The Future of Security

The Trends and Technologies Transforming Security

Version 1.0
Released: February 20, 2014

cloud security alliance SM
Reviewed and Approved

Securosis, L.L.C.

http://securosis.com

Author's Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog but has been enhanced and professionally edited.

Copy and structural editing by Scholle McFarland: scholle@sawmac.com

Special thanks to Chris Pepper for additional editing and content support.

Licensed by Box

Box is a secure way to share content and improve collaboration for businesses of any size, on any device. Desktop, tablet or mobile. The company believes technology should never limit the invention and productivity of enterprising minds. Box is the preferred choice of 225,000 businesses and 25 million customers.

For more information, please visit: www.box.com

Reviewed and Approved by the Cloud Security Alliance

This content of this *independently created* paper has been reviewed and approved by the Cloud Security Alliance. It does not imply endorsement of any specific vendors or products. Securosis would like to thank the CSA for their support in reviewing the content.

For more information visit http://cloudsecurityalliance.org.

Copyright

Table of Contents

EXECUTIVE SUMMARY

The Future of Security

A Disruptive Collision: The Trends and Technologies Transforming Security

Disruption defines the business of information security. New technologies change how businesses work, as well as what risks people take. Attackers shift their strategies. But the better we security professionals predict and prepare for these disruptions, the more effective we can be.

Cloud computing is a radically different technology model — not just the latest flavor of outsourcing. It uses a combination of abstraction and automation to achieve previously impossible levels of efficiency and elasticity. But in the end cloud computing still relies on traditional infrastructure as its foundation.

- **Cloud computing** is a radically different technology model — it is not simply the latest flavor of outsourcing. It uses a combination of *abstraction* and *automation* to achieve previously impossible levels of efficiency and elasticity. This, in turn, creates new business models and alters the economics of technology delivery and consumption.
- The *abstraction* and *automation* used to build clouds disrupt existing security controls and processes. Risks shift; some increase, others decrease. While the fundamentals remain the same, security must adapt to the new environment.
- **Mobile** computing challenges security because we can no longer rely on managing users' devices or the networks they use to access sensitive resources. It *decentralizes* access on a global scale.
- Loss of control over devices and networks forces security to adjust its models to maintain data and workflow security, but the devices themselves are often *more inherently secure* than employee computers.

> Most security professionals focus on the risks of *multitenancy* in cloud computing, but the key risks actually result from **abstraction** and **automation**.

Implications for Security Practitioners

In the future, security practitioners will rely on a different core skill set than many professionals possess today. Priorities shift as some risks decline, others increase, and practices change. The result is a fundamental alteration of the day-to-day practice of security and its required skills:

- *Audit/assessment* and *penetration testing* are essential to understand the highly variable security of providers, and to assure security works as expected.
- *Incident response* is already in high demand, and must expand to cover response in the cloud-distributed enterprise.
- *Secure programming* orchestrates and automates security across cloud, mobile, and internal security tools.
- *Big data security analytics* makes sense of the vast amounts of security data we now collect, and better detect and remediate incidents involving advanced attackers.
- *Security architects* assess and design security controls — internally, across cloud providers, and for applications.

Implications for Security Providers

We already see cloud and mobile adoption and innovation outpacing many security tools and services. Here is how security providers can prepare for the future:

- *Support APIs* so customers can directly integrate your products into infrastructure, applications, and services.
- *Lose the bump in the wire* because cloud-distributed organizations won't centralize all network traffic for you to scan or manage.
- *Provide feeds and logs* so your tool integrates with the Security Operations Center of the future; don't require customers to log into your product to access data.
- *Assume high rates of change* which exceed the scheduled periodic scans and assessments we tend to rely on.

Implications for Cloud Providers

Customers cannot move to cloud providers they can't trust. Providers who make security a top front-office priority reduce the obstacles to customer adoption.

- *Build a security baseline* that is as or more secure than an enterprise datacenter.
- *Defend against advanced attacks*. You are a bigger target than any single customer, and the rewards are higher for the bad guys.
- *Don't alter user data or workflows.* They own them, not you.
- *Protect the cloud supply chain*. A failure of one of your providers shouldn't damage your customers.
- *Support APIs for security* so customers can manage and integrate it themselves.
- *Document security* for both your internal controls and what customers can manage, so they know *how you enable their security strategy*.
- *Provide security logs and feeds* so customers always know what is happening with their data and workloads.

The future of security is here — it just isn't evenly distributed. Keep your eye on these trends, make smart decisions, and plan for the future, and you will start seeing benefits today.

A Disruptive Collision: The Trends and Technological Changes Reshaping Security

Disruption defines the business of information security. New technologies change how businesses work, and what risks people take. Attackers shift their strategies. But the better we security professionals predict and prepare for these disruptions, the more effective we can be.

