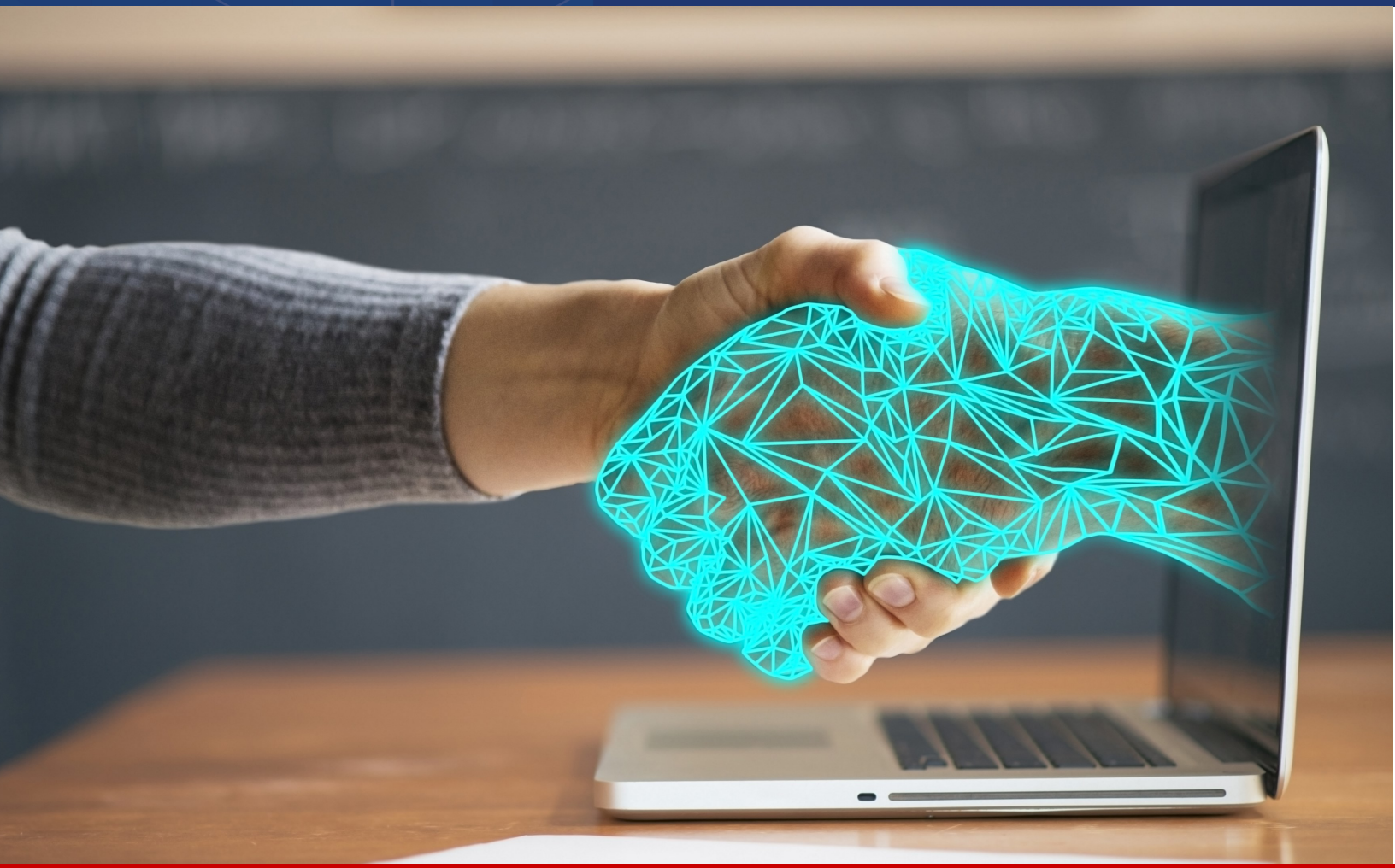
Is Zero Trust Right for Your Business?

Examine what zero trust is and dig into its pros and cons, and uncover its alternatives.



844.638.7328 | SALES@SECNAP.COM | SECNAP.COM

SECNAP NETWORK SECURITY

SECNAP NETWORK SECURITY

What is Zero Trust?

Zero trust has many benefits, but it's not the right security model for every business. This paper will examine what zero trust is, examine its pros and cons, and discuss alternatives.

Zero trust is a strategic security model that was developed as a modern alternative to the traditional "castle and moat" model.

Under castle and moat, all users and devices located inside a network perimeter are implicitly trusted; those outside the perimeter are not and must authenticate each time they attempt to access network resources. The success of "castle and moat" depends on the existence of a clearly defined network perimeter – something that no longer exists due to the increasing use of cloud computing, Internet of Things (IoT) devices, and distributed work.

In contrast, zero trust eliminates implicit trust. Instead of focusing on **where** users are, it focuses on **who** they are. A user accessing organizational resources from their home or a hotel room, using their own device, is treated no differently than if they were on company property, using a company-provisioned device.

Zero Trust Core Pillars

Cybersecurity has been struggling with the recent shifts in digital transformation, remote workers and the blurry lines of personal/work mobile devices.

Here are three core pillars that are considered when implementing zero trust:

Assume breach. Any user or device could be compromised, even if they're connecting from inside the organization's office.

Verify explicitly. All users and devices must prove that they are who they say they are before they can access network resources.

Ensure least-privilege. All users and devices must be granted the minimum level of network access necessary.

V22..1

SECNAP NETWORK SECURITY

Benefits & Drawbacks of Zero Trust

According to Verizon, compromised credentials cause over 80% of successful data breaches. When implemented correctly, zero trust greatly reduces this risk.

