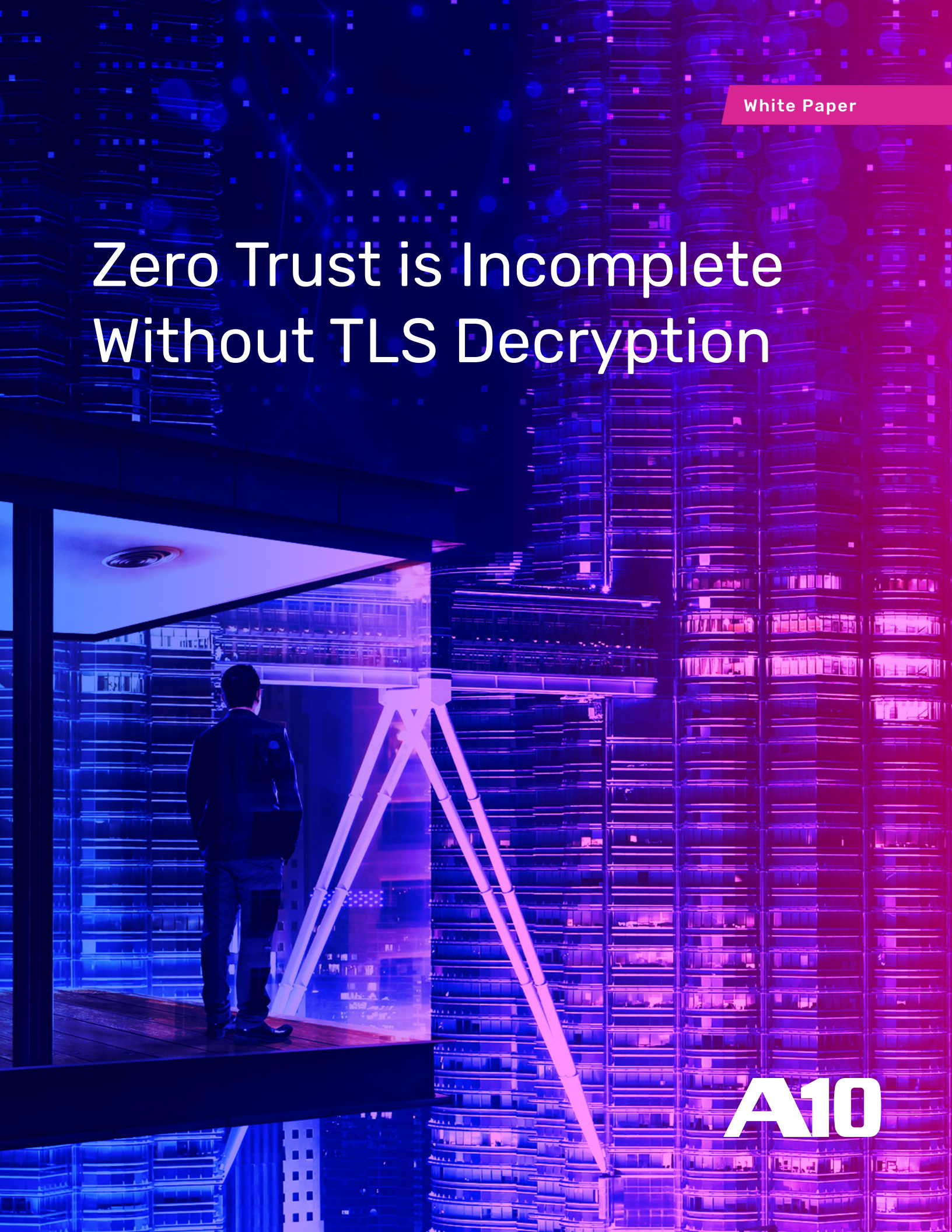
White Paper

Zero Trust is Incomplete Without TLS Decryption



A10

Table of Contents

Executive Summary

Modern cyberattacks are not limited to just network intrusion from the outside. Internal threat actors can often be found at the center of sophisticated attacks.

The Zero Trust model, based on the simple principle of "trust nobody", defines rules which enhance the security of networks against attacks, whether they are initiated from the outside or within. However, with the rise of encryption of internet traffic, it is becoming increasingly difficult to implement the Zero Trust model in an effective way.

