

Business Enablement Demands Tight Identity and Security Integration

Date: April 2009

Author: Jon Oltsik, Principal Analyst

Abstract: Identity management and security were once thought of as independent IT activities but this is rapidly changing. Why? New business processes, web-based applications, external collaboration, and user mobility are driving tight integration between traditional identity management activities like user provisioning and authentication with security requirements like malware detection, information assurance, and auditing. Many technology vendors offer products in one or both of these areas but Microsoft stands out for its tight integration between identity, security, and its existing broad base Windows infrastructure.

Identity and Security: A Historical Perspective

Throughout the history of business computing, identity management and information security were treated as distinctly different IT disciplines. Yes, the two groups cooperated on things like authentication technologies and password management but collaboration remained fairly limited. Identity and security remained separate because:

- **Identity management focused on employee productivity.** Provisioning a new user account was generally driven by the human resources department as part of an overall process to accommodate new employees with essential productivity tools like desks, chairs, employee badges, and network/application access. Behind the scenes, IT took care of the essential identity management details. In some cases, IT operations acquired more sophisticated identity management tools to automate user provisioning, day-to-day operations, and application access but everything was really driven by the original HR request.
- **Security teams concentrated on IT assets and attack containment.** Far removed from HR, security groups were tasked with protecting the network perimeter and PCs from hacker and malicious code attacks. Security professionals tended to be associated with technologies like firewalls and antivirus software rather than the mainstream IT organization or overall employee pool.

Why were these activities so far removed from one another? In the old days of private networks and minimal Internet access, “trusted” employees were viewed as a minimal security risk. One bad apple might steal a laptop or two, but this type of physical threat was all that was expected. The “real” security risks were things like e-mail viruses like “ILOveYou” and “Melissa” as well as hacker activities like network probing and scanning. With little in common, identity and security responsibilities were assigned to different groups with disparate skills who barely knew each other.

New Business Processes Are Driving the Need for Identity and Security Integration

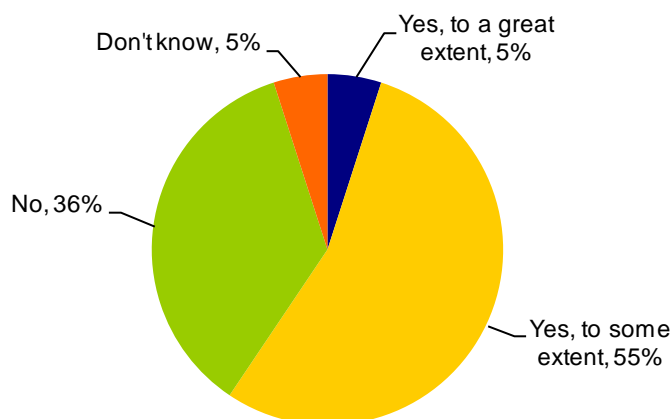
Fast forward to 2000 and beyond and there is a growing recognition that identity and security disciplines must come together within IT organizations, processes, and technologies. Why the need for amalgamation? Many industry pundits point to regulatory compliance requirements but this is only part of the picture. ESG believes that identity and security integration is really driven by an avalanche of new network-based business process requirements.

The simple story goes like this: The rise of Internet connectivity, mobile Internet devices, externally-facing applications, and Internet-based application integration technologies like web services led to open networks and what security professionals call “de-perimeterization.” From a business perspective these trends opened up entirely new business process models like business process outsourcing, supply chain integration, and

collaboration on a global scale. Private networks were now open for business as organizations used the Internet as a way to drive new revenue, expand opportunities, accelerate business initiatives, and lower costs. This trend is illustrated in a recent ESG Research Report¹. 60% of enterprise organizations (i.e. 1,000 employees or more) say that they share confidential data with non-employees (see Figure 1). Most organizations also believe that they will share more confidential data with more external constituencies like business partners, customers, or suppliers in the future as well.

