Zero trust:

A modern approach to cybersecurity

October 2020

Building a better working world

Introduction

Our world is changing at a rapid pace. Over the past decade, technology has ushered in an unprecedented level of change, opening up new opportunities and possibilities. The exponential expansion of data and devices driven by the internet of things (IOT) and the speed of modern-day connectivity enabled by 4G and 5G networking have played an integral part in shaping the world we live in today, connecting us with people around the world and accelerating our economies. At the same time, the rise of digital technologies, software-as-a-service (SaaS) applications and the cloud computing revolution have transformed the way companies function and operate.

Amidst all this, the recent COVID-19 pandemic quickly turned out to be yet another change catalyst, one which posed an existential threat to businesses worldwide. As we've had to respond and adapt to new ways of life in our homes and our workplaces, the employee base today within an enterprise is almost 100% working remote, connected and conducting their work over the internet. All of these macro forces have multiple ramifications and affect enterprise cybersecurity. First, the efficacy of using the network as the primary element to secure corporate resources has been eroded. The age of the corporate networks and security perimeters has come to an end. Second, this also means the attack surface for cyber threats is on a growth curve that is unimaginable. With users and devices going remote and mobile and applications moving to the cloud, enterprises now have to build systems and networks with the assumption that anyone could be on the network at any time. The expectation is that cybersecurity systems will not just protect enterprise assets but enable people to work when, where and how they need and use the devices and applications that maximize their productivity. Enter zero trust, a cybersecurity philosophy of how to think about security in this ever-changing environment.

What is zero trust?

"Zero trust" is a phrase first coined by John Kindervag, an industry analyst, in 2010 based on the realization that traditional security models operate on the outdated assumption that everything inside an organization's network should be trusted and to describe the need to move to a model that relies on continuous verification of trust across every device, user and application. While the idea of zero trust has evolved since then from being network-centric to a more comprehensive security model, at the crux of it, zero trust is the recognition of trust as a vulnerability and the elimination of any implicit trust from digital security systems.

This is done by pivoting from prior "trust but verify" paradigms to newer "never trust, always verify" ones. The zero trust model is built on the following six foundational assertions.

1. The network is always assumed to be hostile and all communication is secured regardless of network location.

2. External and internal threats exist on the network at all times and network locality is not sufficient for deciding trust in a network. Any person or device cannot be trusted just because they are part of the company or connecting from inside it. Assume you are already dealing with both outside adversaries and malicious insiders.

3. All data sources and computing services are considered resources that need to be protected.

4. Every device, user, network and data flow is authenticated and authorized. The former means positive confirmation that an entity confirms who/what they say they are; the latter means the entity has the need, rights and reasons to do what they're doing.

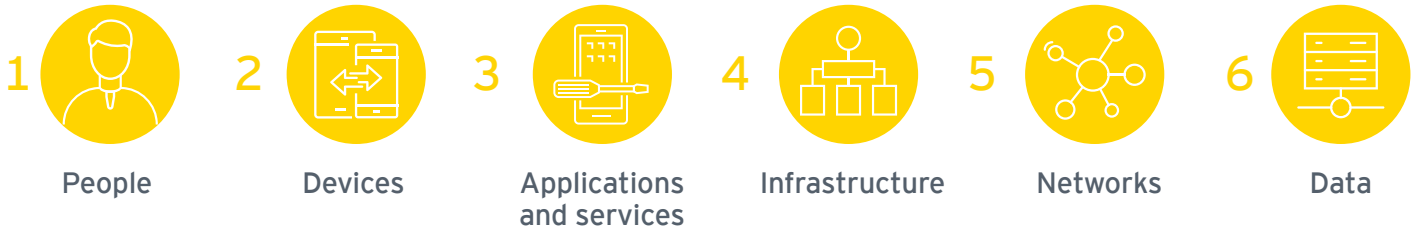
5. Any access to resources is granted on a per-session basis.

6. All security policies are dynamic and incorporate as many sources of contextual data as possible.

In a nutshell, zero trust is a new model and a general philosophy around cybersecurity, an approach that more effectively adapts to the complexity of the modern environment; embraces the mobile workforce; and protects people, devices, applications and data wherever they are located.

