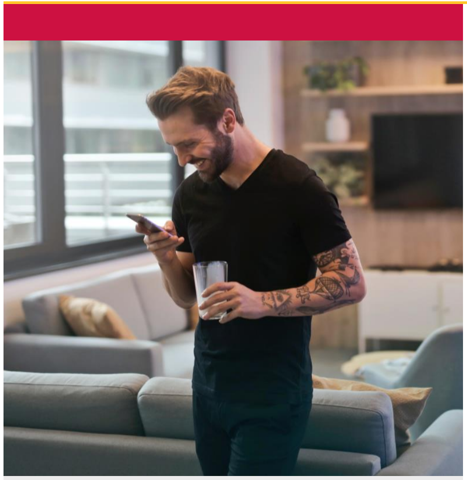
UNISYS | Securing Your Tomorrow®

SETTLING TOP CONSUMER SAFETY CONCERNS WITH ZERO TRUST SECURITY



In dynamic online environments, a Zero Trust security model is gaining popularity as a common sense approach to cybersecurity.

Growing Concerns Over Digital Threats

People around the world worry about cybersecurity more than anything else today. The 2019 Unisys Security Index reveals that the top four security concerns worldwide are all online and digital. People are more concerned about losing their identity or financial information than they are about war, terrorism or natural disasters.

According to the survey, respondents from countries across the globe express that they are “extremely concerned” or “very concerned” about cybersecurity risks:

1. Identity theft – 69 percent
2. Bankcard fraud – 66 percent
3. Hacking/viruses – 63 percent
4. Online shopping – 57 percent

While technology makes daily life more convenient, flexible and accessible for users, it also introduces new attack vectors for exploitation–with potentially grave consequences such as loss of money, privacy and safety. Doing business in the digital economy now involves providing assurance to users that they are secure online.

Evaluating Security Posture

Today’s organizations must honestly evaluate and prioritize digital trust:

- Are critical assets adequately protected from online threats?
- Does the organization have the right security controls in place?
- Can customers trust their personal information will not be compromised?
- Is the organization communicating safeguards to users?
- Are security concerns eroding brand reputation and business results?

Traditional perimeter security can’t scale with constantly evolving digital business requirements and cybersecurity threats. In dynamic online environments, a Zero Trust security model is gaining popularity as a common sense approach to cybersecurity.

Implementing Zero Trust

Zero Trust addresses the inadequacies of traditional security measures by assuming the entire IT ecosystem is already compromised. As network perimeters dissolve with the fluid access requirements of digital business, Zero Trust authenticates users and devices on a least-privilege, need to know basis–protecting data wherever it goes. It emphasizes microsegmentation to isolate critical assets, limiting damage in the event of a breach. And it promotes automation to quickly detect suspicious activity and allow systems to dynamically isolate and self-heal under attack.

Framing Zero Trust investments in economic terms minimizes the risk of incorrectly estimating the resources required to secure data, information and application flows.

In dynamic online environments, a Zero Trust model provides a commonsense approach to cybersecurity. Here are the five steps required for taking Zero Trust from concept to reality:

1. Prioritize
2. Protect
3. Predict
4. Isolate
5. Remediate

Prioritize Cybersecurity Risks

With security concerns at their highest recorded level, businesses need to prioritize allocating resources to address security risks. By starting with full ecosystem visibility, organizations can see and decide where best to invest their resources, quickly and quantitatively selecting projects with the greatest ROI, or fastest ROI, to Zero Trust.

The first step towards implementing Zero Trust is to adopt a strategy that aligns the security investment with the risk profile of the organization. Identifying which threats have the greatest potential impact and the security controls that reduce the most risk for the business, are the underpinnings of an effective cybersecurity program that spends enough — and not more — to achieve the required level of protection. This provides a defensible security position while also maximizing investments in growing the business and providing value to customers.

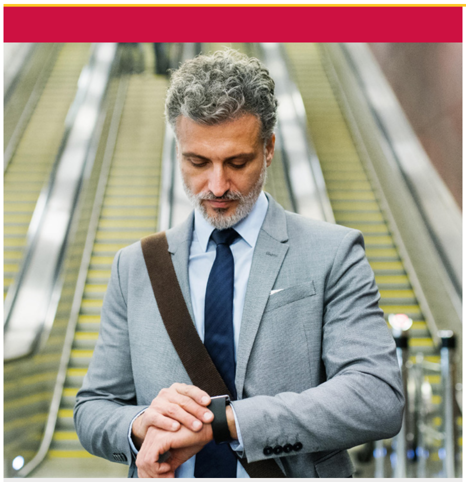
With a detailed understanding of the IT ecosystem and associated risks, organizations can more accurately assign value to technology investments, anticipating the business impact of a breach. Framing Zero Trust investments in economic terms minimizes the risk of incorrectly estimating the resources required to secure data, information and application flows.

Protect Vulnerable Assets

Starting with the most valuable or vulnerable assets, Zero Trust can be rolled out to reduce the attack surface and address threats with the greatest potential impact and maximize risk reduction for the business. Most of the top security concerns identified by the Unisys Security Index are resolved by properly shielding sources of personally identifiable information (PII) and payment details.

To strengthen security posture, endpoint exposures and high-value assets must be protected first. Limiting access to unsupported infrastructure such as legacy systems, high-value data such as personally identifiable information, payment card information and privileged accounts such as IT administration minimizes the impact of a security breach.

