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 security professionals predict and prepare for these disruptions, the more effective we can be.

- **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 increasing, others decreasing. While the fundamentals remain the same, security must adapt to the new environment.
- **Mobile** 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 security models to maintain data and workflow security, but the devices themselves are often *more inherently* secure than employee computers.

Six Trends Changing the Face of Security:

- **Hypersegregation:** Incredibly granular segregation is becoming the norm in networks, platforms, services, and applications. Even if an attacker breaks in, it becomes much harder for them to cause damage or steal information. We become more resilient.
- **Operationalization of Security:** Security is divesting itself of many rote responsibilities like firewall management that IT operations can handle. This, in turn, frees security professionals for tasks that require more security expertise, like analysis, architecture, and response.
- **Incident Response:** We can't stop all attacks, and leading organizations are already shifting more resources to incident detection and response. A focus on incident response will outperform our current security model, which is overly focused on checklists and vulnerabilities.
- **Software Defined Security:** Software Defined Security automates security tasks for more agile security infrastructure. It bridges and orchestrates multiple security products with our environments, for security management that operates at cloud speed and scale.
- **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 concepts and forces attacker perfection, making attacks more costly for the bad guys, and easier to detect.
- **Closing the Action Loop:** Security tools today are disconnected; with a gap between analysis and action. Emerging tools bridge detection, analysis, and action using big data analytics, visualization, and *orchestration,* dramatically improving our security management.

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.

This is an executive summary of the complete paper, *The Future of Security* by Rich Mogull, Securosis LLC

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 the required skills:

- *Audit/assessment and penetration testing* are essential to understanding the highly variable security of providers, and to assure security works as expected.
- *Incident response* are already in high demand, and need to 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 from advanced attackers.
- *Security architects assess and* design the 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* since 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 for data.
- *Assume high rates of change* which exceed 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 for customers adopting cloud.

- *Build a security baseline* that is as, or more, secure than an enterprise datacenter.
- *Defend advanced attacks* since 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 in 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 a customer 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'll start seeing benefits today.