As analysts, we at Securosis focus most of our research on the here and now — on how best to tackle the security challenges faced by CISOs and security professionals when they show up to work in the morning. Occasionally, as part of this research, we note trends with the potential to dramatically affect the security industry and our profession.

This paper starts with a description of the disruptive forces at work in our industry, but its real objective is to lay out their long-term implications for the practice of security — and how we expect security to evolve for security professionals, security vendors, and cloud and other infrastructure providers. Through the report we will back up our analysis with real-world examples that show this transformation isn't a vague possibility in a distant future, but is already well under way.

Although these changes are inevitable, they are far from evenly distributed. As you will see, this provides plenty of time and incentive for professionals and organizations to prepare.

Technological Changes You Cannot Ignore

Clayton Christensen first coined the term "disruptive technology" in 1995 (he later changed the term to "disruptive innovation") to describe new business and technology practices that fundamentally alter, and eventually supersede, existing ones. Innovation always causes change, but *disruptive innovation mandates change*. Innovation creates new opportunities and disrupts old ones.

Cloud Computing

Every major enterprise we talk with today uses cloud services. Even some of the most sensitive industries, such as financial services, are exploring more extensive use of public cloud computing. We see no technical, economic, or even regulatory issues slowing this shift. The financial and operational advantages are simply too strong.

What It Is and Isn't: Cloud computing is a radically different technology model — it is not simply the latest flavor of outsourcing. It uses a combination of *abstraction* and *automation* to achieve previously impossible levels of efficiency and elasticity. This, in turn, creates new business models and alters the economics of technology delivery and consumption.

Cloud computing fundamentally disrupts traditional infrastructure because it is more responsive, more efficient, and potentially more resilient and cost effective than old ways of doing things. Public cloud computing is even more disruptive because it enables organizations to consume only what they need without maintaining overhead, while still rapidly

responding to changing needs at effectively infinite scale (assuming an adequate checkbook). For more information see our paper, *What CISOs Need to Know about Cloud Computing*

Losing Physical Control: Many of today's security controls rely on knowing and managing the physical resources that underpin our technology services. The cloud breaks this model by virtualizing resources (including entire applications) into resource pools managed over the network. We give up physical control and shift management functions to standard network interfaces, creating a new *management plane*. This challenges — and sometimes destroys — traditional security controls.

Abstraction separates something from the underlying physical infrastructure. Virtualization is the technology we use to accomplish this.

Greater reliance on external providers also means greater dependence on their inherent security measures. Providers have a strong incentive to maintain best-in-class security, because failures destroy client trust and their ability to grow their customer base. But cloud service providers' capabilities vary greatly, so cloud consumers must assess and audit providers regularly.

A New Emphasis on Automation: The cloud enables extreme agility, such as servers that exist only for hour or minutes — automatically provisioned, configured, and destroyed without human interaction. Application developers can check in a piece of code that then runs through a dozen automated checks and is pushed into production on a self-configuring platform which scales to meet demand. Security that relies on controlling the rate of change, or that mandates human checks, simply cannot keep up.

Automation is the key difference between cloud and simple virtualization. It adds orchestration capabilities so the cloud can handle previously manual tasks, such as launching a virtual machine, assigning an IP address, and setting administrative credentials.

The cloud's elasticity and agility also enables new operational models such as *DevOps*, an IT model that blurs the lines between development and operations and consolidates historically segregated management functions to improve efficiency and responsiveness. Developers play a stronger role in managing their own infrastructure through heavy use of programming and automation. The cloud enables management of infrastructure using APIs, so it is a major enabler of DevOps. While DevOps is incredibly agile and powerful, it can also be disastrous to security and availability because it condenses many of the usual application development and operations check points.

Old Problems Fade: Some security issues recede in the cloud. For example, networking sniffing is largely impossible. The dynamic nature of cloud servers can reduce the need for traditional patching — you can launch a new fully up-to-date server and shift live traffic to and from it with API calls. Network segmentation becomes the default. Centralizing resources improves our ability to audit and control while still providing ubiquitous access.

Looking at current rates of adoption, we expect public cloud computing to become the dominant technology model over the next ten to fifteen years. As we make this transition the technologies underlying clouds, rather than the increased use of shared infrastructure are what really matters for security.

Mobility

Walk down the street, pull your eyes away from your phone, and look around you. Less than a decade ago we accessed most technology services from desktop and laptop computers. Now we use mobile devices running on near-ubiquitous high-speed wireless networks. It is hard to fully grasp how rapidly this shift has occurred, and its implications for security.

Workers don't wait to be issued a corporate phone — they walk in the door with a computer in their pocket more powerful that what was on their desks five years ago. They expect to access email and other corporate services from wherever they are, on whatever device they have. Some organizations manage to limit this somewhat, but a generation of workers has used phones and tablets since elementary school and these devices are their own. They expect high-speed Internet access wherever they go, all the time. Organizations' ability to restrict workers' computing options will only continue to decline, especially when it conflicts with productivity for an always-on workforce.