In this white paper, readers will learn about modern cyber threats, what the Zero Trust model is and how it can be used to protect users and data against such attacks, the role of visibility in the implementation of Zero Trust and how TLS decryption is essential for the implementation of a fool proof Zero Trust strategy.

Insider Threats

In the past, defending yourself and your sensitive assets was simple – you had a general idea who your enemies were, from where they might attack, and what weapons they might use.

It is analogous to putting all your key assets inside a castle, building strong walls and moats around them, and defending the barriers with all available resources. Defensive strategies were built around this concept for centuries. Throughout history, we have seen that such defenses failed whenever there was sabotage from the inside, made possible by "insiders" with malicious intent. However, there have also been instances where attacks and breaches were made possible by insiders who weren't necessarily aware of the threats. They were bringing in, as in the example of ancient Troy, the Trojan Horse that was used to invade the city.

Fast forward a few thousand years, into the age of the internet, and we're facing similar problems, but in a different context. In a world where everything and everyone is connected, in one way or another, to the internet, it's hard to imagine a network that is truly secure. Data, large amounts of it, are at the center of it all. With industries from healthcare to the education sector to the government using the internet to provide easy access to data, it is no wonder that cybersecurity teams are always working around the clock to try and come up with better ways of defending these networks and the data they store.

Figure 1: The original "insider" attack, made successful by unaware Trojans

The Need for Rethinking Cybersecurity

Initially, we had the concept of zones, perimeters and network segments – placing all the protected assets "inside" the secured network perimeter. However, attackers are always evolving the methods they use; always on the lookout for weak points in your network defenses; and coming up with newer ways of infiltrating the perimeter. Keeping up with them is a challenging and ongoing struggle.

We also need to realize that the "castle and moat" approach to our network defenses was mostly effective against threats that resided outside the network. But what about the threats on the inside? What about modern attacks that work on multiple levels to try to bring your networks down? How do we protect our networks from people who have legitimate access to all its resources? How do we battle the ever-growing and ever-evolving modern cyberattacks?

Add to these questions, regulations like GDPR, and the rising fines, and you will see that having your networks attacked and data breached is one of the worst things that can happen to your company.

With these issues as the backdrop, we are forced to re-assess and re-think the way we defend our networks, users and data.

Zero Trust and Modern Cybersecurity

Zero Trust attempts to fix the problems, and patch the holes, in our cybersecurity strategies. At the core of it, the Zero Trust model is based on the principal of "trust nobody." The Zero Trust model dictates that no one in your network should be trusted completely, that access should be restricted as much as possible, and that trust should be seen as yet another vulnerability that can put your network at risk.

According to Forrester's Dr. Chase Cunningham, one of the main advocates of the Zero Trust model, "most of them (cyberattacks) began with the failure of a few basic security controls and the inevitable lateral movement of attackers." It is evident that we need a better approach and the Zero Trust model promises to deliver just that.

The Zero Trust model dictates that:

- Networks need to be redesigned in a way that east-west traffic and access can be restricted. This can be done by creating micro-segments and micro-perimeters within the network.
- Incident detection and response should be facilitated and improved using comprehensive analytics and automation solutions, as well as centralized management and visibility into the network, data, workloads, users and devices used.
- Access should be restricted as much as possible, limiting excessive privileges for all users.
- In multi-vendor networks, all solutions should integrate and work together seamlessly, enabling compliance and unified security. The solutions should also be easy to use so that additional complexity can be removed.

Going forward, basing our security strategies on the Zero Trust model is essential.

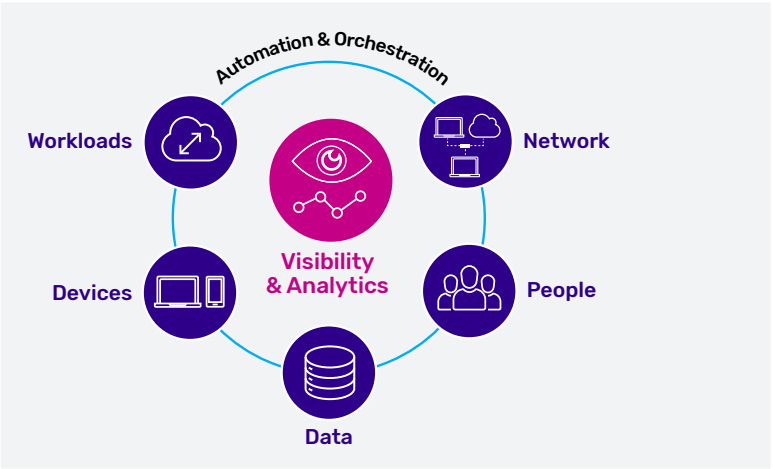


Figure 2: With Zero Trust, visibility is everything – Visibility across the network, data, workloads, people and devices

