In the next three years, software as a service ‘SaaS’ is likely to grow by around 23%. That’s according to reports by Cognizance. It’s growth rests on the adoption of cloud public, private and hybrid.

Without the cloud applications can’t truly pervade an organization, nor can operational or customer benefits be derived. But there’s no point in adopting the cloud if it’s not secure - the proliferation of SaaS demands security, none more so in a GDPR world.
But modern applications are difficult to secure. SaaS based, web, mobile, or custom made all work on different platforms and frameworks. It’s a headache managing all the APIs needed to automate and sync tools. This introduces risk. The greater the number of apps the broader the attack surface and therefore the greater the chance there will be blind posts.

“Keeping up to date with updates and new security policies is never easy

There are also added hazards. Applications are always changing. Keeping up to date with updates and new security policies is never easy, but especially hard in a large cloud environment. Failure to adopt changes puts the organization and customers at further risk. But the biggest obstacle is keeping applications and APIs out of harm’s way. It’s a near on impossible task when attack methods and sources are constantly changing.

More advanced threats

To be specific there are four emerging challenges when it comes to protecting apps. Firstly, managing the good and the bad bots and spotting which is which, secondly securing APIs as IoT adoption intensifies, thirdly the relationship between securing apps and DevOps and ensuring ownership of security, and finally denial of service attacks that use newer tactics such as brute force.

Basic security hygiene dictates that security teams refer to the OWASP Top 10. It’s considered the ‘ten commandments’ in security circles, providing a starting point for ensuring the most common threats and vulnerabilities are managed, detected and mitigated. Web Application Firewalls also come into the fray with guidance on testing for the ways hackers exploit vulnerabilities. However, though the basics are good to have in place, there are always more advanced threats to take care of. Bots being a big one.

Bot management
The more sophisticated bots will go as far as to mimic human behavior.

Astonishingly about half of internet traffic is bot generated. Half of it is from bad bots. Discerning the good from the bad isn’t easy though and explains why around 80% of organizations can’t make a clear distinction between the two.

Bad bots can do a lot of damage like take over user accounts and payment information, scrape confidential data, or hold up inventory and skew marketing metrics. The more sophisticated bots will go as far as to mimic human behavior and bypass tools like CAPTCHA and even device fingerprinting based protection ineffective.

Securing APIs

Then there’s the complications derived from machine-to-machine and internet of things (IoT) communications. The more integrated ‘things’, the more data there is, the more events there are report on, and the more activity there is reliant on APIs to make the ‘things’ useful and agile.

That’s what makes them a target and the threats to API vulnerabilities include injections, protocol attacks, parameter manipulations, invalidated redirects and bot attacks. There’s the risk that business will grant access to sensitive data, without inspecting nor protecting APIs to detect cyberattacks.

Denial of service (DoS)

You might think there’s little to add to the swathes of denial of service warnings. Yet when businesses are still being targeted and feeling the ill effects it’s worth mentioning again that different forms of application-layer DoS attacks are still very effective at bringing application services down.
Even the greatest application protection is worthless if the service itself can be knocked down

This includes HTTP/S floods, low and slow attacks (famous examples being Slowloris, LOIC, Torshammer), dynamic IP attacks, buffer overflow, Brute Force attacks and more. The IoT botnets are the culprits and have made application-layer attacks so popular that they have become the preferred DDoS attack vector. Even the greatest application protection is worthless if the service itself can be knocked down.

Continuous security

It may seem easy to say but for modern DevOps, agility is valued at the expense of security. We see time and again examples of where development and roll-out methodologies, such as continuous delivery, mean applications are exposed to threats each time they are modified.

There’s no doubt it is extremely difficult to maintain a valid security policy and protect sensitive data in dynamic conditions without creating a high number of false positives. But we now find that this task has gone way beyond the capability of humans. Organizations now need machine-learning based solutions that map application resources, analyse possible threats, and create and optimise security policies in real time. Reaching this level in security planning should be a big wake-up call that security automation is an essential not a nice to have.

Running security plans

The board needs to know that investment is critical to protect their profits
It’s critical that the security solution your company adopts protects applications on all platforms, against all attacks, through all the channels and at all times. The board needs to know that investment is critical to protect their profits. As such there are six things they need to know:

- Application security solutions must encompass web and mobile apps, as well as APIs.
- Bot management solutions need to overcome the most sophisticated bot attacks.
- DDoS mitigation must be an essential and integrated part of application security solutions.
- A future-proof solution must protect containerized applications, serverless functions, and integrate with automation, provisioning and orchestration tools.
- To keep up with continuous application delivery, security protections must adapt in real time.
- A fully managed service should be considered to remove complexity and minimise resources. No amount of human power will beat the bots.

That last point is the most critical. Skill is essential in designing and running security plans and policies that work. But the plans can’t be executed without automated tools. There are just too many decisions to make in a split second. Combining both is the path to an effective app protection strategy and a stronger brand to boot.

Author Profile
Jeff Curley
You may also be interested in...

**Five Cyber Security Threats Your Enterprise Must Address**

By now your organization should know the drill. To keep your enterprise safe from unauthorized access you take the basic precautions: create...

**Unifying The Mobile Experience: Cloud, IoT And The AI Evolution Of Acc...**

The industry faces numerous challenges in the coming year. Physical and cyber security threats continue to become more complex, and organiza...

**What Is The Role Of Ethical Hackers To Ensure Cybersecurity?**

Ethical hackers are familiar to the world of cybersecurity. As cybersecurity awareness increases in physical security, they are also playing...