Zero trust building blocks and capabilities

The zero trust approach is most effective when it's extended throughout the entire digital landscape and used as an integrated security strategy. This is done by implementing zero trust controls and technologies across six foundational elements:



People

Humans are at the center of a company and its digital landscape. Be it employees, contractors, partners or customers, a zero trust strategy needs to encompass and account for all their possible interactions with corporate digital assets. The following section details some of the capabilities pertaining to the people element of a zero trust implementation:

Management and governance of digital identities

A robust identity life cycle management system is one of the most foundational pieces of a zero trust implementation. It's key to have a tamper-resistant digital Identity provisioning/onboarding process that includes well-defined HR processes or capabilities like identity proofing (for customers) to confirm the user's identity before provisioning a digital identity. Once provisioned, the digital identity needs to be maintained and up to date. It's also important to ensure users have one digital identity across the board and there is no fragmentation of digital identities. This identity can then be used to control users access to resources using the zero trust principles. The operative principle when it comes to provisioning access to applications and services is just enough access (JEA) or least privilege access. This can be implemented using various existing models like role-based access control (RBAC) or dynamic policy based access control models (PBAC). It is also crucial to frequently and proactively audit users access via access certifications to ensure just enough access.

Authenticators

Once digital identities are set up, every access from a user needs to be gated where the user asserts their identity. A zero trust security posture is highly dependent on the effectiveness of this gating process. From a users standpoint, it is key that users are equipped with multiple forms of credentials where they can reliably assert their identity to the system. While passwords have traditionally been a means to do this, they have proven to be a significant weakness. They are snoopable, crackable and even available on the dark web for sale. While taking a relook at password-based authentication and security systems, it is also important to recognize that the underlying weakness of the password-based authentication is the shared secret (something only you know) model. Zero knowledge-proof cryptography and its application in standards like Fast Identity Online (FIDO) have opened up better models of authentication that are more secure. Additionally, mobile phone-based authenticator apps, biometrics and portable IDs/keys offer credential options based on something you have (possession factor) and something-you-are (inherence factor). The idea is to enable the user with stronger credential options they can leverage to reliably assert their identity prior to access.

The technology set to implement zero trust for the people element should comprise of identity management and governance, ID proofing and access management solutions supporting a variety of multifactor authenticators.

Devices

While most organizations have had device management solutions for devices provisioned and managed by the organizations for a long time, the blurring of lines between personal and professional mobile phones and computers, remote work and BYOD policies have expanded the attack surface to mobile phones, laptops and devices that are not managed by the organization. To add to that, businesses are bolting operational technologies onto IT networks en masse which, along with IOT and many kinds of specialized devices deployed for digital transformations, have led to an exponential increase in the number of unmanaged devices.

What are unmanaged devices ? Depending on the business, in corporate offices they can be smart TVs, ACs, security cameras, Building management systems and printers. In manufacturing they include industrial devices, machines and robots. In hospitals, they include infusion pumps, ventilators, MRIs and X-ray machines.

In a nutshell, a plethora of specialized devices in every industry are now connected to enterprise networks. It is estimated that there will be 41.6 billion new connected devices by 2025. These devices are not only numerous, they are vulnerable and have attracted the attention of attackers. Per an industry report, attacks on enterprise devices are up by 300% just in 2019. These attacks have relied on a range of known vulnerabilities ranging from botnets to insecure software, weak or nonexistent encryption, default plain-text passwords and insecure communication protocols. While there is an immediate need to design controls in this area, the following challenges need to be accounted for while devising a security strategy for devices:

- Device manufacturers design for function and operational efficiency and do not tend to design strong security controls into devices that enterprises are using.
- Systems/controls like patch management and traditional end-point management that require an agent cannot be used for many of these devices.
- Absence of inbuilt data controls/encryption for data that's on the device and transmitted by the device.

To apply zero trust security to devices, enterprise teams need to incorporate security systems that enable them to:

- Know all the devices in the enterprise (device inventory).
- Know the device software and firmware details along with any vulnerabilities and risks.
- Know what data, applications and network resources each device needs access to.
- Be able to assess the contextual risk profile from the device at a given point in time.
- Monitor, control and remove a device at any given moment.

