The shift to a security approach for the full application stack

How technologists can optimize security for modern application stacks

Executive summary

The speed of application development has increased exponentially over the last two years, in line with a dramatic acceleration of digital transformation across all industries. Organizations have fast-tracked the development of innovative and intuitive applications. This is occurring not just in three-tier application stacks, but increasingly across true cloud native environments and across highly complex and distributed microservices architectures.

Rapid cloud adoption and the availability of low-code and no-code platforms has enabled IT teams to accelerate release velocity and build more dynamic applications across more platforms. IT organizations are adapting and innovating to serve the constantly changing needs of end users and to enable hybrid work for employees, along with a multitude of other necessary outcomes.

But this evolution comes with new and evolving security risks. Applications are becoming an increasingly vulnerable asset, as cybersecurity threats emerge at greater speeds and with new levels of sophistication. The sheer volume of application and their assets spread across multiple entities has made monitoring security throughout the DevOps pipeline extremely challenging.

IT teams are battling to stay ahead of an ever-expanding attack surface. However, current efforts to bolster application security are being hampered by information and activity silos. This means application and security teams lack the visibility and tools required to work together to address new risks.

The potential implications of this are profound. Organizations will find themselves exposed to catastrophic service disruption which will damage customer experience, destroy brand credibility and shrink revenues and market share.

This report sets out the current challenges facing IT departments. It explores how a lack of insight into security vulnerabilities and a lack of collaboration between IT operations and security teams are leaving some technologists feeling overwhelmed, and putting applications, end users and organizations themselves at serious risk.

The insights from this research highlight the need for a different process to application security, one which reflects new approaches to application development and enables technologists to secure the full stack of modern applications across the entire application lifecycle. This means providing the most comprehensive protection for applications, from development to production, across code, containers and Kubernetes.

Critically, the key learnings from the research reinforce the need for organizations to move beyond silos within the IT department, and to embrace a DevSecOps model which bridges the gaps between operations and security teams. Technologists need to better understand and appreciate the work of other disciplines across the application lifecycle, and to adopt a collaborative mindset, embracing new structures and skills.

For organizations to reap the rewards of rapid and agile application development and the shift to cloud services and cloud-native architectures, they urgently need to embrace an integrated approach to application security.

Research methodology
Cisco AppDynamics has undertaken comprehensive global research, from board-level directors and CIOs, through to senior and mid-level IT management.

This research entailed:

- Interviews with 1,150 IT professionals in organizations with a turnover of at least $500m (with the exception of Colombia, where organizations with a turnover of at least $100m were included in the sample)
- Interviews were conducted in 13 markets – Australia, Brazil, Canada, Colombia, France, Germany, India, Japan, Mexico, Singapore, United Arab Emirates, United Kingdom and United States
- Respondents worked across a range of industries, including financial services, retail, public sector, IT, manufacturing and automotive, and media and communications
- All research was conducted by Insight Avenue in July and August 2022

Note: Totals in charts / tables for single coded questions sometimes add up to more or less than 100% due to rounding.

Innovation and the application security compromise

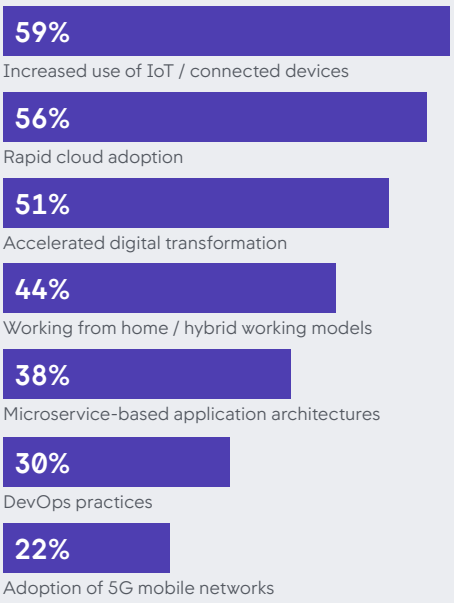
Businesses in all sectors and industries report feeling more exposed to security threats. Overall, 89% of technologists report that their organization has experienced an expansion in its attack surfaces over the last two years, and 46% state that this is already presenting increasing challenges.

