ZERO-TRUST INITIATIVES FOR SMBS IN 2022: 5 TRENDS TO KEEP IN MIND

Most small and midsize businesses (SMBs) today operate in a computing environment where “outside” and “inside” the network perimeter no longer has much meaning. Traditional approaches to cybersecurity are giving way to the principles of **Zero-Trust**, in which access to resources is always *conditional* on demonstrating—and sustaining—a pre-determined level of assurance (aka *trust*) in a handful of key areas.

□ Aberdeen’s benchmark research found that **Zero-Trust is among the Top-5 funded cybersecurity initiatives in 2022**, for >90% of all SMB respondents (defined as organizations having between 20–500 employees).

□ **Technology areas with the highest degree of current deployments** among SMBs include:

- **Endpoints / devices:** Traditional *anti-virus / anti-malware* is quickly giving way to more sophisticated *endpoint detection and response (EDR)*.
- **Users / identities:** Increasingly ineffective *usernames / passwords* are widely being strengthened with *multi-factor authentication* and *cloud access security brokers (CASB)*.
- **Connections:** Trusted connections over disparate networks are being enabled by implementations of *transport encryption*, *session management*, and *network virtualization*.
- **Applications / workloads and data:** These fundamental sources of business value are being not only better integrated (e.g., using *APIs*), but also better protected (e.g., using *data encryption*; *data backup and recovery*).
- **Operations:** Traditional, prevention-oriented approaches to cybersecurity are being complemented with better visibility into what’s happening (e.g., *SIEM*; *third-party threat intelligence*), and better capabilities to respond (e.g., managed detection and response).

□ **External factors are significant drivers for current SMB investments in Zero-Trust initiatives.** These include an increasingly *complex computing infrastructure* (67% of all SMB respondents); an increasingly *sophisticated threats landscape* (60%); and an accelerating *volume and frequency of security hygiene requirements* (54%).

□ **Internal drivers for current SMB investments in Zero-Trust initiatives are also important.** These include *lack of visibility* across an evolving computing infrastructure (42% of all SMB respondents), and *enablement of strategic business objectives* such as Work From Home or digital transformation (38%).

□ **Realistically, Zero-Trust initiatives are implemented in phases**, over an extended period of time—but SMBs should keep these trends in mind as a way of thinking about cybersecurity going forward.

ABERDEEN
STRATEGY & RESEARCH
ILLUMINATE. INSPIRE. IGNITE.