Speed. Agility. Security.

Expert article

Martin Burkhart, Dr. sc. ETH Zurich
Head of Product Management Airlock, Ergon Informatik AG

Published in Ergon magazine 2019
SMART insights

ergon

Digitalisation is transforming our economy, sector after sector, accelerating the evolution of web technologies. These developments are affecting security solutions as well – the trend is clearly pointing towards a convergence of application security, API security and access management. The many benefits of such an integrated approach include a shorter time to market for projects and lower total cost of ownership. However, if organisations are to derive maximum value from digitalisation, they must combine management and IT skills in intelligent ways. Security expert Martin Burkhart elaborates why.

Web application firewalls must learn new tricks

A web application firewall (WAF) is a filter placed in front of a web application to inspect incoming data traffic for potential threats and malicious activity. WAFs are among the most common mechanisms for protecting against attacks at an application level. Companies that let down their guard on this front can rapidly find themselves in very hot water – for example if sensitive customer data is lost and their reputation takes a hit.

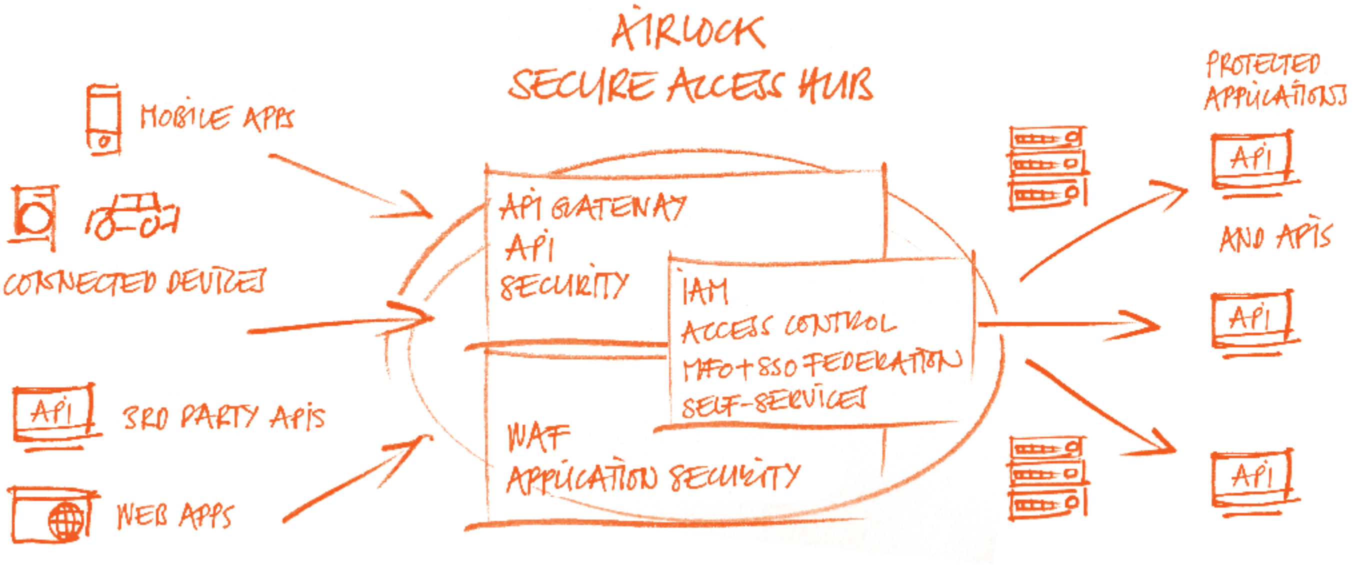
In opening the gates to widespread use of web applications, ongoing digitalisation has meant that today's WAF market has become a highly competitive, global business worth billions. However, signs of upheaval are already on the horizon, as digitalisation is also driving up demand for a better and more interactive user experience. Web applications are thus now being developed to suit a new paradigm that prioritises the integration and networking of a range of different services known as application programming interfaces (APIs). Conventional web applications, for which WAFs were originally developed, will eventually die out. Analyst firm Gartner has predicted that 65% of new web applications will be based on APIs by 2021.

APIs as business enablers

While use of such APIs presents companies with technological challenges, it will also open up new commercial opportunities for them. APIs simplify the speedy deployment of innovative services, making it possible to tap new revenue streams. APIs can also help improve the user experience and enable third-party services, for example, those provided by partner organisations, to be more easily integrated into a firm's own organisation of services.

> "In the near future, this may mean that customers use Facebook or Google to pay bills."

Martin Burkhart, Dr. sc. ETH Zurich,
Head of Product Management Airlock
martin.burkhart@ergon.ch



A range of different security technologies converge in the Airlock secure access hub.

