WHITE PAPER

HIKVISION®

Securing a New Digital World with Zero Trust

How Zero Trust Cybersecurity is Transforming the IoT Industry

Contents

HIKVISION®

INTRODUCTION

Rapid change, often driven by technology, is a constant in our world today. But technological advancements are a mixed blessing, enabling enormous opportunity alongside unprecedented cyber risks. Today, we're in the midst of a new era—the Internet of Things (IoT) Era—witnessing an exponential expansion of data and devices, new connection speeds enabled by 5G networks, and the rise of automation from deep learning. Yet these wonders have simultaneously put the attack surface for cyber threats on a previously unimaginable growth curve[1] . Add to this the increasing complexity of our organizations and our insatiable demand for real-time information at home and at work, and the end result is increased cybersecurity concerns.

So how do we address growing cybersecurity concerns? In recent years, many have heard the term "Zero Trust," a concept developed in 2010[2] , mentioned as an antidote to ever-changing cybersecurity threats. Much more than an IoT-era buzzword, Zero Trust, when thoughtfully implemented, can play an essential role in safeguarding our people, our businesses, and our devices well into the future.

This white paper will explain Zero Trust, outline why it's essential within the IoT industry and describe how Hikvision, a global manufacturer of IoT devices with a focus in video surveillance, endorses the concept of Zero Trust.

A NEW STATUS QUO FOR CYBER THREATS

Every few years, a major cyberattack changes the way we do business and how we secure our personal and business assets. In 2013, the breach of retail giant Target taught us that vendors and vendor systems are uniquely vulnerable, as the attacker used an HVAC vendor's credentials to compromise the network and ultimately the point of sale (POS) systems. Four years later, the 2017 break of Equifax, one of largest consumer credit reporting agencies, compromised the data of nearly 147 million people, as a result of an unpatched application vulnerability and inadequate network segmentation[3]. Since then, cyber threat actors have ranged from ransomware crime rings targeting healthcare institutions, to nation states targeting software supply chains, to opportunistic threat actors seeking exploits for private gain.

How do you address the increasing cyber risk? As both a philosophy and framework, Zero Trust is not only the best option, it may increasingly be the only option.

THE PHILOSOPHY OF ZERO TRUST

Zero Trust is a strategic initiative developed to prevent data breaches by eliminating the concept of trust from an organization's network architecture. Rooted in the principle of "never trust, always verify," Zero Trust is designed to protect modern digital environments by leveraging network segmentation, preventing lateral movement, providing threat prevention, and simplifying granular user-access control[4].

TRUST IS A VULNERABILITY

The Zero Trust concept was created by John Kindervag, during his tenure at Forrester Research. He founded Zero Trust on the realization that traditional security models operate on an outdated assumption that everything inside an organization's network should be trusted. Under this traditional trust model, network functionality assumed that a user's identity is never compromised and all users act responsibly and can be trusted. The Zero Trust model recognizes trust is a vulnerability. Once on a traditional network, users—including threat actors and malicious insiders—are free to move laterally and access or exfiltrate whatever data they have access to. Given the observed behavior of hackers, it is important to remember that the point of infiltration of an attack is often not the target location.

"Zero Trust is a strategic initiative developed to prevent data breaches by eliminating the concept of trust from an organization's network architecture. Rooted in the principle of 'never trust, always verify,' Zero Trust is designed to protect modern digital environments by leveraging network segmentation, preventing lateral movement, providing threat prevention, and simplifying granular user-access control."

[1] Securityroundtable.org: The future is here; in Zero Trust, we trust – John Davis
[2] Dark Reading: "Forrester Pushes 'Zero Trust' Model For Security" <https://www.darkreading.com/attacks-breaches/forrester-pushes-zero-trust-model-%20for-security/d/d-id/1134373>
[3] CSO: "The 15 biggest data breaches of the 21st century https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
[4] Palo Alto Networks: What is a Zero Trust architecture? https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

UNDERSTANDING ZERO TRUST THROUGH THE LENS OF PHYSICAL SECURITY

The term Zero Trust may seem like a misnomer because, there is, in fact, a level of trust granted in a Zero Trust environment. Yet unlike a traditional network, trust is not assumed simply because a device is on the network.

