Enterprise Strategy Group
by TechTarget

# Expanding Zero Trust WITH MDR


Many organizations are turning to zero trust to better secure their rapidly evolving digital enterprises. While the first step in this direction is often the implementation of zero trust network access (ZTNA), this alone is not sufficient to fully and efficiently protect an enterprise's digital assets. By augmenting ZTNA with MDR, security teams can reduce time to value, more easily scale a zero trust implementation, and close the loop between prevention and response.

## ZTNA Can Address Key Needs, but Many Organizations Need Help

Modernizing secure remote access is a clear area of need for many organizations and, thus, a top driver of zero trust initiatives. However, many organizations lack the resources to effectively implement and operate the strategy.

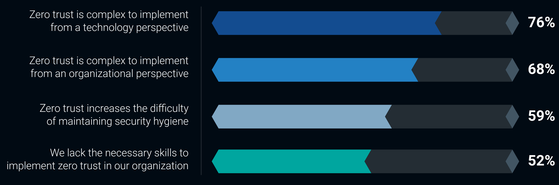
**» The shift to remote work and prevalence of third-party access has accelerated the shift to ZTNA**

**63%**
of employees work remotely or in a hybrid model

**34%**
of all users accessing corporate resources are third parties

**71%**
of organizations have begun to turn to ZTNA

**» Negative perceptions of zero trust (percent that agree/stongly agree)**




## Services and Incident Response Should Be Core Components of Any Zero Trust Strategy

Zero trust is not only about preventing incidents; it's also about efficiently responding when incidents do occur to limit the blast radius. Further, the challenges in effectively implementing a zero trust initiative, especially among more resource-constrained organizations, require services to scale the strategy.

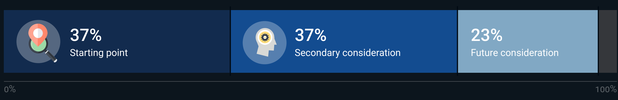
**» Which of the following actions do you believe your organization will take over the next 12-18 months to implement or optimize its zero trust strategies?**

**40%**
Enhance analytics and detection and response capabilities

**38%**
Work with professional services firms to build or refine the zero trust strategy

**38%**
Work with professional services firms to implement zero trust tools

**» How organizations view incident investigation and response in the context of zero trust**




## ZTNA + MDR Leads to Zero Trust Benefits

Modernizing remote access through zero trust and incident response through MDR to augment in-house skills can help organizations achieve tangible security benefits through zero trust.

**» How MDR helps support zero trust**

Using MDR provides many security benefits, including seamless quarantining of digital assets and immediate altering of access rights as conditions warrant. XDR also enables security automation and more efficient security workflows, creating a more efficient approach to cybersecurity.

Moving to a managed services-led zero trust model can make deployments faster and more efficient, while delivering granular policies that are properly adapted to each organization's unique needs.

A managed services-led model through MDR also makes it easier to scale resources than it would be if an organization attempted to hire and train new in-house talent with zero trust expertise.

**» Benefits seen from zero trust adoption**

**77%**
Report seeing both security and business benefits from zero trust.

**Specifically:**

**43%**
report fewer cyber incidents.

**37%**
report better organizational agility.

**36%**
report increased productivity.

**34%**
report increased user satisfaction.

## Conclusion

Moving to a zero trust mindset is essential, and adopting ZTNA is an important first step. In order to reduce complexity, simplify operations, improve cyber resiliency, and overcome the growing skills gap, organizations should take the next step to broaden their zero trust capabilities in an efficient, unified fashion. Specifically, organizations should embrace MDR solutions as managed services in order to broaden and deepen their use of the zero trust security model.

LEARN MORE

BlackBerry Cybersecurity

Source: Enterprise Strategy Group Complete Survey Results, *2021 SASE Trends: Plans Coalesce but Convergence Will Be Phased*, December 2021.
Source: Enterprise Strategy Group Survey Results, *The State of Zero Trust Security Strategies*, May 2021.