Gartner
Technical Professional Advice

G00217744

Maverick* Research: The Death of Authentication

Published: 7 October 2011

Analyst(s): Bob Blakley

Authentication is obsolete in a world of pervasively available personal information; it will disappear over time and be replaced by recognition technologies. Maverick research deliberately exposes unconventional thinking and may not agree with Gartner's official positions.

Table of Contents

Summary of Findings

*Maverick Research

This is "Maverick" research, designed to spark new, unconventional insights. Maverick research is unconstrained by our typical broad consensus-formation process to deliver breakthrough, innovative, and disruptive ideas from our research incubator. We are publishing a collection of more than a dozen Maverick research lines this year, all designed for maximum value and impact. We'll explore each of these lines of research to help you be ahead of the mainstream and take advantage of trends and insights that could impact your IT strategy and your organization. (See Note 1 and Note 2).

Bottom Line: Authentication is a bad technology: It's expensive to implement, it's hard to use, it's too easy to subvert or circumvent, and it fails more and more frequently and more and more spectacularly in today's increasingly risky electronic environment. Until recently, there was no alternative, but now there is: Enough personal information exists in electronic form that we can move from authentication to recognition — and we will.

Context: A large number of recent incidents — characterized in the press and the security community as privacy breaches — are trying to teach us that a tremendous amount of information about people and their activities exists in the electronic world. We can use that information for evil purposes (e.g., to invade people's privacy), or we can ignore it — but we can also use it to improve peoples' online experiences.

Take-Aways:

- Authentication has never worked very well, and it's degrading quickly in effectiveness.
- Until recently, no alternative to authentication existed when we wanted to gain any degree of confidence in peoples' identities.
- The explosion of online data about people and their actions gives us a new option: recognition.
- Recognition is how we identify people in the real world, and we've already started to do it in the electronic world — albeit mostly in low-assurance scenarios.
- Enterprises will move from authentication to recognition over the next decade.
- The change will be gradual, and the two solutions will coexist for several years.
- Authentication vendors need to start preparing for the shift now.

Conclusion: Authentication is everywhere, but it's sick, and it's going to die. It's going to be replaced by recognition — which is the way humans recognize each other in the real world. But the move to recognition will be gradual, and it will require that we pay significant attention to privacy.

Analysis

Pediatricians tell us a baby can recognize its mother by the time it's a month old. Your computer is much dumber than that. It sees you every day for years, and you still have to tell it your name and then find something you lost (like a smart card) and reset something you forgot (like a password) before it figures out who you are. In the future, computers will be much smarter; like Stanley Kubrick's HAL 9000, they'll just recognize you — and you won't need cards, passwords, or any other "authentication" artifacts. And it's already starting to happen.

News

In April 2010, the collection of Wi-Fi location data by Google Street View flared into controversy when German data protection regulators (who had expressed earlier misgivings about photographs of peoples' faces and car license plates invading citizens' privacy under Germany's strict laws), became alarmed by reports that Street View cars were recording information about private citizens' Wi-Fi access points. Although Skyhook Wireless and other firms had been collecting information about Wi-Fi access points for more than five years in Germany and elsewhere, the German authorities pressed Google to explain its practices and what data it was collecting. On 27 April 2010, Google responded to the regulators' request by publishing a statement claiming, among other things, that Google Street View did not collect Wi-Fi payload data in Germany. The German data protection authority asked Google to review the data to confirm this, and Google contracted with a third party to complete the review. The review confirmed that Wi-Fi payload data was indeed collected — from unencrypted Wi-Fi networks — by Google Street View; Google issued a revised statement admitting that this was the case on 29 June 2010. Google's revised statement also announced that Google had discontinued Street View's practice of collecting Wi-Fi access point information. In the wake of the incident, data protection authorities in France and Germany have fined and sanctioned Google, and the U.S. Federal Communications Commission (FCC) has opened an investigation. Despite a 2011 court opinion declaring that Street View is not illegal per se in Germany, Google opted in April 2010 to discontinue collection of any new Street View data in the country.