To use a physical security analogy, imagine a checkpoint that allows employee access to the boarding area of a high-security regional airport. Outside of traveler checkpoints, this airport has a badge reader that only allows employee entry if each individual has a pre-authorized badge. As each person badges in, the turnstile opens and allows the authorized person to enter the building. In general, this practice will keep out unauthorized personnel. Yet as facilities security managers know, even with these controls in place, it's still possible for a threat actor to enter the premises. Consider a few possibilities:

1. A disgruntled airport employee could pose a threat.
2. An employee could either knowingly or unwittingly sign in a threat actor as a guest.
3. A threat actor could steal the badge of an employee to gain entry to the airport.
4. A threat actor could make a copy of an employee's badge without the employee's knowledge.
5. A threat actor could find a way to sneak into the airport through a different entry point.
6. A threat actor could talk their way into the building using social engineering tactics.

This scenario is like an organization's network. The world outside of the airport represents the dangers of the open Internet. Everyone, good and bad, are on the outside. The vast majority of people do not pose a threat to the location, but some actors may want to get in for malicious purposes.

The badge reader/turnstile is like a network gateway firewall. It blocks everything from coming in, unless it is pre-approved, but it allows employees to leave the building without badging out.

The employees entering the airport are like the computing devices on a network. They can all interact with each other with little or no friction. In essence, there is a level of trust that is granted to other employees because they are in the airport and have passed the badge-reader authentication test.

So to secure this perimeter, how would you apply Zero Trust to this airport setting?

"Zero Trust is more than a concept; it's a way of doing things. It's a mindset."

To follow the analogy, first, every employee receiving entry would be assigned to their own designated area, which they are immediately directed to upon entry. To avoid security breaches and contraband, no employees can interact with other staff until they reach their designated area and even then, communication is only possible with preapproved people whose identity can be verified. So while there may be many people in the airport, each person can only interact with verified people with whom they have a need to communicate.

"TRUST THE PROCESS": FROM PROTECT SURFACE TO TRUSTLESS SECURITY

Zero Trust is more than a concept; it's a way of doing things. It's a mindset. It lays the foundation for a cybersecurity approach. In Zero Trust, the first step is to identify a "protect surface." The protect surface is made up of the network's most critical and valuable data, assets, applications and services, which are also known as the organization's "crown jewels." Protect surfaces are unique to each organization. Because it contains only what is most critical to an organization's operations, the protect surface is orders of magnitude smaller than the attack surface, and it is always knowable.

THE MICRO PERIMETER

With your protect surface established, you can identify how traffic moves across the organization in relation to the protect surface. Understanding who the users are, which applications they are using and how they are connecting, is the path to determine and enforce policy that ensures secure access to your data. Once you understand the interdependencies between the "crown jewels" and your users, you should 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. In other words: it's about 100 percent visibility into your IT environment, including the network itself, the applications, the data and the users.

VISIBILITY AND MONITORING

Once you've built your Zero Trust policy around your protect surface, you should continue to monitor and maintain it in real time, looking for things that should be included in the protect surface, interdependencies not yet accounted for, and ways to improve policy. With the right IT security implementations, this monitoring and enforcement can be automated for 24/7 protection.

While user locations can factor into risk, Zero Trust is not necessarily dependent on a location. Users, devices and application workloads are now everywhere, so you cannot enforce Zero Trust in one location—it must be utilized across your entire network environment and all access points. The right users need to have access to the right applications and data for organizations to function.

"Typically, the path for an organization or entity to achieve a Zero Trust security posture is a journey, not an immediate-term activation. This journey involves the coordination of IT alongside operations and product and customer-facing teams, as well as defining security needs across budget priorities, vendor relationships, and collaboration with business units to establish safeguards for critical data and assets."

