COMCAST BUSINESS | MASERGY

Zero Trust

Critical Capabilities Checklist

When it comes to operationalizing Zero Trust, it helps to take the right approach from the beginning. This checklist from analysts at Nemertes can help you identify what you have in place already and what to consider when evaluating solutions.

Critical Capabilities

Identity access management

You need robust IAM with multi-factor authentication, either fully consolidated (one source of identity for all users in all contexts) or deeply integrated at a process level.

> ***EXPERT TIP:*** *IAM is foundational to ZT—making it actually work.*

Segmentation

Beyond access to specific services, IT needs the ability to segment network traffic with a high degree of granularity from the data center core and the LAN to the WAN to the virtual networks in cloud environments.

> ***EXPERT TIP:*** *How do you segment your network to avoid IT complexity?*
> Get the Guide

XDR/BTA

Extended detection and response or behavioral threat analytics solutions are essential, because they close the feedback loop—allowing adjustments to the ZT trust map based on actual network behavior after initial admission is granted.

> ***EXPERT TIP:*** *Solutions are sometimes known as UEBAs (for user and entity behavioral analysis).*

Granular Trust Maps

IT professionals need a mechanism by which to provide and maintain the specific application access rights of authorized entities (e.g. users) reaching for other authorized entities (e.g. applications running in IaaS).

> ***EXPERT TIP:*** *Network architecture diagrams and user groups help visualize connectivity and access rights between all assets in and out of the network.*

ZTNA

Zero-trust network access applies the principles of ZT to the task of connecting entities in the network to each other.

> ***EXPERT TIP:*** *Organizations with successful ZT implementations start by crafting a Zero-Trust-centric architecture first, then adapting existing network and security architectures to align.*

SDP

As one way to achieve ZTNA, a software-defined perimeter solution uses a combination of endpoint clients and access gateways to enforce a fine-grain access policy at the network level.

> ***EXPERT TIP:*** *SDP addresses ZTNA at all levels, including deep segmentation as in a data center or IaaS environment.*

CASB

Cloud access security brokers secure and monitor use of cloud-based solutions, usually SaaS applications. They either block or allow user connections to cloud services and can provide some level of visibility into that use.

> ***EXPERT TIP:*** *CASBs can sit in-line between users and applications, or use APIs to integrate into the solutions and control and monitor access.*

Important Capabilities

Application Tracking

Ideally, the solution should provide for more detailed application usage information tracking than network-level monitoring, for both on-premise and cloud systems.

> ***EXPERT TIP:*** *This capability may be included as a feature in some CASB solutions.*

SASE

"Secure access service edge" (SASE) is a term denoting product suites that address the functions of ZTNA, CASB, SD-WAN, SWG, and cloud-based firewall.

> ***EXPERT TIP:*** *Converged solutions can help IT buy integrated tool sets that cover larger portions of the ZT puzzle.*

NGFW

Next generation firewalls combine traditional firewall functionality with deep packet inspection, application firewalls, intrusion prevention and detection systems (IDS/IPS).

> ***EXPERT TIP:*** *"In theory a ZT environment can get by without NGFWs, but they are essential during the transition and useful long-term as 'pre-filters' to reduce the amount of traffic at other enforcement points."*

Integration

Interoperability with ancillary security solutions, especially for outbound and endpoint security. For example, a ZT architecture should include, provide, or integrate at policy and logging levels with:

- **SWG:** Secure web gateways provide protection from malware for outbound web sessions and ensure enforcement of corporate web access policies.
- **DLP:** Data loss prevention tools control and monitor the transfer of enterprise data, an essential aspect of securing the enterprise but not part of ZT itself.
- **EDR/EPP:** Endpoint detection and response tools expand the ability of endpoints to contribute behavior data to a BTA/XDR and can be policy enforcement points as well.