Mobility challenges security because we can no longer rely on managing users' devices or the networks they use to access sensitive resources. Our ability to manage the user experience is also restricted to whatever features mobile device manufacturers support. Market forces drive companies to appeal to us first as consumers rather than workers — high rates of innovation sometimes conflict with corporate control.

Multitenancy Isn't the Problem

The security implications of abstraction and automation in cloud computing dwarf those of multitenancy. Security professionals have more experience reducing risks in shared infrastructure than they do with highly virtualized and automated environments.

Six Trends Changing the Face of Security

The cloud enables mobility by freeing enterprise assets from their reliance on fixed data centers. Mobility in turn drives cloud adoption to meet user demand. Mobile devices become portals to the cloud, and the cloud becomes the engine for mobile applications and services. Both innovations upend older notions of computing, and seriously interfere with classical information security strategies.

With these changes in mind, we can picture how security will look over the next seven to ten years. We aren't necessarily entering a period of greater risk — just one where we need to adjust approaches and shift resources. Some risks increase, others decrease, and innovative new security approaches leverage these disruptions.

1: Hypersegregation

We have always known the dramatic security benefits of effective compartmentalization, but implementation was typically costly and often negatively impacted other business needs. This is changing on multiple fronts as we gain the ability to heavily segregate by default, with minimal negative impact. Flat networks and operating systems will not only soon be artifacts of the past, but difficult to even implement.

> Hypersegregation makes it much more difficult for attackers to extend their footprint once they gain access to a network or system, and it increases the likelihood of detection.

Most major cloud computing platforms provide cloud-layer software firewalls, by default, around every running virtual machine. In cloud infrastructure every single server is firewalled off from every other one by default. The equivalent in a traditional environment would be either a) host-based firewalls on every host, of every system type, with easily and immediately managed policies across all devices, or b) a physical firewall—which travels with the host if and when it moves—in front of every host on the network.

These simple firewalls are managed via APIs, and by default even segregate every server from every other server — even on the same subnet. There is no such thing as a flat network when you deploy onto Infrastructure as a Service, unless you work hard to reproduce the less secure architecture.

This segregation has the potential to expand into non-cloud networks thanks to *Software Defined Networking,* making hypersegregation the default in any new infrastructure.

The Example of Apple and Others: We also see hypersegregation working extremely effectively in operating systems. Apple's iOS sandboxes every application by default, creating another kind of 'firewall' inside the operating system. This innovation has contributed to iOS's complete lack of widespread malware, going back to the iPhone's debut seven years ago. Apple now extends similar protection to desktop and laptop computers by sandboxing all apps in the Mac App Store.

Google sandboxes all tabs and plugins in the Chrome web browser. Microsoft sandboxes much of Internet Explorer and supports application- level sandboxes. Third-party tools extend sandboxing in operating systems through virtualization technology.

Even application architectures themselves are migrating toward further segregating and isolating application functions to improve resiliency and address security. There are practical examples today of task- and process-level segregation that uses whitelisting to enforce security policy on user and application actions. Some organizations even use different cloud providers to segregate exposure across services.

The result of hypersegregation is that networks, platforms, services, and applications are more resistant to attack. Even when attackers succeed, the damage is limited. We no longer need to address every vulnerability immediately or face exploitation.

2: Operationalization of Security

Security professionals, even today, still perform many rote tasks that don't actually require security expertise. For cost and operational efficiency reasons we see organizations beginning to hand off these tasks to Operations to allow security professionals to focus on what they do best.

Non-security teams already handle patch and antivirus management. Some organizations now extend this practice to firewall management and low-level incident management. Concurrently, more rote-level tasks — and even some higher-order functions in assessment and configuration management — are being automated.

We expect Security to divest itself of many responsibilities for network security and monitoring, manual assessment, identity and access management, application security, and more. This, in turn, will free up security professionals for tasks that require more security expertise — such as incident response, security architecture, security analytics, and audits & assessment.

As most repetitive security tasks become embedded into day-to-day operations, *security professionals will play a greater role as subject matter experts.*

3: Greater Emphasis on Incident Response

One of the benefits of the increasing operationalization of security is that it frees up resources for incident response. Attackers continue to hone their techniques as technology further embeds itself into our lives and economies. Security professionals have largely recognized and accepted that it is impossible to completely stop attacks, so we need greater focus on detecting and responding to incidents.

Leading organizations today are already shifting more and more resources to incident detection and response so they can react faster and better, as we discussed in another paper. It's not enough to simply have an incident response plan, or even the right tools. Entire security programs need to be conceptually re-prioritized and re-architected to focus on detection and response, as well as pure defense, and to manage them across an enterprise extended to the cloud. We will finally use all those big screens hanging in the Security Operations Center to do more than impress prospects and visitors.

