451 Research® Now a Part of S&P Global Market Intelligence | Business Impact Brief

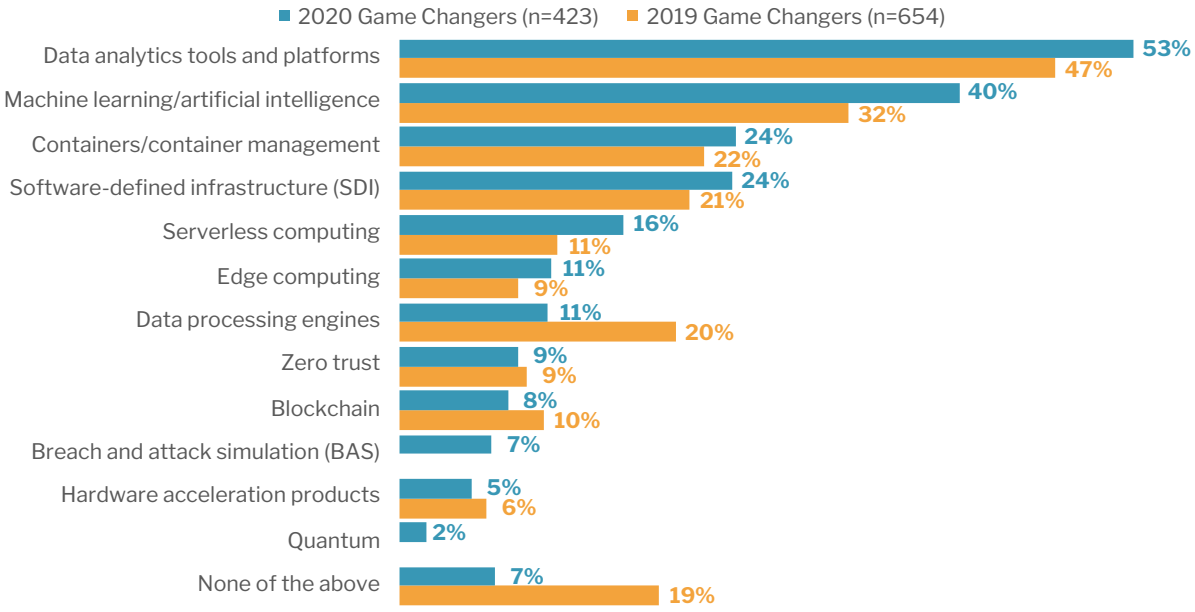
What You Should Already Know about BAS

The 451 Take

Sorting out the effectiveness of any security control is hard. So much depends on context that's difficult to pin down and is ever-changing. Determining the a priori effectiveness of a collection of controls can be an order of magnitude harder. Breach and attack simulation (BAS) platforms have reached a state of maturity where they should be part of the mitigation calculus for organizations that want to gain a deeper understanding of their security posture. A recent 451 Research study has shown that some organizations are already putting this greater operational awareness to work, and many more should be gaining a better understanding of how they can make their existing security tools more effective.

Emerging Technology Game Changers 2020 and 2019

Source: 451 Research's Voice of the Enterprise: Digital Pulse, Budgets and Outlook Q2 2020



The collection of security tools that most organizations have accumulated spans a range of capabilities and were put in place to address defined needs in protection or compliance. The challenge that security teams face is that they haven't had a way to regularly assess the difference between the as-designed ways they've configured this broad set of controls and their delivered effects. Tools have proliferated, but ways to understand efficacy have not. There are audits and penetration exercises that yield lists of findings to be fixed, but these are typically high-resource events that can't be run regularly. As new technologies are put to use in their organizations, new tools often come along with them. Adding more tools only increases operational complexity and creates toil for security teams.

To improve the efficiency of their operations, security teams need to look at protection in the same way attackers do, from all potential angles of attack. It's not possible to understand external performance from inside any single tool. Security teams need an objective source of truth to measure progress. This is the perspective that breach and attack simulation platforms can offer. By reducing the cost of delivered security assessments, security teams can become more efficient by understanding the effects of their actions on a more constant basis. Being able to correlate controls around a threat-based set of metrics, like the MITRE ATT&CK framework, can quantify their effects in meaningful terms.

The 451 Take (continued)

BAS was included for the first time in the emerging technologies section of the 451 Research Voice of the Enterprise: Digital Pulse, Budgets and Outlook Q2 2020 study and is already showing significant deployment (see figure above). CISOs who have been looking to better align their security tools are coming to understand that BAS offers a way to look at spending effectiveness. The control capabilities that different tools offer can be contrasted with their delivered protections. BAS systems can catch configuration errors early in their deployment and get security operations teams to a more agile footing. By reducing the risk that an inadvertent change will go undetected, BAS evaluations can let them iterate configuration changes more frequently and adapt to new business needs faster.

Business Impact

SECURITY CONTROL ALIGNMENT. Most organizations have enough security tools, often too many, but they can't be sure that the coverage they have is complete enough.

SECURITY OPTIMIZATION. Understanding where the most effective controls are can simplify operations and reduce management toil.

STRENGTHENED SECURITY POSTURE. Regular or continuous gap identification can ensure that any drift or errors in configuration are identified and fixed faster.

INCREASED OPERATIONAL EFFICIENCY. By understanding how tools are responding, teams can tune events, alerts and responses to maximize their effectiveness.

Looking Ahead

While infosec teams have had less pressure to manage costs than other areas of IT, there is increasing pressure to justify spending for many organizations, and all need to get better at understanding where they can spend most effectively and do so in ways that are informed by the threats they face. That means they need to invest in ways to gain insight into the real effects of their actions. DevOps teams rely on metrics to understand the most effective ways to interact with customers and how their applications perform.

Most security teams don't have efficacy metrics that they can put to work today. There needs to be a change in mindset to expect to have an objective measure of control effectiveness that's continuously available and integrate it into security operations. It's the same kind of thinking that has driven continuous compliance initiatives, and now there are mature means to implement them. BAS systems are tools that can provide those measures. The challenge for security teams is to leverage the perspectives that BAS tools provide to improve their situational awareness and optimize their overall security posture, improving both effectiveness and efficiency.