R-19-9974
V. Wheatman, R. Stiennon, R. Wagner, J. Pescatore, A. Hallawell, J. Girard, R. Witty, K. Kavanagh

Strategic Analysis Report
30 May 2003

Hype Cycle for Information Security, 2003

Succumbing to vendor hype in the security management area can have expensive consequences. Enterprises should assess their security needs and evaluate the relative maturity of a security technology before adopting it.

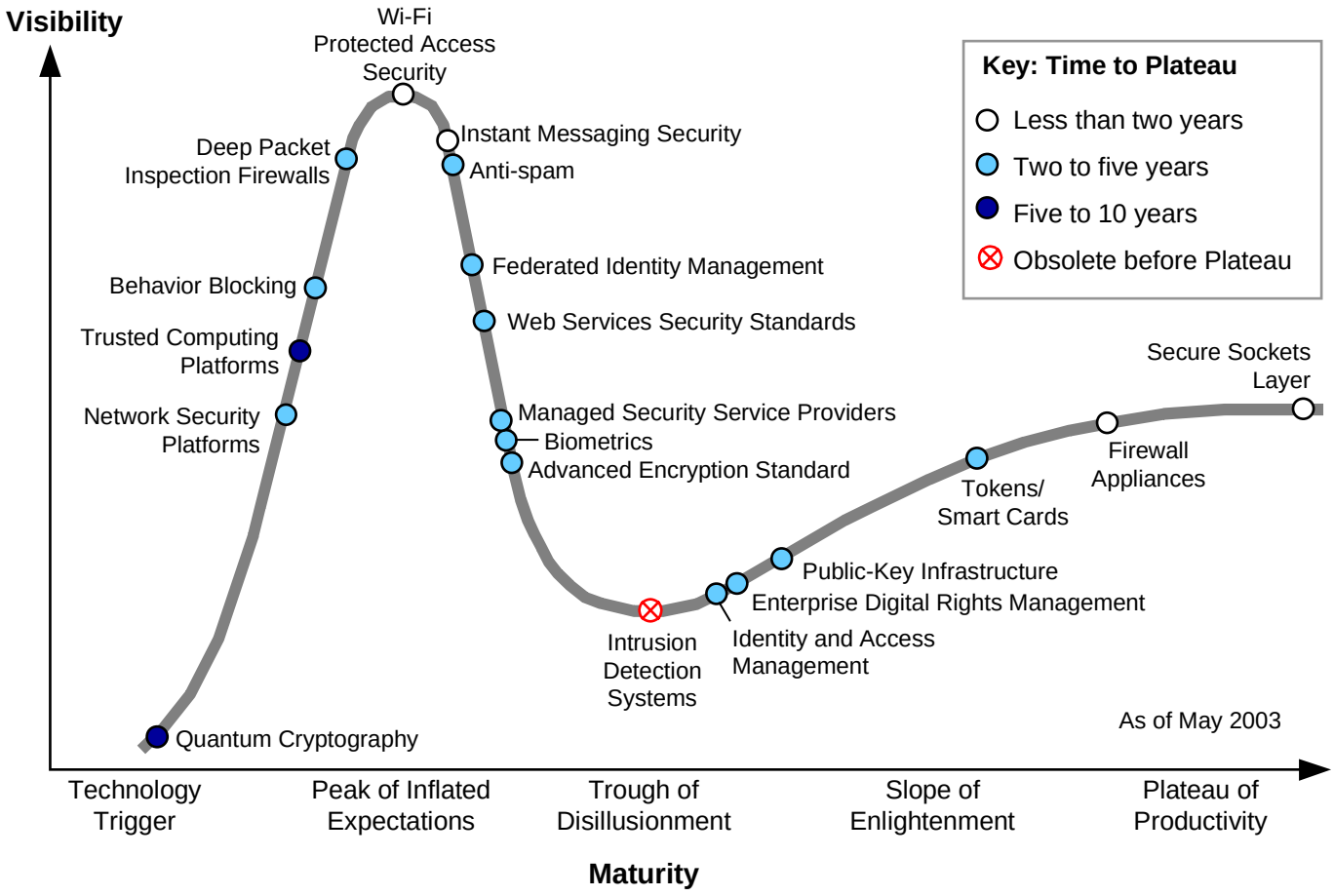
Management Summary

Each new wave of technology disrupts security measures and introduces new vulnerabilities, as clearly evidenced by security challenges raised by new IT usage patterns, such as LANs, e-mail and wireless access. However, security and IT groups face similar challenges when evaluating emerging security solutions to fend off new vulnerabilities raised by IT or business changes. Therefore, each new security management technology follows the Hype Cycle; adopting an emerging technology is a critical decision. If an enterprise launches its efforts too soon, it will suffer the painful and expensive lessons of deploying an immature technology. If it delays investment for too long, it risks being left behind by competitors that have made the technology work to their advantage. In the case of information security, failing to deploy at the right time can leave the enterprise vulnerable to internal and external security threats.

CONTENTS

FIGURES

1.0 The Hype Cycle



Source: Gartner Research (May 2003)

Figure 1. Hype Cycle for Information Security, 2003

2.0 On the Rise

2.1 Quantum Cryptography

Definition: Encryption or key exchange technologies that are based on quantum physics principles. These technologies may or may not include "quantum computing" technology. Technology in production uses quantum physics properties for key exchange only.

Time to Plateau/Adoption Speed: Five to 10 years.

Justification for Hype Cycle Position/Adoption Speed: The first high-end key exchange products were announced in late 2002. Products use quantum phenomena for out-of-band key exchange between known participants deploying private fiber channels across limited distances. Quantum computing is still a futuristic branch of physics/computer science research. There is no indication of near-term commercial viability.

Business Impact Areas: Basic mechanisms for encryption and key sharing for high-strength data and network security. Combats quantum cryptoanalysis — that is, using quantum computers to break existing public-key-based encryption. Long-term developmental cycle; little near-term potential.

Selected Vendors: id Quantique and MagiQ Technologies.

Analysis by Ray Wagner

2.2 Network Security Platforms

