Why Is Zero Trust Broken?

The 451 Take

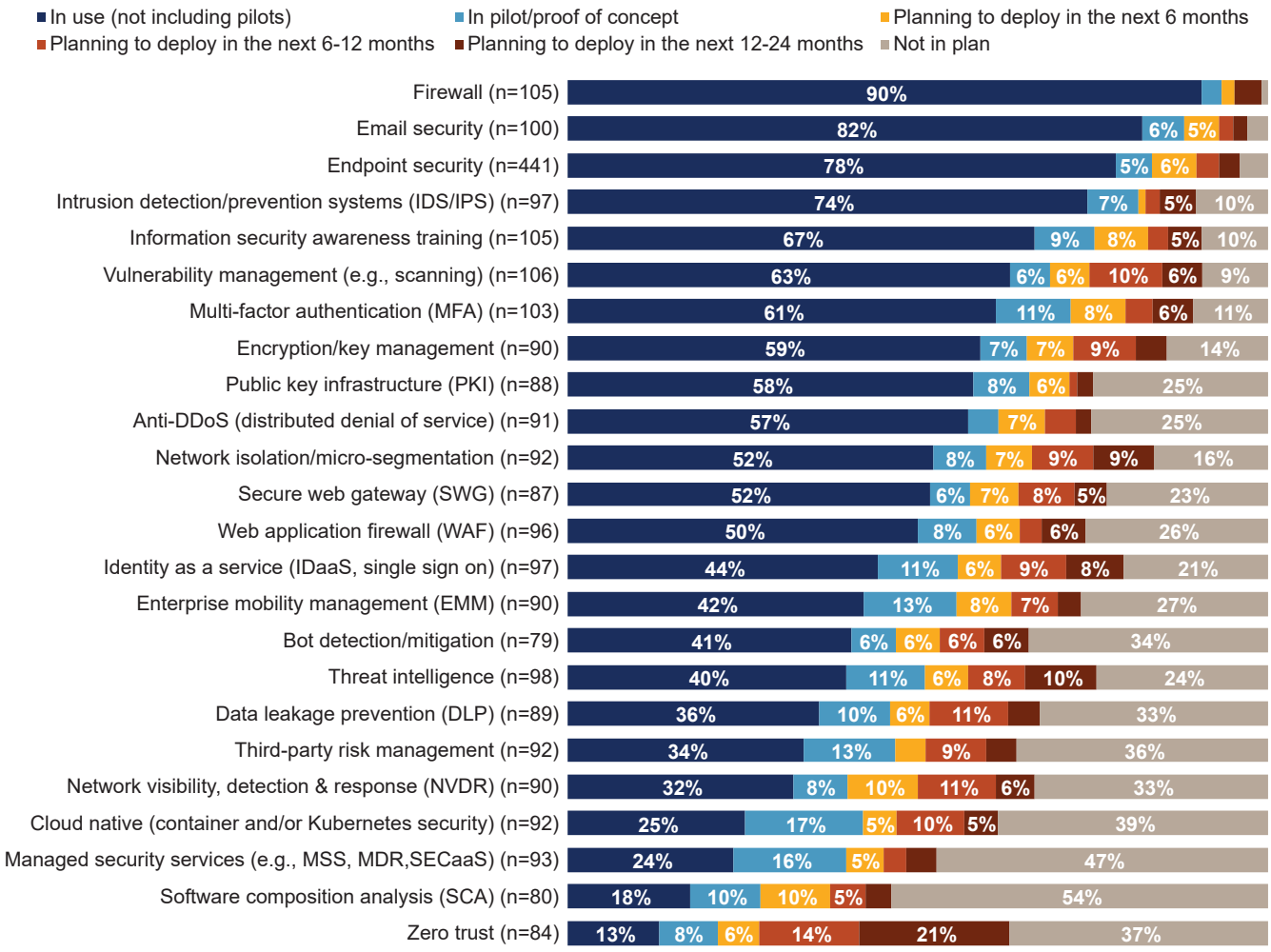
Improving the security posture of the modern enterprise has never been a more urgent goal, and ideas like zero trust are being invoked with greater frequency as a means to achieve this. But can something that is as broadly defined as zero trust really be a guiding star? The lack of a clear definition could lead to approaches that would ultimately be badly broken. While there is keen interest in zero trust, it has to be better understood by enterprises to be useful.

As a concept, zero trust garners a lot of enterprise attention. In a recent 451 Research Voice of the Enterprise: Information Security study, it was reported to be the least implemented of a set of technologies, yet it garners interest at the level of more established initiatives like DLP. In that same study, zero trust is also consistently rated as one of the top five overhyped security buzzwords. Does that mean it's an enigma or an ideal? The reality is somewhere in between. Zero trust can be valuable to enterprises when they can translate the concept into a security strategy that drives their decision-making.

Implementation Status for Information Security Technologies

Q. What is your organization's status of implementation for the following information security technologies? Base: All respondents

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



Enterprises have to take ideas like least privilege and understand how to implement them in their environments. One of the reasons for low levels of adoption of zero trust is that its elements can be risky to retrofit into existing systems. Many enterprises lack the visibility and context to understand the impacts of security policy changes that a zero trust approach would bring, and this can paralyze a rollout with reassessments of what needs to be done and what could be broken.

To move beyond this paralysis, organizations have to deploy platforms with a zero trust mindset built in. Zero trust is not about locking everything down. It's quite the opposite – it's the ability to open up while managing risk by understanding what exposures are being created and controlling their impacts. It's the process of ensuring that necessary work can get done in a secure context. This requires infrastructure that has trust built into its foundation, and visibility and controls infused throughout its structure. By building in these necessary elements, enterprises can create infrastructure that can be secured with operational efficiency, making the right resources available for the right purposes at the right time.

An infrastructure platform that can support zero trust must not only have a solid foundation; it has to automate the security operations tasks that keep it secure. It must have identity integration to ensure that the people and applications running on it are trusted. It must provide proactive security controls that have the context to apply granular policies with the precision needed to operate in today's dynamic environments. Those controls must be as adept at protecting access or APIs as they are at securing data.

By understanding what zero trust means for them, enterprises can move beyond the confusion that surrounds the term and transform it from a buzzy idea into a practical approach to operational security. The combination of visibility, identity and trust is powerful and increases security control effectiveness by reducing the risk of unintended exposures. When that combination is coupled with automation to handle greater scale, it can build security capabilities that enterprises need for efficient security operations.

Business Impact

Improving security effectiveness. Putting zero trust principles to work can increase security effectiveness by focusing controls in areas where they can deliver the best effect.

Increasing situational awareness. Zero trust-based controls can increase visibility with more granular telemetry. Being able to build greater context around events by tying in identity allows better insight into event impacts.

Increased productivity. Building infrastructure that can ensure that the right access is granted at the right time can improve security processes and employee productivity.

Looking Ahead

One of the great benefits of establishing a zero trust security footing is that it puts in place the tools and telemetry to support future models of work, in whichever direction they may go. The combination of detailed context around infrastructure and its integration of identity means that new use cases already have the security tools required to enable them. That in turn enables the level of agility that businesses need in order to maintain their competitive edge in the continuous change that characterizes the marketplace today.