HOW TO REPORT

How To Use Zero Trust To Defend Against Cyberattacks Through An Economic Downturn

Protect Against Cyberattacks With Zero Trust Despite Layoffs And Budget Pressure

December 21, 2022

By Allie Mellen, Carlos Rivera, Jeff Pollard, Heidi Shey, Jess Burn, Brian Wrozek, Paddy Harrington, Heath Mullins, Erik Nost with Joseph Blankenship, David Holmes, Andras Cser, Alexis Tatro, Peggy Dostie

FORRESTER®

Summary

Regardless of an economic downturn, security remains a core competency for a business. This report outlines how security leaders can refocus efforts on Zero Trust in the event of an economic downturn to improve security posture, control costs, and increase influence.

An Economic Downturn Will Pressure Security Programs

Security is not immune to the fallout of an economic downturn. As critical as the security function is, and as much of a buffer compliance can provide against cost cutting, security and risk pros will still feel pain. In an economic downturn:

- **Lower growth in security budgets will feel like budget reductions.** Although security teams enjoyed years of budget increases, from an average of 23% of IT budgets earmarked for security in 2018, to an average of 36% in 2022, Forrester's Security Survey, 2022indicated that security programs struggle with these two challenges: the changing and evolving nature of IT threats and the complexity of the IT environment. As turbulent times arrive, lower-than-expected budget allocations will strain teams that are already stretched thin. At the same time, threat actors continue to target your organization, the IT environment grows more complex, and daily operational tasks consume cycles. Expect more budget pushback than in recent years, plan for necessary tradeoffs, and target for your team to accomplish what your roadmap promised two to three years ago.
- **Cost cutting decisions will be made outside of security.** Outsiders, uninvolved with the day-to-day security, will follow the standard playbook for cutting costs. The path of least resistance includes the always attractive targets: headcount, large line items, and smaller best-of-breed security products — layoffs have already begun at many former cyber unicorns. Additionally, according to Forrester's Priorities Survey, 2022, lowering IT costs is among the top actions for business and technology professionals whose organization is prioritizing reducing costs. Do nothing — or fail to justify your decisions — and expect to lose headcount, encounter forced migrations to bundled offerings, and find outsourcing and labor arbitrage as viable ways to cut costs. The sliver of difference between a rout and a tactical retreat is that in a tactical retreat the leader made the decision, and in a rout the external party decided on your behalf. Plan and come in with business cases, acceptable tradeoffs, and what makes the security team effective to stand a better chance of preserving what matters.
- **Stakeholders that security depends on will lose money and people.** Security matters, and external factors will help protect security spending. That luxury does not extend to all the departments that security leaders work with. Administration, governance, and operational tasks dispersed to functional teams over the past decade as regulation, customer requirements, and cyber insurers demanded more from security teams. IT took over architecture, administration, and configuration of

security tools to alleviate some of the burden. If these teams experience reductions in force, leaders that once willingly accepted operational and administrative tasks may send them back to security outright, or internal support may degrade so much that security needs to reclaim ownership. Losing IT operations personnel with institutional knowledge of key IT and security tools leaves your organization vulnerable if essential tools fail to get appropriate maintenance.

Leverage Zero Trust To Gain Unexpected Wins In Challenging Times

Zero Trust initiatives provide business value by improving security, breaking down departmental silos, and improving the employee experience, all without expensive new tools. Zero Trust is often a simmering strategic priority in the background, but bringing it to the fore during uncertain economic conditions will:

