to help desks are for resetting passwords.

Dozens of software vendors offer products to address the problem in various ways, but such products can be expensive and difficult to implement. Moreover, the products are treating symptoms of the problem—how to streamline the management and administration of multiple passwords, rather than the cause—too many passwords per user. Simplifying the architecture by eliminating the multiple systems, licenses and implementations removes the cause and the problem. With one security sys-

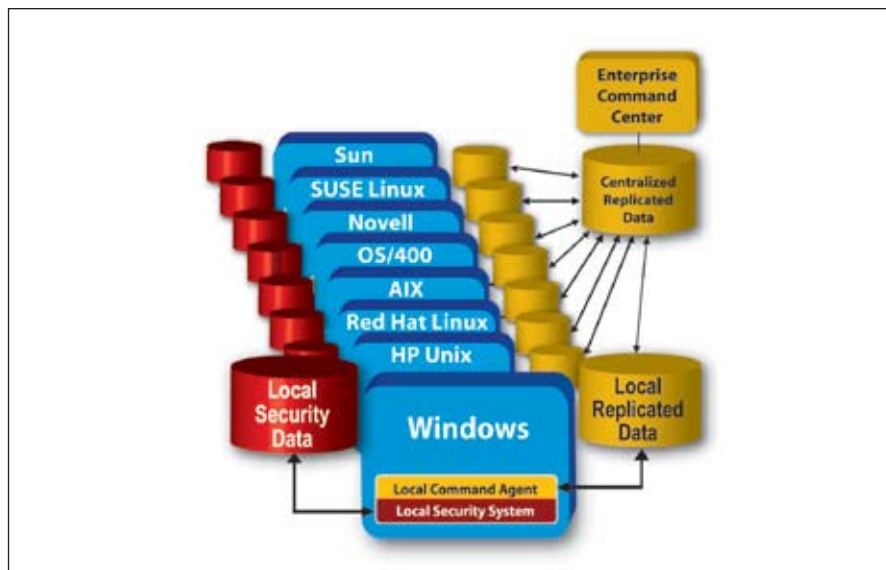


Figure 1: Centralized Replicated Security Data

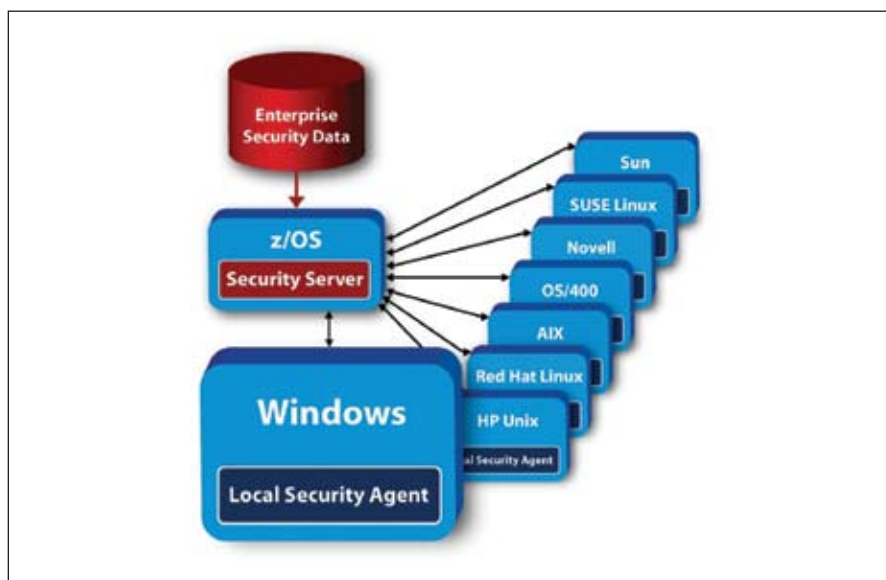


Figure 2: Integrated Security SOA Solution

tem, there's only one password. This virtually eliminates users forgetting their passwords and makes it easy to implement an enterprisewide password policy. The resulting reduction in help desk calls dramatically reduces IT costs, as does the reduced need for software licenses and maintenance on systems throughout the enterprise.

Today's enterprises are faced with deploying two-factor authentication solutions to comply with new regulations. For financial organizations, the need for two-factor authentication is now mandatory. Recent guidelines by the Federal Financial Institutions Examination Council (FFIEC) and Federal Deposit Insurance Corporation (FDIC) mandates require that financial

institutions deploy a layered security approach that includes two-factor authentication for all uses deemed high-risk. High-risk uses are defined as those involving access to customer information or the movement of funds to other parties. Widespread deployment of a two-factor authentication solution on a non-integrated, distributed network is complex and expensive.