On 15 December 2010, Facebook posted a blog entry entitled "Making Photo Tagging Easier." The entry described a capability Facebook calls "tag suggestions." This capability uses face recognition software to compare faces in newly uploaded photos with faces already tagged with peoples' names on Facebook. When tag suggestions finds a match, it suggests a tag to the person uploading the new photo. The introduction of the feature caused a public outcry and triggered a European Union privacy probe and a complaint by the Electronic Privacy Information Center (EPIC) to the U.S. FCC. In response to the controversy, Facebook initially provided some additional information to help users change Facebook privacy settings to restrict others' ability to tag them in photos. In August 2011, after a demand from Hamburg's Data Protection Commissioner to disable the feature by default, Facebook introduced a new "tag approval" feature, which allows users to prevent tagged photos of them from showing up in their own streams, but does not allow users to prevent others from tagging them in photos altogether.

In March 2011, Yiannis Kakavas of Darmstadt Technical University released the Creepy application. Creepy takes as input social network account names (Twitter, Foursquare, Flickr, TwitPic, yfrog, and others are supported) and examines geolocation metadata to build a map of locations the account holder has been at. The most interesting aspect of Creepy is that it enables geolocation based on the photographs a user uploads to public websites by using the EXIF metadata most cameras now embed in digital photos. Several news articles have characterized Creepy as a tool for cyberstalking.

On 24 March 2011, Color launched its iPhone app, also called Color. The app allows users to share photos with every other Color user within 150 feet; nearby users can see not only recently shared photos but also all photos the sharer has ever taken with the app. Color's founders made it clear from the outset that the app is intended for people who have no problem with totally public sharing; CNN quoted Color President Peter Pham as saying "we're all inherently voyeuristic," and Switched quoted Color (and Lala) founder Bill Nguyen as saying "This is like TiVo-ing life; there's no forgetting." *The Wall Street Journal* noted that Color breaks new ground with its "everything's public" approach to privacy, but the main complaints about Color so far have centered on its user experience.

On 20 April 2011, Pete Warden and Alasdair Allen released the iPhone Tracker application at the Where 2.0 conference. This Mac application allowed users to see location information recorded by their iOS4 iPhone handsets on a map overlay. The location data did not technically identify the location of the handset itself; instead it recorded the locations of nearby Wi-Fi access points. Apple had programmed iPhones to capture and report this information in order to build a crowdsourced database to improve the speed and accuracy of the iPhone's location services. An outcry quickly arose; on 27 April, Apple released a statement describing what the iPhone was doing and why. The company characterized the size of the location database maintained by the phone as a bug and promised a fix, which it duly delivered in the iOS 4.3.3 update on 4 May 2011.

On 4 August 2011, Alessandro Acquisti of CMU presented a paper at the BlackHat conference in Las Vegas in which he demonstrated that off-the-shelf face-recognition software could reliably identify a large percentage of individuals based on pictures of their faces and Facebook information — and that this identification could be combined with other publicly available information to create a dossier of quite a lot of data which is generally considered private — including partial Social Security numbers (SSNs).

And it doesn't stop there; in case somebody wants to send a drone-launched Hellfire missile to the Helmand poppy field in the background of that jihadi video you just uploaded, Intelligence Advanced Research Projects Activity (IARPA) is working on an app for that.

Perspective

Each of these incidents was reported as an assault on privacy; bad guys (Google, Facebook, Apple, and various researchers) were "misusing" "our" data to nefarious ends. But together, these and many other similar incidents form a picture of a broad and important change in the way the world works and the way we interact with the world and with each other.

In 1910, Edmond Locard established the Laboratory of Police Techniques in Lyon, France. His laboratory would go on to invent forensic fingerprint identification, and he would formulate the principle that today lies at the foundation of all forensic police work: The Principle of Exchange.

Locard said "Toute action de l'homme, et a fortiori, l'action violent qu'est un crime, ne peut pas se dérouler sans laisser quelque marque" — every action of a man, and especially violent criminal acts, cannot occur without leaving a trace.

This principle — "every action leaves a trace" — is as true of the electronic world as the physical world; electronic interactions leave behind Internet Protocol (IP) addresses, system logs, metadata, caches, cookies, and a host of other traces. But until recently, most of this information went unused, at least for the purpose of identifying people and their actions.

