For a few plants, a complete overhaul of network security may be necessary – for example, updating a protocol to one with continued security patches. However, the majority of plants will find that installation of additional software, security patch updates or a top-down study of network connections will be sufficient to bring cyber security to the necessary levels.

Bridging the gap

In the world of cyber security, there is no silver bullet. However, organisations should remain vigilant and proactive in their defence. To that end, plant managers should implement a multi-layered cyber security strategy to stop the cyberthreat across both IT and OT environments.

Industrial control systems have traditionally been a separate entity from the IT systems used by the corporate enterprise and were therefore outside the remit of IT cyber security teams. However, as the worlds of OT and IT converge, this is a dangerous mentality and securing the entire system is essential.

Because many businesses are now beginning to realise the benefit of adopting digital technologies, IT and OT staff should consider a variety of factors to make this transition as smooth as possible.

The first step is end-to-end security. Businesses making the leap to digital technologies will need to ensure that weak or fragmented security is eliminated. Everything from users and devices should be secured. It's not just about using firewalls either. It's vital that IT and OT staff carry out security audits of both their enterprise and industrial control systems.

Putting network monitoring into place as well as intrusion detection and prevention measures will ensure that cyber breaches are immediately identified as they occur, so that measures can be taken to safeguard the system within minutes. Rolling out user-access and device-access controls will help mitigate the potential risks from connected devices, while implementing security awareness training for all staff will ensure that the system is not left vulnerable.

By bringing together the core competencies of IT and OT firms, manufacturers can manage a cost-effective digitalisation process that offers a personalised and tailored transition. Digitalisation is well and truly in the public consciousness, but now it's up to IT and OT pros to work together to make it a success.

Cyber security is an ongoing concern for a multitude of industries, as the threat of cyber attack is growing year-on-year and is now significantly higher than during the Siberian pipeline attack in 1982. Although update methods such as retrofitting may seem to provide a quick and easy leap into the connected world, an end-to-end cyber security approach that incorporates both IT and OT environments must be considered when integrating legacy systems into existing networks.

About the author

Nick Boughton is the digital lead at systems integrator and industrial cyber security expert Boulting Technology. Boughton has worked in the automation industry for over 30 years. He has gathered experience from roles with automation equipment vendors, process OEMs and system integrators, in sectors such as food and beverage, power, chemical and water.

References

1. Belikovetsky, S; Yampolskiy, M; Toh, J; Elovici, Y. 'dr0wned – Cyber-Physical Attack with Additive Manufacturing'. Via Arxiv. Accessed Jun 2019. https://arxiv.org/pdf/1609.00133.pdf.
2. 'Insider Threat Statistics: The Cost of Insider Threats'. ObserveIT. Accessed Jun 2019. www.observeit.com/cost-of-insider-threat/.

Product vs toolkit: API and IAM security

Jason Macy, Forum Systems

Jason Macy

Marketing departments are great at capitalising on the latest industry trends. Whether it's slapping the 'cloud' badge onto their product or putting 'security' in their verbiage to appease their customers, it is a common marketing approach to reposition a product in a way that will improve sales. In the current era of conglomerate-acquired technologies, large-scale marketing departments will pay top dollar to get air cover from analysts (such as paying for a dot on the Gartner Magic Quadrant) to claim universal capabilities in niche market segments.

Satirical magazine *Private Eye* even has a special section devoted to it called Desperate Marketing where it publishes the worst examples of marketers trying to jump on the latest bandwagon and link their product to the latest event, fad or headline. A royal wedding, the World Cup or a general election can all be newsjacked to promote almost anything, however tenuous the link, it seems.

But in the end it is the customer who pays the price of this 'repositioning' and lack of clarity. If no technological changes are made under the hood to justify the new positioning, then this is nothing more than a shameless marketing exercise. But worse still, if the new term is over-used and applied too liberally to products that don't deserve the moniker, the term itself begins to lose its intended meaning. Ultimately if the new term loses its value, then customers get lulled into complacency and can no longer rely on the claimed technology capabilities to differentiate one product from another and the adoption of products becomes an exercise in group-think.