Users are accessing critical applications and workloads from anywhere: home, coffee shops, corporate offices, and remote branch offices. To enable secure access, Zero Trust requires consistent visibility, enforcement and control that can be delivered directly on the device or through the cloud. Workloads are highly dynamic and move across multiple data centers and public, private, and hybrid clouds. With Zero Trust, you must have deep visibility into the activity and interdependencies across users, devices, networks, applications and data.

Finally, given Zero Trust is an emerging category and technology framework, it should be customized for deployment based on the type of organization and people it secures from threats. Different enterprises may have varied risk assessments for various categories of data and administrative privileges, for instance, and security practices must be tied to security priorities.

DEPLOYING ZERO TRUST TO YOUR NETWORK

Enterprises implementing Zero Trust typically start with stakeholder alignment between business functions to agree on defined objectives and establish consensus in protecting organizational assets. Before implementing Zero Trust, close coordination with organizational leaders and management is necessary: The proper flow of data is likely critical to the success of the business, so executive sponsorship of Zero Trust initiatives is a prerequisite. The implementation itself is typically a function of the security team, in collaboration with the IT and developer teams, if applicable, to establish best practices and goals.

These objectives can begin with defined targets such as the implementation of multi-factor authentication for all users as well as decision trees for appropriately safeguarding incoming data and assets. Typically, the path for an organization or entity to achieve a Zero Trust security posture is a journey, not an short-term activation. This journey involves the coordination of IT alongside operations and product and customer-facing teams, as well as defining security needs across budget priorities, vendor relationships, and collaboration with business units to establish safeguards for critical data and assets.

DEFINING NETWORK IDENTITIES, TRAFFIC AND ACCESS

By definition, Zero Trust assumes all activity on the network is malicious traffic until it is proven otherwise. When it comes to practically implementing the Zero Trust framework, you must have full visibility and understanding of your users (network identities, access rights) and assets (data, applications). Often, enterprises find that network segmentation[5]–controlling traffic between various parts of the computer network–is a clear first step in technical implementation of Zero Trust protocols and frameworks.

"Hikvision strives toward a fully visible ecosystem by maintaining transparency about secure-by-design production processes, regularly executing internal and external penetration testing, reviewing the supply chain consistently, and monitoring all software/ hardware development processes of all products."

However, while network segmentation allows organizations to prioritize and implement security protocols by isolating "crown jewels," Zero Trust does not strictly define access by network segments, as NIST Special Publication 800-207[6] describes. Instead, "trust" is granted at the individual user identity level, rather than from a particular device, network location (such as branch office) or cloud. Zero Trust protects resources (assets, infrastructure, workflows and data) by building into the network architecture—and security playbooks—an assumption that any individual part of the network is at risk for compromise, and should be consistently treated as such.

To enable efficient workflows amidst a Zero Trust enterprise environment, organizations should understand their users' needs, from access to specific clouds to the use of different devices and clouds. Zero Trust architecture offers access by verifying trust from users, such as via secure, two-factored connections with network traffic monitoring, and identifying unnecessary user privileges for access to various points in the network.

DEFENDING AGAINST A RAPIDLY EVOLVING 'CYBER WORLD'

While malicious actors have recently exploited the pandemic climate, the trend for the past few decades has been a greater number of sophisticated malicious cyber actors, increasingly scaling their ability to infiltrate networks, exfiltrate data, and run malicious programs. Organizations can protect themselves from this evolving threat environment by understanding their organization, identifying their "crown jewels," and determining how they can protect their business and most important assets. This security roadmap should be based on a risk assessment, in which the most important risks for the core business and the risk mitigation measures are identified.

[5] Cisco: What Is Network Segmentation? https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html

[6] NIST Special Publication 800-207 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[7] The EU Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2020 https://www.enisa.europa.eu/publications/emerging-trends

Network architects and IT security engineers should build a Zero Trust security posture that considers vulnerabilities across the organization, such as access by contractors, customers, and outside vendors. Often, understanding this complex environment can require a patchwork of security vendors. Due to the complexity of defending an organization against an escalating cyber threat environment, there is an ongoing debate amidst enterprises and even the government sector around the practical strategies of deploying cybersecurity solutions using an in-house IT security team; contracting security to experienced vendors and managed services firms; or a hybrid of the approaches. All mentioned approaches apply, as long as the foundation is built upon a Zero Trust strategy.