Visibility, Encryption and Zero Trust

In recent times, we have witnessed a phenomenal rise in the use of encryption across the internet. Google reports that over 90 percent of the traffic passing through its services is encrypted. The same is true for all the other vendors. This rise has been driven by many factors, including privacy concerns.

However, with encryption comes the creation of a "blind spot" in our network defenses as most of the security devices we use are not designed to decrypt and inspect traffic. The Zero Trust model is not immune to this problem as visibility is considered as one of the key elements to its successful implementation. Without complete encrypted traffic visibility, the model will fail, introducing vulnerabilities that can be exploited by both insiders and hackers.

A centralized and dedicated decryption solution must be placed at the center of the Zero Trust model and should be included as one of the essential components your security strategy.

Many security vendors will make claims of the ability to decrypt their own traffic, working independently of a centralized decryption solution. However, this "distributed decryption" approach can introduce problems of its own, including inferior performance and network bottlenecks, and fixing these would require costly upgrades. In a multi-vendor, multi-device security infrastructure, the distributed decryption also forces you to deploy your private keys in multiple locations, creating an unnecessarily large threat surface in your network, which could be subject to exploitation.

Thunder SSL Insight – Enabling Zero Trust

A10 Networks' Thunder® SSL Insight® solution is a dedicated, centralized decryption solution that provides full visibility to the enterprise security infrastructure for TLS/SSL traffic. Not only that, but the solution also provides a multi-layered security approach, which makes it the perfect candidate to be deployed at the center of a Zero Trust network.

SSL Insight enables the Zero Trust model in more than one way, including:

- **Full Traffic Visibility** – It enables the entire security infrastructure to inspect all traffic in clear-text, at fast speeds, ensuring that no encrypted attacks or data breaches can slip through. Working with a "trust nobody" and "decrypt once, inspect many times" mindset, the solution intercepts all traffic and makes sure it is decrypted and sent to the correct security devices within our secure decrypt zone.

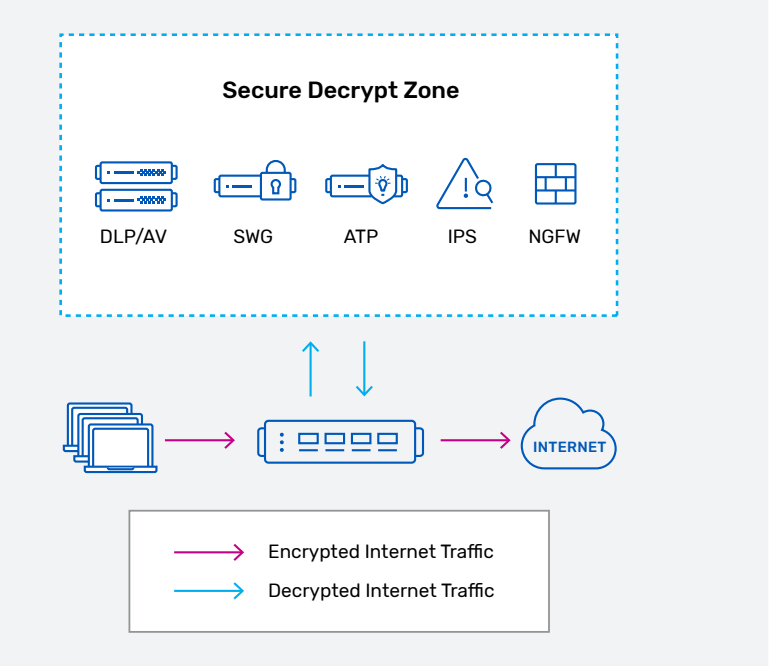


Figure 3: SSL Insight "trusts nobody" and enables inspection of all traffic in the secure decrypt zone

- **Flexible Deployment and Integration** – Since it is vendor agnostic, SSL Insight can easily integrate with security devices already deployed within the network by placing them in a secure decrypt zone, driving down the need for additional costs and upgrades.