Zero Trust access rights establish identity-driven protection that accommodates the fluctuating nature of interactions between employees, partners, suppliers and customers, where access levels must be adjusted based on time, location or data. Organizations can leverage existing identity management systems to grant user access rights based on identity, behavior, and intent. With identity-based access, it’s easier to spot rogue connections, block lateral movement of unauthorized users and guard privileged user devices from malware attacks.



Zero Trust aims to solve the problems of an overly trusting fixed perimeter system by assuming that a threat is already inside the network. Organizations contain the damage from a rogue user or network breach with isolation of important systems and data.

Predict Online Threats

Cybersecurity threats are constantly evolving and 63% of surveyed consumers are concerned with hacking and viruses, making this a top concern for organizations and consumers to address. Organizations can stay ahead of growing threats and strengthen risk posture with predictive threat prevention and objective cyber-risk forecasts powered by machine learning and artificial intelligence (AI).

Security intelligence gathered from users, endpoints and systems identifies suspicious activity and automatically adapts policies. Automating routine security tasks through advanced analytics offloads internal resources to maintain a Zero Trust security posture.

Identity-driven, certificate-based authentication extends trust to devices and enables privileges to be revoked instantly if compromised or presenting suspicious activity, limiting the impact of an attack. In addition, adaptive rights management allows nation-states to adjust access to resources, services and borders based on irrefutable identities through multimodal authentication.

Isolate the Critical

Concern over unauthorized access to, or misuse of, personal information is another top consumer concern. Zero Trust aims to solve the problems of an overly trusting fixed perimeter system by assuming that a threat is already inside the network. Organizations contain the damage from a rogue user or network breach with isolation of important systems and data.

Identity-driven microsegmentation protects through dynamic isolation of critical assets and devices. Redefining fixed perimeters into much smaller, targeted microsegments provides the flexibility to protect individual workloads, users and datasets with constantly evolving security postures.

A secure digital experience ensures trusted transactions are safe from threats by isolating them from untrusted and suspicious users. Communities of interest (COI) with encrypted communications between employees, customers and partners, establishes a secure channel for exchanges. The impact of misused administrative credentials or a dangerous threat on the inside is mitigated by shielding vulnerable systems and critical assets from unauthorized users, rendering them unresponsive to illegitimate or unusual activities.

Remediate Breaches Quickly

As with any other safety matter—natural disasters, criminal activities, terror attacks—developing a plan and practicing it will make responding to the event faster and more successful. Reducing the response time to a cybersecurity breach minimizes the operational impact.

Cyberattacks are inevitable. Organizations must be prepared by containing breach impact with flexible, intelligence-powered security solutions that dynamically isolate and protect critical assets. Resilience means containing and mitigating attacks while protecting important systems, data and access—such as order fulfillment, power generation or customer service—minimizing operational downtime.

Managed security services help organizations stay ahead of emerging cyberthreats and stop them fast when they strike. By establishing best practices in incident response, conducting preparedness exercises and evaluating threat and endpoint security, organizations can move quickly in the event of a breach. Security automation and managed services also enable internal security professionals to plan a long-term Zero Trust strategy instead of being sidetracked by the next attack.

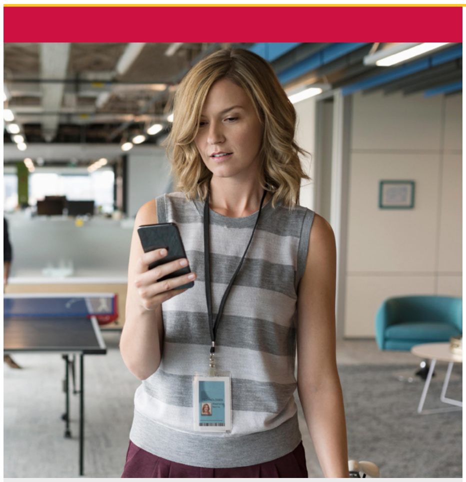
Unisys Is Zero Trust: Implemented

Unisys partners with leading commercial and government organizations worldwide to design, build and maintain Zero Trust security architectures. Adhering to the five-step methodology—prioritize, protect, predict, isolate and remediate—Unisys delivers a start-to-finish Zero Trust implementation.

With identity-driven microsegmentation to isolate critical data and systems, Unisys identifies, validates and secures trusted users, devices and data flows. When fixed policies fail to protect dynamic digital transformations, Unisys Security Solutions create microperimeters and adjust access rights the moment a breach is detected, or an insider is compromised.

Unisys monitors, manages and adapts a Zero Trust architecture through an automation-powered security operations center (SOC)—tuning policies, patching vulnerabilities and updating security controls or privileges for the resilience required to respond and recover quickly from a cyberattack. When a breach occurs, immediate, dynamic isolation quarantines the suspicious user or system, to limit east-west damage.

Outsourcing routine security tasks to a trusted security partner allows organizations to focus on building their business and brand. And when Zero Trust is designed by the same partner that creates and manages digital cloud and workplace services, security is woven into the fabric of technology, processes and culture.



Unisys monitors, manages and adapts a Zero Trust architecture through an automation-powered security operations center (SOC)—tuning policies, patching vulnerabilities and updating security controls or privileges for the resilience required to respond and recover quickly from a cyberattack.

For more information about how Unisys security solutions can help you address today’s cybersecurity concerns visit www.unisys.com/security.

For more information visit www.unisys.com

Printed in the United States of America 06/19 19-0255