Definition: Convergence of several network security markets, including firewalls, intrusion detection, gateway antivirus technology and vulnerability assessment, into appliance-based platforms.

Time to Plateau/Adoption Speed: Two to five years.

Justification for Hype Cycle Position/Adoption Speed: There is a need to reduce the total cost of ownership of network security devices, while increasing responsiveness and providing enhanced security, without forcing enterprises to buy everything from one vendor.

Business Impact Areas: Security platforms will help develop a more-proactive security posture, reduce security cost of ownership, reduce security incident costs and improve security manageability. There is potential for integrated best-of-breed solutions from multiple providers in a uniformly managed "box."

Selected Vendors: CloudShield, CoSine Communications, Crossbeam Systems and TippingPoint Technologies.

Analysis by John Pescatore

2.3 Trusted Computing Platforms

Definition: The inclusion of secure operating systems and trusted hardware in PC and personal digital assistant platforms to support strong digital rights management and information protection.

Time to Plateau/Adoption Speed: Five to 10 years.

Justification for Hype Cycle Position/Adoption Speed: Trusted computing will not be standard in shipped PC platforms until 2005, and it will not reach enough of the installed base to have major impact until 2008. Other platforms, such as cell phones and other consumer equipment, will penetrate after 2008.

Business Impact Areas: New business models enabled by digital rights management, safer use of public computers for employee remote access and stronger intellectual property protection.

Selected Vendors: Intel and Microsoft.

Analysis by John Pescatore

2.4 Behavior Blocking

Definition: Technologies that inspect and may block the behavior of programs that violate enterprise security policy.

Time to Plateau/Adoption Speed: Two to five years.

Justification for Hype Cycle Position/Adoption Speed: Behavior blocking is potentially a more-effective method of preventing malicious-code attacks. It also facilitates end-user lockdown policies. However, behavior blocking technology must be implemented at the desktop, is intrusive (intercepts systems calls), and requires enterprises and end users to accept a policy shift to more-extensive lockdown.

Business Impact Areas: Improved protection against malicious-code attacks prevents downtime and destroyed data, and helps ensure the more-efficient use of enterprise IT resources. Will disrupt or replace antivirus technologies, accelerate shift toward end-user lockdown by enterprise IT groups, and transform overall technology usage culture.

Selected Vendors:, Cisco Systems/Okena, Finjan Software and Sygate Technologies.