A focus on incident response — on more rapidly detecting and responding to attacker-driven incidents — will outperform our current security model, which is overly focused on checklists and vulnerabilities. This will affect everything from technology decisions to budgeting and staffing.

4: Software Defined Security

Today, security largely consists of boxes and agents distinct from the infrastructure we protect. These tools won't go away, but the cloud and increasingly available APIs enable us to directly integrate and manage infrastructure, instead of attempting to protect it from the outside. Security will rely more on tools and techniques that directly connect infrastructure to security tools and management, enabling adaptive and effective *security orchestration*.

Software Defined Security is a natural outcome of increasing cloud computing usage, where the entire infrastructure, platforms, and applications are managed using APIs. Security can then directly manage exposed security features using the same APIs, and better integrate security tools into orchestrated environments, when security tools themselves offer APIs.

This is very different than the way most security tools function today, when many vendors silo off their products and restrict interoperability. We already see growing pressure on security vendors to extend API support, especially for products being deployed with cloud computing.

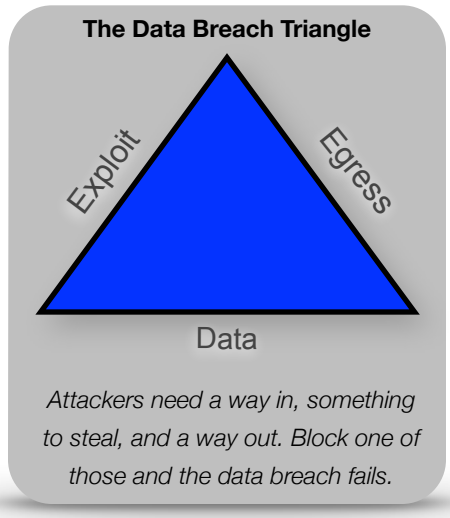
When we tap into APIs we gain incredible security automation capabilities. For example, this example we wrote demonstrates how to automate security configuration policy enforcement. Imagine being able to instantly identify all unmanaged servers in your cloud, without scanning. Imagine automatically assessing new systems for vulnerabilities when they first boot or connect to the network, quarantining them if they fail certain checks. In only a few weeks we wrote a program that completely automates most incident response and forensics tasks for a compromised cloud server. We suspect a real programmer, rather than an industry analyst, could have completed the task in a fraction of the time.

Software Defined Security automates tasks for more agile security infrastructure. It bridges and orchestrates multiple security products with our environments, supporting a security management plane that operates at cloud speed and scale.

5: Active Defense

As the old security saying goes: "A defender needs to be right every time, while an attacker only needs to be right once." Active defense reverses this concept and forces attacker perfection, making attacks more costly for the bad guys. Active defense is strongly reinforced by hypersegregation, the operationalization of security, and Software Defined Security — in turn becoming a cornerstone of incident response.

An attacker needs a way in, something to steal or damage, and a way back out, as explained by the Data Breach Triangle. It's difficult to characterize attackers and then track and understand their activity, even with extensive monitoring. Instead, active defense technologies validate attackers by allowing the infrastructure and applications to interact with them directly, identifying them far more accurately than monitoring alone. This way, even if attackers are initially successful, the slightest mistake can enable us to detect and contain them. Responsive automated defenses interact with attackers to reduce false positives and negatives.



Attackers need a way in, something to steal, and a way out. Block one of those and the data breach fails.

Instead of relying on out-of-date signatures, poor heuristics prone to false positives, or manually combing through packets and logs, we will instead build environments so laden with virtual tripwires and landmines that they would be banned by the Geneva Convention. Heuristic security tends to fail because it often relies on generic analysis of good and bad behavior, which is difficult or impossible to model. Active

defenses interact with intruders while complicating and obfuscating their view of underlying structure. Dynamic interaction is far more likely to properly identify and classify an attacker.

We then pass our findings into global threat intelligence services, and consume real-time intelligence feeds to simultaneously protect ourselves and our peers, while reducing attackers' ability to move on to the next target.

Active defenses will become commonplace and largely replace our current signature-based systems of failure.

6: Closing the Action Loop

Managing security is a complicated dance that requires jumping between disconnected tools. It's not that we lack dashboards and management consoles, but they reside in silos, incapable of providing effective and coordinated security analysis and response. We call the process of detection, analysis, and action the *Action Loop.* (Yes, that's based on the OODA loop, a military term.)

Current tools are too limited. Some observe the environment (such as SIEM, DLP, and full packet capture), but they only show us narrow slices, leaving large gaps between them. This hampers our ability to acquire and relate the information we need to understand incidents. Once we receive an alert, we need to jump into different shells and command lines on multiple servers and appliances in order to see what's really going on. When current tools talk to each other, it is rarely in a meaningful or useful way.

