The 5 Essential Pillars of Zero Trust for BPOs

GUIDE

Security

> Never trust, always verify.
>
> – John Kindervag

A dynamic approach to zero trust is the best way to protect the client data BPOs store, handle, and analyze in an ever-changing security landscape.

The threat landscape is constantly changing, and a static security model is not an option. Zero trust is a dynamic approach to security that enables BPOs to stay ahead of the curve. By continuously investing in zero trust, BPOs can protect their data and systems from the latest threats and ensure a secure environment for the mountains of client data they store, handle, and analyze.

What Is Zero Trust?

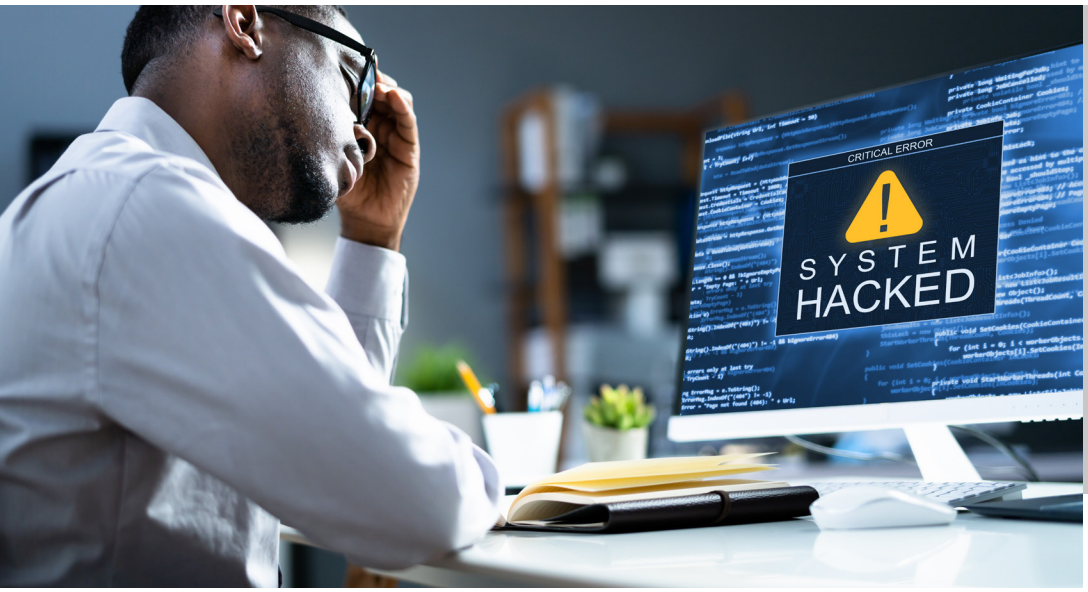
Zero trust is a security concept created by cybersecurity expert John Kindervag. The phrase he coined, "Never trust, always verify," has become the watchword of zero trust advocates and practitioners.

Kindervag broke new ground when he recognized that every instance of trust in a network represented a vulnerability. As he saw it, every user and every device needed to be authenticated and authorized before it could access any part of a network. With zero trust, no activity on the network, no matter where it originates, is presumed to be trustworthy.

Zero trust was a major departure from the status quo, which built security on the idea that a secure perimeter around a network would keep the network safe—much like a moat around a castle. Security experts presumed activities inside the perimeter to be trustworthy because an actor had to pass through perimeter security to get inside. But as with a castle, once a bad actor penetrated the perimeter and was inside, they could wreak havoc.

> "Cybercriminals have more ways than ever to penetrate a network."
>
> – John O'Malley

Learn More About iQor's **Digital CX Solutions**



Every 11 seconds a business is hit by a cyberattack.

– Cybersecurity Ventures

The Castle-and-Moat Approach No Longer Provides Enough Protection

The castle-and-moat approach was fine when everyone worked from the office and the network server was on premises. Today, businesses have data in data centers, in the cloud, in branch locations, and on endpoint devices. Employees work at home, a hotel, or their neighborhood coffee shop.

This is the era of the distributed network, and cybercriminals have more ways than ever to penetrate a network.

How much havoc are bad actors causing? Every 11 seconds a business is hit by a cyberattack. According to Cybercrime Magazine, if Cybercrime were a country, it would have the third largest economy in the world, behind only the U.S. and China.