Analysis by Arabella Hallawell

3.0 At the Peak

3.1 Deep Packet Inspection Firewalls

Definition: Appliances with specialized hardware to terminate Secure Sockets Layer (SSL) sessions, inspect all packet headers, and allow or deny access based on a set of policies or behaviors (see "Deep Packet Inspection: Next Phase of Firewall Evolution," T-18-0340).

Time to Plateau/Adoption Speed: Two to five years.

Justification for Hype Cycle Position/Adoption Speed: Deep packet inspection firewalls have not yet received media attention or vendor support. The message has been lost in intrusion prevention terminology. However, content switches, application firewalls and traditional firewalls are evolving to deep packet inspection.

Business Impact Areas: Will help block attacks via port 80/443 and secure Extensible Markup Language (XML). Provides application-level protection beyond what is offered by stateful inspection or proxy firewalls.

Selected Vendors: Blue Coat Systems, Fortinet, Intruvert Networks, NetContinuum, NetScreen Technologies and TippingPoint.

Analysis by Richard Stiennon

3.2 Wi-Fi Protected Access Security

Definition: Wi-Fi, or Wireless Fidelity, protected access (WPA) is an interim version of 802.1x. It replaces the defective Wireless Equivalent Privacy security mechanism for wireless local-area networks (WLANs) and supports multiple versions of the Extensible Authentication Protocol (EAP).

Time to Plateau/Adoption Speed: Less than two years.

Justification for Hype Cycle Position/Adoption Speed: There has been tremendous media hype that WPA solves WLAN security problems. It has strong backing from all vendors, which believe that WPA will give them a competitive edge in 2003. WPA will encourage new WLAN growth for private and public use because many potential users and their enterprises have delayed implementing WLANs because of bad publicity caused by break-ins. The excitement about WPA will give way to frustration as users invest time in firmware upgrades and discover that some equipment will not be upgradable. WPA is still an interim step to the full 802.11 standard. WPA supports several alternate versions of EAP; a vendor battle must be fought to determine which version(s) of EAP will dominate. Full official compliance with 802.11 likely will require at least one more major firmware release after WPA is stable.

Business Impact Areas: An interoperable solution to rampant global exposure of WLANs.

Selected Vendors: Cisco Systems, D-Link, Linksys, Microsoft, Proxim and Symbol.

Analysis by John Girard

3.3 Instant Messaging Security

Definition: Prevents instant messaging (IM) from being abused by users or "malware" — malicious software that is developed to do harm, including viruses, worms and "Trojan horses." Addresses concerns that some IM systems do not encrypt user IDs and passwords, do not maintain audit trails of messages or file transfers, look to use any available open port (creating a path for harm), and may violate certain regulations about record-keeping. Because IM uses open networks, sensitive information may be exposed (see "What May Lurk in Your IM Session," COM-14-2666).

Time to Plateau/Adoption Speed: Less than two years.

Justification for Hype Cycle Position/Adoption Speed: There are more than 40 vendors in this space. AOL, Yahoo and Microsoft are beginning to enter the market.

Business Impact Areas: IM security will allow enterprises to track all communication over IM for audit purposes and to block viruses and the misuse of IM capabilities, including unaudited file transfers. There will be minor improvement in productivity and the protection of sensitive information.

Selected Vendors: Akonix, Blue Coat, Cordant, eSniff and IM-Age Software.

Analysis by Richard Stiennon

3.4 Anti-spam

Definition: Identifying, blocking or managing unsolicited e-mail messages (see "Anti-spam Products for Enterprises," M-19-0710, and "Anti-spam Services: Focus, Expertise and Breadth of View," M-19-0595).

Time to Plateau: Two to five years.

Justification for Hype Cycle Position/Adoption Speed: There has been extreme hype about spam, and enterprises are demanding effective anti-spam solutions that will not create a significant IT administrative burden. The technology is still immature, but it is changing rapidly. Multiple detection methods, especially effective heuristic and self-learning capabilities, and implementation feedback will create "good enough" anti-spam detection services by year-end 2004.

Business Impact Areas: Reduction in perceived enterprise liability as conduit of inappropriate content, minor improved productivity through fewer wasteful e-mail messages and reduction from risk of malicious code infections. By 2004, consolidation among anti-spam providers and evidence of greater technology maturity will allow for dramatic drops in the price of anti-spam solutions. Enterprises will require greater operational efficiency. E-mail security and management solutions, which integrate anti-spam, antivirus and other e-mail management services, will be used.