While some tools support automation, it is again self-contained, uncoordinated, and (beyond the most simplistic capabilities) more prone to break a business process than stop an attacker. When we want to perform a manual action our environments are typically so segregated and complicated that we can barely manage something as simple as pushing a temporary firewall rule change.

> We will steal analytics from big data; tune them for security; and architect systems that allow us to visualize our security posture, as well as identify and rapidly characterize incidents.

Emerging tools are just beginning to deliver on old dreams. These tools combine the massive amounts of data we currently collect about our environments, at speeds and volumes long promised but never realized. We will be able to look at a high-level SIEM alert, drill down into the specifics, and analyze correlated data from multiple tools, feeds, and sensors — all from the same console. (No, your current SIEM doesn't do this.)

We will also layer more advanced analytics and applications across these platforms to correlate multiple data points to derive intelligence — such as fraud data applied to business transactions.

But the clincher is the closer. Rather than merely *looking* at incident data, we will also *act* on data using the same console. We will review automated responses, model their possible impact with analytics and visualization (real-time attack and defense modeling, based on near-real-time assessment data), and then tune and implement additional actions to contain, stop, and investigate attacks.

What Change Means for You

We are only at the very beginning of these disruptive trends. Over the next ten to twenty years they will fundamentally alter how we consume and deliver technology, in ways we cannot fully predict. Their impact is likely to be greater than from our initial adoption of the Internet.

The disruptions and trends we have described don't encompass all advances in the worlds of technology and security, but they represent the ones which will most fundamentally transform the practice of security over the next decade. For example we haven't directly addressed Software Defined Networks (although aspects show up in our cloud, hypersegregation, and Software Defined Security descriptions), malware ecosystems, or the increasing drive toward pervasive encryption (driven, in no small part, by government spying). Our focus is on the changes which will most fundamentally alter the practice of security, and the resulting outcomes.

These changes come in fits and spurts — distributed unevenly, based on technology adoption rates, economics, and even social factors. But aggregated together they paint a picture we can use to guide decisions today — for both organizations and professionals. All these changes are currently in process, with plenty of real-world examples.

This report focuses on the implications for three groups: security professionals, security vendors and providers, and cloud and infrastructure providers. The people tasked with implementing security, the folks who create the tools and services they use, and the public and private IT departments managing our platforms and services.

Let's start with some high-level principles for understanding how security controls will evolve, then dig into specific implications for our three audiences.

The Questions You Need to Ask

To deal with change, you need to focus on your security strategy. Determine the capabilities and limitations of the technology, what you can do, what your provider or tool will do, and who is responsible for what. Most importantly, do this *instead of* getting stuck trying to figure out how to migrate a specific existing control to the new operating environment.

For example, when choosing a new cloud provider, ask these questions: What security controls do they provide? Which can I manage? Where are the gaps? What security controls can I put in place to address those gaps? Does moving to this provider give me new security capabilities I otherwise lack? How does the cloud provider enable my security strategy?

Alternatively, when selecting a new security tool like active defense, ask: Does this obviate our need for IPS? Does it really improve our ability to detect attackers? What kind of attackers and attacks will it help us detect? How can and will we adjust our response strategy?

Here is one example of how new technology has changed the questions security professionals need to ask:

- Apple's iOS 7 includes mobile device management hooks that restrict data migration on the device to enterprise-approved accounts and apps. These are all strongly encrypted and protected by stringent sandboxing. While this

could significantly improve data security over standard computers, it also means giving up any possibility of Data Loss Prevention (DLP) monitoring. Additionally it requires you to implement a particular flavor of mobile device management. However…

- Cloud storage and collaboration providers keep track of every version of every file they hold for customers. Some even track all device and user access on a per-file basis. Use one of these with your mobile apps, and you might be able to replace DLP monitoring with in-depth real-time auditing of all file activity at the cloud level — including every device that accesses files.

This combination provides a security and audit capability that is effectively impossible with 'traditional' device management and storage, but requires you to change how you implement a series of security controls.

Implications for Security Practitioners

In the future, security practitioners will rely on a different core skill set than many professionals possess today. Priorities shift as some risks decline, others increase, and operational practices change. The result is a fundamental alteration of the day-to-day practice of security.

Some of these changes are due to the disruptions of the cloud and mobility, but much of it is due to the continued advancement of our approaches to security (partially driven by our six trends; also influenced by attackers). Let's look at the different skills and priorities that will be important in the near future.

> We are simultaneously centralizing delivery with the cloud, and decentralizing access with mobile devices.

