Checkmarx
The world runs on code. We secure it.

eBook

Towards Modern Application Development in Financial Services

Ensuring Your AppSec Program Adds Value

Introduction

The financial services sector is experiencing significant and sustained disruption. As established institutions strive to service the demands of the digital native customer generation, they face strong competition from a swarm of agile FinTech market entrants – the banking monopoly is over. Innovation is table stakes as traditional banks work to develop their own new products and services or work to integrate those acquired in an active M&A environment.

The impact of the pandemic has added greater urgency as conventional customer channels have been disrupted and the shift to digital banking accelerated. Customers need to be able to self-serve to maintain their financial lives as flexibly and safely as possible, and expectations are high, shaped by experiences of consumer applications. Banks are under pressure to adopt technologies and methodologies that will deliver the services customers demand, from digital onboarding to online deposit facilities and personal money management services.

Despite this urgency, trust remains the corner stone of financial services. Without customer confidence that their deposits and data are secure, financial institutions simply cannot exist. That is why new software applications and services must meet the highest security standards and comply with an abundance of sector regulations.

This tension between the pressing need for innovation and the imperative to safeguard customer trust must be resolved, and financial services institutions are cautiously treading the path towards modern application development as a solution. On the way, they must overcome the challenges of large amounts of legacy technology and the brake that a naturally cautious approach puts on achieving rapid change. Central to successfully navigating this transformation is establishing an application development approach with a fully integrated application security (AppSec) program that adds securityfocused value throughout the software development life cycle.

This eBook examines the changing software development landscape in the financial services sector. It explores the threats and practical challenges faced and the key considerations for financial services organizations aiming to lay strong foundations for a secure future.

Table of Contents

An Escalating Threat Environment: The Digital Vault Under Siege

Modern day bank heists don't involve guns and getaway cars. These days it is far simpler and less risky for cyber criminals to blast through the digital vault doors to exfiltrate data and money.

Alongside the financial assets under management by banks is the wealth of personally identifiable information (PII) belonging to customers. This has a high resale value on the dark web and is frequently the primary target of sophisticated and persistent cyberattacks.

> *"Attacks against financial institutions rose by 238% between February and April 2020."*
>
> vmware

Indeed, the sector frequently tops the list of "most-attacked" industries and the pandemic has only intensified the situation. ***Research from the VMware Security Business Unit*** found that attacks against financial institutions rose by 238% between February and April 2020 as the COVID-19 surge unfolded. Overall, according to the research, 80% of the surveyed financial institutions reported an increase in cyberattacks in the previous year.

The majority of those attacks are likely to originate in applications, which have proliferated to become the dominant engine of the internet as they drive consumer interactions and transmit, store, and process customer data. Consequently, they have also become the most commonly attacked asset on the web, with ***Research by F5 Labs*** finding that applications were the initial target of breaches in 53% of all attacks tracked over a decade.

The impact of a security breach on customer trust and commercial reputations can be devastating. More than one third of financial services organizations that took part in ***VMware Research*** reported severe reputational damage following a security breach.

In such an environment the imperative for secure software development is clear. The reputational and financial risk posed by successful cyberattacks means security needs to be a priority.

Regulations and Compliance: Moving from Check Box Exercise to Value-Add

Given the intensive threat environment and the critical importance of trust for the functioning of the global financial system, it is understandable that financial institutions are required to operate in accordance with a rigorous and complex set of regulatory standards. These are designed to minimize the risk of theft and fraud while ensuring both customers and the institutions themselves are protected from the devastating impacts of disruption caused by destructive attacks.

Beyond sector-specific regulations there are the broader privacy regulations that safeguard customer information to protect against identity theft and fraud. Key cross-border regulations include PCI DSS, PSD2, GDPR, and Sarbanes-Oxley, while there is a wealth of regional regulations governed by local regulatory authorities.

The compliance burden exerted on software development by the various regulations varies. Some, such as PCI DSS, list specific activities organizations must follow, for example, developer training and the use of manual or automated processes to identify common vulnerabilities like SQL injection, cross-site request forgery, buffer overflows, and more. Others are principles-based and generally state that data must be adequately secured against attacks without giving specific guidance on how that is to be achieved.