'API security' and 'IAM security' are two such terms in the security space that are starting to lose their meaning by their association with vendor marketing, which is diluting the meaning of the 'security' tag applied in this context.

Identity, security and APIs

Let's start by remembering that application program interfaces (APIs) are the central point of modern communication – they are involved in almost every interaction with a digital device or service. APIs specify how software components should interact with each other through a series of protocols and specific communication standards that allow different technologies to work together, regardless of their language or platform. APIs are now commonly seen as the language of the Internet. With the growing adoption of the Internet of Things (IoT), more and more devices, and the applications they run, need a common language to communicate.

The API's role is to act as the single point of entry into a system or application, to streamline the integration process and more easily connect systems together. As such, the API has also become the central target of attack since now you need only to compromise the API to have access to the applications and systems behind it.

Given this clear paradigm shift toward API connections, and the continual news of API breaches in the media, one would think the industry would wake up about the real threats of insecure API architectures. Unfortunately the adoption of technology continues to be the group-think mentality of using Magic Quadrant dot technologies that are all toolkits, adapters and agent-based. These technologies tout 'API security' in their marketing. However, this is smoke and mirrors, as these toolkits are not secure themselves – they merely provide 'security features' that are developer-centric.

Consider for example, a leading API management Gartner Magic Quadrant vendor's own public documentation stating: "Developers should remember to wear the hat of an API hacker before deploying. If a developer neglects to identify the vulnerabilities in an API, the API could become an open gateway for malicious activity."

Interpretation: we don't really have API security in our product, we just use those words to appease our customers and rather we rely on developers to know how to protect against unknown evolving threats.

Is it reasonable to put this burden entirely on developers? Developers tend to focus more on agility and functionality over security and with the pressure to deliver new releases on a regular basis, even well-intentioned, responsible programmers are sure to make mistakes and introduce vulnerabilities to an API. Regardless, if the technology itself isn't secure, a developer can code security all day long only to find that the rug can be pulled out by a hacker. This is all lost in the moniker of security provided in the documentation and is not often realised until the company makes the headlines for an API breach.

Access control

In similar vein, modern architectures must have identity access management (IAM) technologies deployed to provide access control and authentication to APIs, applications and services. IAM has been defined by Gartner as the security and business discipline that 'enables the right individuals to access the right resources at the right times and for the right reasons'.[1]

Note again the word 'security' is used, another example of over-reliance on wording alone for a sense of protection. Access control is not security, it's merely access control. IAM technologies are meant to provide the 'yes' or 'no' answer to whether the access is allowed. However, as with APIs, IAM enforcement points, known as policy enforcement points (PEPs), have become increasingly targeted for compromise. An attacker understands that while you can build all the access control rules you want, if the attacker can compromise the policy enforcement point, any 'no' can be turned into a 'yes', giving attackers access to anything they want.

Both APIs and IAM are direct routes into compromising your systems, applications, and data. So, how do you protect against these attacks? Using toolkits for APIs and IAM forces the problem on developers to build security and protect business assets. Legacy IT security components are helpless against API threats and the cost of a breach to business reputation is far too harmful to place complete trust in developer-centric security. API security and IAM security are the unknown lurking deficiencies of the actual technology being used to deploy them because these technologies are toolkits, agents and adapters, not security products.

Don't blame the tool

API and IAM technologies are both predominantly frameworks based on toolkits and adapter-based solutions designed to connect, not designed to secure. Marketing for API toolkits and IAM toolkits tout security features such as encryption and access control that lull customers into a false sense of security but, because security is mentioned as a feature over and over again, customers may come to believe that their systems are safe.

As stated earlier, and in fairness, the toolkit vendors are not wholly to blame since their marketing is driven out of the need to placate their customers' legitimate concerns about security.

As IAM and API toolkits, frameworks and adapter-based solutions continue to claim to be security products, customers must look beyond the marketing statements to understand the difference between a security product and a toolkit.