Selected Vendors: ActiveState, Brightmail, CipherTrust, Frontbridge, McAfee, MessageLabs, Send Mail, SurfControl and Tumbleweed.

Analysis by Arabella Hallawell

4.0 Sliding Into the Trough

4.1 Federated Identity Management

Definition: Sharing identification credentials among several entities. Trust is transferred from one identifying and authenticating entity to another based on a common authentication framework.

Time to Plateau/Adoption Speed: Two to five years.

Justification for Hype Cycle Position/Adoption Speed: There are no community-based production implementations to date, only initial deployment plans.

Business Impact Areas: Business facilitation, cost containment and operational efficiency. Initial implementations will be internal and business-to-business. In the future, the focus will be on stressing the importance of standards compliance in all product implementations.

Selected Vendors: Microsoft Passport and the Liberty Alliance.

Analysis by Roberta Witty

4.2 Web Services Security Standards

Definition: Security standards for XML-based Web services, such as XML-Encryption, XML-Digital Signature, XML Key Management Specification, Security Assertion Markup Language (SAML), Extensible Rights Markup Language, Extensible Access Control Markup Language (XACML), Service Provisioning Markup Language and Web Services Security (WS-Security).

Time to Plateau/Adoption Speed: Two to five years.

Justification for Hype Cycle Position/Adoption Speed: Strong support from major Web services players, as well as the World Wide Web Consortium, the Organization for the Advancement of Structured Information Standards and the Web Services Interoperability Organization, are driving the these standards. Final extensions to WS-Security are due in the second half of 2003, with presentation as standards likely in early 2004. Most other initiatives are release standards at this point, or they will be in 2003. Major products are including some compatibility with standards, such as SAML, XACML and XML-Encryption, and proposed specifications, such as WS-Security.

Business Impact Areas: Interoperable and discoverable mechanisms for secured linking of Web services across public networks. Technologies will include standardized security tokens for identity, access control, policy agreement, trust and platforms to manage Web services security enterprisewide.

Selected Vendors: Entrust, IBM, Microsoft, Netegrity, Oblix, VeriSign, Vordel and Westbridge Technologies.

Analysis by Ray Wagner

4.3 Managed Security Service Providers

Definition: Outsourcing of remote management and monitoring of security devices, including firewalls, intrusion detection systems and gateway antivirus systems. (See "Surviving the Managed Security Services Shakeout," DF-13-1973).

Time to Plateau/Adoption Speed: Two to five years.

Justification for Hype Cycle Position/Adoption Speed: The consolidation of smaller managed security service providers (MSSPs) will continue as larger, established vendors acquire pure-play vendors to gain technology and customers.

Business Impact Areas: Enterprises, particularly smaller companies, can focus on their businesses while outsourcing part or all of their network and other information security functions to MSSPs. They will benefit from an improved security posture through active monitoring and management of security technology, lower costs for 24x7 infrastructure and resources, and reduced security incident costs.

Selected Vendors: AT&T, Computer Sciences Corp., Counterpane Internet Security, EDS, Guardent, IBM, Internet Security Systems, RedSiren, SAIC, Symantec, Ubizen and Unisys.

Analysis by Kelly Kavanagh

4.4 Biometrics

Definition: The use of an element of "what you are" as a form of identification and authentication. Includes finger or hand scans, handwriting on a tablet, keyboard ballistics, iris scans and facial recognition (see "Trusted E-Signatures Through PKI, Smart Cards and Biometrics," COM-17-0295, and "Biometrics: How Do They Measure Up?" COM-15-1727).

Time to Plateau/Adoption Speed: Two to five years.

Justification for Hype Cycle Position/Adoption Speed: False acquisition and acceptance rates are too high for broad-based usage, and there are privacy concerns. However, for relatively small implementations, adequate solutions are available.

Business Impact Areas: Improved identification using a token that cannot be lost. If successful in overcoming technological limitations, biometrics will offer nontoken-based identification and authentication of users.

Selected Vendors: Bioscrypt, DigitalPersona, Identix, Polaroid, Viisage Technology and Sony.