An integrated SOA two-factor solution can help an organization simply and cost-effectively comply with regulatory mandates requiring two-factor authentication. With an integrated approach, companies don't need to implement specific two-factor authentication schemes for each distributed system and application. Instead, they can

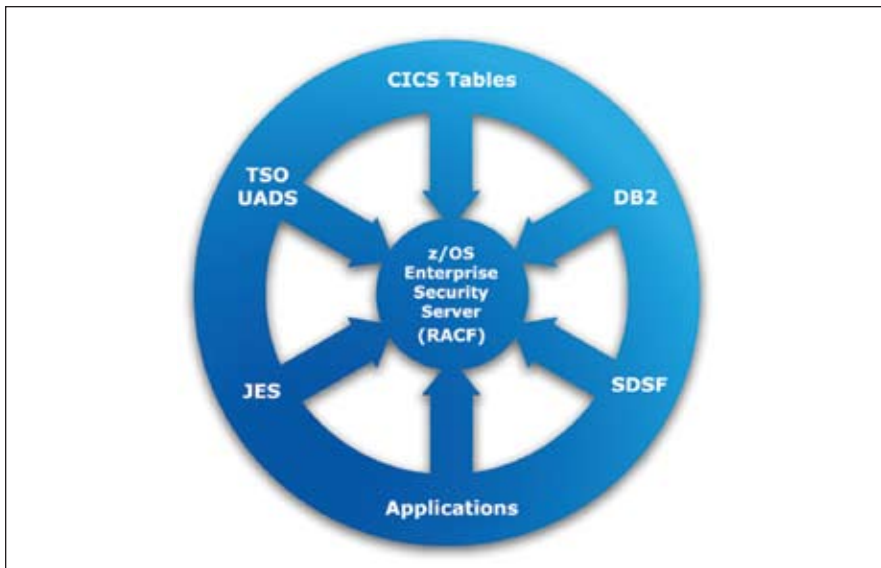


Figure 3: RACF Centralization as a Proven Model

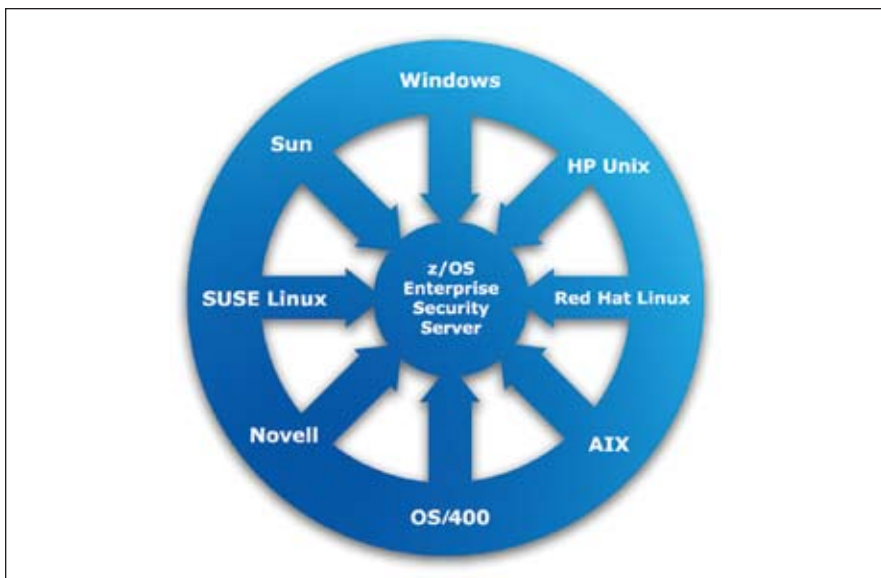


Figure 4: Multi-Platform Integration for a Single Secure Domain

use two-factor authentication capabilities housed on the mainframe security server and provide them as a service that distributed systems throughout the enterprise can call. This approach eliminates the need for multiple licenses and simplifies the deployment process.

### Tried and True

Treating the enterprise as a single secure domain is a proven, trusted architecture. During the '70s and '80s, when organizations did all their processing on mainframes, IBM's operating systems, subsystems and other program offerings were a collection of independent, disparate IT systems working together. Many of these systems were treated as individual secure domains,

each with their own security systems. Over time, customers started demanding a simpler solution that would require less management and administration and fewer passwords.

During this same period, the science of IT security developed rapidly and IBM provided customers what they wanted: a single security server system for the entire mainframe and everything running on it. RACF is arguably an early implementation of an SOA where RACF is a service the mainframe can call to provide security services for the entire enterprise. IBM was so successful that subsystems such as CICS no longer even have an internal security system; CICS relies on RACF security services.

Some naysayers may state that there

are implied dangers associated with a single security server across the enterprise because it introduces a single point of failure or creates a performance bottleneck. These are the same concerns people had during the '80s, when IBM moved toward the centralized, integrated security server. Today, no one questions the reliability, availability, and service of these systems. The industry has proved it can build fault-tolerant systems with automatic recovery and high throughput.