> *"Applications were the initial target of breaches in 53% of all attacks tracked over a decade."*

Ultimately, however, the regulatory environment requires banks to have visibility into the risks and vulnerabilities of their software and systems. They must adopt an auditable, repeatable AppSec scanning process that is sufficiently robust and capable of highlighting material vulnerabilities. Achieving this entails the implementation of a suite of AppSec testing solutions used to track and report on when scans are completed and what the outcomes were over time.

These AppSec solutions should include:

- static code analysis
- software composition analysis
- interactive (runtime) code analysis

Compliance checking may be viewed by many as an unavoidable but cumbersome task that can obstruct the software delivery life cycle. Even with the best intentions, compliance can become something of a check box exercise. However, with advanced AppSec solutions that integrate seamlessly into source code management and continuous integration platforms, and deliver scan results to developers in the format they want to receive them, compliance can become a value-add exercise that underpins a more secure and effective development process.

The Evolving FinServ Application and Software Development World: Progressing Towards Modern Application Development

Faced with urgent drive for digitization set in a rigorous regulatory landscape and a high-risk cybersecurity environment, the way financial services companies develop and deliver software is evolving rapidly.

Software delivery speed is a critical factor in maintaining an edge in what is now a much more competitive market, so banks have shifted away from conventional software development waterfall methodologies.

Agile methodologies have been gathering ground and the introduction of DevOps concepts such as Continuous Integration and Continuous Delivery (CI/CD) into an Agile environment helps break down silos by integrating software developments and software operations, to increase quality and efficiency and make new features available to users more quickly.

> *"There is no point adopting Agile if you have to break a build to fix security issues."*

Shifting Left

Many financial institutions are now maturing on the DevOps journey, but need to make the critical next step in order to evolve towards modern application development. This means making the "shift left" to incorporate security intrinsically and detect vulnerabilities earlier in the software development life cycle – after all, there is no point adopting Agile if you have to break a build to fix security issues.

This approach helps to resolve the historical tensions between developers and security teams, where developers are under pressure to deliver applications within a tight timeframe, while security teams are focused on preventing breaches via exploitable vulnerabilities. By deploying AppSec solutions that automate scanning at critical points during the development and build processes, and rapidly delivers results back into the developers preferred environment – complete with intelligence around potential fixes – the delivery cadence can be maintained while security and compliance concerns are also satisfied.

