lightstream

ZERO TRUST 101

Critical steps for implementing a Zero–Trust strategy and a guide to deciphering all the industry buzzwords.

LIGHTSTREAM
208 N 2100 West, Suite 200
Salt Lake City, UT 84116
Phone: 877-95-LIGHT

Follow us on

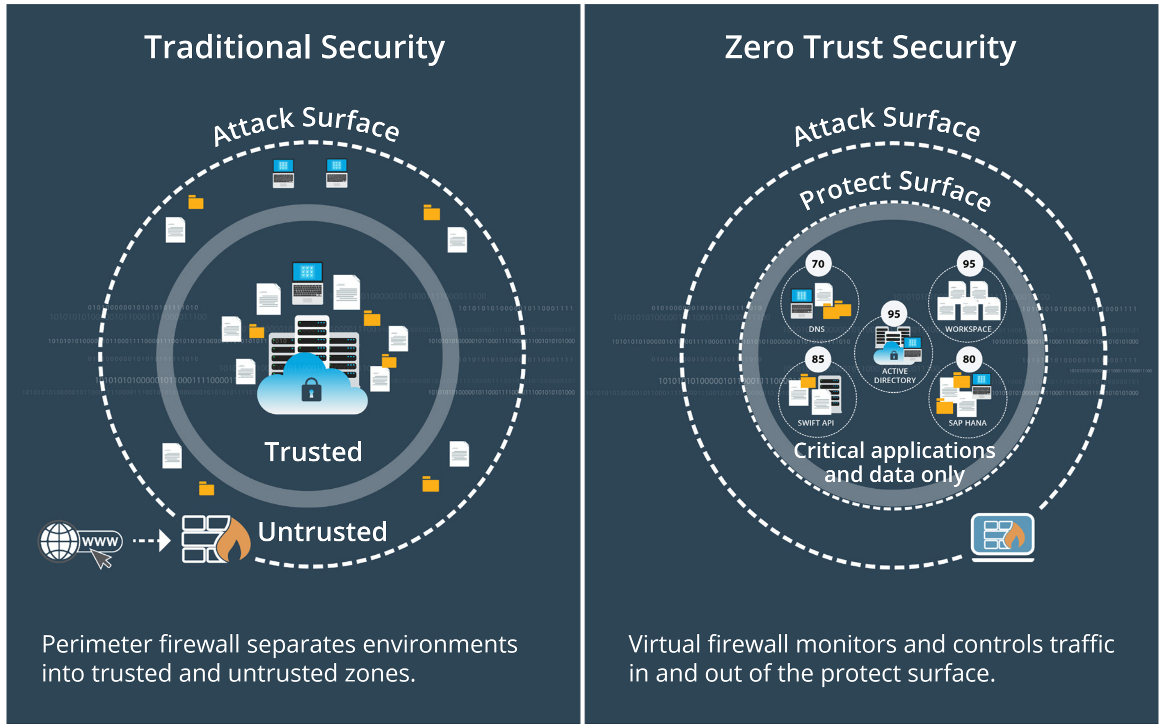
Let us tell you more about the amazing things we do.

THE 5-STEP MODEL TO IMPLEMENTING ZERO TRUST

01 | DEFINE THE PRODUCT SURFACE
02 | MAP THE TRANSACTION FLOWS
03 | BUILD A ZERO TRUST ARCHITECTURE
04 | CREATE A ZERO TRUST POLICY
05 | MONITOR AND MAINTAIN THE NETWORK

As technologies evolve, so does the threat landscape, and the old way of doing things simply no longer holds up. Network admins not only need to worry about protecting their organizations from outside threats, but from zero-day malware to insider threats as well. The traditional perimeter-based security model is rife with vulnerabilities that bad actors are all too happy to exploit, which is why, now more than ever, organizations need to evolve into a more advanced security strategy: a Zero Trust framework and architecture.

Zero Trust embraces the new reality—users need access from any device, at any time. And the security framework needs to support that. Zero Trust assumes each access attempt comes from an untrusted network, requiring verification at every step of the way, thus better protecting your organization's data and sensitive information.



Traditional Security

Perimeter firewall separates environments into trusted and untrusted zones.