FIGURE 1. MOST LARGE ORGANIZATIONS SHARE CONFIDENTIAL DATA WITH NON-EMPLOYEES

**Does your organization share its confidential data with non-employees (i.e., business partners, suppliers, customers, etc.)?
(Percent of respondents, N=308)**



Source: Enterprise Strategy Group, 2008

With measurable business benefits, CEOs encouraged IT to bolster their identity management capabilities to provide outsiders with network/application access and get them productive as quickly as possible. While business executives encouraged these network-based business processes, security professionals understood that they carried an invisible yet insidious cost—a potential increase in security risk. Opening networks and applications to outsiders meant a greater population of endpoints capable of spreading malicious code attacks. Sharing confidential data with non-employees greatly exacerbated the risk of a data breach. New web-based applications increased the risk of an application layer security attack like SQL injection or cross-site scripting. From a security perspective in fact, each new user, device, network, or application connecting to internal resources presented a host of new threat vectors that needed to be understood, blocked, and monitored for suspicious activity.

Ultimately, success with new network-based business processes demands a balance of identity and security management. Identity without security will accelerate business initiatives but introduce a tidal wave of security risks that are bound to lead to security events, data breaches, and regulatory compliance violations. Alternatively, security controls and “defense-in-depth” safeguards will protect IT assets but can’t help provision external users, create roles, or get external constituencies productive.

Identity and Security Must Become the Yin and Yang of Business Enablement

The venerable Chinese Yin-Yang symbol is often used to represent a balance between two forces that harmonize in the formation of a complete process. This ancient icon provides a good metaphor for the union of identity and security as complementary IT disciplines needed to secure business collaboration and processes, while enhancing productivity. In this way, identity and security can automate user management AND reduce risks by:

¹ ESG Research Report: *Protecting Confidential Data Revisited*, April, 2009.

- **Granting outsiders secure access to the network and applications.** An “outsider” can be a remote employee, on-site contractor, or Asian-based supplier—the common assumption is that they are connecting to internal IT assets like networks, servers, applications, and files over the Internet. To get these users productive while maintaining a high level of security, large organizations need strong user provisioning, authentication, federated identity capabilities, and device inspection technologies such as Microsoft’s Network Access Protection (NAP).
- **Including data security.** In the old identity management world, the term “identity” was reserved exclusively for people but the marriage of identity and security for business enablement takes identity beyond humanity alone. In this new yin-yang world, identity is extended to include data identity in terms of classification and associated security policies. This granularity is necessary in order to protect data confidentiality and integrity while accommodating mobility and the added risk of network-based business processes. For example, the CFO may have access to all financial data on her office PC but not from an unknown laptop on an unprotected wireless network. External attorneys working on an acquisition may be granted access to classified documents but be prohibited from saving or altering them.
- **Marrying identity with entitlements and security policies.** Once a user is granted access to a network or application it is important to limit activities based upon user role and responsibilities. This has often been done in a haphazard fashion based on network controls like firewalls and ACLs and custom rules coded into individual applications. This ad-hoc process compromises security and can’t scale. As identity and security unite, network and application access policy enforcement can be based upon roles and become more automated. New user provisioning can be tightly coupled with entitlement rules. Network authentication can allow a large customer access to particular IP addresses using a limited number of ports and protocols. Application access can be limited to particular actions and URLs.
- **Auditing usage and behavior.** Since people are still “the weakest link in the security chain,” it is important to monitor users in order to detect and audit suspicious or malicious behavior. When a supplier’s accounts receivable administrator introduces SQL queries into URL requests on the corporate accounting system, security managers will want immediate notification of the event, historical data about this person’s usage patterns, and time-stamped audit reports for non-repudiation.
- **Detecting and preventing security events.** As more and more users, devices, and protocols enter the network, basic security packet/content filtering, anomaly detection, and prevention systems become even more important than they are today. Large organizations must anchor their security defenses with critical technologies like firewalls, IDS/IPS, application firewalls, DLP, e-mail gateways, and endpoint security software.

It is important to note that these capabilities cannot be accomplished without tight integration between identity management and information security through the entire technology stack from the network to the application layer. Without this integration, large organizations will struggle to customize services for specific users, enforce granular access policies, and detect sophisticated security attacks in real-time.