Technologists point to a wide range of reasons why attack surfaces have grown, the largest being the increased use of Internet of Things (IoT) and connected devices within their organization. Rapid cloud adoption, accelerated digital transformation, and new hybrid working models have also served to expand attack surfaces.

Microservice-based application architectures and DevOps methodologies are also significantly increasing attack surfaces and exposing applications to new vulnerabilities.

The research reveals the extent to which accelerated digital transformation, which started at the outset of the pandemic and has continued to accelerate, has impacted application security.

Reasons why attacks surfaces have expanded



Why do you think attack surfaces are expanding in organizations like yours?

92%

of global technologists admit that the rush to rapidly innovate and respond to the changing needs of customers and users during the pandemic has come at the expense of robust application security during software development.

New application security challenges

The research uncovers a wide range of challenges in relation to application security that technologists will face over the next 12 months. These include a lack of visibility into attack surfaces and vulnerabilities, keeping pace with a constantly evolving threat landscape, and the need to prioritize speed of application development, rather than focus on operations and security.

Against this backdrop, technologists are concerned that their businesses are becoming less secure. As many as 78% feel that their organization is vulnerable to a multi-staged security attack that would affect the full application stack over the next 12 months.

Organizations need to act quickly to address this escalating application security challenge but, worryingly, 88% of technologists state that their organization could be doing more to secure the full stack of modern applications across the entire application lifecycle. They are struggling to find the right balance between development velocity, application performance and security.

And the implications of this are all too obvious. Technologists know that the lack of a robust application security setup could result in poor application performance and service disruption and, ultimately, reputational damage and loss of revenue.

81%

of technologists report that a lack of application security skills and resources is now an issue for their organization.

78%

say the lack of a shared vision between application development and security teams is presenting a challenge to application security over the next 12 months.

The top six application security challenges for technologists in 2023

- Lack of visibility into attack surfaces and vulnerabilities
- Difficulty prioritizing threats based on severity, impact and business context
- Discovery and protection of sensitive data
- Issues keeping up with a rapidly changing application security landscape
- Challenges balancing speed, application performance and security
- Volume of security threats and alerts

Lack of visibility and contextualization leads to 'security limbo'

In order to reduce application security risk, technologists need to understand where new threats are coming from across a sprawling topology of applications and their highly distributed assets.

As security threats evolve in sophistication and volume, technologists must consider whether they have access to the tools and insights they need to truly address these new security challenges. More than two thirds (68%) report that their current security solutions work well in silos but not together, meaning that they can't get a comprehensive view of their organization's security posture.

With widespread adoption of multi-cloud environments, application components increasingly run on a mix of platforms and on-premise databases which are leaving visibility gaps and increasing the risk of a security event.

The risk is that technologists will lose control of where data sits within their application portfolios, and this opens up a potentially huge data security risk, given the volumes of sensitive data which exist within many of these applications.

IT teams are being bombarded with security alerts from across the application stack but they simply can't cut through the data noise. It's almost impossible to understand the risk level of security issues in order to prioritize remediation based on business impact. As a result, technologists are feeling overwhelmed by new security vulnerabilities and threats.

Business transaction insights are vital to help IT teams to measure the importance of – and to prioritize – threats based on severity scoring. This score considers the context of the threat, determining whether it's a business-critical area of the environment or application.

58%

of technologists admit that their organization often ends up in 'security limbo' because they don't know what to focus on and prioritize.

93%

of technologists believe that it's important to be able to contextualize security so that they can correlate risk in relation to other key areas such as application performance, end user experience, and business metrics, and in doing so prioritize vulnerability fixes based on potential business impact.

The ITOps – Security divide

One of the biggest challenges for organizations when it comes to application security is the lack of collaboration and understanding between IT operations teams and security teams.

The research indicates that some developer teams avoid including security teams in their projects until the very last stages, believing that input from security colleagues will introduce friction into the development phase and slow down innovation. Indeed, the majority (55%) of technologists currently consider security to be more of an inhibitor of innovation than an enabler of innovation within their organizations.

