

I D C V E N D O R S P O T L I G H T

Consolidating and Managing Security Policies at the Enterprise Level for Distributed Systems

May 2008

Adapted from *Worldwide Security Services Taxonomy, 2007*, by Christian A. Christiansen, Curtis Price, and Irida Xheneti, IDC #209491

Sponsored by Vanguard Integrity Professionals, Inc.

In large enterprises and governmental organizations where distributed IT is practiced, security is often managed on a server-by-server, operating system- or application-specific basis. This approach is expensive, cumbersome, and less than secure. It also makes it more difficult to sustain compliance. Instead, IT departments could be managing security policy across a distributed enterprise from a centralized point that encompasses all servers, operating systems, applications and endpoints. Adding a security layer or “dashboard” does not ease the burden of maintaining and administering each individual system. An integrated solution that consolidates enterprise-wide security on a single security server and takes a single secure domain approach is far more practical, cost-effective, and compliant. This Vendor Spotlight examines an integrated approach to enterprise-wide security and how it benefits large-scale IT organizations. The paper also discusses the integrated suite of security software products offered by Vanguard Integrity Professionals.

The Lessons of History

An oft-quoted insight into human behavior is that those who forget the lessons of history are doomed to repeat the mistakes made in the past. When it concerns enterprise-level information technology (IT), new ideas and technology solutions often seem superior to anything in current or past use. Yet it is worth remembering that problems and their solutions often remain unchanged over time, with only the size of the machine, the operating environment, or other minor details differing.

This is certainly true of security. Security issues first arose during the mainframe age of IT, as far back as the 1950s. Computing systems were deployed for a variety of tasks: accounting, manufacturing, inventory, etc. Over the years, new types of computers emerged: minicomputers, PCs, servers, and with each, a different operating system and approach to security.

Smaller computers and line-of-business (LOB) systems were linked, or connected through networks, to the mainframe. In time these became distributed systems. Computers and mobile devices now connect in-house, off-site, and to external networks, leading to an entirely new type of “end-point” security. Thus, as the complexity of systems has grown, the perception is that they are even more difficult to manage from a security perspective. This does not have to be true.

The Need for a Single-Domain Security Model

Because of distributed environments, security has become a many-headed monster in the IT organization. In addition to the mainframe system, there may be multiple operating systems in use for various systems and servers. Currently, the most common approach is to provide each distinct system with its own local security, user accounts and IT security staff, which increases overhead and risks. These accounts may have different security levels, access control screens, administration

procedures, control procedures, reporting procedures, and password change cycles. Users are commonly required to remember how to gain access to, and perform tasks in, at least three systems, and often as many as seven.

Any attempt to centralize security data requires that data from each individual system be replicated at the centralized repository level for IT administration. This duplication is expensive and risky to maintain. A skilled help desk must be staffed to support users who encounter problems and lose passwords.

Meanwhile, compliance issues continue to grow. IT management must deal with a plethora of regulations, standards, frameworks, controls and policies, assessment issues and audit procedures on a daily basis. For example, government regulations in the U.S. such as SOX, HIPAA and GLB, and internationally with Basel II, J-SOX and EU privacy directives. A number of agencies of the Federal government, including the Federal Deposit Insurance Corporation and Homeland Security, now require two-factor authentication for high-risk users. In addition there are industry-specific regulations that may apply for financial activity, such as those from the FFIEC (Federal Financial Institutions Examination Council) and PCI (Payment Card Industry, the Data Security Standard).

Updating a Proven Solution for Today's Security Challenges

An integrated approach to security using a single secure domain model addresses the issues and problems with security in a distributed IT environment. For example, data replication in a distributed environment creates problems for compliance. Because IT can't track these data sets, the replication of data may cause a breach, albeit inadvertently.

A centralized, integrated system is needed to control that information, one architected to provide a single copy of the rules, greatly reducing or eliminating replication of security policies. Similarly, a centralized system can provide a single password and one set of password rules. Logically and physically the system provides a centralized policy engine and rules database, but administration tasks can be distributed and delegated as required.

Moreover, an integrated single secure domain solution allows IT to manage disparate security policies across distributed environments. Using a single policy engine, the distributed environment can become, from a security perspective, one homogeneous environment. This integrated approach reaches across all systems and OS platforms and provides a single point of access for users. Each of the individual, distributed systems or servers is integrated through a single enterprise security server, which manages security policy for the entire environment.