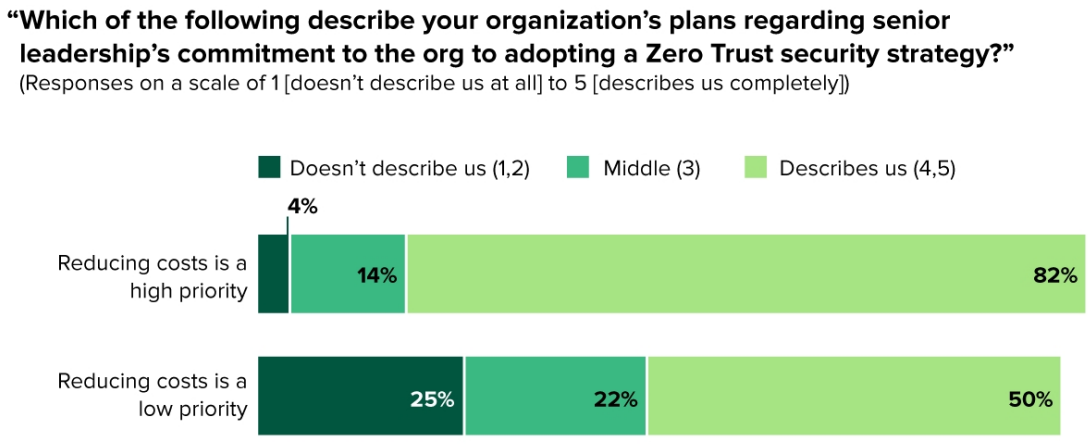
- **Enhance security and audit experiences without requiring new tools.** Maintaining accurate documentation is often cast aside for more pressing issues like handling active incidents or new technology implementations. However, there's a lot to cover for a strong Zero Trust implementation within governance, classification, policies, configurations, and hardening of devices. Well-documented and well-written policy is a security and compliance enabler for an organization. It sets expectations and acts as a roadmap for auditors and employees. Advance your capabilities here, and you will create less work to demonstrate compliance, give clearer guidance for internal stakeholders, and experience less painful audits. Include the specifics for how to adhere to the policies in clearly documented standards and procedures that map to Zero Trust controls and approaches.
- **Facilitate cost cutting across the business.** You can use Zero Trust initiatives to strategically reduce business complexity and cut costs. For example, according to the Forrester report Using Zero Trust To Kill The Employee Password, several large US-based organizations in different verticals allocate over $1 million annually for password-related support costs alone. Implementing automated IAM can dramatically reduce the friction associated with passwords, as well as the costs, and is one example of Zero Trust principles leading to business benefits. In addition, according to Forrester's Security Survey, 2022, 82% of organizations that are prioritizing reducing costs in the next 12 months have senior leadership committed to adopting a Zero Trust security strategy. In contrast, only 50% of those that do not prioritize reducing costs are committed to adopting Zero Trust (see Figure 1). Zero Trust objectives can help cut out other business costs by

reducing tooling, redundancies, and required training.

- **Build influence within the rest of the C-suite.** Layoffs in other parts of the organization that security depends on can hinder the security team. However, it's also an opportunity for security leaders to support other, more strapped business units, which is a key priority for agile business leaders. Per Forrester's Security Survey, 2022, 16% of security decision-makers say the CISO reports into IT operations and 17% say they report into the CIO. Come prepared with a plan of how your team can support leadership through market changes while still showing security value. For example, implementation of Zero Trust often falls to IT, but with a strapped IT team, it will be necessary for security to step in. Gaining favor with the CIO and other C-level executives in a time of need can help security pros increase influence in the organization and show commitment to business success.

Figure 1

Organizations That Prioritize Reducing Costs Also Prioritize Zero Trust



Note: "Don't know" is not shown.

Base: 2,790 global security decision-makers whose organization is prioritizing reducing costs, and 161 who are not prioritizing reducing costs in the next 12 months

Source: Forrester's Security Survey, 2022

Source: Forrester's Security Survey, 2022

Push Security Transformation Forward While Cutting Business Costs

Despite economic headwinds that would otherwise threaten security improvements, Zero Trust can help security pros better align to business needs through economic shifts while ensuring the security of the organization. To push security transformation forward while cutting business costs:

- **Bolster underserved initiatives such as maturing processes.** As security budget growth stagnates, security leaders have an opportunity to redirect resources from new tool implementation to process efforts like codifying policy. Catalog your policies, third-party requirements, business continuity management, data flow diagrams, and support runbooks alongside mandatory compliance efforts and device hardening. A successful Zero Trust initiative thrives on a foundation of governance and process, and this upfront effort of improving your maturity lays the groundwork for simplification of IT complexity, reduction in security alerts, and cost cutting.
- **Facilitate cost cutting.** Zero Trust gives security pros an opportunity to strategically evaluate and reduce cost for parts of the business. For example, by adopting a Zero Trust approach for secure network access, the IT team can allow BYOD, reduce spend on corporate-issued devices, and extend corporate device refresh cycles. Instead of buying a new tool, use a combination of policy enforcement and built-in capabilities to improve defenses, such as using built-in OS security. Killing the VPN, moving to passwordless, managing (and optimizing) assets, and other common Zero Trust objectives not only improve the security of the organization, but also help cut costs.
- **Further progress by letting your security pros get their hands dirty.** IT teams are often responsible for the implementation and maintenance of Zero Trust policies and technologies. If the IT team loses staff to layoffs or hiring freezes, it may limit progress on Zero Trust initiatives. However, security has the talent to handle Zero Trust implementation with or without IT. Much of the security talent that now operates in architect, analyst, or governance roles started their careers in IT — so use that talent. Make the best of the loss of IT counterparts as a knowledge transfer and mentorship opportunity between seasoned security pros and early career members of the security team. Provide incentives for the sharing of institutional knowledge and the development of skills related to IT operations responsibilities.

FORRESTER®

We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

Learn more.

Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

Learn more.

Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

Learn more.

FOLLOW FORRESTER

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com