ZERO TRUST WITHIN THE IOT INDUSTRY

In today's world, IoT's immense applications make it so much more than the sum of billions of connected things. IoT encompasses critical infrastructure, such as traffic controls and power grids. IoT secures voting systems that uphold our faith in our most revered democratic processes. IoT also ensures that our citizens, communities and economic systems are safe and healthy, with the support of video security cameras and building management systems. Because the stakes surrounding IoT are so high, the potential benefits are so great, and the possible downsides are so dramatic when security is not taken into account from the start, organizations should embrace a comprehensive Zero Trust strategy[8].

UNIVERSAL IOT CREATES NEW CYBERSECURITY CONSIDERATIONS

It is clear that IoT will touch upon our lives at home, at work and in the community. The rapid adoption of smart homes, smart buildings and smart cities, facilitated by a cascade of IoT components embedded in everyday devices, will soon make IoT commonplace. The current estimates of anywhere from 20 to 50 billion connected things over the next several years may be the tip of the iceberg. IoT will be a core enabler of everything we do.

The increased number of IoT devices that are connected to the Internet can be seen as a serious extension of the attack surface, which lays an additional burden on the required visibility of the security organization. Not only should the "old-fashioned" computer systems (e.g. servers, endpoints, on-premises environment) be monitored constantly, but so should all connected IoT devices through which attackers can gain access to the computing infrastructure of an organization. Therefore, it is essential that security professionals apply Zero Trust to IoT and vice versa. You cannot address cybersecurity for such a massive and pervasive category of technology without the same Zero Trust strategy you are applying to your applications, networks and computing infrastructure.

[8] Securityroundtable.org: The only way to secure IoT is Zero Trust – Jamison Utter https://www.securityroundtable.org/the-only-way-to-secure-iot-is-zero-trust/

A SECURE-BY-DESIGN APPROACH TO IOT

IoT connection points such as sensors are very small, and are rapidly becoming even smaller. While these form factors are ideal for organizations that want to embed IoT functionality into a broad range of applications, it's important to keep in mind that IoT devices have limited physical and virtual space for traditional cybersecurity tools.
This makes it very difficult to overlay security on top of IoT devices—and especially after the deployment and roll-out of these IoT devices. As a result, organizations must design IoT-centric cybersecurity into systems from the very beginning. They should also be tightly integrated with the Zero Trust framework already built into data centers, networks, cloud connections, and mobile endpoints.

Similar concerns apply to larger and more complex IoT devices, like video security cameras. These IoT devices have the advantage that some cybersecurity tools can be installed within them. However, this is only possible when the IoT devices are produced with security in mind. This means that security should be built into the device during the complete production process (from the conceptual phase through the delivery phase),. This is often referred to as "Secure-by-Design."

HOW TO DEPLOY VIDEO SURVEILLANCE IN A ZERO TRUST ENVIRONMENT

In a changing digital world with enterprises and organizations migrating to cloud and distributed work environments, IT security has never been more paramount. Increasingly, enterprises that deploy Zero Trust cybersecurity frameworks are at a competitive advantage as cyber threats increase. Customers, partners, and stakeholders expect stricter safeguards for their IT environments, assets, and data.

ZERO TRUST AS AN ENABLER

Several organizations and governments use Zero Trust as an argument to exclude other organizations from their business or activities. However, this is not necessarily the meaning nor intention of the Zero Trust framework and its applications. Zero Trust can comprehensively secure organizations and their businesses in a way that traditional security models struggle to achieve, by requiring authentication and clear access policies for all users, as well as ensuring trust is not granted without verification. Zero Trust is not necessarily developed to exclude others, but is instead developed to ensure a complete framework for securing an organization's computing infrastructure and the ecosystem from near-constantly evolving threats and cyber risk. This ensures that risks to the business are minimized, and security can become a business enabler.

THE ADOPTION OF ZERO TRUST WITHIN THE VIDEO SURVEILLANCE INDUSTRY

Zero Trust is an accepted concept within the IT industry and is now also slowly moving into the physical security domain. One reason for this development is the convergence of IT security and physical security.