While most technologists claim that regular check-ins take place between ITOps and security teams, more than a third report that these teams only collaborate when there is a potential issue, if at all. This lack of collaboration brings a wide range of negative consequences for IT teams and the wider organization. Most importantly it means that organizations are more likely to suffer from security blind spots or gaps in their security protection, and that IT teams struggle to balance different priorities between speed of application development, application performance and security.

Six implications of the lack of collaboration between ITOps and security teams

- Increased vulnerability to security threats and blind spots
- Difficulties balancing speed, performance and security priorities
- Slow reaction times when addressing security incidents
- Poor application performance impacting customers / employees
- Damage to brand reputation
- Negative impact on team morale and trust

The benefits of a DevSecOps approach

Organizations need to be able to remediate security issues but maintain an 'always on' way of business. They need to find the balance between application development speed and security, breaking down silos within the IT department and bridging the gap between IT operations and security.

This is why a DevSecOps approach, where application security and compliance testing are integrated throughout the software development lifecycle, is now an imperative. DevSecOps is achieved through both security automation, which integrates security gates throughout development without slowing down the process, as well as a strategic and cultural shift ensuring that teams integrate security into each phase of the development process. This mindset empowers everyone to take responsibility for security and pushes developers to identify and prioritize security issues at every step, resulting in more secure products and better security management, before, during and after release.

76%

of technologists believe that a DevSecOps approach is essential for organizations to effectively protect against a multi-staged security attack on the full application stack.

The Top 6 benefits of a DevSecOps approach

- Improved security and reduced risk
- Faster development time
- Improved collaboration
- Improved code quality through involvement of security teams
- Increased innovation
- Increased audit efficiency

Encouragingly, the research reveals the extent to which this transition is already happening in businesses across all sectors and industries. 43% of organizations have already started taking a DevSecOps approach within their IT department and a further 46% are currently considering making the shift.

Technologists see a wide range of benefits to adopting DevSecOps, from improved security and faster development times through to improved code quality and increased innovation.

Interestingly, there is a strong appetite amongst technologists to work more collaboratively with colleagues from other disciplines. They are tired of team silos and fragmented processes which add complexity and stress to their jobs. In fact, 58% of technologists report that tensions between application and security teams would make them consider moving jobs.

It is becoming more difficult than ever to access high quality developer and security skills which means organizations simply can't afford to lose their best talent due to cultural issues and outdated structures. They have to enable their technologists to perform at their best and deliver maximum business impact.

The shift to a DevSecOps approach requires both technological and cultural change. ITOps and security teams need to feel comfortable working together and to develop a better understanding and appreciation of the other's role and impact.

Interestingly, as well as adopting new mindsets, the research exposes a need for technologists from all disciplines to broaden their skillsets. This means ITOps teams becoming more aware of, and knowledgeable about security, and security professionals developing a deeper understanding of application development and factors that affect performance.

While recognizing the potential benefits of DevSecOps, the data shows a broad range of concerns that technologists have about moving to this approach. These include worries about the cost and time involved, and a lack of skills, knowledge and experience to effect the necessary change. Almost a third of technologists cite a lack of funding and internal support as barriers to transitioning to DevSecOps and almost a quarter fear that the shift could lead to a deceleration in the pace of software delivery.

79%

of technologists believe that successful modern technologists are those who can be both specialists in their particular field and generalists across other areas of the technology stack.

85%

state that cultural changes to support the shift to a DevSecOps approach are important to improve application security in their organization.

Priority areas to optimize application security

The research identifies a series of factors that organizations need to consider in order to evolve and improve their application security strategy.

92% of technologists believe that the adoption of a security approach for the full application stack is important to improve application security, and 89% point to increased automation to detect and block security issues at runtime.

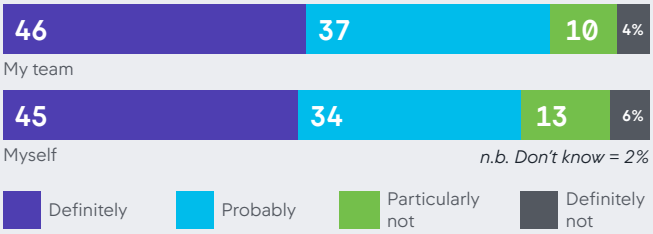
Other elements which are needed to optimize application security include continuous detection and prioritization, the adoption of an SRE (Site Reliability Engineer) model and the implementation of Artificial Intelligence (AI) in application security processes.