For most of human history, the natural world had eyes everywhere but no memory; the electronic world originally had memory everywhere but no eyes. But there is only one world now; the fable that electronic systems were somehow distinct from the natural world is now a fantasy. The U.K.'s closed-circuit TV (CCTV) cameras were an early symptom, but now every telephone is a camera and an audio recorder; every tollbooth, every automated teller machine (ATM), every border crossing, and many stoplights photograph us and store the results; every supermarket check-out scanner and Web page records our visit. Chief Seattle told us "when your children's children shall think themselves alone in the field, the store, the shop, upon highway, or in the silence of the woods, they will not be alone. In all the earth there is no place dedicated to solitude" — and it is so. In all the earth, there is no place dedicated to solitude. Every action leaves a trace, and the traces are gathered up into databases and used in ways we have a hard time imagining.

Some privacy advocates would love to put this genie back in the bottle; this is the motivation behind requirements to limit collection of personal information. It's unlikely this can happen; electronic systems simply don't work without identifying information. Routers need IP addresses to move packets back and forth between senders and receivers. ISPs need to assign IP addresses to their customers in order to provide service, and they need to identify the customers in order to bill for service. Mobile phone network operators have to be able to establish the geographic location of phone handsets so they know which tower to activate when they want to make a subscriber's phone ring. And the list goes on and on. Every online action leaves a trace because every action MUST leave a trace. We could erase some of these traces (after a period of time probably specified by law enforcement), but the electronic world isn't very good at erasing or forgetting things; many pieces of identifying information exist in multiple copies, in multiple systems, owned by multiple organizations — even finding all the things we'd like to erase would be a daunting task.

But a visitor from another planet would not look at the news reported above and say "privacy is under attack"; he (or she, or it) would say "the humans are finally starting to notice all the traces they leave behind in the electronic world."

Privacy advocates focus on the situations in which the traces identify us despite the fact that we don't want to be identified. In some situations, however, we do want to be identified, and current mechanisms aren't working very well — and before we set the rules of the new world in stone, we should look at those situations, too.

Precedent

In 1676, Antonie van Leeuwenhoek notified London's Royal Society that he had used a microscope of his own design to view single-celled organisms. The discovery was immediately controversial; the Royal Society questioned his sanity and his eyesight, and the church questioned his orthodoxy. Although physicians were already theorizing that smallpox was caused by a microorganism as early as 1700, it took more than a century for the germ theory of disease to be accepted even by the scientific community. Ignaz Semmelweiss, who dramatically reduced infant mortality in a Vienna hospital by requiring doctors to wash their hands in 1847, was ridiculed by the Viennese medical establishment for his troubles — and it wasn't until after John Snow's famous treatment of the 1854 London cholera epidemic by removing the handle of an infected pump that the role of microorganisms in human illness began to be widely understood and believed.

It took a long time for society to change its behavior in response to the discovery of microorganisms in part because they were hard to see without special equipment. Leeuwenhoek kept his microscope designs and fabrication techniques secret to preserve his advantage over other investigators. High-quality mass-produced microscopes didn't become available until Zeiss started producing them in the 1860s. Once good microscopes could be bought at a reasonable price, significant numbers of people were able to see bacteria and other tiny things for themselves — and when people see things differently, we think and act differently. The microscope extended our senses, and what we saw changed how we lived; before Semmelweiss, we burned witches when an epidemic broke out; afterward, we washed our hands.

Like the microscope, the smartphone augments our senses. What it shows us is the traces we leave in the electronic world, which have existed invisibly for a long time now. Like the microscope, the smartphone — and what it reveals to our newly augmented senses — will change our behavior.

Prognosis

Authentication is a consequence of — or perhaps a reaction to — our blindness online. In real life, we seldom authenticate except when the stakes are very high. What we do instead is recognize. When you show up at my door, you bring your face, and your voice, and your style of dress, and your mannerisms, and your knowledge of our shared history. Generally, if we're already acquainted, that's enough — our identities are established to the satisfaction of both of us.

If we're not acquainted, we introduce ourselves, and we begin to work on forging a relationship. Forming solid relationships takes time, and sometimes we need to work with strangers (or people not well known to us) on important matters — for example, we sometimes need to withdraw thousands of dollars in cash from a bank branch where none of the employees knows us. We've invented social mechanisms to deal with high-stakes introductions. Letters of introduction were one such mechanism — the letter uses the writer's relationship with the reader to vouch for its subject. Benjamin Franklin wrote a letter of introduction to his colonial colleagues for the Englishman Thomas Paine; the letter may have saved Paine's life when he arrived in the New World gravely ill and Franklin's friends and relatives took him in.