Product vs toolkit

The challenge faced by API toolkit vendors – and the key difference between a security toolkit and a security product – is they must continually add security features to a baseline that is inherently insecure. This is akin to adding bars around the windows of a house but leaving the front door wide open. These insecure API solutions will be continually plagued with the chicken and egg of exploit and patch, which is the reverse of what you should expect in your API security solution strategy.

By contrast, an API or IAM security product is built with a secure, locked-down architecture with self-integrity checks to ensure that the product itself is not able to be compromised. This is the essential difference between a product and a toolkit. A toolkit providing security is far from being a secure product. While a toolkit bolts on security capabilities, the underlying architecture is still vulnerable to attack. Do you know whether your toolkit has all of its original parts? A hacker would certainly like you to think so. Should you build a car by gathering hundreds of different parts, or instead simply buy the car?

A new security product technology is available that combines API and IAM capabilities. This product technology is called an API security gateway and it is the industry's answer to protecting and ensuring successful API and IAM strategies. Instead of the parts, it is the car. The API security gateway has emerged as a distinct and unique category of API and IAM technology where 'security' means the literal, cyber-hardening of the product itself so that API and IAM enablement can be done without risk of compromise.

Three layers

An API gateway that is genuinely secure and able to call itself an API security gateway will typically provide three layers of fundamental protection:

- **Secure, locked-down OS** to detect and prevent compromise and ensure the inability to break the security model of the system by constantly self-validating the integrity of the system, disallowing third-party applications to be installed, and disallowing root access to the OS.
- **Cyber-secure policy enforcement points (PEPs)** to ensure secure enforcement of the authentication and authorisation of users and prevent PEP compromise which could turn a 'no' into a 'yes'.
- **Real-time protection and monitoring** to proactively monitor and enforce compliant traffic to applications and services and take protective measures if threats are detected.

API revolution

We are in the middle of an API revolution and APIs are seeing explosive growth in every industry sector around the world. We are witnessing the beginning of a new Gold Rush as IT security experts rush to stake their solution's claim as the most secure approach.

At the moment, there is still a sense that we are living through a Wild West period of history where IT security experts are competing to define the secure architecture that will prove to be the industry standard. Many of the voices are just adding noise to an already deafening din, while others are giving businesses a false sense of security due to overlooked vulnerabilities in their design. Toolkits, adapters and frameworks are not the answer to security, they are the cause of insecurity.

When considering product vs toolkit, again, ask yourself whether you would build a car using hundreds of different parts, or if you would instead buy the car.

About the author

Jason Macy is chief technical officer at Forum Systems (www.forumsys.com), responsible for innovation and product strategy for global operations. He is responsible for the architecture and lifecycle of technologies that comprise the API testing and API simulation product lines deployed in over 100,000 sites worldwide. Earlier in his career, Macy worked as the lead architect for Raytheon and was responsible for deployment, acceptance testing and successful commissioning of the air traffic control system currently live and in use at Schiphol Airport in Amsterdam, Holland. Macy holds dual degrees in computer science and computer engineering.

Reference

1. 'Identity and Access Management (IAM)'. Gartner. Accessed Jun 2019. https://blogs.gartner.com/it-glossary/identity-and-access-management-iam/.

A framework for effective threat hunting

Dr Akashdeep Bhardwaj, University of Petroleum & Energy Studies, India and Dr Sam Goundar, University of South Pacific, Fiji

Dr Akashdeep Bhardwaj

Dr Sam Goundar

In today's dynamic cyber security environment, with its rapidly changing threat landscape, companies are becoming increasingly aware of the necessity of getting ahead of new cyber attack trends. It is for this reason that threat hunting has become so popular. A new wave of attacks has become exceptionally proficient in successful, undetected intrusions, breaching network defences, exploiting system vulnerabilities and obtaining access to organisations' systems and data.

The attack methodology adopted by cyber criminals is such that it may be several weeks, or perhaps months, before an organisation even becomes aware of an intrusion. This calls for implementing a proactive posture to detect and mitigate the attacks. Traditional security operations rely on having a 24x7 team manually monitoring alerts. These alerts are reported