




# THE NEW ECONOMICS OF CLOUD SECURITY

# YOUR CLOUD JOURNEY HAS BEGUN. NOW COMES THE FUN OF FIGURING OUT HOW TO SECURE IT.

Capturing the benefits of speed, scalability, and agility from your cloud applications is a precursor for business success. And that is why you are deploying more applications and workloads with critical business data in the cloud. You might be developing new workloads and Security as a Service (SaaS) applications to take advantage of the public cloud, or migrating existing applications. You might be a 100-year-old enterprise, or a born-in-the-cloud shop. No matter your situation, it is highly likely that you are using the cloud as your preferred infrastructure of choice for rolling out new business applications. Meanwhile, the frequency, sophistication, and diversity of global threats continue to increase. So to take full advantage of everything the cloud gives you, you must enable relevant controls across a more complicated infrastructure.

But the flexibility of the cloud and use of integrated services make it different than securing on-premises applications, workloads, and data. You have to invest in different tools, implement different processes, and find and retain staff with cloud expertise. And let's be honest: even though you may be doing it today, you shouldn't deploy a new cloud-based workload without a thoughtful security strategy in place.

Part of getting cloud innovation right is enabling security up front. And if it's done properly, you can use the benefits of security solutions built for cloud to your advantage—as opposed to using legacy on-premises security solutions that will slow down your cloud deployments, and may leave your data and applications exposed. The speed of cloud innovation requires a security solution designed to work in the cloud to lower costs, speed up deployment, and reduce risks. That's the new economics.



**\$4 MILLION**  
The average cost of a breach<sup>1</sup>

# LEGACY SECURITY TOOLING: DIFFICULT TO MANAGE. EXPENSIVE. RISKY. OTHER THAN THAT, IT WORKS GREAT.

Until now, organizations that have addressed security have taken the conventional approach: buy and deploy third-party security software and find and retain the security staff to make sure that it is working around the clock. And this is for the few companies that can afford it—since the cost to build out a minimally viable, fully functioning 24/7 security operations center can run millions of dollars per year.

To effectively protect cloud-based workloads with the legacy approach, you would have to do the following:

- Purchase, deploy, integrate, tune, and manage a variety of security products that are capable of detecting and protecting your cloud-based workloads and web applications—all across a variety of attack vectors targeting your web- and server-based applications and their data.
- Reconfigure your cloud infrastructure to conform to the requirements of on-premises security tools.

- Hire and build out a threat intelligence team that is capable of understanding the threat landscape, attack patterns and evolving toolkits used—the team needed to determine when and how exposures and events should be addressed.
- Hire enough experts to staff a security operations center 24/7 to monitor your environment, filter through the thousands of events your tools are generating, and prioritize vulnerabilities to fix and identify attacks before they damage your business.

Not a pretty picture. And even if you do all of the above, you'll still very likely fall short of your goal. Here's why.



The number of cybersecurity jobs unfilled in the US alone<sup>2</sup>

# EVEN IF YOU BUILD YOUR OWN SECURITY OPERATIONS CENTER, THERE IS NO GUARANTEE IT WILL BE EFFECTIVE.

It's inevitable. In-house security teams end up struggling with a wall of noise: a glut of logs overflowing with discrete security "events" that reveal attackers attempting to penetrate systems, leaving precious little time left to deal with actual security incidents.

A typical customer is inundated with thousands of these alerts on a daily basis. Many of them are false positives: they look like threats, but they're really not. Meanwhile, other events that are legitimate get lost in the noise. And sophisticated attacks are leveraging methods that appear to be legitimate transactions but are in fact malicious in nature—using methods including SQL injection and cross-site scripting. These attack methods can require petabytes of security data to be analyzed, since no signature or rule-based detection method alone can identify these customized attack patterns.

Why go down this path just to build another problem for yourself? And moreover, why stick yourself with a security infrastructure that undermines all the great reasons why you went to the cloud in the first place?

“ALERT LOGIC HELPS INVESTIS BY WORKING WITH US MORE AS AN EXTENSION OF OUR TEAM THAN A VENDOR. NOW WE HAVE A MANAGED SECURITY SOLUTION IN THE AWS CLOUD WITH ADDED PEACE OF MIND THAT ALERT LOGIC IS THERE FOR US 24/7/365.”

—Martyn Arbon  
Chief Technology Officer,  
Investis



\$1.3 MILLION

Average annual cost of false positive alerts<sup>1</sup>

# HOW CAN YOU PROTECT YOUR ASSETS WITHOUT SLOWING DOWN YOUR CLOUD AGENDA? OR BREAKING THE BANK?

It's a quandary. You need to be able to launch new security controls as quickly as you launch new cloud services, or you lose the very advantages that prompted you to undertake your cloud investments in the first place.

## You need to:

- Protect more data assets, applications and workloads against an ever-growing variety of advanced threats.
- Protect workloads owned by application developers and lines of business—workloads that can scale up

or down in minutes depending on customer demand.

- Keep your top-line generating cloud applications and workloads available.
- Meet both customer and regulatory-compliance requirements—mandates that you can't ignore but that require you to invest in staffing and tasks that don't build value for the business.
- Move at cloud speed supporting ever-compressed continuous delivery cycles.
- Do it all for the same budget.

So...welcome to the new economics of cloud security. While the old way was a balancing act between controlling risk and cost, in the new economics, you also have to factor in the speed of the cloud. And not surprisingly, the solution is cloud based, too: **a fully managed Security-as-a-Service solution built to protect cloud applications and workloads.** Out with the old economics. In with the new.

## THE IMPACT OF BREACHES AND THE RESULTING DOWNTIME

**\$1,140** PER HOUR

For every \$10 million in annual revenue generated by an application or process, assuming that revenue is continuous and that all revenue lost goes unrecovered<sup>3</sup>

**\$500k–\$1MILLION**

The average cost of a critical application failure per hour<sup>4</sup>

# NEW ECONOMICS PRINCIPLE #1: DITCH THE RIDICULOUSLY HUGE CAPEX AND OPEX COSTS.

Security the old way is a huge capital and operational expense, treated as an unavoidable cost of doing business. With a fully managed Security-as-a-Service solution, you slash the overhead and can spend your IT budget on innovation and growing the business.

- **Eliminate large up-front capital expenditures.** A monthly subscription eliminates large up-front payments for purchasing security software and hardware devices.

- **Lower ongoing costs.** A fully managed Security-as-a-Service-based solution handles the updating, patching, tuning, and configuration of security services, lowering ongoing operational costs. And an integrated team of security experts—included in the subscription—monitors, triages, enriches, and escalates the right security incidents so you avoid the hidden costs of effectively managing today's complex threats and compliance requirements.

- **Simplify workload security.** Combining configuration and application vulnerability assessment, 24/7/365 threat detection, the ability to block malicious activity targeting your web applications, and compliance attestation into a unified service simplifies your security program.
- **Avoid investment in redundant security tools.** A "single pane of glass" approach secures on-premises, hosting, and cloud environments with one solution.

## \$632,282

in avoided labor costs associated with threat research and monitoring, log management, and web application firewall management for an average Alert Logic customer.<sup>5</sup>

## \$548,544

in avoided expense for infrastructure capital and maintenance for a composite organization compared to an equivalent insourced solution.<sup>5</sup>

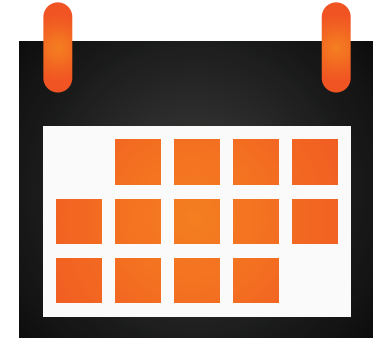
# NEW ECONOMICS PRINCIPLE #2: GET MORE VALUE FROM YOUR SECURITY INVESTMENTS—FASTER.

Security the old way involves spending bucketloads of time up front before you can thwart a single attack. A fully managed Security-as-a-Service solution helps you realize faster value from your security initiatives and your cloud initiatives overall.

- **Launch rapidly.** Reduce the time of deployment from months for building your own security operations center to days using an integrated Security-as-a-Service model.
- **Keep the business running.** Quickly meet regulatory, industry, and customers' security requirements, and safeguard your customers and organization without lengthy procurement and deployment cycles.
- **Leverage the broader threat intelligence network.** Without having to monitor it yourself and without building your own threat intelligence team.

“ALERT LOGIC FOCUSES ON OUR IT SECURITY SO WE DON'T HAVE TO. WE KNOW WHAT WE NEED FOR OUR BUSINESS TO THRIVE, AND WE ARE CONFIDENT ALERT LOGIC CAN DELIVER WHAT WE NEED WHEN WE NEED IT TO SAFEGUARD OUR INFRASTRUCTURE FROM THREATS AND VULNERABILITIES.”

—James Hirmas  
Co-Founder and CEO,  
GenomeNext



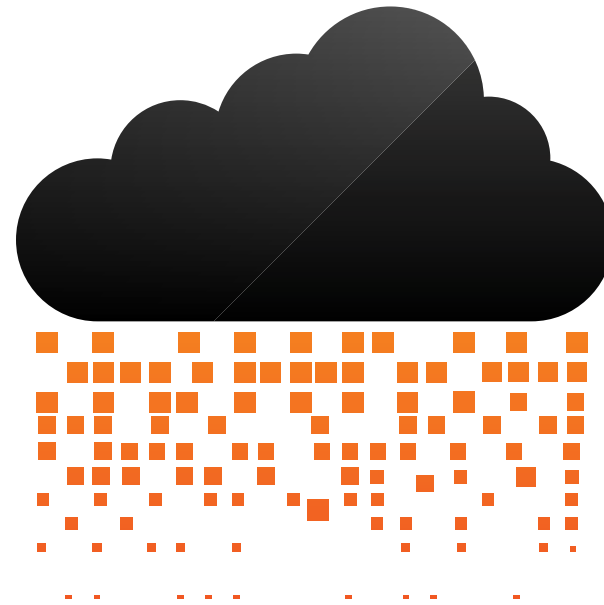
# 0 MONTHS

Payback period for an outsourced, cloud-native solution with 52 percent ROI based on a representative composite organization<sup>5</sup>

# NEW ECONOMICS PRINCIPLE #3: TO SECURE THE CLOUD, USE A SOLUTION BUILT FOR THE CLOUD.

It only makes sense that if you're going to secure cloud applications, your security approach should also take advantage of everything the cloud gives you. Including speed and instant scalability, which are some of the biggest reasons you went to the cloud in the first place.

- **Eliminate choke points** in application delivery and performance with API-integrated controls.
- **Keep pace** with elastic workloads with auto-scaling support.
- **Scan** for application and configuration vulnerabilities in minutes during building, testing, and production.
- **Deploy controls in minutes** through integration with Amazon Web Services and Microsoft Azure APIs, Chef recipes, and Puppet templates.



“ IF AN ORGANIZATION WANTS WHAT WE DO, A COST-EFFECTIVE SOLUTION THAT PROVIDES THE SECURITY INTELLIGENCE YOU NEED TO PROTECT YOUR ENVIRONMENT, THEY NEED ALERT LOGIC. ”

—Rick Cahoon, Director Enterprise Security and Support, Wilbur-Ellis

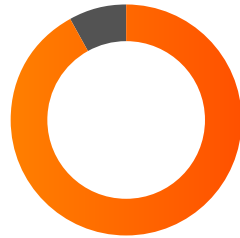


# NEW ECONOMICS PRINCIPLE #4: REDUCE YOUR RISK. AND LOOK LIKE A FINANCIAL GENIUS WHILE YOU DO IT.

Security the old way says to reduce your risk, you pour resources into security controls and expertise. A fully managed Security-as-a-Service solution lowers your overall risk in a way that just makes sense: offloading the task to someone who already has the infrastructure, data, analytics platforms, continuously evolving detection capabilities, and security experts in place.

- Controls that span workloads across locations, applying the right method to detect and block the attacks targeting your environment
- Multiple detection methods applied in concert, augmented with the in-depth knowledge and common sense of global security specialists

- Holistic risk reduction from one vendor, spanning exposure assessment, intrusion detection, and web application access control, using an integrated system that is proactively managed and monitored by global security operations experts
- Threat avoidance through advanced detection and assessment technologies and expertise that focus on confirmed and verified incidents, not just events



92%

of IT pros value the capability to quickly identify and remedy attacks.<sup>6</sup>



87%

of IT pros want a security operations center with the capability to implement security controls in response to evolving threats.<sup>6</sup>

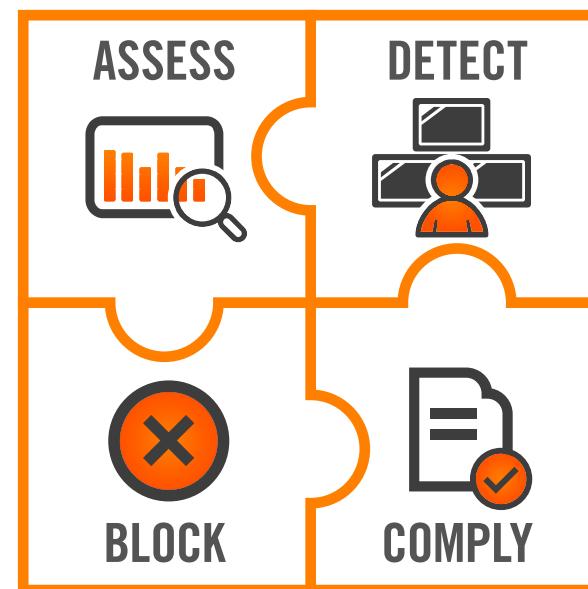
# THE NEW ECONOMICS IS HERE. HOW THE HECK DO YOU TAKE ADVANTAGE OF IT?

The new economics of cloud security is about striking the optimum balance between risk, cost and speed. You can't let security get in the way of the speed the cloud gives you.

Alert Logic® puts the new economics of cloud security to work for you, with fully managed security delivered as a service and built for cloud and hybrid environments. This makes it easy to purchase, launch, and achieve your security goals, all without investing in in-house cloud-security expertise.

- No large capital investment, lengthy implementation, or heavy training requirement
- Simple subscription model that protects at a much lower cost than traditional security solutions

- No software upgrades to manage or expensive security experts to train and retain
- Security technology backed by a team of certified security and compliance experts working 24/7 to keep your data safe and secure and your environment compliant
- Management and monitoring by security experts for continuous protection
- A single vendor that supplies an integrated security value chain— from products through services— to assess, detect and block threats and meet compliance mandates



Hosting



Data Center

# CASE STUDY

**Bentley Systems** provides software tools that support some of the world's largest construction projects, including roadways, bridges, airports, skyscrapers, and industrial plants. The high-profile nature of the projects dictates that security and data integrity are always major considerations.



## By turning to Alert Logic for security, Bentley:

- Attained compliance with key industry standards, including Sarbanes-Oxley and the stringent ISO 27001 information security mandate.
- Met its goal of achieving scalability, flexibility, and the ability to perform across a diverse set of environments, both on-premises and cloud based.
- Handled requirements for intrusion detection, vulnerability assessments, and real-time log file collection and management.
- Secured applications, workloads, and data hosted by Microsoft Azure, Amazon Web Services, and Bentley's regional cloud provider.

“**WE’VE ENHANCED OUR OVERALL SECURITY POSTURE WHILE LEVERAGING THE ALERT LOGIC NAME WITH OUR PROSPECTS. PEOPLE ARE FAMILIAR WITH THE ALERT LOGIC BRAND AND WHAT IT REPRESENTS, AND THIS GIVES US THE INSTANT CREDIBILITY THAT WE’RE USING BEST-IN-CLASS COMPONENTS TO EMPOWER OUR SOLUTIONS.**”

—Tom Cibelli  
Solutions Engineering Manager

# LET US SHOW YOU HOW TO APPLY THE NEW ECONOMICS OF CLOUD SECURITY.

## START HERE. START NOW.

Based on the experiences of thousands of organizations, the Alert Logic® Value Assessment Tool calculates your potential cost savings from using a fully managed Security-as-a-Service solution.

1. Ponemon Institute, June 2016.
2. ["2016 Data Breach Investigations Report," Verizon.](#)
3. ["Network Security: Why the Growth Is Moving from In-House to Managed Services," Aberdeen Group, Analyst Insight, May 2013.](#)
4. Stephen Elliot, "DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified," IDC Insights, December 2014.
5. ["The Total Economic Impact™ of Alert Logic Solutions," Forrester Total Economic Impact Study, December 2014.](#)
6. ["Evolve Your Security Operations Strategy to Account for Cloud," Forrester Consulting, June 2016.](#)