O2 business

DEMYSTIFYING ZERO TRUST

We're pleased to share this research report conducted and written by our partner, Sophos

A Sophos white paper July 2020

Telefónica

SOPHOS

SOPHOS

Demystifying Zero Trust

The age of the corporate network and single security perimeter is coming to an end. Users are increasingly working remotely, conducting their work over the public internet. The rise of Software-as-a-Service (SaaS) apps, cloud platforms, and other cloud-based services has eroded the efficacy of using the network as the primary element to secure a resource. We can no longer rely on a single, sealed-off corporate network and afford trust to all the systems that reside within it as the boundaries between networks are now blurred.

Enter zero trust; a cybersecurity philosophy on how to think about security and how to do security. Zero trust is based upon the principle of "trust nothing, verify everything" and focusing on protecting resources regardless of where they are physically or digitally and to never trust anything by default.

No one vendor, product, or technology will get you to zero trust. Rather it requires a cultural shift and a lot of different solutions to shift the paradigms by which we secure our resources.

This paper looks at the concept of zero trust, the benefits of implementing a zero trust model, and provides guidance on the steps that organizations need to take to transition towards it.

Times have changed

Trust is a dangerous word in the information technology field, especially when that trust is implicit - when it's unqualified or unquestioned.

Creating a large, sealed-off corporate network security perimeter and trusting everything inside of it has proven time and again to be a flawed design. These soft, chewy centers are a hacker's dream. Once inside, they're often invisible. Spreading across the network, accessing important systems, and more is trivial as the security controls and strongest checks are only at the perimeter.

Whether you like it or not, the perimeter has been eroded.

Users want to work remotely, on untrusted networks like the public Wi-Fi at a coffee shop. They want their data stored in the cloud so they can access it whenever they need to. They want to use or use their own personal devices to access corporate data and resources. Frictionless access is demanded by our users so that they can work whenever, wherever, and however they desire.

The use of software-as-a-service (SaaS) apps, cloud platforms, and other cloud-based services leaves data outside of the corporate perimeter, and public cloud platforms mean many of the devices or services once run within the corporate perimeter are now run outside of it. Our workloads are moving to wherever is most cost-effective to process them, away from networks we own, control, and trust.

Everything is everywhere. The old "corporate network" model with static defenses fails to empower businesses to embrace things like the cloud while simultaneously protecting their data, their users, and their customers. A paradigm shift is required.

Enter zero trust

Zero trust is a holistic approach to security that addresses these threats and changes in how businesses work. It's a model and a philosophy for how to think about and how to do security.

No one and no thing should be automatically trusted, be it inside or outside of the corporate network, even the network itself. Implicit trust based on network location, with static defenses like a traditional firewall, must be limited.

Eventually something needs to be trusted, but with zero trust, this trust is temporary and established dynamically from multiple sources of data, more than we've ever used in the past, and it is constantly re-evaluated. Sources of data includes information about the access request itself, user information, system information, access requirement information, and threat intelligence. Furthermore, access to data and/or resources is only granted as and when required, on a per-connection basis.

We've plenty of experience with untrusted networks through our daily use of the internet. Computers that face the public internet are secured in a very different manner to those inside the traditional perimeter, requiring extra scrutiny and layers of defense to protect them from external threats.

The zero trust model guides you to treat all devices as if they were internet-facing and, instead of having one single perimeter, you must create many micro perimeters (or microsegments), applying checks and controls around everything and between everything.

The core benefits of adopting zero trust

Adopting a zero trust model brings innumerable benefits, so, to make your life easier, we've picked out some of the core ones.

Control of the entire IT estate

From inside the office all the way to the cloud platforms you use. No more lack of control outside the corporate perimeter or struggles with remote users.

Manage and secure all users in the same way

By no longer seeing things as inside or outside the corporate perimeter, you can treat all users in the same way. This both simplifies IT security while also ensuring all devices and users are treated equally.

Maintain security even when you don't own/have full control over the infrastructure in use

By using identity, location, device health, MFA, and overlaying monitoring and analysis, you're still able to have strong security across any kind of environment, platform, or service.

Drastically reduce the movement of malware or attackers

Rather than having free rein of the entire network once they're inside, attackers only have access to the bare minimum of systems the compromised user had access to. By continuing to distrust the authenticated user, checks will be in place between those systems, further limiting the ability to spread.

A summary of zero trust

Zero trust is a big idea, and there is a lot of evolving discussion around it. At its essence, we can condense the major concepts for zero trust into several proverbs that you should keep in mind along your journey.

There is no "inside" the network

Pretend that you're running your entire business from an untrusted location, like a coffee shop's public Wi-Fi, and that all your devices are connected directly to the most dangerous of all networks: the public internet. By imagining this as your reality, you're forced to apply security in ways where you can't rely on being behind a traditional corporate perimeter.