Appetite for AppSec Solutions That Deliver Strong ROI

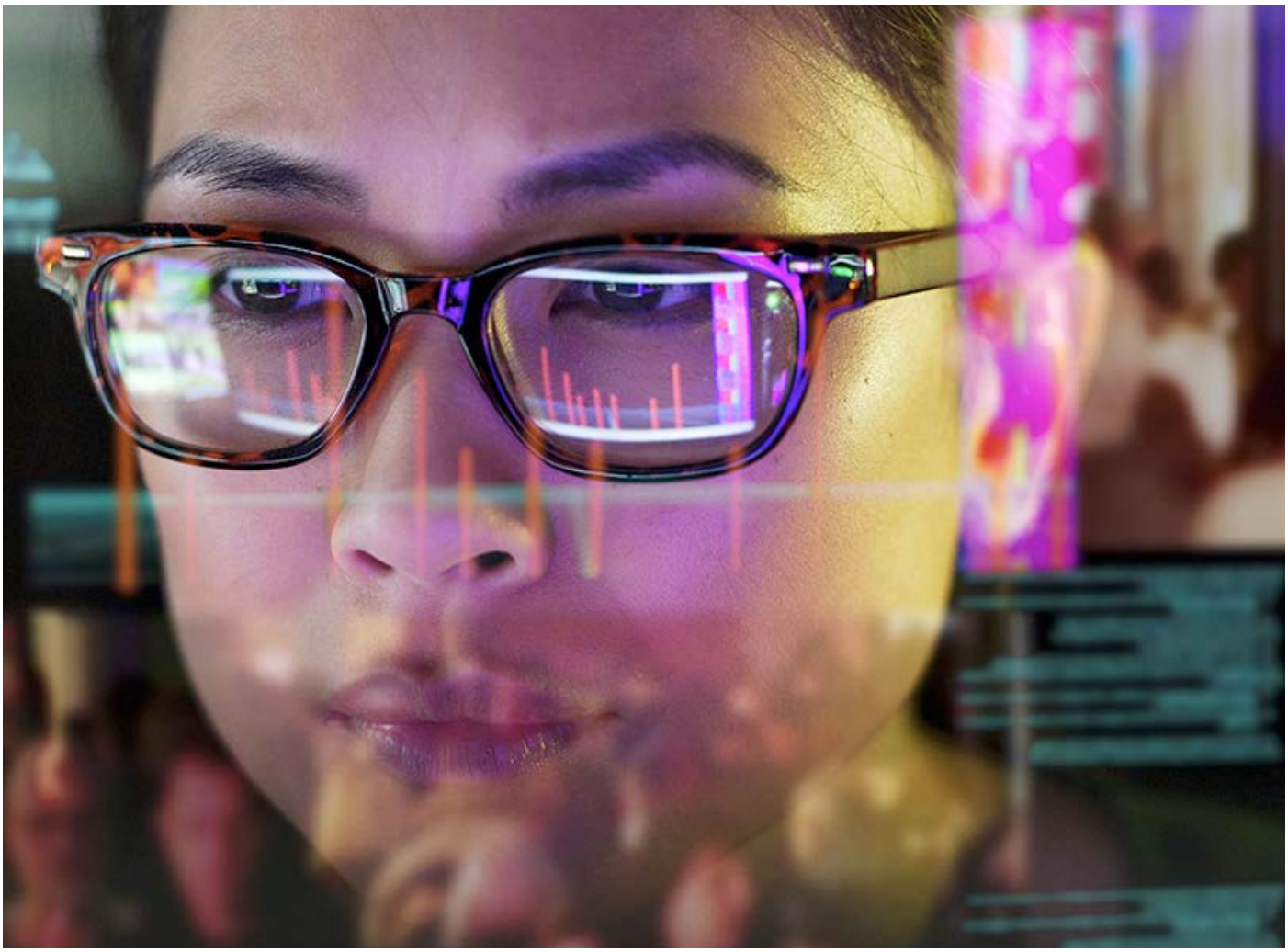
AppSec solutions designed to do this need to be almost infinitely scalable, capable of scanning millions of lines of code per day as the appetite for secure applications continues to grow. Speed and accuracy are paramount, as false positives negatively impact developer confidence and can impede AppSec solution adoption.

The right AppSec solutions can achieve ROI quickly, as vulnerabilities are identified earlier in the SDLC, making them easier to fix. It also saves developers considerable time and reduces regulatory risk exposure.

Ambition for Automation

There is considerable ambition in the financial services sector to ramp up AppSec programs, with some organizations proposing that every single piece of code – amounting to billions of lines per month - should be scanned. This simply isn't possible in the typical developer-submitted model in an IDE, meaning automation is essential.

By automatically triggering scans at defined points in the build process, vulnerabilities can be identified without developers having to interrupt their workflow to initiate scans.



How AppSec solutions generate ROI:

Reduces coding vulnerabilities: gain increased visibility of vulnerabilities without interrupting developer workflow.

Enables the retirement of legacy security tools: reduces the risk posture and release delays associated with using out-of-date scan tools.

Increases developer productivity and awareness: provides remediation tips, in conjunction with an integrated training and awareness solution that builds in-house developer secure coding skills.

Nucleus Research analyzed the deployment of Checkmarx Static Application Security Testing and Checkmarx Codebashing in a leading European financial services institution. The independent analysis found:

- 104,000 hours saved
- 1.7m EURO saved
- 393% ROI
- Payback term: 4.8 months

> *There is a paradox in the domain of DevSecOps: with an increasing amount of software there are an increasing amount of vulnerabilities, there's an increasing amount of tools that address these vulnerabilities and there is an increasing amount of work. This means there is a choke on the number of skilled people who are qualified to do this work and so there is misuse of other professionals, like software developers, to do security work. It is only through automation that we can exit this paradox.*
>
> *— Chief Product Owner, Major Bank in Netherlands*

VIEW WEBINAR

The Factors Blocking Progress Towards Modern Application Development

The Challenge of Legacy Systems

The technology environment of established financial institutions is incredibly complex. Legacy systems at the core of the banking sector can date back as far as the 1960s, generating a level of technical debt that can cripple the business's ability to compete with far more agile FinTechs.