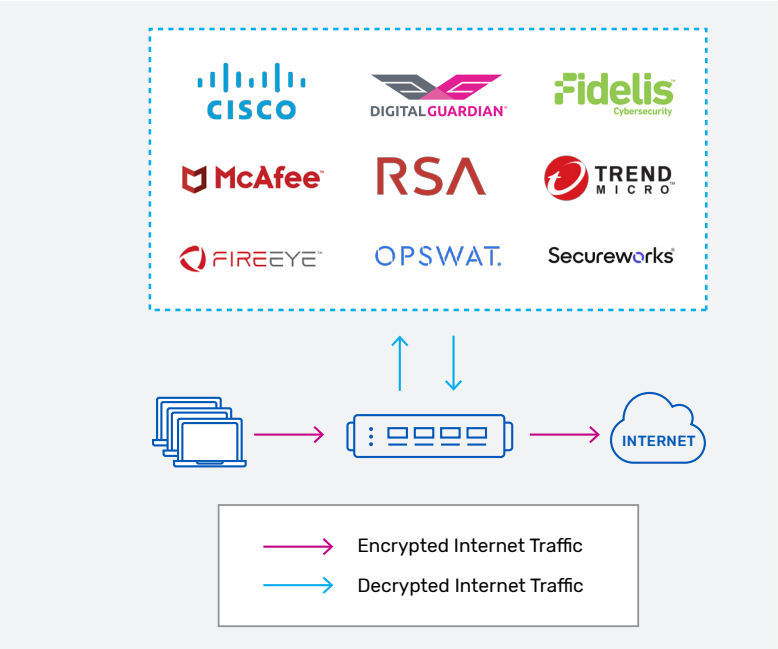


Figure 04: SSL Insight is vendor agnostic and can easily integrate with all kinds of security devices

- **Multi-Layered Security Services** – These are additional security services, including URL filtering, application visibility and control, threat intelligence and threat investigation, that help strengthen the security efficacy of the entire enterprise network.
- **User Access Control** – SSL Insight can enforce authentication and authorization policies to restrict unneeded access, log access information and provide the ability to apply different security policies based on user and group IDs.
- **Micro Segmentation** – SSL Insight facilitates micro-segmentation in many ways, thanks to its ability to provide granular traffic control, user and group ID-based traffic control, and support for multi-tenancy.
- **Enabling Compliance** – SSL Insight protects users and data from costly data breaches, ensuring that they remain compliant with regulations like GDPR. At the same time, with granular traffic control, it ensures that users are compliant with standards like PCI-DSS and HIPAA.
- **Securing Cloud Access** – SaaS security, primarily for, but not limited to, Microsoft Office 365, is provided by enforcing tenant access control and visibility into user activities.
- **Centralized Management and Analytics** – Uniform security policies can be enforced across all SSL Insight deployments with A10 Harmony Controller. The solution also provides full visibility into all deployments, no matter where they are, as well as detailed shadow IT and SaaS traffic visibility, which can help define a better security strategy.
- **Ease of Use** – With the help of A10 Harmony® Controller and AppCentric Templates (ACT), the SSL Insight solution can be deployed, within minutes, in any network environment, without causing any network outages or disruptions, making it the easiest decryption solution available.

Conclusion

Without centralized and dedicated TLS/SSL decryption solutions like SSL Insight, the Zero Trust model is unable to do what it was designed to do – protect our networks, users and data from threats residing inside and outside the network. SSL Insight provides a complete solution that not only enables the inspection of all incoming and outgoing traffic, but also provides additional security services that can help strengthen your Zero Trust strategy, so your network does not have the same fate as ancient Troy.

To learn more about SSL Insight, visit https://www.a10networks.com/solutions/network-security/ssl-inspection/

About A10 Networks

A10 Networks (NYSE: ATEN) enables service providers, cloud providers and enterprises to ensure their 5G networks and multi-cloud applications are secure. With advanced analytics, machine learning and intelligent automation, business-critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers in 117 countries worldwide.

For more information, visit: a10networks.com or tweet @a10Networks

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-WP-21163-EN-01 APR 2020