There will always be corporate "trusted" networks for administration and in-house systems, but the goal is to keep ordinary users off these networks, using application proxies and other technologies, drastically reducing the attack surface.

Trust nothing, verify everything

Assume that there are attackers both on the inside of your networks and on the outside and they are there all the time, constantly attacking. No user or device should be automatically trusted and should authenticate itself before a connection can even be considered. By imagining you're under constant attack from every direction, you are pushed to build rock-solid authentication and authorization to your resources, layer your defenses, and constantly monitor and analyze everything happening across your estates.

Security should adapt in real time

The security policies you put in place to achieve zero trust should be dynamic and automatically change based on insight from as many sources of data, from as many different technologies as possible. A static policy like "THIS USER" on "THIS DEVICE" can access "THIS THING" won't protect you if that device has been compromised while that user is on it. If your policy also took into account device health, such as the identification of malicious behaviors, your policy could use this to dynamically adapt to the situation with zero effort from an admin.

This has been a part of Sophos' strategy and philosophy for cybersecurity for a long time. You might know it as Synchronized Security, where our products can share the unique insights they each have with one another. This enables us to have adaptive, dynamic policies, taking advantage of all these insights so that a policy is never static and easily circumnavigated.

Much of this is just good security policy and best practices which you may already be doing and if you've prepared for GDPR, you've done a lot of this work already.

Principles of zero trust

Trust nothing. Ever. For when you trust nothing, you are forced to seek relevant security measures wherever there is a risk.

Verify everything. Do not assume that passing a check naturally affords trust. Having credentials doesn't mean you are trustable. It just means you have credentials. And credentials can be stolen.

We can break this into four simple principles to keep in mind.

Always identify

You need a singular, authoritative source of identity and use it everywhere with Single Sign On (SSO). Everything should be authenticated, with multi-factor authentication (MFA). No matter where the user is, whatever they are trying to access, validate their credentials, validate they have their second (or third) factor, and regularly require re-authentication.

If credentials are stolen or a system is hijacked, MFA and regular re-authentication will quickly put a stop to an attacker.

Always control

Apply controls and checks wherever they are needed and adopt and enforce the principle of least privilege – users should only have access to the bare minimum that they need to perform their job. If there is a human resources system only used by German staff, then only the German staff should have access. No one else should have access, even if the risk of having access is deemed low.

Always analyze

Just because an authentication was successful, or access is granted to that user or device, doesn't mean that it is trustable. Insider threats and malicious actors may gain access to valid credentials. Record all network and system activity and regularly analyze and inspect it to verify what occurs post authentication. SIEMs (security information and event management), EDR (endpoint detection and response) as well as MDR (managed detection and response) have emerged to serve exactly this need.

Always secure

Use an "inside out" approach to cybersecurity. You should be focusing on your important data and working your way out, identifying points of vulnerability along your data's journey within your network from the moment it is created until the moment it is destroyed.

Always consider risk above all else, not compliance or regulation. Applying security purely to meet a compliance check or regulation requirement is dangerous. Compliance requirements don't know what is in your network, the flows and workloads, systems and technologies. They don't know the risks relevant to every possible element of your network. Considering risk and modelling the threats your organization faces will ensure you know where security should be increased, relaxed, and where microsegments should be created.

Moving towards zero trust

So how do you move towards zero trust and take advantage of all the benefits it offers?

Define your surface and identify resources | Map standard and privileged pathways | Architect a Zero Trust network | Create Zero Trust Policies | Monitor and maintain your perimeters

Define your surface and identify resources

First, you need to define what surface you are hoping to secure, control, and monitor. What are all the resources, services, apps, and devices used in your business? Having a clear scope of everything that is in use across the entire network helps you then seek to apply our new zero trust mentality to it.

Map standard and privileged pathways

Once you've got everything scoped out, you then need to map standard pathways – what are the flows, behaviors, and relationships between everything that are standard and expected? This group of users will access this application, this device will connect to that network, this service uses that datastore and so on, but also, what are the privileged pathways? This administrator will want to connect to this management console and use remote desktop protocol (RDP) to access that server hosting sensitive data, etc. Privileged pathways will almost certainly want extra security or controls applied to them.

Architect a zero trust network

Now that you know what is in scope and what the relationships are between everything, you can start to apply the zero trust philosophy to it. Identify which security measures and access controls you want to apply and where, what technology will best mitigate which risk, and so on.

Create zero trust policies

Next, you need to implement zero trust policies that will make use of as many different sources of data as possible to add context to any connection or request.

Monitor and maintain your perimeters

Finally, and perhaps most importantly, you need to overlay everything with detailed monitoring so that you can maintain our newly created perimeters.

This is one of the biggest changes administrators face. Where once you could install and configure antivirus and never need to look at the console, with zero trust, you need to change your habits.