Another mechanism for introducing strangers is the password; passwords are secret code words given to scouts and messengers to allow them to pass through lines of friendly — but suspicious and heavily armed — pickets guarding the perimeter of an army encampment.

Authentication is really good for introductions — allowing Ben Franklin to introduce Tom Paine to Franklin's buddies in Philadelphia as "a guy you can trust." But once Richard Bache and Robert Aitken have examined Ben's letter and decided to trust Tom, they can throw the letter away — they know Tom now, and they can recognize him the next time they see him.

And Richard and Robert should throw the letter away; authenticating people we already know wastes time and effort, and in electronic systems, it creates vulnerabilities. It requires those being authenticated to remember something complicated or carry something inconvenient. It requires a degree of skill and goodwill on the part of those being authenticated. It does too much work: most of the time the person being authenticated is not a stranger to the organization, and could (if enough information were available) be identified as a returning, known user without requiring additional proof.

And authentication plays the game on the enemy's terms; someone who wants to impersonate Bob Blakley can present himself to an authentication system and claim to be Bob Blakley — at which point an authentication system will try to prove this false claim by verifying the impostor's forged credential. If the credential can be verified, most authentication systems won't evaluate evidence that the user might be an impostor — even if that evidence is present.

But in the electronic world, we couldn't throw away the letters of introduction and the passwords because we couldn't recognize: none of our senses operated in the electronic world until recently. We could not hear each other's voices; we saw as in a mirror, darkly and not face to face. Because we were unable to recognize, we kept introducing and authenticating over and over again by requiring users to remember passwords or carry tokens. It hasn't worked very well; a whole litany of failures — including most recently the PIN-cracking that allowed News of the World to snoop on voice mails, the acquisition by a hacker of the DigiNotar Certificate Authority's administrative password, and the intrusion that led to the subversion of a large number of RSA SecurID hardware authentication tokens — provide ample evidence of authentication's failures.

The good news is that (as we've seen) enough information now exists in the electronic environment to allow us to start recognizing people; if we want to, we can just stop authenticating except when we really need to introduce.

Prediction

Over time, authentication will be replaced by recognition in most applications.

Here's How It Will Happen

Recognition will start by augmenting authentication, and will gradually supplant it…

Phase 1:

Security designers and the public at large will begin to realize that the "new sense" provided by augmented reality applications connected to rich sources of personal data can be used for recognition. This phase is already well under way; as the examples listed in the "News" section of this report — and especially Alessandro Acquisti's research — demonstrate.

Phase 2:

Organizations with requirements for high levels of identity assurance will use recognition as an adjunct to authentication — for example, to provide additional confidence in the user's identity when an especially sensitive or consequential transaction is attempted, or when there is some reason to doubt that the authentication process has correctly identified the user. This phase is also already under way; device fingerprinting (or, more broadly, "endpoint authentication"), Web fraud detection, and risk-based authentication solutions are increasingly being used by banks to augment their authentication processes.

Phase 3:

Organizations will realize that their recognition techniques' assurance level is higher than that of the authentication techniques they supposedly supplement, and that while recognition involves no user actions and few user experience issues, authentication is a major user dissatisfier and a disproportionate consumer of help desk resources.

Phase 4:

Organizations will abandon authentication — except for introduction use cases — in favor of the recognition technologies already in place once they conclude that authentication is an additional expense that cannot be cost-justified based on increased identity assurance.

Organizations will move through these phases at different rates, depending on their risk appetites, tolerance for new solutions, and regulatory obligations. In 2013, few organizations will be relying solely or primarily on recognition; by 2020, most will be.

Here's What It Will Look Like

Bob walks into his bank and wants to withdraw $9,000 for that new Leica Noctilux 50mm f/0.95 lens he's had his eye on. He's going to buy the lens from B&H Photo in New York City (because B&H is the only retailer that has the lens in stock). He's already in New York, so he's obviously not going to his bank branch in Round Rock, Texas. The teller, who's never seen Bob before, greets him.

TELLER: How can I help you today?

BOB: I'd like to withdraw $9,000 in cash.