The technology solution set to implement zero trust for devices should ideally consist of a combination of unified endpoint/device management (UEM) for managed devices and a device/endpoint security platform that can address the before-mentioned security needs for unmanaged devices. Additionally, for devices which pose a high risk that cannot be managed, network segmentation or micro-perimeter technologies can be leveraged to control the network access or isolate them from other IT devices or networks.

Applications/services

Most current-day enterprises support a variety of applications and APIs/micro-services that could be hosted anywhere, from on-prem data centers to third-party data centers, public or private clouds along with a portfolio of SaaS applications and services from external vendors. Additionally, the computerization of information technology has led to the emergence and growth of shadow IT where applications and services (like the popular messaging, social media or cloud storage apps) are increasing being used by employees without the knowledge of the IT departments. While taking these aspects into consideration, the approach to designing zero trust security for applications and services should include the following.

- **Application and services inventory —** It's key now more than ever to build and maintain an inventory comprising all the applications and services used by the enterprise. The applications and services also need to be assigned a unique identity/identifier that is consistently used across the enterprise. While there are various cloud-native inventory and discovery services to do this, the hybrid nature of most current-day enterprises would mean a combination of processes and systems will need to be devised to successfully build a comprehensive inventory.

- **Strong gating —** Implementation of robust and consistent access management controls across the board. Any access to applications and services is only permitted after the users successfully assert their identity via zero trust-based identity systems. The gating/access control should be dynamic to account for changes in context (device, network) along with user and device behavioral data points. Any access granted should be on a per-session basis with in-session monitoring capabilities.

- **Governance —** With Agile and DevOps CI/CD practices widely being adopted, establishing a strong governance system/structure to ensure the ever-evolving set of applications and services within the enterprise are up to date on security controls and align with the enterprise security strategy.

The technology solution set to implement zero trust for applications and services should comprise adaptive access management solutions, API/application/web gateways, cloud access security brokers, and user and event behavior analytics (UEBA).

Infrastructure and workloads

Widespread adoption of infrastructure and platform-as-a-service, virtualization technologies and cloud computing have led to enterprise technology infrastructure being spread out beyond traditional data centers. Most mid-sized to large enterprises have already moved some of their infrastructure and workloads into the cloud for better agility and efficiency. Nearly three-quarters of businesses are running a hybrid and/or multicloud strategy today, according to Forrester. Additionally, the rapid pace of modern-day development of products, services leveraging Agile methodologies and CI/CD pipelines mean the infrastructure footprint is ever-increasing.

A zero trust approach to infrastructure in this context should include the following:

Comprehensive privileged account strategy — It's well established that a considerable number of insider threat and external attacks involved privileged access abuse. It's essential that organizations identify all privileged accounts across all their infrastructure including their public or private clouds along with admin accounts for various SaaS applications used. It is also key to account for all non-human entities machines, services and APIs that have privileged or elevated access. A comprehensive privileged account management strategy should be devised that can apply to the enterprise ecosystem that includes cloud providers, DevOps CI/CD pipeline tools and container technologies.

A zero trust-based privileged account management strategy should include:

1. Adaptive/dynamic gating that relies on contextual access decisions.
2. Multifactor authentication (MFA).
3. Ensure least effective privilege through stringent provisioning controls, monitoring and periodic audits.
4. Zero trust admin environments via isolated jump boxes with distributed connectors (or) network micro-segmentation.