It is also understandable that established banks have a very low risk tolerance when it comes to modernizing these core systems. The risks associated with anything less than a perfect outcome are so high that they act as a considerable brake on progress.

Cloud Caution

The financial services sector sits at a crossroads of cloud adoption. Fastmoving FinTech entrants are born in the cloud and benefit from every aspect of its flexibility and scalability. Coming from the other direction are the established, institutions whose technology footprint is based on mainframes and monolithic architectures. Despite the ***publication of guidelines*** on cloud use by regulators such as the European Banking Authority, a significant proportion remain cautious, preferring to keep their crown jewels "safely" on-premises.

Added to this is the significant cultural shift required to fully embrace the potential of cloud-native modern application development, which is proving a challenge for many established financial services institutions. Instead of large applications sitting on mainframes, developers must break the application up into microservices which all need to talk to each other through APIs, which also need to be factored into the security program.

Faced with the obstacle of a wholesale cultural paradigm shift, many financial institutions are opting for interim measures; they are bolting on FinTech solutions, creating a digital banking façade. In this scenario, customer-facing applications are developed and run in the cloud, while back-end systems are still operating on-premises.

Focus on the Future

It is not only legacy systems and architecture that pose a challenge for financial services businesses. As they look to the future, both traditional banks and new market entrants are operating in a highly active mergers and acquisitions market.

Established banks are seeking to acquire the innovative technology and customer experience power of FinTechs, while FinTechs are aiming to tap into consumer confidence in heritage brands by integrating with established players. Developer and security teams are faced with having to absorb and integrate very different approaches to technology and software development and make them work together, without compromising on security. It is therefore essential that AppSec solutions can integrate and automate across multiple SCM and CI platforms, development approaches, and deployment scenarios.

For organizations that sit at the crossroads between cloud and onpremises, and that need to be capable of integrating innovative startups with legacy systems, it is vital that the AppSec program can cope with both. An on-premises approach is essential for those organizations that have not yet embraced cloud, but there should always be one eye on the future – after all, talented early career developers are learning to code in the cloud and, if financial institutions want to attract and retain the next generation of skilled developers in a competitive market, they need to offer an environment that is both familiar and exciting.

AppSec solutions that supports on-premises, hybrid, and cloud-based options ensures that the organization is prepared for current and future scenarios. It means teams have the same experience no matter where the solutions are hosted, or even where software is developed, which aids adoption and usability.

Comprehensive language support is also critical, and for similar reasons. Many traditional financial institutions still have applications running that were developed using COBOL, but all modern banking customers expect to use mobile apps, which means support for the latest versions of Swift and Kotlin coding languages.

Adding Value to In-House Expertise with Managed AppSec Services:

A leading European payment services provider operating in the highly regulated payment sector needed to ensure its applications fully comply with regulations such as PCI DSS and PSD2.

The business was experiencing a strong period of growth and diversifying into new areas, putting pressure on in-house teams. It turned to Checkmarx to boost internal resources and help to transform and drive forward its AppSec posture. Checkmarx provides an all-inclusive managed service that reduces the burden of the software security program on the in-house team. The company has support from Checkmarx's team of security experts who are all experienced developers, skilled at implementing state of the art AppSec programs.

Addressing the Application Security Skills Shortage

Banks are no stranger to the problem of skills shortages. As the specialists who developed the original mainframe architectures on which many are still based reach retirement, there is a lack of talent in the pipeline to replace them – another factor creating an imperative for modernization.