The Benefits of the Mainframe Platform for Integrated Security

A centralized and integrated security system that uses a single, security server to establish and administer security policy ensures that distributed environments are indeed homogeneous, and that all disparate systems will be able to share protocols and messaging. When this centralized approach is deployed on mainframe systems using the Resource Access Control Facility (RACF) database, security data is stored and managed using the most highly secure database in the enterprise, and the mainframe becomes the single security server.

This single secure domain model builds out from the original Resource Access Control Facility (RACF) architecture — mainframe security that verifies user ID and password and controls access to authorized files and resources — to establish a number of business services, including security, which can propagate throughout the distributed environment. The model redefines the distributed environment by making functions and calls uniformly understood by all systems — in a word, homogeneous.

Because the integrated security environment is managed at the highest policy level, audits and regulatory compliance are automatic. Not only can IT management monitor compliance, but users can monitor their own compliance as well.

Additionally, the single domain security approach reduces costs. Distributed environments are commonly made up of discrete silos, each with its own security administration and management costs, hardware and software costs, and compliance and reporting costs. An integrated security solution consolidates security, eliminating these costly redundancies. It also minimizes system integration. The ongoing costs of system integration can be quite high, as each new configuration adds new potential security vulnerabilities and fixes.

Anticipating Future Security Issues

In addition to the certainty of death and taxes, organizations can now add security threats to information systems and increasing security management challenges. Threats both from outside and internal sources will only grow more frequent, more challenging, and more dangerous in the future. The plethora of new devices and systems will make security management even more difficult.

As new devices and systems come online, for example, enterprises will need to determine how to secure them. They will be faced with whether to add a new security server, which is focused on managing the new devices or systems, or managing them using a centralized, single security server that is flexible enough to anticipate and adapt to future needs. The single secure domain approach can make it easier for organizations to securely adapt to the growing complexity.

Identity and access management (IAM), will also continue to challenge IT, especially with respect to endpoint access devices. The deployment of a single access password, especially for two-factor authentication, is essential. Tokenless, or soft token, technology will facilitate secure access using mobile devices such as a cellphone as a “virtual token.”

Information protection and control (IPC) has become a first line of defense for IT security. Threats from criminal hackers range from corporate IT intrusion to the theft of endpoint devices. Additional threats come from nefarious employees who steal and then sell confidential or proprietary intellectual property. A single secure domain model makes it easier to track illicit actions and change passwords that have been compromised.

As Web Services have proliferated and become an extension of the distributed computing environment, they must be considered within the context of the enterprise’s security and subject to the same considerations. In order to address Web Services security issues, an integrated, top-down approach policy is essential.

Compliance is, and will remain, a nettlesome requirement for IT, business units, and auditors alike. Both government and industry regulations require data aggregation and event management, as well as the ability to identify and correct internal threats that arise from user activities. In addition, more laws addressing disclosure of data loss and security breaches are being enacted all the time. A strong offensive strategy is clearly the best defense. The single secure domain model can also provide greater accountability, to the degree that it enables greater certainty of the information — key to passing compliance audits.

Considering Vanguard Integrity Professionals

Vanguard Integrity Professionals, founded in 1986 and headquartered in Las Vegas, Nevada, is the largest independent vendor of RACF security and administration add-on tools in the industry. The company has offices in Nevada, California and the United Kingdom and serves more than 1,000

customers around the world with a comprehensive array of software solutions designed to strengthen security across a variety of operating platforms.

Vanguard provides its solutions to large enterprises in industries including education, finance, healthcare, manufacturing, transportation, insurance and retail, as well as government agencies. The company offers a comprehensive suite of three solution sets:

First is an identity and access management software solution (a category IDC refers to as IAM, or Identity and Access Management) that supports the entire enterprise as if it is a single, secure domain:

- Vanguard Authenticator for enterprise access control access to the entire IT infrastructure from a single, central location with a scalable, modular, and integrated authentication solution
- Vanguard ez/SignOn enables a single password for different operating system environments throughout the enterprise
- Vanguard ez/Integrator a powerful, easy-to-use, application programming interface (API) that links distributed software to the mainframe without having to create a new security infrastructure
- Vanguard ez/Token is a two-factor RSA authentication solution that allows users to authenticate through either RSA SecurID or ActivIdentity tokens to the zSeries Server, or through any other application currently using RACF authentication
- Vanguard Tokenless Two Factor offers strong enterprise-wide authentication capabilities using one-time use, time-sensitive passcodes sent to a “virtual token,” the user’s cell phone.
- Vanguard PasswordReset allows user to reset their own passwords, which reduces password reset costs