Analysis by Vic Wheatman

4.5 Advanced Encryption Standard

Definition: The National Institute of Standards and Technology selected the Advanced Encryption Standard (AES) to protect electronic information and officially replace the U.S.-government-endorsed Data Encryption Standard (DES), which the government adopted in 1977 (see "Plan to Migrate to Advanced Encryption Standard," FT-14-9343).

Time to Plateau/Adoption Speed: Two to five years.

Justification for Hype Cycle Position/Adoption Speed: Enterprises that use DES should plan to migrate to AES as soon as feasible. However, unless they face unacceptable system sluggishness, enterprises that use the Triple DES (3DES) standard should wait until system upgrades permit a low-cost AES implementation. DES has been broken; 3DES is difficult to break, but it is processor-intensive.

Business Impact Areas: Improved symmetric encryption over easily broken single DES.

Selected Vendors: Baltimore Technologies, Certicom, Phaos Technology and RSA Security.

Analysis by Vic Wheatman

4.6 Intrusion Detection Systems

Definition: Software running on a host or a network sensor that identifies malicious activity and creates an alert.

Time to Plateau/Adoption Speed: Obsolete before Plateau.

Justification for Hype Cycle Position/Adoption Speed: Intrusion detection systems are a market failure. Vendors are now hyping intrusion prevention systems, which also have stalled. The functionality is moving

into firewalls, which will perform deep packet inspection for content and malicious traffic blocking, as well as antivirus activities.

Business Impact Areas: Security and network management.

Selected Vendors: Cisco, Enterasys Networks, Entercept, Internet Security Systems, Symantec and Tripwire.

Analysis by Richard Stiennon

5.0 Climbing the Slope

5.1 Identity and Access Management

Definition: Identity management is the capability to manage (create, modify and delete) all user accounts, profiles and other information that can be identified with each person across the heterogeneous IT environment via a combination of user roles and business rules. In addition, identity management abstracts and automatically correlates data from HR, CRM, e-mail systems and other "identity stores," and from the managed systems. Fulfillment is accomplished in a variety of ways: in response to a self-service request (for example) self-registration, a line management request (for example, the manager has a new employee starting on a certain date, or a user needs access to an application), a change in an HR system (for example, employee termination) or a bulk load for purposes of a new application or merger/acquisition.

Access management is the capability to manage (across multiple target systems) an access control policy (or policies), including policy administration and enforcement.

Time to Plateau/Adoption Speed: Two to five years.

Justification for Hype Cycle Position/Adoption Speed: There are a number of implementations for managing internal or external users. Limitations have been on managing the entire business process of access request processing, not just the "hire or fire" process.

Business Impact Areas: Business facilitation, cost containment, regulatory compliance, operational efficiency and risk management. In the future, the focus will be on business process automation, an enterprise console to manage all users and in-depth application user provisioning.

Selected Vendors: BMC Software, Business Layers, Computer Associates International, Courion, Entrust, IBM/Tivoli, Microsoft, Netegrity, Novell, Oblix, OpenNetwork Technologies, RSA Security, Thor Technologies and Waveset Technologies.

Analysis by Roberta Witty

5.2 Enterprise Digital Rights Management

Definition: Applying digital rights management principles to enterprise messaging, documents and intellectual property to protect against inappropriate or unintended disclosure of proprietary or confidential enterprise information.

Time to Plateau/Adoption Speed: Two to five years.

Justification for Hype Cycle Position/Adoption Speed: Microsoft has announced that its Rights Management Server technology will be included in the Windows 2003 Server. This is a precursor to

widespread deployment of the technology formerly called "Palladium," which provides hardware and lower-level OS support for security mechanisms, including rights management.

Business Impact Areas: Limits access to confidential enterprise data, focusing on casual or unintended disclosure of information.

Selected Vendors: Authentica and Microsoft.

Analysis by Ray Wagner

5.3 Public-Key Infrastructure

Definition: A system for generating and managing digital certificates that identify the holder of assigned public and private key pairs, which can be used for identification/authentication, encryption and digital signing (see "Public-Key Infrastructure Q&A," QA-18-7301).

Time to Plateau/Adoption Speed: Two to five years.

Justification for Hype Cycle Position/Adoption Speed: The original, much-hyped public-key infrastructure (PKI) vision is changing to recognize the difficulty of deploying infrastructure by moving key management functions away from centralization attempts and placing these functions close to supported applications, and by applying public-key technology to Web services security.