Zero Trust Security

Virtual firewall monitors and controls traffic in and out of the protect surface.

! Zero Trust reduces the number of potential entry points for cyberattacks.

If you're ready to implement a Zero Trust strategy, use the 5-step model adopted globally by local NCSCs (National Cybersecurity Centers). The model takes an iterative approach, which allows you to learn and reflect after each step. Any improvements you observe can be added into new interactions to help build a more resilient and secure environment, made up of people, processes, and systems.

1 Define the product surface

Identify the DAAS (data, applications, assets, and services) elements you want to protect and then group them into protect surfaces. Use some of our lessons learned to ensure your success.

ALIGN WITH BUSINESS AND ASSET OWNERS	Not all managers have a strategic view or are keeping an eye on the day-to-day. Work across the organization instead with business and asset owners who understand the economic value of the asset and the potential business impact to them.
START SMALL	Start small and expand later. First, grab three applications and put security devices like firewalls around them. Once you can do that well, you'll just need variations on earlier well-known work.
PAY ATTENTION TO OBJECTIONS	Listen to objections early that can live in operations, like performance, concerns about it working with an inline firewall, or questions about monitoring.
INVEST IN CAPABILITIES TO TELL THE ZERO TRUST JOURNEY TO NON-TECHNICIANS	Building awareness around Zero Trust has evolved over the years. Invest in ways to talk about the journey to Zero Trust, including why it's necessary, how it's possible, and that what you have is indeed Zero Trust.
DEMYSTIFY JARGON	Formulate your protect surfaces in easy-to-understand language so everyone understands the value. People may not understand IP ranges, but they do understand the protect surface "general ledger."

2 Map the Transaction Flows

Identify users' density and privileges, applications, and services and map the transaction flows between your protect surfaces to document which traffic or transaction flows are active between the protect surfaces.

Why map transaction flows? Mapping the transaction flows to and from the protect surface shows how various DAAS components interact with other resources on your network, helping you determine where to place the proper controls. How traffic moves across the network, specific to the data in the protect surface, determines the design.

When you start mapping transaction flows, you will want to ask yourself a few questions: Can I do this on my own? Do I have the capabilities and technologies to extract the flow of information from my environment? Do I have the technology in place that can do data discovery or flow identification? Engage asset owners and the organization to identify flows before you assign security activities.

3 Build a Zero Trust Architecture

Define and build a Zero Trust architecture, including associated security measures. The five-step model illuminates the best way to design this architecture—these can't be predetermined. Each Zero Trust environment is custom-made for each protect surface.

4 Create a Zero Trust Policy

You need to instantiate Zero Trust as a Layer 7 policy statement, which requires Layer 7 controls. Use the Kipling Method of Zero Trust policy writing to determine who and what can access your protect surface. (See page 9 for a policy overview.)