Fortunately, zero trust is catching on.

Standards Help Business Process Outsourcers (BPOs) Transition to Zero Trust

Zero trust is a concept, not a product. You can't set it and forget it. For years, zero trust experts often described it in different ways, which could be confusing for BPOs that wanted to implement zero trust and build a zero trust architecture (ZTA).

That changed when, after a series of data breaches in various agencies, the U.S. government made a strong commitment to zero trust. The National Institute of Science and Technology (NIST) published NIST 800–207, "Zero Trust Architecture," to help organizations transition from legacy security systems to zero trust. In 2021 and 2022, the president issued executive orders requiring all U.S. federal agencies to adhere to NIST 800–207 and to ensure the responsible development of digital assets.

Now vetted and validated by many commercial customers, vendors, and government agency stakeholders, private organizations and enterprises widely recognize NIST 800–207 as the reigning zero trust standard. By providing helpful guidance—especially for organizations with no experience in zero trust—NIST 800–207 has provided clarity for BPOs and all organizations that want to phase in zero trust.

3 Principles of Zero Trust

CrowdStrike cites the three principles of zero trust as:

- **Continuous verification.** Verify all users and their permitted level of access before granting access to any resources. Only "least-privileged access" should be granted to any user, meaning users have access to only the resources they need.

Interested in learning more about iQor's zero trust initiatives?

Contact us today.

Before granting access, consider the context:

- Is the request coming from a user or an application?
- Is it known how the requestor will use the data?

- **Limit the "blast radius."** In case a breach does occur, minimize the damage it could cause.
- **Automate context collection and response.** Automatically analyze behavioral data against the entire IT stack to develop the most accurate response to an access request or perceived threat.

Zero Trust Needs of BPOs

When a BPO manages an omnichannel customer experience (CX) program, massive amounts of data (Big Data) are collected. Every customer interaction—phone, text, chat, email—is recorded and analyzed. Various applications are used to analyze the data produced from these interactions. Automation makes processes more efficient.

Hundreds or thousands of customer service agents and supervisors, many of whom work at home (WAH), have access to the data. Agents providing back office services handle thousands of personally identifiable records.

These activities are repeated for every client, every day.

And these 5 pillars of zero trust protect them from bad actors.

5 Pillars of Zero Trust for BPOs

Regardless of the scope of a dynamic zero trust implementation, these five pillars are must-haves for BPOs.

1. Multifactor Authentication

Multifactor authentication hardens security access to networks by requiring users to confirm their identity through two or more factors.

Zero trust practices offer you peace of mind that your outsourced business processes are protected so you can be confident your customer experiences create smiles.

Authentication factors are things you…

- **Know:** username/password, PIN, security questions.
- **Have:** RSA key, fast identity online (FIDO) key, phone, registered endpoint, certificate.
- **Are:** biometric scan – fingerprint, palm, eye, voice, facial.
- **Locate:** source IP, known device location, GPS.

Organizations can use multifactor authentication in numerous ways, including:

- **OTP:** After entering your user ID and password, the system asks you how you'd like to receive a one-time password (OTP), via SMS, chat, or email. After you select your preferred method, the system sends you the OTP and provides a form field for you to fill in after you've received it.
- **Third-Party Sync:** At the login screen, the system asks for your password and an OTP provided by a third-party application that syncs the OTP it sends to your smartphone with the login page.
- **Biometric Scan:** Login includes a user ID, an OTP, and a fingerprint scan.
- **Hardware Token:** To log in, press the button on your hardware token device to generate a new passcode and enter it into the first or second password field on the login screen.
- **FIDO2:** Open-standard FIDO2 delivers hardware-based authentication through your existing FIDO2-enabled device such as a smartphone, security key, or hardware token enabling you to simply enter your biometric or pin-based authentication to log in.

Multifactor authentication emerged as an important line of defense against bad actors as they became more adept at stealing user IDs and passwords through brute force (trial and error) and social engineering (convincing people to divulge their login credentials) attacks, such as:

- **Phishing:** Using fraudulent emails and websites to deceive users into revealing personal information or inadvertently installing malware.
- **Smishing:** Using text messages or messaging apps to obtain sensitive information from unsuspecting individuals.
- **Spear Phishing:** More personalized than phishing, spear phishing targets a specific person or group with a personalized message seemingly coming from a known sender.
- **Keyloggers:** Often installed through vulnerable browsers that fall prey to bad actors, a keylogger records every keystroke made by the user to gain access to confidential information.
- **Credential Stuffing:** Attackers use lists of credentials obtained through a data breach in one system to gain access to another system.
- **Brute Force and Reverse Brute Force Attacks:** Bad actors obtain the username or account number (brute force) or password (reverse brute force) and use automation tools to determine the missing key to gain access.
- **Man-in-the-Middle (MitM) Attacks:** Bad actors intercept messages between two parties to obtain and/or alter data with malicious intent.