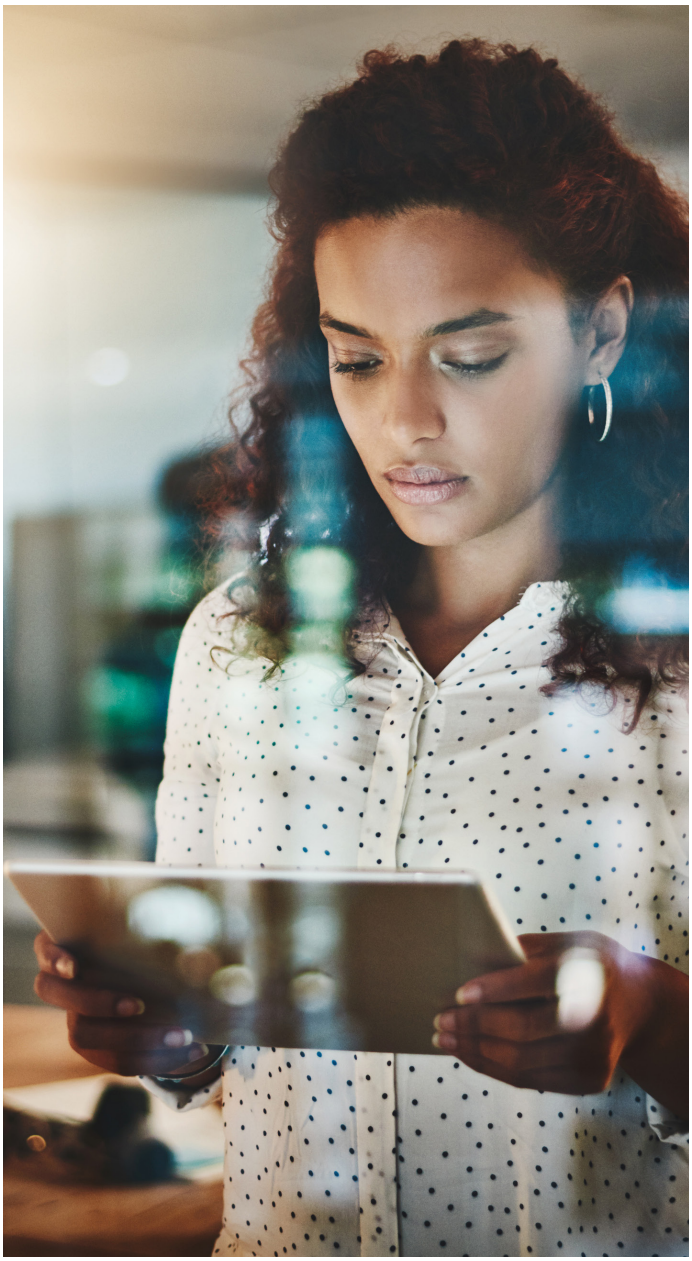
Service meshs - Enterprises today typically have a mixture of services hosted on legacy infrastructure/virtual machines (VM)s and containers that are increasingly replacing legacy software deployment models. Although containers provide greater efficiency and scalability, they can have significant implications for security by the very nature of containers being ephemeral. A zero trust approach to infrastructure requires an identity for all infrastructure including servers, VMs, containers and its components independent of where they run. It's key to incorporate a service mesh layer that ensures strong gating for communication between services that includes services run on legacy infrastructure as well as the ones run within containers. The goal is to ensure all communication between services is permissioned.

The technology set to implement zero trust for the infrastructure or workloads should comprise privileged access management and service mesh solutions.

Networks

Network security is an area of increasing cyber technology spending by most enterprises and is a key element of zero trust as all applications, services and data are ultimately accessed over network infrastructure. While there is no one size fits all, the following section details a set of capabilities to consider for zero trust-based network security.

Micro-segmentation — Network micro-segmentation is the process of isolating sensitive systems into a series of network segments so that a breach of the network won't give cyber criminals or malicious insiders free rein across the entire enterprise landscape. The idea is to understand the inter dependencies between the infrastructure, services and data and then put controls in place as close to the protect surface as possible, creating a micro-perimeter around it. This micro-perimeter moves with the protect surface, wherever it goes. While the concept of micro-segmentation itself isnt new, segmentation gateways and next-generation firewall technologies (NGFW) enable such network micro-segmentation at granular levels. The idea is to efficiently segment the network to lock it down, yet enable permissioned access.



Software-defined perimeters (SDP) — SDPs are used to provide secure access to private applications without allowing users access to enterprise networks. They are often a replacement for traditional technologies like VPN. SDP technologies render enterprise resources "dark" where no DNS, internal IP address or visible port information is communicated until proper gating (authentication and authorization) takes place. So unauthorized users can't traverse the network looking for resources to infiltrate. This reduces the attack surface significantly by mitigating or eliminating numerous threats like APTs and malware.