You need to be monitoring the events that take place, taking advantage of tools like EDR to understand the root cause of how a threat entered the environment, and what events took place before a detection or after a potential breach.

Services like MDR can really help here, enabling cybersecurity experts to assist you with monitoring your network and crushing threats on your behalf

The zero trust technology stack

It takes a lot of technologies to secure all the resources and assets you'll have on a network. There is no one single vendor, product, or technology that will solve all your problems.

A zero trust technology stack needs to address two major areas – the management of zero trust, and the security and control of your various resources and assets.

Management is broken into three sub-areas:

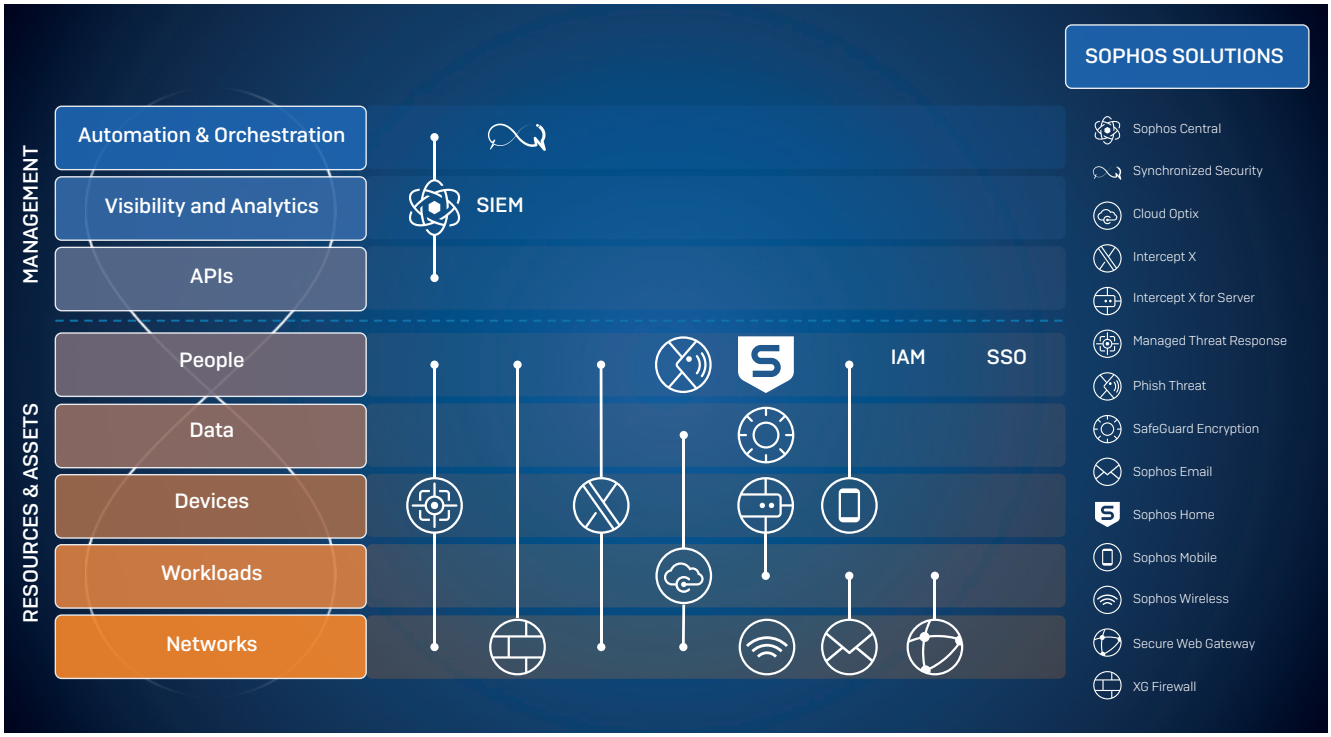
1. Automation and orchestration – for defining dynamic policies, coordinating all the different technologies, and putting everything into place
2. Visibility and analytics – for maintaining oversight of the network and ensuring everything is working as well as identify threats and breaches if or when they occur
3. APIs – for integrating your various technologies together, getting data out of one system and into another

Resources and assets are broken down into five sub-areas:

1. People – the users, admins, etc. who work for or with your business
2. Data – the lifeblood of all organizations and perhaps the most important asset to secure
3. Devices – the servers, laptops, virtual machines, etc. you use to conduct your business
4. Workloads – the services and apps you use to process data, perform calculations, generate reports, etc
5. Networks – the communication channels over which data flows, web, email, Wi-Fi, the internet, and so on

How Sophos can help

While a single vendor cannot move your organization to a zero trust model, Sophos has a huge range of technologies to help you get there.



The management of zero trust

Sophos Central our cloud-native cybersecurity platform, enables you to manage a zero trust environment. It orchestrates all our technologies in a single console, providing you with oversight of all technologies in a single place and APIs to wire together any other third-party technologies you are using.