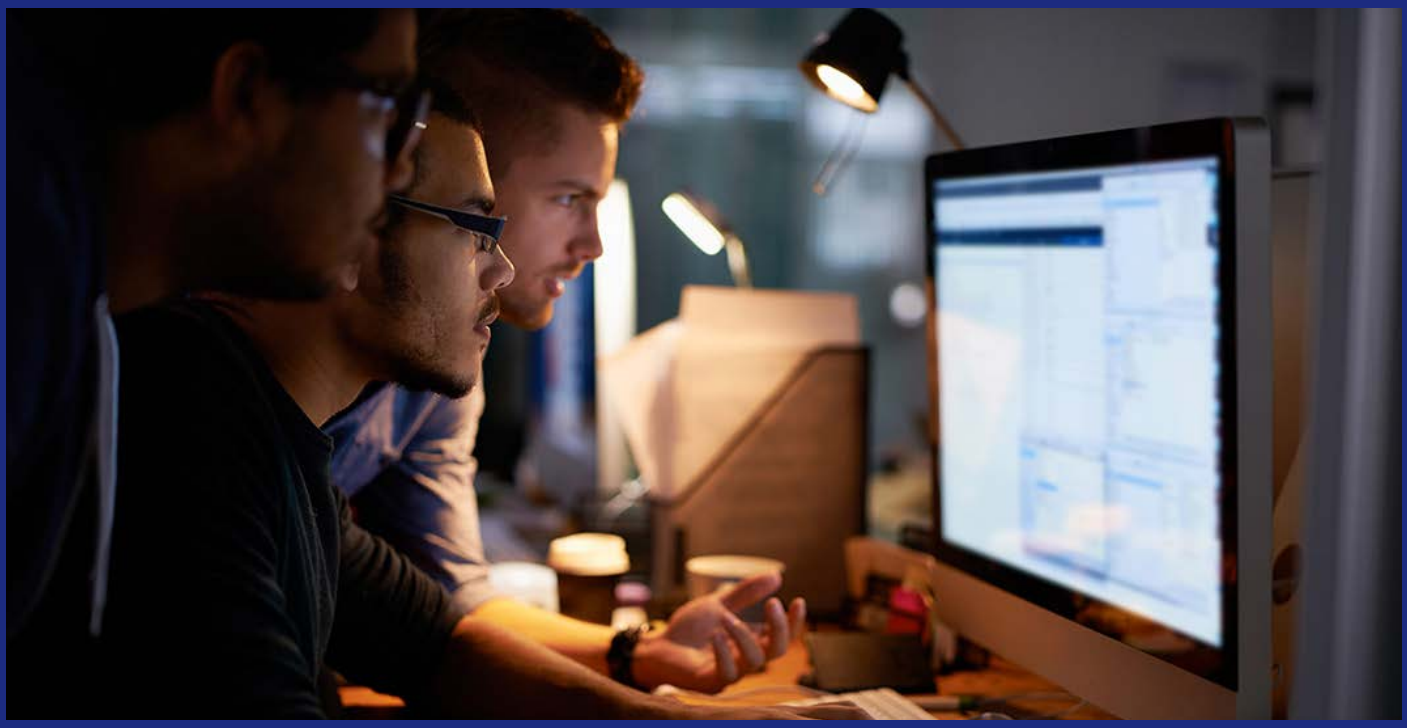
But it is not just legacy skills that are in short supply. Finding skilled full-stack developers who are also security specialists is a significant challenge even for large organizations with considerable talent acquisition power. Yet having developers with good security and compliance awareness is foundational to the shift to DevSecOps.

Consequently, organizations are aiming to diversify the skillset of their in-house developer teams and ultimately make them better coders through the adoption of AppSec solutions that don't just inform developers of code vulnerabilities, but also provide information about the best way to fix the issues while improving secure coding awareness and abilities.

This is delivered by an interactive training platform that is designed to inject AppSec awareness across the SDLC through just-in-time, bite-size lessons that relate directly to the issues developers are facing in the code they are working on. The learning-while-coding approach rapidly accelerates developers' AppSec awareness and encourages adoption of a security mindset by helping them solve live problems.

Another option for organizations to supplement in-house skills is to engage a managed service alongside their AppSec solutions whereby the vendor provides experienced AppSec experts to implement a high-impact security approach based on the organization's business, technology, and risk management needs. This may not be possible for traditional institutions with a low tolerance for outsourcing security projects, but it is perfect for fastmoving FinTechs that aim to eventually build in-house capability.

In this way, robust and integrated AppSec solutions – together with program support from the vendor if appropriate – can play a strategic role in facilitating the shift to DevSecOps, helping resolve the tension between speed and security and giving developers confidence in delivering secure software.