Next-Generation Skills

As with any transition, old jobs won't be eliminated immediately, but the best opportunities will go to those with knowledge and expertise aligned to new needs. These roles are also likely to command a salary premium until the bulk of the labor market catches up, so even if you don't think demand for current skills will decline, you still have a vested interest in gaining the new skills.

All these roles and skills exist today, but we expect them to move into the core of the security profession.

- *Incident Response* is already seeing tremendous growth in demand, as organizations shift from trying to keep attackers out (which never works) to more rapidly detect, contain, and remediate successful attacks. This requires extensive security expertise and cannot be handed off to Operations.
- *Secure Programming* includes assisting with adding security functions to other applications, evaluating code for security issues (although most of that will be automated), and programming Software Defined Security functions to orchestrate and automate security across tools. To be effective this requires both programming and security domain expertise. Some practitioners will find themselves more on the secure application development side (integrating security into applications), while others focus on developing security applications themselves. The same basic skills apply either way.
- *Big Data Security Analytics* are needed to make sense of the massive security data sets we are already starting to accumulate. This skill set is essential to better detect and remediate security incidents, and critical for visualization and closing the action loop. Most security information and management tools are already migrating to big data platforms, but making sense of this information cannot be completely automated — especially as organizations add custom application feeds.
- *Security Architects* help design secure applications. They assess and recommend security controls and integration across different cloud and infrastructure providers (especially as we gain more ability to directly manage security in

the infrastructure itself). They work with security programmers to design and implement internal security orchestration and automation applications.

- *Audit/Assessment and Penetration Testing* increase in importance as we need to spend more time assessing external providers, and host more of our internal applications on Internet-accessible services. Vendor risk assessment of cloud providers is already a major challenge for most organizations. It's particularly difficult to make sense of the wildly divergent third-party attestations, self-assessments, provider documentation, and contracts.
- *Chief Information Security Officers* will continue to rise in importance and require experience in the skills sets we have described. The position will be as political as it is technical. The trend toward greater CISO responsibility and accountability started years ago, with organizations increasingly relying on Internet-based technologies and cybercrime beginning to cause more visible losses. There is no reason to expect any of these trends to abate, and CISOs will need a solid grounding in the skills described above.

New Priorities

In ten years a typical security team will operate quite differently than most teams do today. Skills will evolve and priorities will change to align the different capabilities of security tools with the platforms they protect, as well as with the new ways organizations consume and deliver technology. Four new priorities will dominate:

Assessment and Vendor Risk Management: Some companies we talk with today already use hundreds of different cloud services — mainly smaller Software as a Service providers with niche offerings targeting particular business units or initiatives (such as short-term marketing campaigns). There is little consistency in security or documentation across them, and we don't expect this to change any time soon. The native security capabilities of mobile platforms differ wildly, and their ecosystems of mobile applications are incredibly diverse.

We expect to see much greater emphasis on assessment and vendor risk management, including penetration testing. These assessments will require security technology knowledge, not merely contractual and RFP reviews.

Incident Response: Right now spending on incident response technologies and operations is a small fraction of the typical security budget. In the future we expect it to become — at least in some cases — a *majority* of the budget.

Software Defined Security: Security will also focus more on integrating directly into IT operations at a deep technical level. Software Defined Security will be enabled by the proliferation of APIs that manage infrastructure, platform, and service security features directly. We already see this happening with examples such as next-generation firewalls integrating with Software Defined Networking and IAM integrating with external services using SAML. We even see automated vulnerability assessments kicked off by cloud controllers when new instances launch.

Operationalization of Security: All this will be made possible by the ongoing operationalization of security. Security professionals will be able to focus on areas where their expertise is critical, even when that means letting go of security-sensitive tasks easily managed, with guidance, by non-security IT Operations.

Implications for Security Vendors and Providers

These shifts will dramatically affect existing security products and services. We already see cloud and mobile adoption and innovation outpacing many security tools and services. Right now these changes aren't materially affecting profits, but companies face serious financial risks if they fail to adapt in time.

Some vendors merely convert existing products into virtual appliances or make other minor tweaks. For technical and operational reasons we expect these "cloudwashing" efforts to fail. Tools need to fit the job. As we've shown, the cloud and device mobility aren't merely virtual versions of existing architectures. The application architectures and operational

models we see in leading web properties today differ significantly from traditional web application stacks. They will become the dominant models over time.

Security tools need to be as agile and elastic as the infrastructure, endpoints, and services they protect. They also need to fit the new workflows and operational models we see emerging with these advancements (such as DevOps).

The implications for security vendors and providers fall into two buckets:

- Security tools and services must undergo fundamental architectural and operational changes to operate in a reshaped security landscape.
- Customers will shift security spending — a change that will directly impact security market opportunities.