Hikvision, an IoT manufacturer with a focus on video surveillance, recognizes this convergence and views cybersecurity as an absolute imperative for its business. Hikvision strives toward a fully visible ecosystem by maintaining transparency about Secure-by-Design production processes, regularly executing internal and external penetration testing, reviewing the supply chain consistently, and monitoring all software/hardware development processes of all products. Cooperation with suppliers and partners is essential for achieving the required visibility and transparency.

HOW TO DEPLOY ZERO TRUST ACROSS VIDEO SURVEILLANCE IN FOUR STEPS

As mentioned before, the adoption of the Zero Trust concept within the video surveillance industry is fairly new worldwide. Here are four steps that show how Zero Trust can be deployed pragmatically within the video surveillance industry.

1. Know your business

- Start by listing how a video surveillance system will help the organization
- Think of how the video surveillance system may interface with other business and systems in the organization
- Try to list all stakeholders and how they may use or interact with the video surveillance system
- Think of all the risks associated with the video surveillance system and the severity, then think of ways to mitigate the risks

2. Design a secure network

- Group video surveillance equipment in a segmented network environment, isolated from the organization's other systems (payroll, accounting, HR, CRM, R&D, etc.)
- Define possible groups of users who may access the video surveillance system
- Define the location and time for each group of users to access the video surveillance system

3. Implement a secure network

- Place all video surveillance equipment in a dedicated and segmented network behind a router and a firewall
- Define deny-all-IP-and-Port in the firewall ruleset, and then open only the local IP addresses and ports that need to access the video surveillance system. Also, open IP addresses and ports of other systems that need to interface with the video surveillance system
- Use a VPN-capable router or firewall for remote access to the video surveillance system
- Institute multi-factor authentication for remote access and cross-system access
- Implement a network monitoring system and/or IDS/IPS system to set up alerts if the video surveillance system is not accessed at a pre-determined period and location
- Use switches and routers that restrict and monitor port usage for enhanced security
- Encrypt all storage data

4. Configure a secure video surveillance system

- Configure 802.1x for video surveillance devices
- Configure and whitelist all IP addresses and MAC addresses that have the need to access the video surveillance system
- Enable HTTPS and restrict only TLS 1.2 or higher for transmission from/to video surveillance devices with enhanced encryption
- Set illegal login attempts to lock up devices
- Disable SSH to prevent shell login to all video surveillance devices

EFFECTIVE ZERO TRUST WITHIN THE VIDEO SURVEILLANCE INDUSTRY

By following these four steps, Zero Trust can be deployed successfully within the video surveillance industry, resulting in the following:

- All users have been predefined and prescreened
- Users must use VPN to access video surveillance remotely
- Only predefined systems are allowed to interface with video surveillance
- Multi-factor authentication is required for remote access and cross-system access
- No other network packets are allowed other than video surveillance (defined by firewall)
- Unusual logins are monitored and alerted

Does taking these steps to implement Zero Trust guarantee 100 percent security? The answer is no. Unfortunately, it is impossible to guarantee absolute security. But, Zero Trust will improve the overall cybersecurity significantly and provide all stakeholders within the IoT industry more visibility on what's happening in their network, and more control over access, so that they can act accordingly amidst a growing threat environment. In this way, Zero Trust contributes to a more secure IoT world. As more organizations adopt Zero Trust principles, malicious actors will find it increasingly harder to conduct attacks and increasingly difficult to conduct malicious activity without being identified and remedied.

Hikvision USA Inc.
18639 Railroad Street
City of Industry, CA 91748

Hikvision Canada Inc.
4848 Levy Street
Saint-Laurent, Quebec H4R 2P1

Hikvision Europe
Dirk Storklaan 3
2132 PX Hoofddorp, The Netherlands

Contact Information
Toll-Free: +1 866-200-6690 (U.S. and Canada)
Phone: +1 909-895-0400
Email: sales.usa@hikvision.com
hikvision.com

Connect with us:

HIKVISION®