While multifactor authentication may add a minute to the login time, it adds an important layer of protection to the network by making it much harder for bad actors to get in.

2. Network Security and Microsegmentation

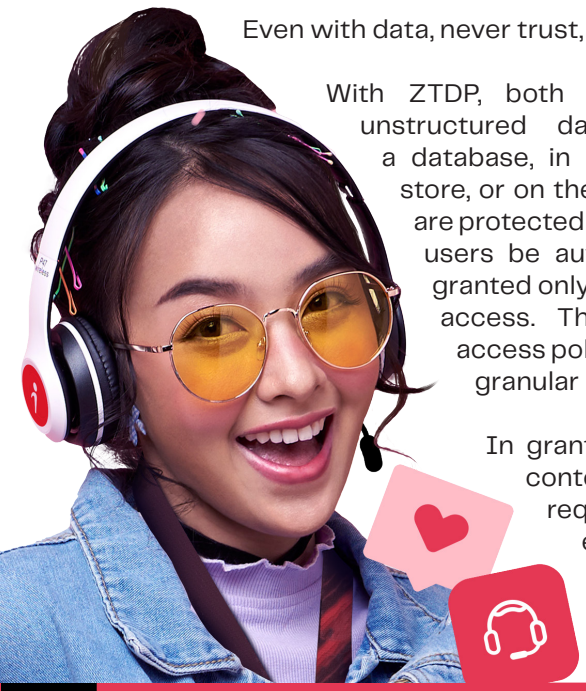
Multifactor authentication provides protection against bad actors trying to breach the network's perimeter. Microsegmentation protects the network from bad actors who somehow make it into the network and then attempt to cause damage throughout the network.

Microsegmentation employs software to virtually isolate parts of the network where applications can run—known as a workload—from each other.

With each workload isolated and every attempt to move from one workload to another requiring authentication and approval, microsegmentation limits any damage done in one workload from reaching another. It also ensures that any user in one workload who attempts to access sensitive data in another workload has the appropriate permissions. This is an area of continued investment for iQor into 2024 and beyond.

3. Data Security

Multifactor authentication and microsegmentation protect areas and resources of the network from bad actors. Zero trust data protection (ZTDP) protects the data itself by applying the principles of zero trust (detailed above) to data. In other words, ZTDP is an extension of zero trust. Instead of being network and resource centric, ZTDP is data centric.



Even with data, never trust, always verify.

With ZTDP, both structured and unstructured data—whether in a database, in a protected file store, or on the move (in use)—are protected by requiring that users be authenticated and granted only least-privileged access. This necessitates access policies at the most granular levels.

In granting access, the context of the access request is considered. Contexts to be considered might include:

- **Is the request coming from a user or an application?**
- **Is it known how the requestor will use the data?**

Automation is used to evaluate and enforce access policies. All data requests are logged, regardless of the outcome of the request.

4. Device Authentication and Authorization

Authentication and authorization are two steps that sound similar but have different meanings.

Authentication is the process by which a user or device is confirmed to be who they claim to be. Typically, the network authenticates users by their user ID, password, and another required authentication factor.

Devices are often authenticated by IP address. If the authenticated user's IP address is what's expected, the device is authenticated for that user. If the authenticated user's IP address isn't what's expected, the network may ask for further proof that they are who they claim to be. Also, a notification may be sent to the user that someone has logged in with their credentials from an unrecognized device, instructing them to contact the network administrator if it wasn't them.

Much of the communication in complex networks is between devices that work autonomously, such as routers and switches. To make sure bad actors don't mimic these devices, security teams use encryption to protect and send data between devices.

Authorization is the process of providing least-privileged access to the authenticated device for areas and resources requested.

