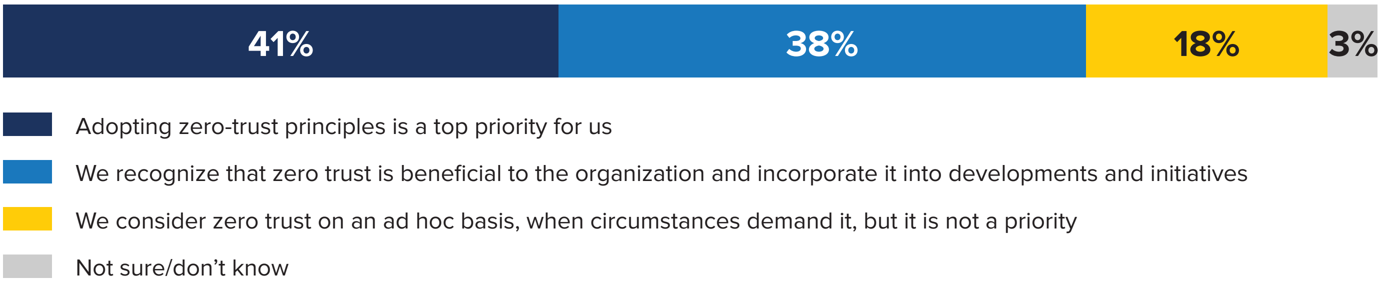
How to Keep Operations Running by Extending Zero-Trust Frameworks to OT Environments

OT connected assets are opening up industrial networks to a vast, advanced, and lucrative cyberthreat landscape for cybercriminals to exploit. Extending zero-trust frameworks to OT environments will ensure more secure, resilient, and automated operations.

Which of the following zero-trust statements is true for your organization?



Source: IDC Security Survey 2022 (n = 700)

How does your organization protect its IIoT deployments?

64%	Endpoint security
52%	Edge security gateway
47%	Network access control (NAC)
43%	PKI or other device identity solutions
42%	Industry firewall
40%	Embedded security in the device/ sensor
33%	Zero-trust architecture
29%	Intrusion detection and prevention
1%	Others; please specify

Source: IDC Security Survey 2022 (n = 233)

Zero trust is high on the security agenda. 41% of organizations are adopting zero-trust principles as a top priority, with a defined strategy and goals and support from senior management for new investments and initiatives. But zero trust is not a product, solution, or specific network that can purchased; it is a strategic approach to security, which makes it a more difficult architecture to implement. Only a third of organizations currently leverage zero trust to protect their IIoT deployments.

Zero Trust

Zero-trust architecture is based on the principle of denying access by default to anything requesting access to the network. This requires constant monitoring of threats to the business, continuous maintenance of the environment, and, because it is a framework and goes further than a technical solution, alignment of solutions to governance and compliance requirements.

Zero trust is a top-of-mind initiative for most organizations as business models change and organizations move forward with their DX initiatives. Zero trust is an enterprisewide strategy to reduce overall risk to the business. With more enterprise applications moving to the cloud and more devices connecting to the network (IoT and OT assets), the value of traditional perimeter infrastructure protection diminishes. Organizations find it challenging to cope with ongoing disruptions while securing users, devices, assets, and applications. This increases operational inefficiencies as well as the risk of security breaches.

What Does it Mean for OT?

In IT security, confidentiality is at the top of the CIA (confidentiality, integrity, availability) triangle. In OT environments, however, availability becomes the most critical aspect, which requires a change in risk management strategies.

Extending a zero-trust framework to OT deployments can enhance security and reduce risk, but it requires a complete understanding of all assets on the network, not just traditional IT endpoints. This will enable organizations to create segmentation decisions to reduce the attack surface and overall risk without impacting availability.

Connected assets can very easily become the weak link or entry point in any organization. Extending a zero-trust framework to OT deployments can enhance security and reduce risk, but it requires a complete understanding of all assets on the network, not just traditional IT endpoints. This will enable organizations to create segmentation decisions to reduce the attack surface and the overall risk without impacting availability.

Extend Zero Trust to OT Now: Advice to Get Started

- Zero trust must go beyond traditional definitions of users and identity to include all devices and assets.
- Ensure deep visibility on the network to identify and monitor every device (including communications of data to/from where, from whom/what).
- Automate enforcement of policy as well as detection and blocking of threats.
- Segment the network to address zero-trust principles into all environments by creating zones — enterprise, IoT, and OT could be kept separate.
- Contain known vulnerable, unsecure, or unpatchable devices in farther zones to reduce the attack surface.

IDC's Take

The convergence of IT and OT has been an unstoppable trend in the past few years. It is an opportunity for many companies to move toward more resilient decision-making operations to meet future operation requirements. From being two different worlds, IT and OT are increasingly communicating and integrating to improve organizations' operational performance and to fill the historical gap between operational and business processes, while opening OT up to a vast and advanced cyberthreat landscape.

Adopting a zero-trust approach not only for traditional IT infrastructure but also for OT environments with granular access permissions at the application level will increase secure connectivity and interoperability between IT and OT while reducing risks and threats to the whole operation.

Message from the Sponsor:

TXOne's OT zero-trust approach secures organizations against highly effective cyberattacks that have become a common threat to commerce. Easily enforce OT zero-trust–based policies with **ICS-native solutions**.