Accelerate and secure cloud application migrations

mnemonic in partnership with 

September 2021

The changing world of application security

There are many reasons why organisations are eager to move applications from traditional on-premise infrastructure towards more forward-leaning cloud architecture designs. Scalability, flexibility and innovation are some of the key business drivers that are accelerating many cloud transformation initiatives we see today. To stay competitive and build on innovation, many organisations are moving towards a "cloud first" strategy to ensure all new initiatives and enhancements to their infrastructure will default to cloud service deliverables.

The importance of application security

Cloud service providers offer their services based on shared responsibility models between the cloud provider and their customers. While the underlying infrastructure and physical security are managed by the cloud provider, each customer is responsible for application-level security and for securing communication between clients and the applications.

The threat landscape has changed rapidly during the last few years and one consistent challenge is the number of application vulnerabilities that are being targeted. Recent events have also once again proved the challenges with relying on third-party open-source libraries that have security issues.

F5 estimates that roughly 50% of all internet traffic is made up of bots looking for application vulnerabilities. Protecting against these kind of threats while still delivering stable and efficient services to customers is vital.

Supporting both the business need for delivering new services and applications to the market faster while still ensuring security is optimised is a challenging balance. With the applications being the customer front-end and the place where they interact with your organisation, any downtime, stability issues or security issues will damage reputation and might result in customers looking to shop elsewhere.

Google research indicates that more than 50% of mobile website users will leave if a webpage does not load within three seconds. This means that any security control introduced must be transparent and support a seamless customer experience.

The following section will outline some of the common security challenges organisations are faced with, and solutions that can help mitigate these challenges and enable the adoption of cloud applications securely.

Cloud application security challenge #1: protecting applications from active threats

Applications that are exposed to the internet face a persistent and continuous onslaught of scanning and attacks, all day, every day.

To deliver secure and stable services that are available on the internet, organisations are tasked in identifying legitimate traffic and ensuring it passes unimpeded while blocking suspicious or malicious traffic. This daunting task is combined with attacks and techniques that continue to evolve, an attack surface that is widening, and threat actors that are driven by extreme monetary gain.

Whether your organisation's key concern is related to cloud application deliveries that are protecting against API protocol vulnerabilities, application-layer denial-of-service (DoS), malicious bots or OWASP Top 10 threats, your application delivery must be redesigned to meet the new threat landscape.

Traditional Web Application Firewalls were created to address the problem of web application servers running code that was vulnerable to a myriad of known attacks, especially cross-site scripting (XSS) and SQL injection. WAFs have been deployed over the years to address these common

vulnerabilities, but not without issues of false positives and operational complexity. The original open source WAF, ModSecurity, is often the target of bypass attacks or evasion techniques that attempt to defeat the largely passive, filter-based mechanisms it uses to detect malicious requests Next-gen firewalls (NGFW) claim "application-aware" features and can also stop some injection attacks (XSS, SQLi, and so on). But, NGFW still relies on passive filter detection and doesn't examine every HTTP request. Instead, it works much like an IPS, sampling requests and examining their first few bytes, not the full request payload. As a result, application layer bypass attacks against NGFW technologies are common. Plus, IP address reputation feeds implemented on NGFW and other firewall technologies have proven ineffective against botnets and other automated threats.

WAF technology has improved over the years, but it's still largely based on those passive, filter-based methods used to detect malicious payloads and check for protocol compliance in web requests. In addition, the operational complexity of managing WAF policies has caused many organizations to leave some applications unprotected. In many high-profile breaches, a known application vulnerability was exploited because the targeted organization couldn't patch the application server or deploy WAF policy quickly enough.

The source of most attacks, regardless of type, is automated. DDoS attacks, data breaches, vulnerability scans, credential stuffing, brute force, resource hoarding, and other attack types are almost all automated. Attackers use automation to launch large-scale attacks and probe for vulnerabilities despite often having less financial and human capital than the organizations they target. In many cases, these automated attacks contain no malicious payload and are crafted to bypass defenses by mimicking legitimate user traffic.

Application layer (or layer 7) DDoS attacks have become a more common attack vector because they can target a resource-intensive URL with legitimate requests and simply overwhelm the application infrastructure. Similarly, credential stuffing (the automated use of compromised usernames and passwords) and brute force attacks designed to bypass login authentication are crafted by the attacker as legitimate requests. These login attacks are often "low and slow" to avoid detection as a DoS attack. Malicious automated traffic and bots make up 30-40 percent of traffic on a typical site, but as much as 90 percent or more of the traffic to a targeted asset within that same site. The target might be a login page, as in brute force or credential stuffing, or a heavy URL, as in a layer 7 DoS attack. In a resource hoarding attack, the attacker might target the purchase pages for desirable tickets, sneakers, or other items. Scraping attacks similarly target data that'll be mined for later use. These targeted attacks aren't just difficult to detect, they also consume a disproportionate amount of infrastructure resources.