The technology set to implement zero trust for the network element should comprise of NGFW, secure web gateways (SWG) and SDP solutions. The emerging set of zero trust-focused SDP solutions called zero trust network access (ZTNA) and secure access service edge (SaSE) solutions offer an integrated set of options in this space.

Data

Ultimately, data is the most prized asset of a modern enterprise. One of the main strategic goals of cybersecurity in the digital age is to combat and mitigate data loss and data breaches. With more data than ever, from more sources than ever, this entails ensuring data is protected while at rest, in use and in transit, even if it leaves the devices, applications, infrastructure and networks.

The precursor to zero trust security for data is the process of data discovery and classification. The purpose of data discovery and classification is to ensure that security teams know what data the enterprise has, where it is located and how sensitive the data is. Once it's understood what data needs to be protected, the data life cycle and its business criticality, data loss threats to this data can be identified.

Data controls are then designed to address these threats. While various existing data loss prevention control strategies like masking, anonymization and different forms of encryption can be leveraged as controls, a zero trust approach to data security should also be:

- Dynamic and risk-adaptive and that takes full operational context (including user behavior) into account and does not just depend on static policies.
- Include control points across the full length and breadth of the enterprise (public, private clouds, SaaS applications).
- Include enforcement controls to protect data based on the calculated behavioral risk level of users and the value of data accessed.

The technology set to implement zero trust for data could comprise of a combination of data loss prevention (DLP) and dynamic data protection solutions.

Monitoring, detection and response

While the above sections outlined various controls that enable comprehensive coverage across the enterprise, an optimal zero trust implementation is one where the entire enterprise digital landscape is connected and all the security systems function as one fully integrated platform/ecosystem. While it's important for security systems to be able to see across their apps, endpoints, network, users, devices to detect, and respond to security threat and incidents, zero trust-based security systems should also be able to tap into and leverage signals from across the board to make informed and automated security decisions, preempt security threats and ensure a quicker response to security incidents.

The integration of security signals with the solution components in an adaptive loop is the goal. The following section details a set of additional capabilities that should be a part of the technology stack deployed by an enterprise embarking on a zero trust implementation to enable this:

Visibility

Being able to have the visibility of all activity within the enterprise digital landscape to command and control various zero trust solution elements/components is key to a successful zero trust implementation. This entails the capability to ingest, categorize and aggregate data from disparate sources and systems such as IAM systems, users, devices, DLP, network systems, etc. While most enterprises have an existing SIEM or a log-monitoring system that helps collect, aggregate and process logs and events from various enterprise systems and data sources, this data (logs/events) is not always designed for security purposes. Additionally, the systems that are the source of data often operate in silos and provide different types of security information that sometimes even conflict with one another. As part of a zero trust implementation, it's key to review and tune existing complete monitoring/SIEM solutions to ensure security systems have a comprehensive and holistic view of IT infrastructure. It is extremely beneficial to implement observability as property of the network and the systems therein. Observability is a measure of how something is working internally, concluded from what occurs externally. It requires application and service development incorporate the idea of enabling and strengthening security decisions.

Cyber analytics and threat detection

With well-defined visibility/SIEM capabilities and observability built into systems, the sheer volume of security events, logs and data generated from modern enterprise systems necessitates security systems with cyber analytics capabilities. Cyber analytics involves the use of data aggregation, attribution and analysis to extract the information necessary for a proactive approach to security. Cyber analytics solutions incorporate data science and big data techniques to process real-time data along with historic data, and leverage machine learning to model, detect and proactively identify threats. With the rise of national state-sponsored cyber attacks, evolving adversary tactics and the dynamic nature of the threat landscape, it is pivotal to leverage high-quality threat intelligence feeds as inputs to prevent or mitigate cyber attacks. An effective threat intelligence should provide additional external security context (e.g., Who are the attackers and what are their motivations? What are their tactics, techniques? What are the indicators of compromise?) that's relevant, timely, complete and accurate.

