451 Research

S&P Global
Market Intelligence **Business Impact Brief**

The New Security Imperative for CIOs: Bringing IT Operations and Security Together With DevSecOps

The 451 Take

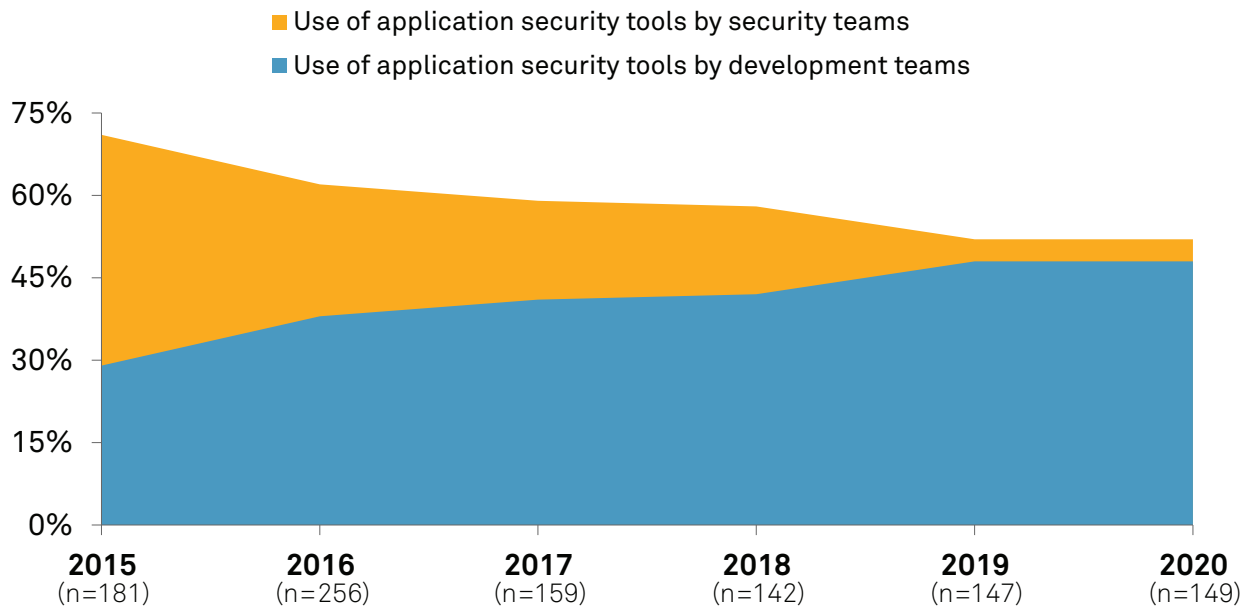
CIOs will change the shape of IT organizations in new ways to continue driving the digital maturity of their businesses.

Demand is rising for digital tools and processes to better serve customers, generate revenue and deliver products. Yet recent cyberattacks should bring into focus that business technology must be safe as well as reliable. It must be protected from threats to sensitive digital assets, customers and partners. In fact, the impact of the SolarWinds threat campaign and the ransomware attacks against Colonial Pipeline, JBS and others also affected multiple industries downstream, making clear the threat to entire supply chains.

This has resulted in a change in perception of who is responsible for securing business technology. In the past, monitoring and mitigating security threats throughout an organization may have been seen as the province of an organization's security team. Going forward, the integration of security will become a mandate not only for security specialists, but for all those responsible for the development, architecture and deployment of technology. The multiple domains this mandate touches points to one center of leadership: the CIO.

Evidence of this trend is already apparent. Only a few years ago, tools to assure the security of business applications were predominantly used by security teams. Today, as DevOps trends integrate application development with multiple aspects of technology operations, IT decision-makers are increasingly allocating application security tools to development teams, with security tools becoming used as much by developers as by security specialists.

IT Decision-Makers Are Increasingly Allocating Application Security Tools to Developers



Q. How is the usage of application security tools allocated across the following two teams in your organization?

Base: Respondents currently using application security

Source: 451 Research's Voice of the Enterprise: Information Security, Vendor Evaluations 2020 Quarterly Advisory Report

Opportunities abound for security to become more directly integrated into DevOps efforts, with CIOs leading the charge. Below are some critical steps to realizing this imperative.

Business Impact

Evaluate how security will become more dependent on IT development and operations telemetry. The monitoring data that organizations depend on to assure the performance and availability of modern technology – encompassed in the concept of 'IT observability' – increasingly represents a source of data directly relevant to securing the organization. Security and DevOps teams alike must recognize the value of this data to their shared mandates in order to safeguard the business and deliver reliable IT integrity.

Secure IT to help mitigate the potential effects of a data breach. In the past, the impact of a cybersecurity incident may have been challenging to measure. Today, evidence is abundant. Data breach penalties may reach millions of dollars – but even those may pale when entire logistics chains fail, as in attacks in just the past year. From lost revenue and impact on corporate value measured in stock price, to a damaged brand and loss of competitive footing that may be difficult to recover, businesses are now more acutely aware of the risks.

Set the tone at the top. When business teams are incentivized to generate revenue and implement features and functions in essential technology, profitability is the objective. In the past, adding requirements to build security into this functionality may have been seen too often as a detraction from these values, adding cost and time to value. Today, security is no longer optional – businesses must recognize that security is an investment to assure the viability of the business itself. Security buys the freedom for the business to pursue its primary aims. It's the responsibility of senior management to recognize this reality and communicate it effectively throughout the business. It's more than a good idea: executive sponsorship is essential to assure backing for the necessary investment.

Integrate expertise across teams. Implementing security in modern business technology requires security expertise to understand exposures, while builders and IT ops teams must know how to remediate exposures without impact on critical functionality. This requires cooperation across these domains of expertise. To achieve secure development at the speed of modern IT, cooperating teams must be literate in the tools and tactics essential to maintaining the pace required. Security teams should become familiar enough with the tools and processes of development, build and deployment to know how to make the most of the opportunity. DevOps teams, meanwhile, must understand how to enable their techniques and practices to be exposed to, and integrated with, efficient security measures.

Demonstrate that continuous improvement requires continuous, comprehensive observability. Once a culture of cooperation and literacy across development, operations and security teams can be established, organizations must arm cross-functional teams with the tools required to maintain security at a high level. This points to the developing role of IT observability in securing modern IT. Security and DevOps teams can better identify where weaknesses occur when they adopt tools that monitor the environment for adherence to security priorities and identify evidence of efforts to compromise resources, as well as how they can be remediated in operations, and prevented in future development. The ability to triage and identify security issues is part of observability, and the ability to act upon and isolate problem infrastructure should be integrated into modern business technology systems.

Looking Ahead

As businesses depend increasingly on technology, technology becomes more central to the business. In today's world, that means a deeper integration of security with IT operations and IT observability. How do we expect technology leaders to execute on these demands, not only in technology but in culture, practices and expertise?

- Encourage even greater cross-functional literacy across teams. Security teams must become better versed in DevOps practices and tools, while DevOps pros must increasingly embrace the integration of security practices and technology. Together, these teams must develop greater fluency in cooperating in ways that enhance security while reducing friction in development.

- IT observability in particular can be a key enabler, as it becomes more deeply integrated into security operations to monitor and defend modern IT environments. Building integrations between existing tools vs. adding more point products can help teams collaborate and work more efficiently, furthering efforts to truly realize the concept of DevSecOps.