Second is security and access management software for mainframe environments, and the entire enterprise for companies that have implemented Vanguard’s identity authentication software products. Vanguard’s security and access management solution enables IT security personnel to accomplish more work faster and with more accuracy than they can using native RACF systems. The complete solution includes the following products:

- Vanguard Administrator for complete, easy and automated security administration and reporting without the need to use the RACF command line interface
- Vanguard Advisor a dynamic security reporting and real-time problem solving tool that collects and analyzes security events and generates reports for management
- Vanguard Security Center an easy-to-use Windows-based GUI for security administration of mainframe environments
- Vanguard Enforcer an intrusion prevention system developed by NASA that recently received EAL3+ certification
- Vanguard Policy Manager for strict control of RACF command execution and adherence to corporate standards and policies
- Vanguard ez/AccessControl for extending mainframe security and access management to the Windows environment
- Vanguard PasswordReset allows users to reset their own passwords, which reduces password reset costs

The third group of Vanguard products is focused on auditing and compliance and is designed to automate processes to reduce the burden. The solution includes the following products:

- Vanguard Analyzer an automated integrity verification and auditing analysis tool that verifies audit compliance, identifies vulnerabilities and reduces audit expense
- Vanguard InCompliance an easy-to-use auditing and compliance maintenance tool that continuously monitors a system's compliance status
- Vanguard Enforcer for continuously monitoring and analyzing security-relevant events and activities to identify potential intrusion scenarios and restore the environment to a compliant state
- Vanguard Administrator for generating reports that identify which users have access authority and which processes they have been assigned to perform
- Vanguard Policy Manager for control over RACF command execution to ensure compliance with regulations and internal security policies

Vanguard's software is designed to reduce the complexity of enterprise security. The company's belief is that the effectiveness of IT security is directly related to how easy it is for an organization to securely administer its systems, devices and applications. Vanguard's goal is to automate and facilitate security processes as much as possible, eliminating the need for technical administrators for security management and administration, and significantly easing deployment and maintenance. In one reported instance, PasswordReset helped a customer dramatically reduce its password reset costs by reducing its number of support calls by 4,000 per month.

In addition to software, Vanguard offers customers consulting, training, and industry conference services, all built upon the foundation of enterprise-wide IT security. The company is in the unique position to offer an enterprise-level solution proven effective for nearly a quarter of a century.

Challenges

However, Vanguard does face market challenges. The company needs to clearly articulate its vision of enterprise security, and by doing so persuade its customers that they can no longer view the network world and the mainframe systems world as discrete systems with separate security and compliance requirements.

Also, international compliance goes beyond Sarbanes-Oxley, so Vanguard needs to offer templates for more international regulations, such as J-SOX in Japan and country-specific European privacy regulations, as well as for industry regulations such as PCI DSS (Payment Card Industry Data Security Standard).

Conclusion: Leveraging the Past to Leap Ahead

In the golden age of mainframe computing, many industry observers assumed that computers would always function like power plants, with one machine serving a mass of users. Centralized IT was eventually superseded, of course, by decentralized, distributed network architectures. Today, companies have the option of adaptive solutions, yet one factor remains: large IT organizations work from the top down, relying on their mainframes to perform key computational tasks.

Similarly, when it comes to security, it makes greater sense to administer and manage security as a policy from the highest computing level in the organization. It is costly and impractical to use multiple, platform-dependent solutions. The mainframe, due to its centralized functionality, provides a practical basis for managing a heterogeneous security environment.

An integrated, single-domain security solution can be deployed through an enterprise-level security server, allowing users access through a single, local security agent. This is how security has been administered on mainframe computers for a quarter century — a time-tested, proven solution that can be effectively implemented in distributed IT environments.

A single-domain security implementation means fewer people are needed to manage and maintain security at the individual systems level, which reduces risks and costs by decreasing the number of people authorized to grant security access. Consolidating sign-ons, for example, translates into lower security risks; audits are more effective and less expensive; and compliance issues are dealt with more quickly and effectively.

Many IT departments approach security as a patchwork of problems needing specific solutions, which leads to security silos. Vanguard must overcome this organizational inertia toward point solutions, but if the company can successfully address the challenges previously described, Vanguard has a significant opportunity for success.

ABOUT THIS PUBLICATION

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC.

For more information on IDC visit www.idc.com. For more information on IDC GMS visit www.idc.com/gms.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com