API security = web security
APIs also present organisations with new risks, however. Business interfaces and internal data built with APIs are more immediately exposed on the Internet than in the past – mobile apps and smart "things" use APIs directly and globally. The encapsulation of data we have become used to in comprehensive, conventional web applications has largely been dispensed with and attackers are now also able to access underlying APIs directly, leaving them vulnerable to exactly the same security risks, such as the OWASP top 10, as any regular web application.

Traditional security products for APIs, such as XML gateways, are only capable of providing the protection required in this brave new world under certain conditions, while modern applications are characterised by their agility and lightness. APIs have mostly been used in the protected B2B sector over recent decades and options for interaction were restricted by comprehensive standards. Web security considerations were of secondary importance here. Today, businesses need modern API gateways that can deal with contemporary API requirements and reliably handle web security issues.

APIs need access management
The most compelling reason for using API gateways is access management. External access to APIs must be possible while also being secured via a range of standards, such as OAuth 2.0, OpenID Connect and SAML. This involves both the authorisation and the authentication of users, which in turn requires integration with a uniform web login, a single sign-on and an identity and access management (IAM) system.

There are now even regulatory guidelines that require APIs to be opened up. A classic example here is the European Payment Services Directive 2 (PSD2), a new EU-wide guideline that will change the face of banking as we know it. In short, PSD2 allows bank customers, both consumers and companies, to use third parties to manage their finances. In the near future, this may mean that banking customers use Facebook or Google to pay bills, make money transfers or analyse their outgoings, while their money stays safe in their account. Banks in the EU are obliged to allow these third parties access to their customers' accounts via open APIs and this will enable the third parties to build up their own financial services that will be in competition with the banks in terms of data and infrastructure. Such access must of course be strongly authenticated to contain security risks.

IAM and the customer

IAM products are generally used to manage user access to critical information within a company. Identity and access management involves identifying and controlling the roles and access rights of individual users and user groups, as well as defining the situations in which users are granted or denied such rights. These users may be either in-house staff, or external partners or customers.

By contrast with enterprise IAM systems, so-called “customer IAM” (cIAM) solutions are more suitable for managing heterogeneous, external user groups. cIAM systems offer simple scalability where large numbers of users are involved and a seamless user experience that is achieved with integrated user interfaces. Users can manage their access to their own data autonomously by means of so-called “user self-services”. Such services include functions like resetting a password, updating profile information, registering devices or consenting to the processing of personal data – the General Data Protection Regulation or GDPR. These are important considerations, as users of digital channels are typically frustrated wasting time “on hold” to helpdesks. Customers want to be able to solve problems themselves at a time that suits them. Naturally, access should not be made unnecessarily difficult with laborious, multi-stage authentication procedures, so flexibility is particularly critical when it comes to user authentication. The risk identified may vary, depending on the action requested and the context of the access attempt, and adaptive authentication protocols must ensure that security requirements are met without plaguing users with unnecessary questions.

More than the sum of its parts

So where is all this going? In short, WAFs will have to protect APIs. API gateways will, in turn, have to learn web security. APIs need access control and it is increasingly clear that managing users with conventional enterprise IAM systems is suboptimal. Moreover, we are all well aware of the shortcomings of overly simplistic “spot solutions” that leave plenty of gaps at transition points.

The Airlock Secure Access Hub, comprising a WAF, an API gateway and a customer IAM system, is an integrated, coherent solution designed to handle the secure access management requirements of the future. The individual components interoperate via intelligent interfaces. With 20 years’ experience of protecting sensitive web applications under our belt, we are convinced that Airlock is the best route to sustainable digital security.

Fossilised organisational structures – an unexpected obstacle

An additional problem that often comes as something of a surprise initially is organisational in nature: how can you purchase a secure access hub in which a wide spectrum of technologies converge to form one large system? Nowadays, responsibility for such issues is generally distributed across a range of different departments, such as IT infrastructure, network operations, the CIO or user administration. In turn, the benefits of an integrated approach, such as lower total cost of ownership and quicker time to market, will usually be felt by the business and a seamless customer experience will benefit marketing. Yet neither of these departments is generally involved in purchasing IT security solutions.

Digitalisation is not only changing technologies, it is affecting business processes and breathing new life into fossilised organisational structures. Greater flexibility, collaboration and agility are called for and here, however, the ball is ultimately in each company’s court. Forward-looking firms are confronting the questions of integrated security head-on and are laying solid foundations for their digital future.

Interested in more?

Get your free copy of
the SMART insights magazine:
www.ergon.ch/2019-smart-insights