An enterprisewide security SOA emphasizes simplicity of design without compromising security. As a result, customers can achieve their objectives without deploying more complex and expensive layered technology (see Figures 3 and 4).

Expanding the scope of RACF to provide a comprehensive policy management and access control infrastructure across all networked platforms (and encompassing applications running on these platforms) is feasible and desirable.

Vendor-developed products have emerged to meet this need today. Established companies have developed solutions by exploiting RACF to extend controls beyond the mainframe envi-

## ZIP + ENCRYPTION

Secure Transfer and Storage  
of zSeries Data

ZIP/390 - ZIP/VSE

- ✓ Protects data to help comply with privacy mandates and regulatory requirements like SARBOX, GLBA, HIPAA and more.
- ✓ Secures data delivery to desktops and servers throughout the organization and beyond to partners and suppliers.
- ✓ Secures data with standard ZIP Keyword, ZIP AES and PGP strong encryption.
- ✓ The ease of deployment and use of ZIP and PGP.
- ✓ Enables secure and efficient file transfer and storage.

ZIP INTO COMPLIANCE

- WinZip & PKZIP compatible ZIP Utility for zSERIES
- CryptoAPI for encrypting Credit Card, SSN# and other record level data.
- PGP and Adobe PDF support tool!
- Special PKWARE replacement pricing

Download a FREE trial today at:  
<http://zje.data21.com>

# A true integrated approach to enterprise security is one that treats the entire trusted enterprise as a single secure domain—resulting in one system to secure, not thousands.

ronment into the distributed world. The result is leveraging a proven security product that provides security administrators at large companies with a common set of tools to administer security controls outside the z/OS environment, yet reaping the benefits associated with robust auditing and high-speed performance available with System z servers.

## A Time for Change

The three common business drivers forcing organizations to re-evaluate their security practices and methodologies today include high costs, regulations, and intrusion prevention.

**Costs:** Distributed networks most often operate in silos. In each environment, there are server costs, management costs, administration costs, software licensing costs, and reporting and compliance costs. In each of those cost structures there's an additional price tag for security, which can translate to thousands of dollars per user. These costs can be dramatically reduced

with an integrated security practice.

**Compliance:** Increasing compliance requirements have created overly complex security systems and security reporting structures that are often implemented on-the-fly to meet challenging deadlines. These complex administration processes often require extra staffing to accomplish "manual" integration of systems, information, and management. The result is system inefficiencies that are consuming man hours and budget dollars and reducing the effectiveness of the IT management team. A glaring example is password resetting and removal. When a staff member leaves, multiple systems must be notified to alter or remove that person's access and permissions. There's a strong likelihood that some systems don't get changed in a timely manner, if at all. This seemingly simple task creates a huge weakness in an organization's security practices. Additionally, because these activities often are manually reported, there's no means of verifying

whether the password(s) were changed or revoked without polling each individual system.

**Intrusion prevention:** Even a small breach can have catastrophic consequences. No company can afford to lose customer data, intellectual property, or their reputation due to an intrusion. Whether malicious or not, intrusions have a domino effect on the organization that can wreck careers and rack up sizable costs to address security repairs, insurance claims, data restoration, lost production, and damage to the company's reputation.

The total cost of an intrusion isn't truly measurable because only some of the damage can be identified in dollars and cents.

## Conclusion

Organizations must address these complex security issues to meet the ever-changing, increasingly complex demands placed on their enterprise security system.

An integrated, SOA approach to enterprise security that treats the entire enterprise as a single, secure domain helps an organization satisfy security and compliance requirements without significant investments in hardware platforms, security systems, or staff. By combining their existing infrastructure with proven security methodologies, an enterprise can be secure, compliant, and efficient. Organizations that opt for delivering enterprise security as a service will benefit from a more secure environment, significantly lower costs, and more accurate administration, reporting, and compliance. **Z**

## About the Author



Ronn H. Bailey is founder, CEO and CTO of Vanguard Integrity Professionals. He has been a recognized leader in information security technology for more than three decades. He has worked closely with governmental agencies and *Fortune* 1000

companies worldwide, to identify, clarify, and resolve continually evolving issues related to computer system security, controls, audits, and privacy. He is an inventor and holds several security-related patents; his most recent patent was awarded for a new form of predictive intrusion detection and prevention from a single point for user sign-on across an enterprise. He is a principle author of Enforcer, intrusion detection and prevention software for the IBM System z server that received Common Criteria EAL3+ certification in March 2007. Email: [ronn.bailey@go2vanguard.com](mailto:ronn.bailey@go2vanguard.com) Website: [www.go2vanguard.com](http://www.go2vanguard.com)