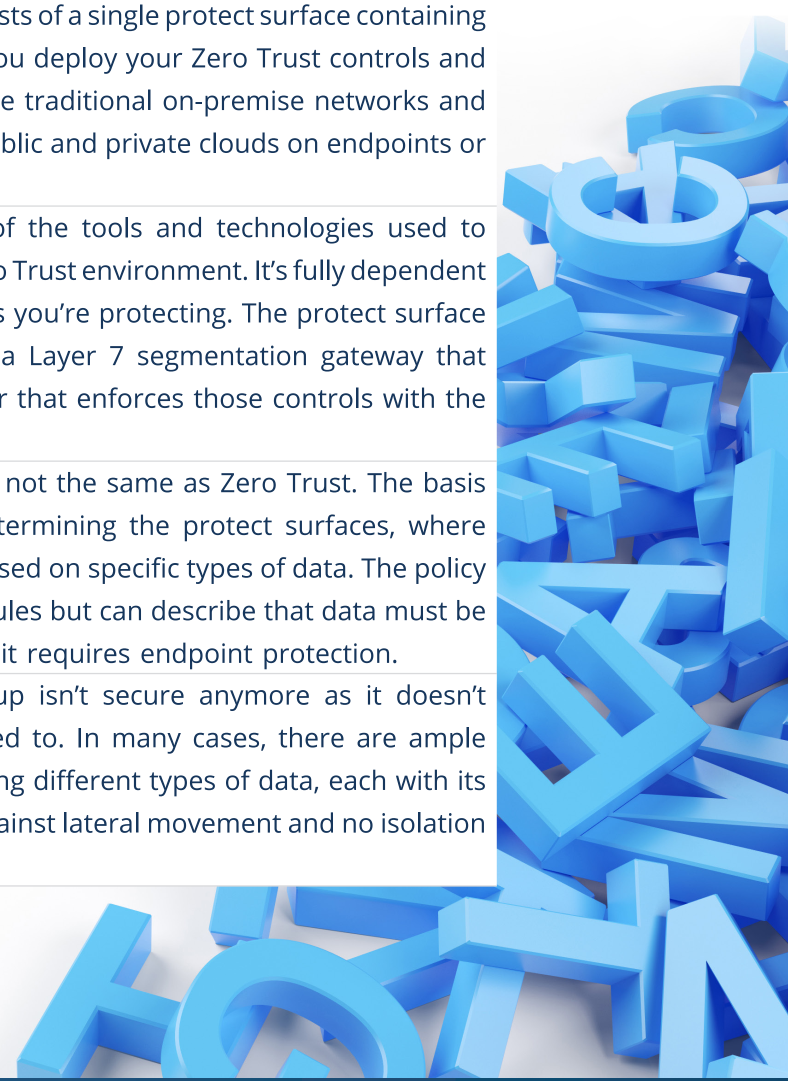
5 Monitor and Maintain the Network

Inspect and log all traffic, including through Layer 7. The telemetry this process provides doesn't just help prevent data breaches and other significant cybersecurity events, but also provides valuable security improvement insights. Each protect surface becomes more robust and better protected over time.

Telemetry from the cloud, network, and endpoint controls can be analyzed using behavioral analytics, machine learning, and artificial intelligence to stop attacks in real-time and improve security posture over the long term.

All the Zero Trust terminology you need to know.

ZERO TRUST	Zero Trust is a strategic initiative that helps to prevent successful data breaches. It does so by eliminating digital trust from your organization. It's based on the principle of "never trust, always verify" and is a strategy that is decoupled from technology. While technologies will change over time, the strategy will remain the same.
ZERO TRUST ENVIRONMENT	A Zero Trust environment designates the location of your Zero Trust architecture. It consists of a single protect surface containing a single DAAS element. You deploy your Zero Trust controls and policies here. They include traditional on-premise networks and data centers as well as public and private clouds on endpoints or across an SD-WAN.
ZERO TRUST ARCHITECTURE	This is the compilation of the tools and technologies used to deploy and build your Zero Trust environment. It's fully dependent upon the protect surfaces you're protecting. The protect surface is typically protected by a Layer 7 segmentation gateway that creates a micro-perimeter that enforces those controls with the Kipling Method policy.
NETWORK SEGMENTATION	Network segmentation is not the same as Zero Trust. The basis for Zero Trust lies in determining the protect surfaces, where each protect surface is based on specific types of data. The policy is not limited to firewall rules but can describe that data must be stored encrypted or that it requires endpoint protection.
DMZ	The traditional DMZ setup isn't secure anymore as it doesn't protect what it's supposed to. In many cases, there are ample services in the DMZ serving different types of data, each with its risks. It doesn't protect against lateral movement and no isolation in case of a compromise.