Microsoft Is Pursuing a Yin-Yang Strategy

Many IT vendors have individual products for either identity or security but not both. Others have a broader portfolio of identity and security products but these tools typically lack the tight integration necessary. Microsoft is actually an exception to these rules. With its heritage in a distributed computing infrastructure, Microsoft has always included a strong identity and security focus throughout its development, design, and product portfolio. More recently, Microsoft extended its level of identity and security integration by:

- **Adding security functionality into its identity offerings.** In 2007, Microsoft merged its Microsoft Identity Integration Server (MIIS) with smart card and certificate management to create a new product called Identity Lifecycle Manager (ILM). With this move, ILM now offers traditional identity management functionality like user provisioning, workflow, identity synchronization, federated identity, user self service

and SSO with tools for password management, credential management, and PKI. To improve and automate operations, ILM also includes central policy management, command-and-control, and reporting/auditing. Taken as a whole, ILM should help organizations define user roles and get them productive quickly and securely.

- **Extending security protection to the data.** In order to protect sensitive data, Microsoft added a number of Windows-based safeguards and 3rd party integration partnerships. For example, desktop managers can use Active Directory Group Policies to restrict user access to file shares or disable USB ports on endpoint PCs. Windows includes BitLocker for full-disk encryption while EFS file level encryption will soon be integrated with ILM for PKI. Finally, Microsoft Rights Management Services (RMS) provides granular entitlement management on a document or file basis. Microsoft is currently extending this functionality by integrating with data discovery and classification from RSA Security. This data-level security allows Microsoft customers to share and protect data simultaneously.
- **Offering network security, authentication, and authorization.** Microsoft today provides perimeter security and remote access capabilities through the Windows VPN, ISA Server firewall, and its SSL VPN product, Intelligent Application Gateway (IAG). Finally, Microsoft NAP can be used to authenticate endpoint devices, perform device health and compliance inspection, and enforce access policies at the network edge. NAP supports a concept called “Server and Domain Isolation” which uses IPsec for authentication and network authorization. To prevent network probing or Denial of Service (DOS) attacks, this security can be used to set up a point-to-point connection between external clients and applications with internal servers.
- **Targeting security “hot spots.”** Over the past few years, Microsoft has also entered the security market directly with its Forefront products for application and endpoint security. These products are essential for security event detection and prevention as the amount of external users, data sharing, and network traffic continues to escalate in support of business processes. Microsoft Forefront (code name) “Stirling” will further enhance this protection through its Beta cycle in 2009 and planned release in 2010 (note that the Forefront Security for Exchange and Forefront Threat Management Gateway which are both part of Microsoft Forefront [code name] ‘Stirling’ ship in late 2009). Additionally, Microsoft will be advancing its federated identity and access capabilities with Microsoft code name “Geneva,” an open platform for simplified user access based on claims.

As previously mentioned, business enablement depends upon tight integration between identity and security, not the presence of products alone. Aside from product integration projects like Microsoft Forefront (code name) ‘Stirling,’ Microsoft also offers tight integration between identity, security, and the Windows infrastructure, and its roadmap promises to extend that integration even further with the platform and its System Center offerings. Furthermore, Microsoft is taking this collaborative strategy to its organization by integrating the security and identity product teams together.

Identity and security integration is evident across the Microsoft portfolio. For example, Active Directory acts as the central identity repository and can be used to create and enforce endpoint policies, store X.509 certificates, or work in conjunction with NAP to enforce network access policies using RADIUS or DHCP. Microsoft System Center can be used to configure PCs, distribute security patches, or map identity and security processes to overall IT service and other Microsoft infrastructure offerings like Windows. All Microsoft software, including identity management and information security products, must also go through the stringent Secure Development Lifecycle (SDL) process to ensure that security is “baked-in” to each product through design, development, testing, and production. With this type of integration, Microsoft is not only merging identity and security for business enablement but also making these services more responsive to IT processes and operations.

The Bottom Line

There is no doubt that balancing identity management and information security is essential for enabling new business processes that are inexorably connected to Internet connectivity and applications. The first step for CIOs is to come to this realization and assess internal process, skills, and technology, and then build an integration plan in these areas.

As IT executives look for identity and security products that can support their business goals, they must insist upon tight integration—from user provisioning and authentication through network and application entitlements through data confidentiality and integrity. This integration is essential as it can allow IT to address business needs quickly without disproportionately increasing security risk.

When viewed in this context, Microsoft identity and security integration may trump the competition as Microsoft provides identity/security product integration as well as seamless interoperability with the existing Windows infrastructure. As such, smart CIOs should place Microsoft on their short list of potential vendor partners for identity, security, and overall business enablement.