One Emerging Challenge: API Security

In the context of modern application development, APIs are becoming a major feature in the insurance and FinTech sectors and, as customers become increasingly demanding of personalized, mobile solutions that leverage open banking, so we are seeing APIs become more of a factor in mainstream banking too. With them come considerable security concerns.

Gartner ***predicted*** that APIs would account for 90% of an application's attack surface by 2021, with API abuses set to become the most frequent attack vector by 2022. As more organizations continue to rely on mobile apps for customer access, and take a cloud-native development and deployment approach, APIs will naturally continue to increase in usage in this sector. Just like any other software driven service, APIs have a host of natural risks that emerge when poor coding practices are applied during application development.

In response to the emerging risks associated with APIs, the ***OWASP Top Ten API project***, spearheaded by Checkmarx researchers, has been developed and released, and as always, provides a list of API risks.

Organizations who use APIs for a host of reasons like mobile apps, digital payments, transfers between financial institutions, and other more complex (or sensitive) financial transactions can tremendously benefit from the OWASP project to educate developers about common coding errors and pitfalls. Finally, APIs hold tremendous promise to bridge the gap between modern applications and legacy systems by providing a needed interaction and abstraction layer. APIs can fully support access to data, interactions with data, and transferal of data, often with ease between very dissimilar systems and approaches.

Organizations evaluating AppSec solutions need to enquire about their capability to discover, evaluate, and confirm the security of code used to implement APIs while addressing common coding errors, pitfalls, and coding oversights.

Ten Key Features to Look for in AppSec Solutions for Financial Services

In the context of both legacy and modern application development, and on-premises vs. cloud development and deployments, the list of key features below must be considered when implementing a comprehensive AppSec program that will grow alongside the digital transformation being experienced by financial services organizations worldwide. They are as follows:

01

Supports static code analysis, software composition analysis, and interactive (runtime) code analysis.

02

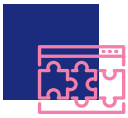
Includes seamless integration and automation capabilities into the CI and build systems in use.

03

Delivers speedy incremental and full scan capabilities plus scan engine customization options.

04

Provides out-of-thebox accuracy and advanced custom query options.



05

Supplies remediation guidance and best fix location to speed vulnerability triage.

06

Supports a comprehensive list of coding languages, frameworks, and package managers.

07

Includes on-premises, hybrid, and cloudhosted deployment options.

08

Incorporates developer AppSec awareness and training to build inhouse secure coding skills.

09

Offers managed services options to deliver interim or continuous support as needed.

10

Enables an ROI in terms of risk reduction, regulatory compliance, and measurable time savings.

Conclusion

The financial services sector is under enormous pressure to develop innovative software and provide advanced, personalized services. Strong security and compliance are fundamental to maintaining customer trust and managing regulatory risk.

Moving towards modern application development is the right approach but progress varies across the sector. Different organizations face differing challenges depending on their legacy technology, their risk tolerance, and the in-house resources they have available.

A robust AppSec program bolstered by the right AppSec solutions can add value to organizations whatever stage they have reached by integrating security seamlessly into software development, relieving the pressure on in-house developers, and making them more productive. It can also help address the prevailing skills shortage by allowing companies to measurably upskill existing employees.

About Checkmarx

Checkmarx is constantly pushing the boundaries of Application Security Testing to make security seamless and simple for the world's developers while giving CISOs the confidence and control they need. As the AppSec testing leader, we provide the industry's most comprehensive solutions, giving development and security teams unparalleled accuracy, coverage, visibility, and guidance to reduce risk across all components of modern software – including proprietary code, open source, APIs, and Infrastructure as code. Over 1,675 customers, including 45% of the Fortune 50, trust our security technology, expert research, and global services to securely optimize development at speed and scale. For more information, visit our website, check out our blog, or follow us on LinkedIn.

Checkmarx

Checkmarx at a Glance

1,675+
Customers in 70 countries

750
Employees in 25 countries

45%
of the Fortune 50 are customers

30+
Languages & frameworks

500k+
KICS downloads in 2021

The world runs on code. We secure it.