This principle of least privilege (PoLP) is a foundational aspect of zero trust to help improve an organization's security posture by reducing their attack surface. The process of authorization involves verifying the user's or device's identity and then assigning access privileges that correspond to the user's role, responsibilities, and need-to-know. This is typically done by assigning the user or device a set of permissions that dictate the applications, data, and resources they can and cannot access.

5. Continuous Monitoring of All Actors

The transition from traditional unified networks with castle-and-moat security models to zero trust raises three important topics for IT: visibility, automation, and analytics.

Visibility
IT maintains a high level of resource visibility in a traditional network. With zero trust and network microsegmentation, resources are segmented into small pieces. Traditional monitoring and network management were developed to provide visibility to one network, not to many small segments that comprise a network.

Lack of visibility can lead to a network with unpatched devices, unmonitored systems, and shadow IT, where IT-related hardware and software are used without the knowledge and consent of IT or security.

Meanwhile, zero trust depends on continuous monitoring of all actors. Automation and analytics make up for the visibility deficit.

Automation and Analytics
Zero trust relies on software that automatically and consistently monitors all network segments, data correlations (how strongly sets of data are linked together), and logs to form a baseline of user behavior.

When analysis of the monitored data indicates there are anomalies in user behavior, they are reported to IT and security stakeholders as potential threats in real time. Real-time notification gives stakeholders their best chance to mitigate a threat before it does any damage.

Benefits to BPO Clients

When BPOs implement the five pillars of zero trust to protect their networks, their clients can feel confident that the BPO is taking every step to limit access to their data to users with the proper access privileges.

They can also feel confident that their BPO takes strong measures to protect their own operations against bad actors, so the business processes the client outsources to them have less chance of being compromised by cyberattacks.

These practices offer BPO clients peace of mind that their outsourced business processes are protected so they can focus on achieving desired KPIs.

Zero Trust Is the Future of Security for BPOs

Brands in all sectors are evaluating and in some stage of their planning a zero-trust security implementation.

BPOs use Big Data to find new agent-coaching opportunities to predict employee attrition and much more. They save, manage, and analyze massive amounts of data and can't afford to have that data breached, stolen, or corrupted. Zero trust is the standard that provides maximum cyber protection for BPOs and their clients.

Zero trust requires considerable know-how and time to implement. There's no such thing as a "finished" zero trust program. Technology keeps changing, and cybercriminals keep finding more ways to breach systems to deny service, steal secrets, or demand ransom. As circumstances change, organizations that employ zero trust need to change with them.

As more BPOs implement zero trust, brands in search of a BPO may well start asking, "How are you coming along on your zero trust security roadmap?"

As BPOs continue to invest in and implement zero trust practices, brands in search of a BPO partner can discuss current and planned zero trust initiatives.

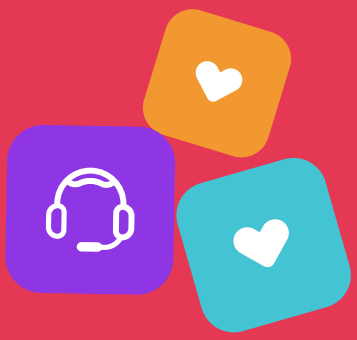
Experience the iQor Difference

At iQor, we partner with clients to design the optimal mix of CX automation and people where security is always top of mind. As a managed services provider of customer engagement and technology-enabled business process outsourcing (BPO) solutions, iQor provides a comprehensive suite of full-service and self-service scalable offerings that are purpose-built to deliver amazing customer experiences.

Our award-winning CX services include:

- A global presence with 50 contact centers across 10 countries.
- A CX private cloud that maximizes performance and scales rapidly across multiple geographies on short notice.
- A partnership approach where we deploy agents and C-level executives to help maximize your ROI.
- The perfect blend of intelligent automation for scale and performance coupled with an irresistible culture comprised of people who love to delight your customers.
- Virtual and hybrid customer support options to connect with customers seamlessly, when and where they want.
- The ability to launch a customer support program quickly, even when you need thousands of agents ready to support your customers.
- A best-in-class workforce management team and supporting technology to create a centralized organization that can better serve your entire business.

iQor helps brands deliver the world's most sought-after customer experiences. Interested in learning more about the iQor difference? If you're ready to start a conversation with a customer experience expert, contact us to learn about how we can help you create more smiles.



Smile!
With iQor

Learn More About iQor's Digital Customer Experience Solutions at www.iqor.com.