Business Impact Areas: Improved management of public/private key pairs is needed for a variety of applications. PKI offers ways for enterprises to strengthen user identification and authentication, and helps manage public/private key pairs that are useful for several security applications.

Selected Vendors: Baltimore Technologies, Entrust, GeoTrust, Microsoft, VeriSign and RSA Security.

Analysis by Vic Wheatman

5.4 Tokens/Smart Cards

Definition: Access authentication mechanisms.

Time to Plateau/Adoption Speed: Two to five years.

Justification for Hype Cycle Position/Adoption Speed: Pervasive, strong, authenticated access control is a solution to user ID/password vulnerabilities. The goal is to make the login process "hack-proof." One-time password tokens require a server, but few changes to applications. Smart card systems require readers. The technologies are mature, but suffer from two barriers — the cost of implementing tokens and the lack of readers for smart cards.

Business Impact Areas: Tokens and smart cards can provide portability across many systems; the access control cannot be used without something the user "knows" and "has" in the form of physical control of the token. Benefits include ease of use and nonrepudiation. Smart cards can provide a secure repository of user data in the authentication device. Software versions of tokens and smart cards are becoming more attractive as methods improve to make them portable in software, and to make them run as guest processes on mobile devices.

Selected Vendors: ActivCard, DataCard, Datakey, Gemplus, RSA Security, Schlumberger (DeXa.Badge) and Secure Computing.

Analysis by John Girard

6.0 Entering the Plateau

6.1 Firewall Appliances

Definition: Combined OS and software delivered on a "hardened" platform.

Time to Plateau/Adoption Speed: Less than two years.

Justification for Hype Cycle Position/Adoption Speed: This is a mature market. Only one software vendor (Check Point Software Technologies) delivers more than 50 percent of its product on an appliance.

Business Impact Areas: Will facilitate ease of deployment and management. Firewall appliances operate at higher performance levels than software-only solutions.

Selected Vendors: Check Point, Nokia, SonicWALL, Symantec and WatchGuard Technologies.

Analysis by Richard Stiennon

6.2 Secure Sockets Layer

Definition: Data traveling over open networks between Web browsers and servers is encrypted to protect privacy by using server-side digital certificates that represent public/private key pairs (see "Secure Sockets Layer Sometimes Isn't," T-16-0632).

Time to Plateau/Adoption Speed: Less than two years.

Justification for Hype Cycle Position/Adoption Speed: SSL is proving to be scalable and applicable to many Web-based applications for protecting privacy on open networks.

Business Impact Areas: Facilitates improved protection of data. SSL is being applied to forms of secure e-mail, virtual private networks and various Web-based applications. With load balancing and acceleration, SSL is highly scalable.

Selected Vendors: Certificate providers include Entrust, GeoTrust, Thawte Consulting and VeriSign.

Analysis by Vic Wheatman

7.0 Conclusion

Investing in an overhyped security technology too early can result in a waste of enterprise security funds. Investing too late can affect an enterprise's competitive position and increase vulnerabilities. Enterprises should focus on their assessment of business needs and threats to prioritize their security needs.

Appendix A: Hype Cycle Definitions

Technology Trigger: A breakthrough, public demonstration, product launch or other event generates significant press and industry interest.

Peak of Inflated Expectations: During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the technology is pushed to its limits. The only enterprises making money are conference organizers and magazine publishers.

Trough of Disillusionment: Because the technology does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.

Slope of Enlightenment: Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the technology's applicability, risks and benefits. Commercial, off-the-shelf methodologies and tools ease the development process.

Plateau of Productivity: The real-world benefits of the technology are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. The final height of the plateau varies according to whether the technology is broadly applicable or benefits only a niche market. Approximately 30 percent of the technology's target audience has or is adopting the technology as it enters the Plateau.

Time to Plateau/Adoption Speed: The time required for the technology to reach the Plateau of Productivity.

Appendix B: Acronym Key

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
DES	Data Encryption Standard
EAP	Extensible Authentication Protocol
IM	instant messaging
MSSP	managed security service provider
SAML	Security Assertion Markup Language
SSL	Secure Sockets Layer
WLAN	wireless local-area network
WPA	Wi-Fi Protected Access
XACML	Extensible Access Control Markup Language
XML	Extensible Markup Language