The tools used to automate these attacks include headless browsers (for example Phantom.js and Selenium), vulnerability scanners (the same ones used by penetration testers), command line scripts, browser extensions, and even malware-infected machines.

Recommendation:

F5 Advanced Web Application Firewall (WAF)

mnemonic has assisted many organisations in designing, optimising and maintaining WAF solutions that are protecting common consumer-facing services to ensure security and stability meets the business' strict requirements. Security challenges related to cloud application deliveries has required new technologies and features to be introduced to meet these needs. Advanced WAF solutions now utilise machine learning, threat intelligence, behaviour analytics, stolen credentials protection as well as optimised security to defend against the OWASP Top 10 vulnerabilities. Using a WAF to secure REST/JSON, XML and GWT APIs is also advancing to support emerging use cases.

Cloud application security challenge #2: protecting modern apps and apis

Modern apps are commonly split up into a vast number of microservices that run in containers, communicate via APIs, and are deployed via automated CI/CD pipelines. A microservice can be viewed as a small and independent software process that can be developed and updated independently. Modularity is introduced as it becomes easier to test and improve a specific process. Scalability becomes more automated when independent microservice processes can be monitored and scaled independently as needed. As an application can contain a large number of independent microservices, that are commonly managed by specialised developer teams, such collaborations have become very common as it speeds up development cycles and fuels innovation. Security must be included in all the steps of the pipeline.

According to NGINX, nearly 85% of new workloads are now deployed in containers and a similar 83% of Internet traffic is now API calls. As an increasing number of applications are now defaulting to microservices that run in containers, communicate via APIs, and deploy via automated CI/CD pipelines, the security posture has changed. This paradigm shift requires a rethinking of how security should be implemented to work seamlessly in DevOps environments.

While a WAF technology works perfectly well to protect against a wide number of security concerns, there is a trend now towards complementing WAFs with additional security measures to support needs from DevOps teams to Integrate the non-disruptive security controls authorized by the security team into their automation and CI/CD processes. This requires application security controls to be implemented across distributed environments such as web applications, containers, microservices and APIs. These security controls must be implemented in a cost-efficient way without negatively impacting release cycles or application performance.

Microservices and DevOps help accelerate application development and deployment. Organisations are challenged with ensuring this pipeline can operate securely without impeding the pace of innovation and releases. For modern web app development, the option to build security directly into the CI/CI pipeline makes a lot of sense. This is also the approach we will look into in the next section of this whitepaper.

Recommendation:

F5 NGINX App Protect

In partnership with F5, mnemonic delivers relevant security controls both based on the F5 Advanced WAF feature set, but also by implementing additional security controls based on the NGINX App Protect platform. The NGINX App Protect integrates security and WAF natively into the CI/CD pipeline and is agnostic of the underlying infrastructure. NGINX App Protect will act as a gatekeeper providing continual assessment on a perimeter around individual apps or groups of apps to inspect incoming traffic and enforce security policies. This can be applied to apps deployed on-premises, in the cloud or within a hybrid cloud as well as for containerised architectures such as the

Kubernetes framework.

Cloud application security challenge #3: identifying and remediating application vulnerabilities

Applications and services that are exposed on the Internet are attractive targets for adversaries. Would-be attackers systematically and continuously scan and probe these systems in hopes of finding a vulnerability that can be exploited.

Modern applications are also becoming more complex, have more dependencies on third-parties, and are developed and released more rapidly than ever before. Vulnerabilities can be introduced through changes in your application, security patches not being applied, misconfigurations, or even changes introduced by third-parties that are outside of your control, and without notification.

To operate securely with the speed of innovation, organisations need visibility into the vulnerabilities and risks that are present in their public facing systems.

The next section will introduce a security service that helps customers with such scenarios using a proven partner to perform real-world tests to evaluate your external-facing security posture.

Recommendation:

Argus Continuous Vulnerability Management for External Systems (ACVM)

How exposed are your web applications to the outside world? Applications and services that are exposed on the Internet are attractive targets for adversaries. Would-be attackers systematically and continuously scan and probe these systems in hopes of finding a vulnerability that can be exploited.