How to Prepare for the Future

These guiding principles will help prepare security companies to compete:

- *Support consumption and delivery of APIs:* Adding the ability to integrate with infrastructure, applications, and services directly using APIs increases security agility, supports Software Defined Security, and embeds security management more directly into platforms and services. For example, network security tools should integrate directly with Software Defined Networking and cloud platforms so users can manage network security in one place.

  Customers complain to us that they can't normalize firewall settings between their regular infrastructure and cloud providers; they don't want to manage them separately. Security tools also need to provide APIs so they can be integrated into cloud automation. If a tool becomes a rate limiter it will get kicked to the curb. Software Development Kits and robust APIs will likely become competitive differentiators since they make it easier to directly integrate security into operations, instead of interfering and altering workflows that provide strong business benefits.

  APIs tie the cloud together, and are fundamental to all cloud platforms. Security tools that don't enable them for customers do not work in cloud deployments.

- *Don't rely on controlling or accessing all network traffic:* A large number of security tools today, from web filtering and DLP to IPS, rely on completely controlling network traffic and adding additional bumps in the wire for analysis and action. The more we move into cloud computing and extensive mobility, the fewer opportunities exist to capture connections and manage security in the network. Everything is simply too distributed, with enterprises routing less and less traffic through a core network.

  Where possible integrate directly with the platforms and services via APIs, or embed security into host agents designed to work in highly agile cloud environments. You can't assume that enterprises will route mobile workers' traffic through you, so services need to rely on Mobile Device Management APIs and providing more granular protection at the app and service level.

- *Provide extensive logs and feeds:* Security logs and tools shouldn't be a black hole for data. The Security Operations Center of the future will aggregate and correlate data using big data techniques, and it will need access to raw data feeds to be most effective. Expect demands to be more extensive for existing SIEMs.
- *Assume unprecedented rates of change:* Today, especially in audit and assessment, we rely on managing a relatively static infrastructure. But when some cloud applications are designed to rely on servers that run for less than an hour, even a daily vulnerability scan is instantly out of date. Products should be as *stateless* as possible; relying on continually connecting and assessing the environment instead of assuming things change slowly.

Companies that support APIs, rely less on bumps in the wire, provide extensive data feeds, and assume rapid rates of change are much better positioned to fit expanding use of cloud and mobile devices. It's a serious challenge because we need to protect a large volume of distributed services and users, without anything like the central control we are used to.

We work extensively with security vendors. It is hard to overstate how few we see preparing for these shifts.

Implications for Cloud and Infrastructure Providers

Security is (becoming) a top priority for cloud and infrastructure providers of all types. For providers with enterprise customers and those which handle regulated data, security is likely the first priority. As important as it is to offer compelling and innovative services to customers, a major security failure has the potential to wipe out clients' ability to trust you — even before you deal with the legal liabilities.

If you handle valued information on behalf of your customers, you are, for nearly all intents and purposes, a form of bank.

Trust Is a Feature

Enterprises can't transition to the cloud without trust. Their stakeholders and regulators simply won't support it. Consumers may, to a point, but only the largest and most popular properties can withstand the loss of trust induced by a major breach. There are six corollaries:

- Customers need a baseline of security features to migrate to the cloud. This varies by the type of service, but features such as federated identity, data security, and internal access controls are table stakes. Cloud providers need a baseline of inherent security to withstand attacks, as well as customer-accessible security features to enable clients to implement their own security strategies.
- You are a far bigger target than any single customer, and will experience advanced attacks on a regular basis. Centralizing resources alters the economics of attacks, inducing bad guys to incur higher costs for the higher rewards of access to all a cloud provider's customers at once.
- User own their data. Even if it isn't in a contract or SLA, if you affect their data in a way they don't expect, that breaks trust just as surely as a breach.
- Users own their business logic, even when implemented in your service. As with data, if you change a process or expose it to outsiders, that is a breach of trust.
- Multitenancy isolation failures are a material risk for you and your customers. If a customer's data is accidentally exposed to another customer, that is, again, a breach of security and trust. People have been hunting multitenancy breaks in online services for years, and criminals sign up for services just to hunt for more.
- Trust applies to your entire cloud supply chain. Many cloud providers also rely on other providers. If you own the customer trust relationship, you are responsible for *any* failure in the digital supply chain.
- Transparency and documentation — from your internal security and hiring practices, to incidents affecting customer data, to customer usage and trans-national compliance guidelines for users — help assure trust and are a competitive differentiator.

It isn't enough to simply *be secure* — you also need to *build trust* and *enable your customers' security strategies*. Security, risk, privacy, and compliance move from the back office to the front office to cement this relationship. Visionary security features, not merely defenses, will be a strong differentiator.