TELLER: Sure. Do you consent to our accessing your electronic information for recognition purposes on a one-time basis? We won't store or share any of the information we use.

BOB: Yes (Bob really wants the lens).

TELLER: OK, please call this number from your iPhone.

> Bob calls the number, and the bank's system does a caller ID check and collects a device fingerprint.

TELLER: Now please connect to this website from your phone's browser, and click OK when you see the popup box.

> Bob opens Mobile Safari and sees a popup box that says "Allow Giant Still-Solvent Bank to access your past week's location data?" He clicks "OK." The bank's system uses Bob's cell number to retrieve his name and home address from a data aggregator and his Texas Driver's license data from the Texas Department of Public Safety. The bank then checks Bob's phone location history and verifies that the phone was at Bob's home address at 1 a.m. last night and the night before, and then checks the Texas Tollways database to verify that Bob's phone was on Texas Highway 130 at the same time the Tollways authority charged $0.75 to Bob's account when his car passed under the automated toll collection gantry on the way to the Austin Bergstrom airport yesterday. Finally, the bank's system pulls up Bob's driver's license picture and displays it to the teller.

> The teller opens his drawer.

TELLER: Here's your $9,000, Dr. Blakley. Have a nice time in New York!

Market Impact

The technologies necessary to support recognition exist and are already emerging (see "Hype Cycle for Emerging Technologies, 2011"). Authentication vendors ignore this trend at their peril; the market for authentication will continue to grow, but it will grow toward recognition mechanisms and away from traditional authentication systems.

As this trend solidifies, strong authentication vendors will begin to acquire or partner with biometrics vendors. The main driver of this market consolidation won't be adoption of biometric recognition modalities, which have their own accuracy and user experience issues; instead, what will drive consolidation is the authentication vendors' recognition that biometrics vendors understand how to design processes, workflows, management systems, and exception handling procedures for recognition use cases.

Many parallel markets will contribute technology to a recognition-based identity assurance ecosystem; markets that will contribute include:

- Web fraud detection
- Behavior detection
- Fraud analytics
- Context aware computing

- Device fingerprinting and endpoint authentication
- Passive biometrics (e.g., face recognition, voice recognition, gait recognition, and keystroke dynamics)

Strengths

Recognition has many advantages over traditional authentication.

Authentication doesn't work very well, as the examples cited above illustrate. Authentication also suffers from serious user experience issues, and the market for authentication is getting increasingly fragmented as the existing technologies fail to keep up with the threat; for a taxonomy of currently available authentication technologies, see "A Taxonomy of Authentication Methods, Update."

Recognition systems aren't a new design problem; biometric recognition (or "identification," to use the biometrics market's own term) system-design patterns provide a sound basis for the non-biometric (or not exclusively biometric) recognition systems of the future.

The user experience of recognition systems (which don't depend on "something you lost" or "something you can't remember") will be much better than that of today's authentication systems.

Weaknesses

Recognition will have weaknesses, too.

The biggest issue will be privacy. People are uncomfortable with revealing large amounts of information about their behavior, movements, relationships, and purchases. As Gartner has already laid out in "Privacy," the only way to address these issues is to ensure that recognition systems are carefully designed to protect and enhance the dignity of individuals. This is best done through consent mechanisms and intelligent data deletion policies — transactional data should be kept only for as long as is needed to validate the transaction, and shouldn't be shared outside the set of parties necessary to complete the transaction.

The next biggest issue will be ensuring that the organizations doing the recognition — and therefore retrieving personal information about people — don't misuse the information they use to recognize us. Organizations themselves will have to have their identities verified by data aggregators and other data sources, and laws and contracts will need to strictly regulate access to and use of recognition data.

Recognition systems will also be subject to all the usual attacks; people will impersonate one another by stealing devices, by forging or copying each others' data, by performing man-in-the-middle attacks, by infiltrating and corrupting server systems, and so on. Merchant (and other counterparty) systems will be engineered by attackers or by their owners to misidentify users in order to defraud the unwitting. None of this is new, and none of it will be worse in recognition-based systems than it currently is in authentication-based systems.

Recommendations

The transition from authentication to recognition will be revolutionary, but it will occur in an evolutionary way. Organizations will have time to plan, prepare, and adapt. Here's what they should do.