Modern applications are also becoming more complex, have more dependencies on third-parties, and are developed and released more rapidly than ever before. Vulnerabilities can be introduced through changes in your application, security patches not being applied, misconfigurations, or even changes introduced by third-parties that are outside of your control, and without notification. To operate securely with the speed of innovation, organisations need visibility into the vulnerabilities and risks that are present in their public facing systems.

mnemonic Argus Continuous Vulnerability Monitoring for External Systems provides visibility into the risks associated with your external-facing digital assets. Rapid detection of new vulnerabilities, poor configuration and policy drifts in combination with actionable advice empowers your resources to conduct quick, structured and prioritised remediation. This way your systems and exposed applications are scanned and monitored from the same perspective as would be attackers, providing a true picture of the exposure and risks of your public-facing systems

It is important to pinpoint the importance of performing recurring and continuous scanning, reporting and alerting as this enables the early discovery of potential risks that can be addressed before they are discovered by adversaries.

The service harnesses 20 years of organisational experience in vulnerability management and security testing, built into a streamlined and rapid deployment model that requires minimal configuration. This is a proven service that will also help your organisation stay compliant with security regulations, best practice and industry standards, and meet common reporting requirements with pre-built templates.

How security monitoring will support cloud initiatives

The combined combination of market-leading security solutions from F5 and security services from mnemonic will provide organisations with a very competent setup to support cloud application migrations and hardening to ensure your users will

experience a fast and secure service.

By utilising best-of-breed security technologies from F5 and NGINX combined with expertise from mnemonic, customers will have strong partners that can ensure security is optimized so web applications can be delivered in a secure and flexible way.

mnemonic regularly works with organisations through such transitions and cloud-first strategies by assessing security implications and assisting customers at different stages of their application development and migration initiatives. From guidance in the planning phase and assessing service providers, to technical testing and reviews of applications, APIs and configurations, through to implementing security technology and 24/7 security monitoring of the transitioned applications, mnemonic offers a full spectrum of cloud security services. These services are core modules in the mnemonic Argus Managed Defence platform. With complete enterprise coverage, including cloud, data centre, network and endpoint, mnemonic offers access to an expert team of security analysts, incident responders and threat researchers who will act as an extension to organisation's security teams to help defend against today's complex and targeted cyberattacks.

The service provides advanced correlation across six key areas – networks, e-mail, log data, endpoints, vulnerability & asset data and cloud services – to gain complete visibility and detect cyber threats that may have otherwise gone unnoticed. When a threat is detected, security analysts will give customers the actionable information and recommended actions needed to immediately respond to the threat. By filtering out the noise, Argus Managed Defence allows security teams to concentrate on responding to confirmed threats and stop wasting time chasing false positives.

Powered by the Argus security platform, driven by Threat Intelligence and acknowledged by Gartner as one of the top managed security services in the world, Argus Managed Defence allows customers to strengthen security, reduce operational costs and focus on their daily business.

mnemonic and the partnership with F5

mnemonic helps businesses manage their security risks, protect their data and defend against cyber threats. An expert team of 250+ security consultants, product specialists, threat researchers, incident responders and ethical hackers, combined with our Argus security platform ensures we stay ahead of advanced cyberattacks and protect our customers from evolving threats. mnemonic is acknowledged by Garter as a notable vendor in Managed Detection and Response (MDR) services, threat intelligence and advanced targeted detection, and a trusted source of threat intelligence to Europol and other agencies globally.

F5 is a strategic partner that mnemonic has worked with for nearly two decades. This relationship has proven successful in many critical deployments and as a result, mnemonic is now proud to have a team of competent F5 experts that assists customers in anything from daily maintenance, support, but also when it comes to redesign and planning for future deployments, like cloud application migrations.

About F5

F5 (NASDAQ: FFIV) powers applications from development through their entire life cycle, across any multi-cloud environment, so our customers – enterprise businesses, service providers, governments, and consumer brands–can deliver differentiated, high-performing, and secure digital experiences. To learn more about F5, go to f5.com.

mnemonic

Securing your business.

About mnemonic

mnemonic helps businesses manage their security risks, protect their data and defend against cyber threats. Our expert team combined with our Argus security platform ensures we stay ahead of advanced cyberattacks and protect our customers from evolving threats. Acknowledged by Gartner as a notable vendor in delivering Managed Detection and Response (MDR) services, threat intelligence and advanced targeted attack detection, we are among the largest IT security service providers in Europe, the preferred security partner of the region's top companies and a trusted source of threat intelligence to Europol and other law enforcement agencies globally. With intelligence-driven managed security services, 250+ security experts and partnerships with leading security vendors, mnemonic enables businesses to stay secure and compliant while reducing costs.

For more information, please contact mnemonic.