SEGMENTATION GATEWAY	A segmentation gateway (SG) is a Layer 7 gateway designed to segment networks based on users, applications, and data. They are the primary technology used to enforce the Layer 7 policy in Zero Trust environments. SGs can be physical (PSG) when used in traditional on-premise networks or virtual (VSG) when used in public or private clouds.
MICO-PERIMETER	When an SG connects to a protect surface and you deploy a Layer 7 Kigling Method policy, a micro-perimeter is placed around the protect surface. This ensures that only known and approved validated traffic has access to the protect surface. It's recommended you move your SG as close as possible to the protect surface for the most effective preventative controls enforced by the micro-perimeter.
MIRCO-SEGMENTATION	This is the act of creating a small segment in a network so attackers have difficulty moving around and accessing internal resources. A micro-perimeter is a type of micro-segment.
ASSERTED IDENTITY	Identity is an assertion of the abstraction of a user of a network. The identity system asserts that a device is generating packets under the control of the asserted identity. The asserted identity is the validated and authenticated "who" statement (that's part of the Kipling Method policy assertion: Who should have access to a resource?).
LEAST-PRIVILEGED ACCESS	This asks the question, "Does a user need access to a specific resource to get their job done?" By mandating a least-privilege policy, a user's ability to perform malicious action on a resource is severely limited. This mitigates both stolen credentials and insider attacks.
GRANULAR ACCESS CONTROL	Granular access control is the outcome of an explicitly defined Zero Trust Kipling Method policy statement. Multiple access control criteria provide a fine-grained policy for access to a protect surface, making it substantially more difficult to perform a successful attack against that protect surface.
TRUST LEVELS	Trust is a human emotion that's injected into digital systems for no technical reason—it is not measurable or binary. All successful cyber-attacks exploit trust, making it a dangerous vulnerability that you need to mitigate. In Zero Trust, all packets are untrusted and treated the same as every other packet flowing across the system. The trust level is identified as zero.
DATA TOXICITY	This is the doctrine that defines sensitive data as toxic to your organization if it has been stolen or exfiltrated from your networks or systems and is in control of malicious actors. Every organization has both toxic and non-toxic data, but you can recognize toxic data types by remembering the 4Ps of toxic data: PCI, PII, PHI, and IP.

Defining Product Surfaces

When defining protect surfaces, consider the name, characteristics, relevance score, and reasoning.

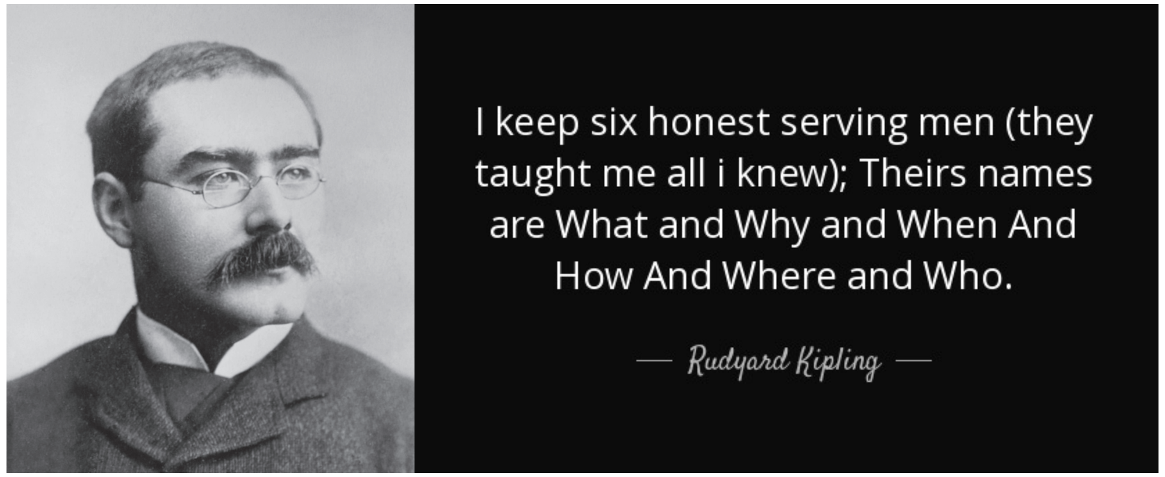
PROTECT SURFACE	This is the inversion of the attack surface (which includes the entire internet). Using a Zero Trust strategy, you can reduce the overall attack surface. Each protect surface contains a single DAAS element, and every Zero Trust environment has multiple protect surfaces.
NAME	The name represents the name of the set of DAAS elements you want to protect. Use clear, unambiguous language.
RELEVANCE SCORE	Your relevance score represents the Confidentiality, Integrity, and Availability (CIA) of the protect surface. Many organizations use CIA ratings to determine the rating of the assets. In Zero Trust, you consider the entire protect surface—not just from the asset view—as a set of DAAS elements, and the individual component with the highest rating reflects the relevance score of the collective.
REASONING	The reasoning is the argumentation you need for a specific protection level for the protect surface, which you need to build a Zero Trust architecture.