Additionally, IT administrators obtain full visibility into all users, systems, and devices in their data environments. Administrators can see exactly who's connecting to the network, from where, and what resources they're accessing. Users and devices cannot access the network at all until they are verified explicitly. If a threat actor does manage to compromise the network, privilege escalation is much more difficult.

However, as effective as zero trust is, it has some significant drawbacks, particularly if an organization does not have the internal resources to properly implement and maintain it. These include:

Massive Time Commitment

Zero trust experts often point out that zero trust is a marathon, not a sprint. What they fail to mention is that it's also a race with no finish line.

Because zero trust requires organizations to rework their entire security model, it takes quite a bit of time to implement. It also requires perpetual ongoing maintenance. Access control lists do not maintain themselves. Network segmentation and micro segmentation must be reviewed, and possibly reworked, each time the data environment changes. Users, devices, and applications must be micromanaged.

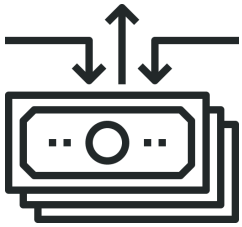
Potential Security Gaps

If a zero trust security model is not implemented properly and maintained diligently, organizations can be left with significant security gaps.

One of the biggest potential gaps involves insider threats. While strict authentication and least-privilege access significantly reduce the risk of insider threats, employees could still fall prey to phishing and other social engineering techniques. A comprehensive zero trust model must include a robust identity and access management (IAM) stack that includes an enterprise-grade password manager and multi-factor authentication (MFA).

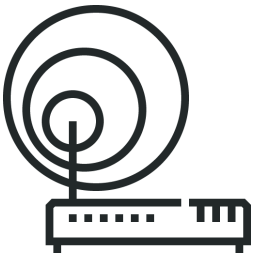
Additionally, if employees find zero-trust procedures too cumbersome, they may seek ways to circumvent them, which leads to the next drawback.

Benefits & Drawbacks of Zero Trust (Continued...)



Potential Impacts on Business Productivity

By its nature, zero trust adds extra security steps to workflows. It is easy to say that all users should be granted only the minimum network access needed to do their jobs, but it is extremely difficult to make this a reality without compromising productivity. Access control lists (ACLs) must be precisely defined at all times. This impacts both the IT staff, who must maintain the ACLs, and end users, who could run into problems if they do not have the access they need to complete their tasks.



Technical Debt, and Lots of It

A zero trust security model requires secure hardware. Organizations must be prepared to patch or update their existing equipment, and in some cases, replace it altogether. This is a tall order for budget-strapped small and medium-sized businesses (SMBs). Sometimes, even if an organization can afford to replace their old equipment, it is not feasible to do so, as they are dependent on the hardware to run legacy line-of-business systems and apps that cannot be realistically refactored or replaced.

Zero-Day Attacks Remain a Risk

Zero trust is heavy on credential protection. While compromised and stolen credentials are responsible for most data breaches and ransomware attacks, they are not the only cyber threat organizations face.

"Zero-day" is an umbrella term for a software or hardware vulnerability that was discovered so recently, the vendor hasn't had time to release a patch for it yet. Hence, the vendor has "zero days" to fix it before an attacker can take advantage of it. Some of the largest ransomware attacks to date were caused by zero-day exploits, including the Kaseya supply chain attack.[1]

Since threat actors do not necessarily need to depend on stolen credentials to exploit a zero-day vulnerability, zero trust is an imperfect solution for defending against this particular threat.

[1] https://thehackernews.com/2021/07/revil-used-0-day-in-kaseya-ransomware.html

CloudJacketXDR: Your Zero Trust Alternative

If it seems like a zero trust security model is not the right choice for your organization, there is an alternative. SECNAP's CloudJacket XDR platform is based on a layered defense, which combines improved protection, enhanced detection capabilities, and a cost of ownership that is affordable for even small and mid-market companies.

CloudJacket XDR provides a unified security incident detection and response platform that collects and correlates logs and other data from network devices. Leveraging our SIEM technology, these logs and other data sources are normalized, digested through our patented and patent-pending alert logic engine, then sent directly to our security operations center (SOC). This enables our SOC analysts to provide security threat detection faster and more effectively than competing SIEM technology, with lower mean time to detect (MTTD) and mean time to respond (MTTR). Our SOC analysts are able to review 99% of alerts without client intervention, which prevents your team from being inundated with false positives and suffering "alert fatigue."

CloudJacket XDR is an ideal solution for organizations that want to implement zero trust, but do not have the resources to properly maintain it.

Not ready to decide?

Start with a Security Assessment to get a clear view of your organization's security posture. Reducing your attack surface and closing gaps is always a good first step.

SECNAP NETWORK SECURITY

Get a complimentary and customized consultation regarding your organization's cybersecurity strategy.

About SECNAP Network Security

Since 2001, SECNAP Network Security has been combining human intelligence with innovative technology to protect organizations of all sizes against cyber threats, including data breaches, ransomware, phishing, and advanced persistent threats (APTs). Our proprietary, patented and patent pending CloudJacketX managed security-as-a-service platform addresses common pain points faced by IT teams, such as alert fatigue, challenges with meeting regulatory compliance requirements, lack of resources, and hidden vulnerabilities.

SECNAP's proactive cybersecurity approach combines ongoing network security assessments with managed detection and response (MDR) services, an advanced SIEM solution, and a patented intrusion detection and prevention system (IDS/IPS) to provide multiple layers of detection and protection, which are monitored 24/7 by our U.S.-based security operations centers (SOCs). SECNAP utilizes proprietary security technologies that were developed in-house.

AICPA SOC

GSA Advantage!