Indeed, given the volume of new security threats which organizations are facing, Artificial Intelligence (AI) and Machine Learning (ML) are now essential to identify gaps, predict vulnerabilities and automate processes to remediate any security holes. As bad actors ramp up their use of AI and ML, it's vital that enterprise security teams don't fall behind.

As with so many other areas of IT, technologists believe that having the right skills in place is vital for their organization to thrive in the new application security landscape.

Currently, less than half of technologists feel fully confident that they themselves and their teams have the necessary skills to manage the application security threats their organization currently faces. This skills gap is something that organizations need to address as a matter of priority.

Extent to which technologists and IT teams have necessary skills to manage application security threats



79%

of technologists state that the implementation of a security approach for the full application stack is now a priority for their organization.

76%

believe that AI will play an increasingly important role in addressing the challenges around speed, scale and skills that their organization faces in application security.

Conclusion – A security approach for the full application stack is critical to future-proof digital transformation

Cloud-driven digital transformation is empowering IT teams to build and deploy applications with great speed and agility, but organizations continue to apply outdated security strategies that are no longer fit for purpose in the modern application landscape.

Organizations face very real and increasingly severe security threats which have the potential to damage end user experience, erode brand credibility and reduce revenues.

This research paints a picture of growing complexity and IT departments being unable to manage the ever-increasing amount of sprawl. Current systems have served their purpose, but now need to evolve to meet the new needs of distributed applications. Technologists also need to do more to address application security risks and ensure they have the right tools, insights, and team structures to effect meaningful change. Without making this necessary shift, they will find it even harder to navigate the tension point between application speed and security. And as a result, they will be stuck in limbo, unsure of what to do next and where to focus resources to best help the business.

Faced with this challenge, organizations are urgently looking to adopt an integrated approach to application security that enables them to secure the full stack that comprises modern applications across their entire lifecycle. This includes complete protection for their applications, from development through to production and across code, containers, and Kubernetes.

Robust automation, using the power and capabilities of AI and ML, is key to a successful DevSecOps strategy, identifying threats and resolving them in real-time, without the need for human intervention.

Technologists need to be able to understand the code, and everything around it, with continuous detection and prioritization, so that they can detect and block exploits automatically, maximizing speed and uptime while minimizing risk. And they need combined application and security monitoring, to see how vulnerabilities and incidents may impact the business and then strategically prioritize their resources and responses.

However, organizations must recognize that this shift in approach extends beyond the implementation of new tools and technologies. It requires a holistic strategy, which combines automation, continuous detection, and prioritization, with upskilling and cultural change.

IT teams must embrace the shift to a DevSecOps approach, working together to ensure security is top of mind from the outset of the build process and throughout the application lifecycle. And technologists need to push themselves to better understand and appreciate the work of other disciplines, learning new skills and striving to become the rounded IT professionals that will thrive in the future.

Encouragingly, the research indicates that the move to DevSecOps is gaining strong momentum, with increasing numbers of organizations starting their journeys.

Application security can no longer be treated in isolation and approached in departmental silos if digital transformation goals are to be realized; it can no longer be viewed as a barrier to innovation. Instead, application security needs to be recognized as a core element of the application lifecycle and the foundation for organizations to deliver agile development and accelerated innovation.

About Cisco AppDynamics

Cisco AppDynamics is a leading provider of Observability and Application Performance Monitoring technology. AppDynamics helps customers observe what matters inside and beyond their IT environments. Combined with the power of Cisco, AppDynamics enables organizations to deliver exceptional user experiences by centralizing and correlating data into contextualized insights of critical business metrics – providing them with the power to prioritize actions based on business needs.

To find out more and learn how Cisco AppDynamics is helping organizations shift to a security approach for the full application stack, click here.

cisco AppDynamics

MKT 832 2022