THE KIPLING METHOD POLICY (KMP)

DAAS Elements

Data, Applications, Assets, and Services (DAAS) define the sensitive resources that should go into individual protect surfaces.

DATA	This is the sensitive data that can get organizations into trouble if it's exfiltrated or misused. This includes payment card information (PCI), protected health information (PHI), personally identifiable information (PII), and intellectual property (IP).
APPLICATIONS	These refer to the applications that use sensitive data or control critical assets.
ASSETS	Assets often include information technology (IT), operational technology (OT), or internet of things (IoT) devices such as point of sale terminals, SCADA controls, manufacturing systems, and networked medical devices.
SERVICES	These are sensitive services that are exceptionally fragile. The most common services you should protect in a Zero Trust manner include DNS, DHCP, ActiveDirectory®, and NTP.



I keep six honest serving men (they taught me all i knew); Theirs names are What and Why and When And How And Where and Who.

— Rudyard Kipling —

The Kipling Method policy allows you to create a Zero Trust policy effortlessly by answering the who, what, where, when, why, and how questions.

What is the Kipling Method Policy?

Known as Zero Trust policy, the Kipling Method was named after Rudyard Kipling, who introduced the idea of who, what, when, where, why, and how in a poem in 1902. Using the KMP, you can create easily understood and auditable Zero Trust policy statements for various technologies using natural language rules based on who, what, where, when, why, and how.

- **Who?** The who question asks who should be allowed to access a resource. This defines the validated asserted identity, replacing the source IP address (a traditional firewall rule).
- **What?** This question asks what the destination of the traffic is. What application is the asserted identity allowed to use to access the resource? Most often, you use applications to access protect surfaces—the application traffic should be validated at Layer 7 to keep attackers from impersonating the application at the port and protocol level (and using the rule maliciously). Your what statement replaces port and protocol designations.
- **Where?** When asking the where question, the focus is on where the resource is located. The location of your protect surface could be anywhere you store data or deploy assets. Your where statement replaces the destination IP address you find in a traditional firewall rule.
- **When?** The when statement asks, "When is the asserted identity allowed to access a resource?" It defines a timeframe. Organizations typically instantiate rules 24/7, but many should be time-limited instead and turned off when authorized users aren't using them. Attackers take advantage of these always-on rules and attack when approved users are away from the system, making the attacks more difficult to discover.
- **Why?** This question asks why the user is allowed to access the resource. Most often, you put data or an asset into a protect surface because of their sensitivity—this is usually defined by a compliance mandate or business driver. You can tag a packet to identify sensitive data or systems, which creates metadata that various controls use to inform or automate policy statements.
- **How?** The how question asks how you can obtain access and through which application. It defines the criteria used to allow the asserted identity to access a resource. These criteria often apply additional controls or inspection on the packet as it accesses the resource. Controls that were previously separate products deployed individually are now deployed as a service, which can be applied to individual rules. The advanced controls include IPS, DLP, sandboxing, decryption, and other features available on an individual control.

Curiosity to solve the complex drives us

We live in the age of constant business transformation.

The Cloud, Big Data, AI and the Internet-of-Things open limitless possibilities—and even more expectations.

And with those expectations comes unfathomable complexity. Addressing them requires amazing strategy and execution of integrated technologies—all networked to provide greater visibility, predictability and cognition.

Fortunately, we've envisioned this day coming for a while.

We've addressed enterprise complexities of on-premise, in-the-cloud, and all the networks in between. We've offered solutions that drive business transformation. And we've worked to find more ways to help you meet higher expectations.

We are Lightstream.

Our passion to serve customers and our curiosity to solve the complex drives us.

We listen to and work with you to carve a path where vision and execution intersect—enabling new capabilities, driving efficiency, and spurring innovation and growth.

Because when you work with a partner who helps you understand where you can go and how to get there, complexity can be averted and every possibility can be realized.

That's where we live—and that's where we're ready to take you.

Complexity Averted. Possibilities Realized.

We've helped many public and private organizations to establish and implement a Zero Trust approach, both before and after the adoption of remote and hybrid work schedules. For a one-on-one consultation to discuss how to ensure your cloud is secure, contact us now.