End-User Recommendations

Enterprises should start experimenting with recognition technologies (device fingerprinting, passive biometrics, risk-based authentication, and identity analytics) today to get onto the experience curve for recognition. View these experiments as investments in developing a recognition capability (including process maturity and staff expertise), as well as a "here and now" authentication strength enhancement.

Enterprises should plan to periodically evaluate the cost-benefit equation for each of their authentication and recognition technologies.

Enterprises should not plan to implement recognition systems in-house; recognition requires skills most security staffs don't yet have, and it requires access to a wide variety of sources of personal data that are likely to be much more economical to use through intermediaries who can negotiate bulk-transaction rates. Flawed implementations of recognition can also lead to significant reputation damage and privacy compliance risk.

Vendor Recommendations

Strong authentication vendors should put research and development effort into recognition technologies and processes starting immediately.

Authentication vendors should consider alliances with biometrics (especially face and voice) vendors in order to develop expertise in design and operation of recognition systems. Keep a weather eye out for opportunities to turn these alliances into mergers or acquisitions.

Authentication vendors should develop a strategy to move to recognition. Initially, the strategy should be a contingency, but vendors need to define the events they will look for that will signal a market shift from authentication to recognition and be ready to move in a hurry when those events happen.

Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

- Tom Austin."Maverick* Research: Gain Value From Our Incubator of Unconventional Wisdom." *Gartner*. 7 Oct 2011.
- Mark Diodati. "Authentication." *Gartner*. 24 Feb 2011.
- Mark Diodati. "On the Verge: Strong Authentication as a Service." *Gartner*. 15 Jun 2010.

- Bob Blakley. "Designing Biometric Authentication and Identification Systems." *Gartner*. 13 Mar 2008.
- Ian Glazer, Bob Blakley. "Privacy." *Gartner*. 3 Apr 2009.

Other related Gartner research:

- Gregg Kreizman. "Hype Cycle for Identity and Access Management Technologies, 2011." *Gartner*. 13 Jul 2011.
- Avivah Litan. "The Five Layers of Fraud Prevention and Using Them to Beat Malware." *Gartner*. 21 Apr 2011.
- Avivah Litan. "Where Strong Authentication Fails and What You Can Do About It." *Gartner*. 3 Dec 2009. (This research is provided for historical perspective; portions of this document may not reflect current conditions.)
- Avivah Litan. "Updated FFIEC Guidance on U.S. Online Banking Security was Overdue." *Gartner*. 1 Jul 2011.
- Ant Allan, Avivah Litan. "Plan to Supplement RSA SecurID Replacement Tokens with Other Measures." *Gartner*. 8 Jun 2011.
- Ant Allan. "Market Overview: Authentication." *Gartner*. 26 Sep 2008.
- Ant Allan. "Market Scope for Enterprise Broad-Portfolio Authentication Vendors." *Gartner*. 17 Sep 2010.
- Ant Allan. "A Taxonomy of Authentication Methods, Update." *Gartner*. 25 May 2011.
- Ant Allan. "Authentication: Ten Myths and Misconceptions Debunked." *Gartner*. 4 Mar 2011.
- Avivah Litan. "Best Practices in Mobile User Authentication and Layered Fraud Prevention." *Gartner*. 11 Aug 2011.
- Jeff Vining. "Using Voice Recognition Technology to Capture Criminals." *Gartner*. 17 Feb 2011.
- Jackie Fenn, Hung LeHong. "Hype Cycle for Emerging Technologies, 2011." *Gartner*. 28 Jul 2011.
- Stephen Prentice, Jackie Fenn. "Hype Cycle for Human-Computer Interaction, 2011." *Gartner*. 28 Jul 2011.

Acronym Key and Glossary Terms

CCTV	closed-circuit TV
FCC	Federal Communications Commission
SSN	Social Security number

Note 1 Roots of the Word "Maverick"

Derived from the name of Texas rancher Samuel Maverick and his steadfast refusal to brand his cattle, "maverick" connotes someone who willfully takes an independent — and frequently disruptive or unorthodox — stand against prevailing modes of thought and action.

Note 2 Commonly Held Belief

The commonly held belief this note challenges is that authentication is critical to establishing identities of computer system users, and today’s flawed authentication methods will be replaced by stronger, more usable, and more reliable authentication methods in the future.

Regional Headquarters

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" on its website, http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp.