ALERT LOGIC®

Enterprises are building and moving applications and workloads to the cloud for compelling business reasons. The speed of the cloud, however, brings a new dynamic to security that is best met by a cloud-native, Security-as-a-Service solution. While the cost advantages of these solutions are impressive compared to traditional perimeter and self-managed on-premises security, the new economics of cloud security is about more than numbers. It is about freeing IT departments to innovate and take full advantage of everything that the cloud offers so they can do what they are tasked to do:

LEVERAGE TECHNOLOGY TO DRIVE THE BUSINESS.

HOW CLOUD COMPUTING HAS CHANGED SECURITY

Organizations are building and moving applications, workloads, and data to the cloud for sound business reasons, including speed, scalability, and agility as well as lower capital expenses. With the underlying cloud platforms secured by others, it is tempting to think that security is not an issue. However, that assumption is false. Cloud vendors are not responsible for the security of applications, workloads, and data that reside on their infrastructure. The owners of the applications are responsible for that. In fact, applications—especially web applications—are in many respects the most vulnerable part of the stack.

Application owners, however, struggle to find the resources to secure their cloud workloads. Cloud environments are highly elastic, while on-premises environments have a fixed perimeter. Applications are complex and continually evolving, offering many avenues for compromise—some of which are disguised as legitimate transactions. Threats are continually evolving, and detection techniques must evolve in-line. Meanwhile, the specialized knowledge to secure web applications and workloads running in the cloud is in short supply. Qualified security analysts in general are difficult to find, expensive to continuously train, and challenging to retain. And organizations that maintain their own security operations often find that their experts are unable to keep their heads above the sea of security events—typically thousands of seemingly unrelated events every day—and focus on the events that really matter.

Securing applications and their data—regardless of their location, is therefore expensive and difficult to manage. But cloud-based applications face an even more daunting set of considerations, as organizations look to quickly roll out new capabilities and innovations to drive business ahead. How can teams solve the security conundrum and capitalize on all the reasons they went to the cloud?

THE CLOUD'S NEW DYNAMIC: THE NEED FOR SPEED

The legacy approach to on-premises security has traditionally been a trade-off between risk and cost. To reduce risk, organizations invest in more security tools and controls. The cloud introduces a new dynamic: speed. The multiple dimensions of cloud speed include speed of deployment, performance of the applications, and the speed to scale infrastructure to keep up with surges in demand. Modern IT organizations need to develop, deploy, scale, *and secure* at the speed the cloud provides—without introducing choke points that can degrade development and production pipelines, or impede application access and infrastructure scaling requirements.

SOLUTION: FULLY MANAGED SECURITY-AS-A-SERVICE

In order to secure applications, workloads, and data in cloud, on-premises, and hybrid environments, only a Security-as-a-Service solution (SaaS) addresses risk and cost, as well as the new dynamic of speed.

LOWER COST

Such a solution eliminates the huge capital expense required for scaling up on-premises security to accommodate cloud workloads, including the expensive patchwork of tools and analyst systems. This includes costs for experts to deploy, manage, analyze, and tune detection systems; integrate threat intelligence and security research; and monitor, triage, and remediate incidents.

CLOUD SPEED

Preintegrated for rapid deployment with instant scalability, a built-for-cloud solution eliminates the hardware and software procurement and staffing required to handle security in-house. It also addresses the requirement to not slow down introduction of new applications, enhancements, and revenue opportunities, thanks to automated security controls that continually scan applications and cloud configuration for vulnerabilities during development and deployment, in addition to integrating threat detection and blocking capabilities within DevOps cycles.

REDUCE RISK

Global multi-tenant operations, securing thousands of cloud and hybrid environments, can attract highly qualified security specialists applying continually evolving knowledge of attacks. This scale and depth of expertise enables them to correlate and analyze the petabytes of data needed to separate actionable security incidents from the background noise and prioritize, respond, and remediate in real time.

ORGANIZATIONAL IMPACTS AND ADVANTAGES

A Security-as-a-Service solution—designed to protect web applications and cloud workloads—leverages the fundamental economics of the cloud. This includes no capital expense, and the ability to scale up or down on demand. It also includes several other advantages specific to cloud-based security.

SAAS-BASED FOR RAPID DEPLOYMENT

Traditional perimeter- or host-based security tools typically require months to be deployed because of the time required to procure and deploy them, as well as to find and hire the staff to manage and monitor them. A fully managed cloud-based solution can be launched in minutes to days,enabling immediate value and ongoing protection as applications evolve
and infrastructure scales.

FULLY MANAGED FOR SIMPLICITY

A fully managed solution handles the full range of security goals, including assessing vulnerabilities, detecting attacks, blocking malicious activity, and documenting internal and external compliance. It integrates threat intelligence, security research, data science, and proactive 24/7/365 incident escalation and verification behind the scenes so organizations avoid the complexity. It also avoids the maintenance overhead of an insourced solution such as updating, patching, tuning, and configuration.

TOTAL ECONOMIC IMPACT

Forrester modeled a typical organization and applied its Total Economic Impact analysis to compare the economic benefit of a Security-as-a-Service solution against a traditional, unmanaged on-premises tool approach.

The three-year economic benefit for the fully managed SaaS approach:

$632,282
labor costs avoided

$548,544
infrastructure capital and maintenance expense avoided

52%
return on investment

0
months to achieve payback

THREAT RESEARCH, MONITORING, AND INVESTIGATION

Even if an organization has deployed intrusion-detection and intrusion-prevention systems and is managing them in-house, they require skilled security analysts, researchers, and data scientists to leverage the threat intelligence, correlate events from siloed tools, monitor for events all day and night, and interpret and enrich the data for remediation. These specialists are difficult to recruit and retain.

- More than one million cybersecurity jobs are unfilled in the US alone.[1]
- Sixty-three percent of organizations say it takes three months or more to fill open information security positions within their organization, or that they can't fill those positions at all.[2]
- Sixty percent of organizations say that less than half of applicants are qualified when they first hire them.[2]
- Eighty-six percent of organizations say they need to resort to on-the-job training to develop necessary technical skills.[2]

Security-as-a-Service offers the ability to manage the complex detection and analysis requirements across a wide attack surface and enables teams to act faster to address risks and attacks—without having to bring on expensive security experts either in-house or through pricey security management outsourcing contracts. Integrating security expertise and continual analysis into an SaaS-based solution provides prioritized exposures and actionable, high-value incidents, based on global threat intelligence and real-time attack analysis across thousands of customers.

ECONOMIC IMPACT FOR MODELED ORGANIZATION:

$184,649
cost savings over three years by not having to hire security analysts

1. "2016 Data Breach Investigations Report," Verizon
2. "State of Cybersecurity: Implications for 2016," ISACA and RSA Conference

ROTE TASKS AND STAFFING TO PERFORM THEM

In in-house security environments, large amounts of IT time are spent on noncore functions; in fact, 65 percent of IT's time is spent on tactical considerations for simply managing the patchwork of tools and infrastructure.[3] Security-as-a-Service delivers organizational benefits by allowing IT to focus on innovation and value creation rather than on rote security tasks.

Moreover, time spent on these tasks doesn't necessarily make the organization more secure. Less than one-third of organizations say that they are comfortable with their cybersecurity team's ability to respond to anything other than simple incidents.[1] A fully managed Security-as-a-Service solution from Alert Logic® provides real-time monitoring, research, and investigation of alerts and threat data to provide actionable alerts within 15 minutes of identification.

INFRASTRUCTURE AND MAINTENANCE

The multitude of tools to assess, detect, block, and comply across cloud, on-premises, and hosted environments represents both capital and operational expenses. A Security-as-a-Service solution avoids:

- Large up-front payments for purchasing security software and hardware devices, replacing them with a monthly subscription.
- Investment in redundant security tools because it provides both on-premises and cloud security with one managed-security solution.
- The ongoing overhead required to manage and maintain those tools.
- The opportunity cost of focusing precious IT expertise on routine system maintenance instead of projects and innovation.

SECURITY INCIDENTS AVOIDED

The cost of security incidents varies greatly with the data exposed and the systems impacted. Attacks can be costly due to the potential for data loss, fines due to noncompliance with regulations, business disruption, and revenue loss. Impact on the corporate brand and reputation can be incalculable.

If an adversary compromises a production system that needs to be taken offline, the average cost of such a critical application failure per hour is $500,000 to $1 million.[4]

With fully managed Security-as-a-Service, lower risk comes from the use of multiple threat-detection methods. Many are only possible through the economies of scale of a multitenant solution serving thousands of organizations. They include the tasks performed by security analysts outlined above, but also extend to advanced analytics, machine learning, and applying tens of thousands of vulnerability and configuration checks.

ECONOMIC IMPACT FOR MODELED ORGANIZATION:

$447,633

cost savings over three years realized by not adding head count to the team

ECONOMIC IMPACT FOR MODELED ORGANIZATION:

$548,555

cost savings over three years by avoiding infrastructure costs

ECONOMIC IMPACT FOR MODELED ORGANIZATION:

$183,185

cost savings over three years, based on a real-world attack example and costs of remediation

CONCLUSION

While the economics by the numbers alone are impressive, the new economics of cloud security is not just more affordable security. It is a comprehensive, cloud-native, cloud-fluent, and proactively managed security approach that allows organizations to put the focus where it belongs: on innovation, development, and deployment of applications that drive revenue and fuel business-critical operations.

3. Forrester Business Technographics Global Security 2016

4. "Network Security: Why the Growth Is Moving from In-House to Managed Services," Aberdeen Group, Analyst Insight, May 2013