Security orchestration automation and response (SOAR)

Manual security operations slow the response time to cyber attacks and give attackers more time to exfiltrate data and inflict lasting damage. A zero trust approach should embrace SOAR to help security teams manage and respond to endless alarms at machine speed. SOAR capabilities allow organizations to optimize security operations in three key areas: threat and vulnerability management, incident response and security operations automation. SOAR solutions also help define, prioritize and standardize workflows that respond to cyber incidents. They improve overall efficiency by automating the response to security incidents, feed signals back into the solution components and make security more self-operating.

Capability matrix

Zero trust element	Capabilities
People	Identity management and governance, ID proofing, multifactor authenticators
Devices	Unified endpoint management, endpoint detection (unmanaged devices)
Applications and services	Adaptive authentication, web and API gateways, cloud access security brokers, UEBA
Infrastructure and workloads	PAM, service/app mesh
Networking	Next-generation firewalls, secure web gateways and software-defined perimeter
Data	Dynamic data protection and data loss prevention
Monitoring, detection and response	SIEM, cyber analytics, threat Intelligence, SOAR

Putting zero trust into action

While zero trust represents a clear pivot in how to go about cybersecurity, it's implementation leverages and builds upon some of the security technologies and capabilities already used in most enterprises. So the first step towards zero trust is to perform a current-state assessment to gauge the capabilities of existing security technologies and the maturity levels against the set of capabilities required for zero trust (the capability and solution matrix outlined in this document can be leveraged as a reference). Once, the current state is well understood, a zero trust architectural vision/strategy needs to be devised that also takes the company's business and organizational goals into account. A well-defined zero trust vision/strategy not only sets the tone organizationally, it also helps get senior business leadership buy-in. Additionally, it serves as a guide for various tactical and operational decisions during the execution.

The next step towards zero trust is building a zero trust road map and a program that details the path to develop the capabilities identified for zero trust and deploy them in your organization. Some of the key considerations to take into account:

- No single vendor or provider can deliver all of the capabilities and components required to implement zero trust for an enterprise. It will require piecing together multiple vendor or homegrown solutions and technologies to achieve the end zero trust state.
- Identifying current or future business or security initiatives (e.g., cloud migrations or infrastructure/network upgrades) that can incorporate zero trust goals and act as pilot implementations.
- Identifying the people, process and technology dependencies between various capabilities and prioritizing for efficiency.
- Setting realistic objectives and key results (OKRs) and time frames to achieve them.

Finally, once the road map is defined and the zero trust program execution kicks off, it is also pivotal to set up a governance structure to ensure successful execution and evolution of zero trust within your organization.

Benefits of zero trust

While the zero trust security model is undoubtedly effective from a security standpoint, it also delivers considerable business value. The following section lists five different benefits of zero trust:

1. **Enables and accelerates digital transformation by increasing business speed agility and adapting the security architecture to evolving business needs.**

2. **Offers greater flexibility for staff, partners and customers. Improves overall operational efficiency by reducing complexity.**

3. **Enhances security posture, elevates safeguarding the firm's intellectual property to a core competency and shields the firm's reputation.**

4. **Reduces the overall cost of security through consolidation, automation and lower breach costs.**

