451 Research

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

Building in Infrastructure Trust

The 451 Take

The headlines are increasingly filled with news of damaging security breaches that are products of infrastructure protection failures. It can seem daunting to overcome the complexities in typical enterprise environments, but there are paths to more effective and efficient security capabilities that infrastructure and platform buyers should be considering today. By improving platform security and establishing a foundation of trust, organizations large and small can simplify security operations.

Of all the aspects of information security, operational security can seem like the least glamorous, but it is the focus of considerable budgetary spending and constitutes the majority of the work that consumes security teams. That makes operational security a highly valuable area for improvement. Yet many organizations continue to struggle to secure the foundations of their infrastructure. In 451 Research's latest Voice of the Enterprise (VotE) study on Information Security, respondents cited vulnerability management and remediation second highest in a list of top projects, continuing a long-term trend. That's a testament to how difficult it has been to master. The increasing velocity with which attackers are exploiting vulnerabilities requires that organizations build stronger operational skills and more effective processes to manage this threat.

Security Pain Points and Projects

Source: 451 Research's Voice of the Enterprise: Information Security, Workloads & Key Projects 2020

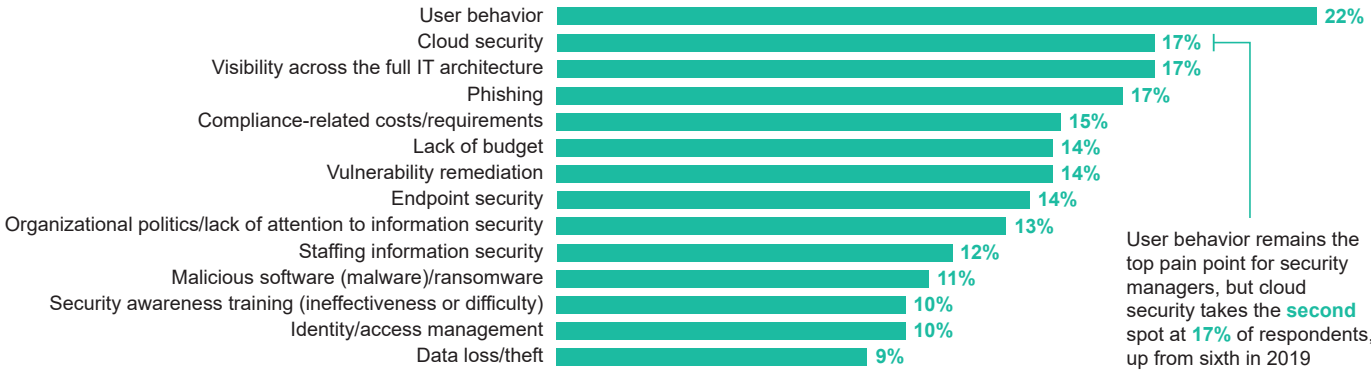
Q: What are your organization's top three information security pain points? Please select up to three.

Base: All respondents (n=442)

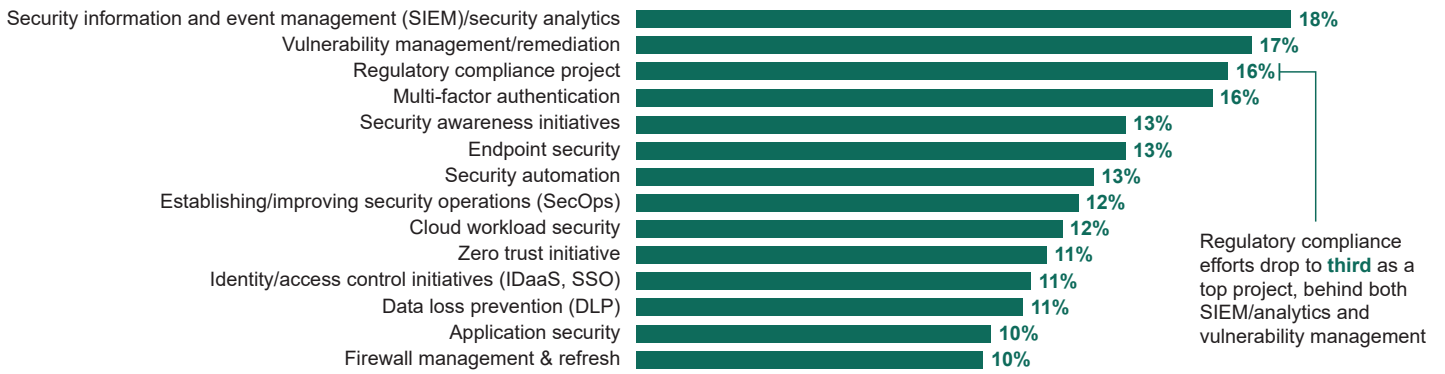
Q: What will be your top three information security projects over the next 12 months? Please select up to three.

Base: All respondents (n=461)

Top Three Information Security Pain Points



Top Three Information Security Projects



The 451 Take (continued)

One of the most effective ways to reduce security toil is to embed important security capabilities into the infrastructure platforms on which the organization depends. It's a tactic that hyperscale operators have already put to work by leveraging security abstractions that allow individual elements to automatically manage updating and version management independently. Decoupling these tasks can reduce the need for maintenance downtime. These are areas where security automation can be most effective and are a product of effective supply chain security.

However, there has to be a high level of supply chain trust to put these kinds of improvements to work. One of the biggest factors that holds organizations back from full automation is concern about risks associated with updates and patching. Those concerns are based on a long history of independently managed processes coming into conflict. To fix these problems, supply chain security needs to be integrated at a much more granular level, coordinating across dependencies between hardware, firmware and software versions. And it needs to be anchored with a hardware root of trust. Strengthening the supply chain to manage any potential issues can put automation to work with high confidence and low risk.

Improving supply chain trust isn't simply a matter of implementing a better process of vetting suppliers; it's not applying one more scanning engine to look for indicators after successful attacks. It's being proactive and adopting a zero trust mindset to stay ahead of attacks by putting better technology to work to ensure that fundamentals, like a hardware root of trust, are actually used as an effective anchor for the full software stack. It's ensuring the security of the software supply chain that is feeding the infrastructure and building the tooling that is necessary to make it manageable at scale. Effective infrastructure security can't be about compromises that hamper performance or hold an organization back; it has to move security teams faster and accelerate operations.

Business Impact

A SECURE INFRASTRUCTURE FOUNDATION SIMPLIFIES FOUNDATIONAL SECURITY OPERATIONS. Operational security tasks, like vulnerability protection, management and patching, can be baked into platforms to reduce complexity.

BETTER-MANAGED THREAT LANDSCAPE. Improved supply chain security can reduce threat potential and free security resources for critical and emerging threats.

INFRASTRUCTURE THAT IS AGILE AND SECURE. Security protections can be delivered without performance penalties that could limit scaling and impact productivity when they're built into infrastructure up front. Building infrastructure by leveraging platform capabilities that already integrate better security controls can allow provisioning to happen faster to respond to business needs. Native security automation can be a force multiplier for security teams.

Looking Ahead

Organizations need to build infrastructure that will support them today and well into the future – and that will do so with levels of security that keep up with the rapidly advancing threat landscape. That means organizations will need to be able to scale to support the density and speed of containers and other innovations while wrapping protections into their operational practices. Integrating supply chain improvements for both software and hardware will build a solid base, and putting automation to work will reduce complexity. All of these efforts should be working to protect the organization's data by establishing protections that can move with data as it is created and used. Layering this set of security capabilities across their infrastructure will give organizations protections that can travel with them into whatever the future holds.