Building Security in

The following features and principles allow customers to align their security needs with cloud services, and are likely to become competitive differentiators over time:

- *Support APIs for security functions:* Cloud platforms and infrastructure shouldn't merely expose APIs for cloud features; but also for security functions such as identity management, access control, network security, and whatever else falls under customer control. This enables security management and integration. Don't require customers to log into your web portal to manage security. But do expose all those functions in your user interface.
- *Provide logs and activity feeds:* Extensive logging and auditing are vital for security — especially for monitoring the cloud management plane. Expose as much data as you can, as quickly as possible. Transparency is a powerful security enabler provided by centralization of services and data. Feeds should be easily consumable in standard formats such as JSON.
- *Simplify federated identity management:* Federation allows organizations to extend their existing identity and access management to the cloud while retaining control. Supporting federation for dozens or hundreds of external providers is daunting, with entire products available to address that issue. Make it as easy as possible for your customers to use federation, and stick to popular standards that integrate with existing enterprise directories. Also support the full lifecycle of identity management, from creation and propagation to changing roles and retirement.
- *Extend security to endpoints:* We have focused on the cloud, but mobility is marching right alongside, and is just as disruptive. Endpoint access to services and data — including apps, APIs, and web interfaces — should support all security features equally across platforms. Clearly document security differences across platforms, such as the different data exposure risks on an iOS device versus an Android device versus a laptop.
- *Encrypt by default:* If you hold customer data, encrypt it in motion and at rest. Even if you don't think encryption adds much security, it empowers trust and supports compliance. Allow customers to control their own keys if they prefer. This is technically and operationally complex, but becomes a competitive differentiator, and can eliminate many data security concerns and facilitate cloud adoption.
- *Maintain security table stakes:* Different types of services, handling different types of workflows and data, tend to share a needed baseline of security. Fall below it and customers will be drawn to the competition. For example, IaaS providers must include basic network security at a per-server level. SaaS providers need to support different user roles for access management. These requirements change over time, so watch your competition and listen to customer requests.
- *Document security:* Provide extensive documentation for both your internal security controls and the security features customers can use. Have them externally audited and assessed. This allows customers to know where the security lines are drawn, where they need to implement their own security controls, and how. Pay particular attention to documenting the administrator controls that restrict your staff's ability to see customer data and audit when they do.

Conclusion

Once, many years ago, I had the good fortune to enjoy a few beers with futurist and science fiction author Bruce Sterling. That night he told me that his job as a futurist is to try to predict the world seven to ten years from now, which is where informed estimates become speculative fiction. As analysts we normally look out three to five years, and at seven to ten years the accuracy of our predictions declines.

Unless we cheat.

Nothing we described in this paper is science fiction. There are real-world examples of everything we have discussed, in production deployments with brand names. This paper doesn't predict a future ten years out — it merely pulls together the leading edge of what we see today, with the understanding that it typically takes seven to ten years to coalesce and trickle out to the broader world. Looking at technology adoption cycles, and the sheer amount of effort it takes to transition the majority of existing workloads to cloud computing and new security platforms, even ten years may be an aggressive goal for many organizations.

The future of security is here — it just isn't evenly distributed. Keep your eye on these trends, make smart decisions, and plan for the future, and you will start seeing benefits today.

Who We Are

About the Analyst

Rich Mogull, Analyst and CEO

Rich has twenty years experience in information security, physical security, and risk management. He specializes in cloud security, data security, emerging security technologies, and security management. Rich is the primary developer of the Cloud Security Alliance CCSK training program. Prior to founding Securosis, Rich was a Research Vice President at Gartner on the security team where he also served as research co-chair for the Gartner Security Summit. Prior to his seven years at Gartner, Rich worked as an independent consultant, web application developer, software development manager at the University of Colorado, and systems and network administrator. Rich is the Security Editor of TidBITS, on the advisory board of DevOps.com, and a frequent contributor to publications ranging from Information Security Magazine to Macworld. He is a frequent industry speaker at events including the RSA Security Conference, Black Hat, and DefCon, and has spoken on every continent except Antarctica (where he is happy to speak for free — assuming travel is covered).

About Securosis

Securosis, L.L.C. is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services.

We provide services in four main areas:

- Publishing and speaking: Including independent objective white papers, webcasts, and in-person presentations.
- Strategic consulting for end users: Including project accelerator workshops, product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessments.
- Strategic consulting for vendors: Including market and product analysis and strategy, technology guidance, product evaluations, and merger and acquisition assessments.
- Investor consulting: Technical due diligence including product and market evaluations, available in conjunction with deep product assessments with our research partners.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Securosis has partnered with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis.

Supporters

The following organizations reviewed and support this research. *Their inclusion does not imply endorsement by Securosis, and no financial considerations were made*.

"The future of information security lies with protecting the data assets — not just the systems that store and transmit them. Our security controls must adapt to follow data throughout a complex ecosystem of providers and partners, customers and third parties."

Gavin Mead, Managing Director, KPMG Information Protection & Business Resilience