You may also consider a SIEM to aggregate logging from your non-Sophos and Sophos products to make it easier to have full oversight of what is going on. Our APIs make it easy to get information out of our Sophos Central platform and into whatever SIEM you're using.

Sophos Synchronized Security (controlled through Sophos Central) also plays a big role here. With Synchronized Security enabled, Sophos solutions share information with one another and automatically respond to incidents. In the context of zero trust, solutions are able to adapt to scenarios through dynamic policy and automate complex tasks like isolating machines and more.

Security and the control of resources and assets

Many of our products help you secure multiple resources and assets at the same time but, by no means does that mean you can employ just one technology and move on. Securing people, for instance, requires a large number of different technologies as part of a resilient zero trust architected network.

Cloud Optix delivers the continuous analysis and visibility organizations need to detect, respond, and prevent cloud security and compliance gaps that leave them exposed. Within a zero trust environment, Cloud Optix can help to secure, within the public cloud, data, devices, workloads, and networks.

Intercept X offers unmatched endpoint protection and is able to stop the widest range of attacks with a unique combination of deep learning malware detection, exploit prevention, behavioral detections, and anti-ransomware. Within a zero trust environment, Intercept X can help to secure all your resources and assets.

Intercept X for Server is designed to secure cloud, on-premises, or hybrid server environments. Within a zero trust environment, Intercept X for Server can help to secure both your devices and workloads.

Managed Threat Response (MTR) is our expert led threat response solution. It fuses machine learning technology with human intelligence and provides 24/7 threat hunting, detection, and response capabilities. Within a zero trust environment, MTR can help to secure all your resources and assets.

Phish Threat is our dedicated anti-phishing solution. It provides your employees with security awareness training as well as accompanying reporting designed to enable you to gauge your organization's phishing threat readiness. Within a zero trust environment, Phish Threat can help you to secure your people.

SafeGuard Encryption encrypts content as soon as it is created. It proactively protects your data by continuously validating the user, application, and security integrity of a device before allowing access to encrypted data and thus, within a zero trust environment, can help to secure your data.

Secure Web Gateway facilitates advanced web protection, providing unprecedented levels of web security, control and insights. Within a zero trust environment, Secure Web Gateway can help to secure both networks and workloads.

Sophos Email utilizes artificial intelligence to provide smarter predictive email security. Within a zero trust environment, Sophos Email can help to secure your networks and workloads.

Sophos Home is designed to protect computers within your home and is based on the same technology featured in many of our business products. Within a zero trust environment, Sophos Home can help to secure your people.

Sophos Mobile is our secure Unified Endpoint Management (UEM) solution that helps businesses spend less time and effort to manage and secure traditional and mobile endpoints. Within a zero trust environment, Sophos Mobile can help to secure your devices, data and people.

Sophos Wireless provides an easy, effective way to manage and secure your wireless networks. Within a zero trust environment, Sophos wireless can help to secure your networks.

XG Firewall provides comprehensive next-generation firewall protection that exposes hidden risks, blocks unknown threats, and automatically responds to incidents. Within a zero trust environment, XG Firewall can help to secure all of your resources and assets.

Employing these technologies will put you in good stead when moving to a zero trust model. However, as previously stated, no one vendor or technology, including Sophos, can move you to a zero trust environment. To empower your users to use cloud services wherever they are, you will additionally need a strong Identity Access Management (IAM) solution with Single-Sign On (SSO) in place to make use of your single authoritative source of identity across all systems and services – this is a key part of zero trust.

You can learn more about, and start instant demos of, our products and services at www.sophos.com.

Our vision for cybersecurity

Zero trust and our vision for cybersecurity, Synchronized Security, share many of the same goals and complement each other.

Synchronized Security is cybersecurity as a system. It continuously analyzes, adapts, and automates the most complex tasks in IT while dynamically monitoring all system activity, user behavior, network traffic, and compliance postures in real time. All technologies share information between each other, providing insight and visibility to one another where one alone would be blind.

Tech should talk. Only through this talking can we achieve the adaptive and dynamic policies we need, based on multiple data sources, to achieve a zero trust network.

Conclusion

As it stands, zero trust is but a philosophy towards cybersecurity with very few able to readily embrace it. However, as security perimeters continually erode, the need for adoption will become increasingly prevalent. Cybercriminals are only getting more innovative and defences are struggling to keep up with this. The zero trust model represents a way to truly minimize threats all the while setting new standards in cybersecurity protocol.

It's time to think differently. It's time to evolve.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

20-03-10 WP-EN (DD)

SOPHOS

O2 business

Telefónica

SOPHOS

Published in June 2020. All information is correct at time of publication. Telefónica UK Limited Registered in England no.1743099.
Registered Office: 260 Bath Road, Slough, SL1 4DX