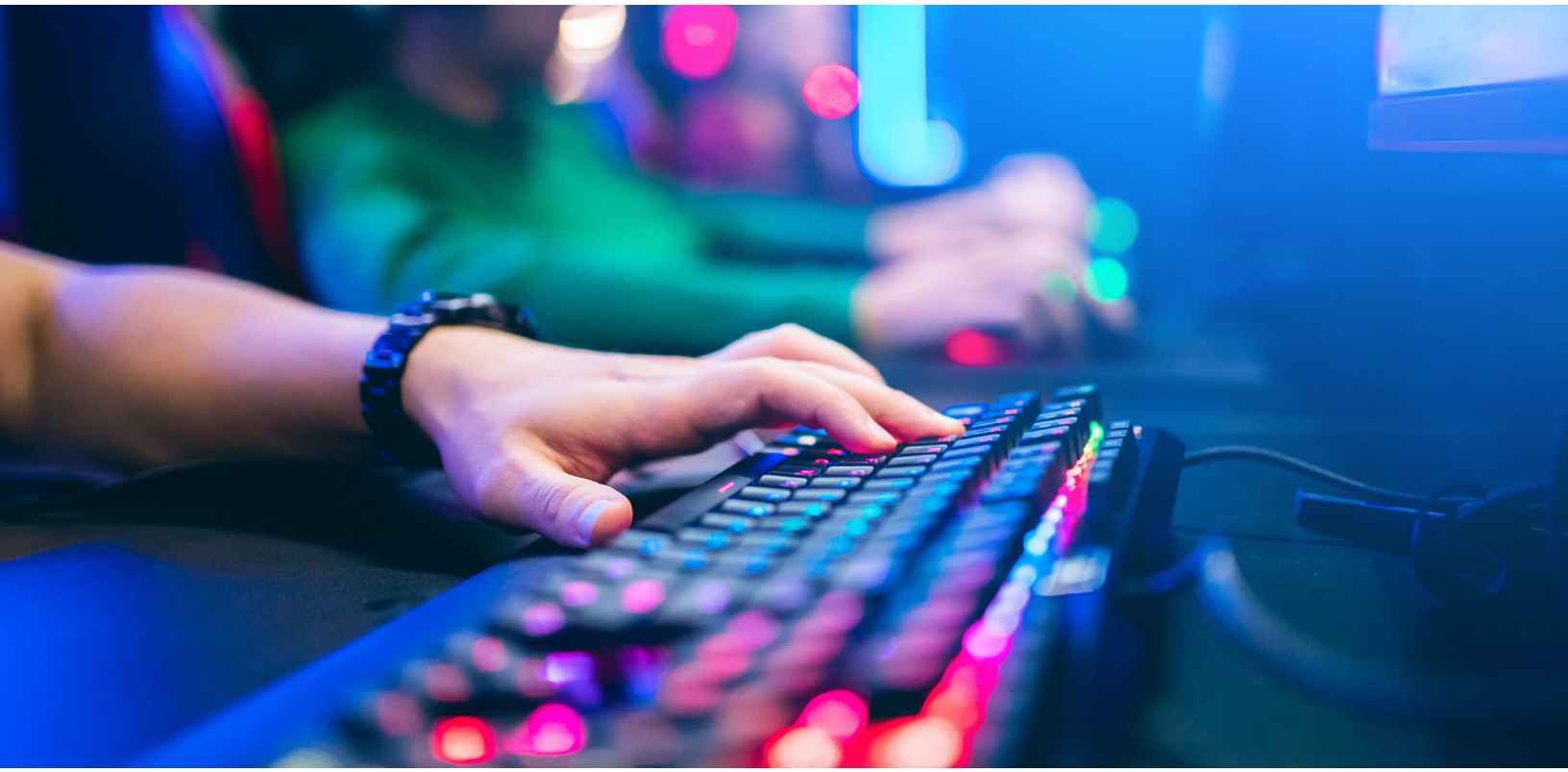
5. **Reduces complexity and the overall cost of ongoing compliance initiatives.**

Conclusion

Opening the door to new possibilities

As we look past the COVID-19 pandemic to the next normal, every enterprise is on a zero trust journey whether they realize it or not. From a cybersecurity standpoint, this means building resilient security systems that thrive in uncertain conditions and can adapt to a diverse group of people's ever-changing circumstances. Whether it's an organization or an individual, our ability to be empathetic helps us understand and adapt to the needs of others during times of disruption. While digital technologies will continue to influence and shape the world around us, in this next normal, cybersecurity is as much about security as it is about enabling productivity and collaboration through secure, inclusive user experiences.

And zero trust might just be the answer!



Author

Paul V Merugu
Senior Manager
Tech Consulting
Ernst & Young LLP
paul.v.merugu@ey.com

The views reflected in this article are those of the author and do not necessarily reflect the views of Ernst & Young LLP or other members of the global EY organization.

EY | Assurance | Tax | Strategy and Transactions | Consulting

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

2009-3578175 | ED None.
EYG no.

ey.com