## Zero Trust Security

Introduced by Forrester Research, the Zero Trust security model addresses some of the limitations of perimeter-based network security strategies by removing the assumption of trust from the equation. With Zero Trust, essential security capabilities are deployed in a way that provides policy enforcement and protection for all users, devices, applications, and data resources, as well as the communications traffic between them, regardless of location.

In particular, with Zero Trust there is no default trust for any entity – including users, devices, applications, and packets – regardless of what it is and its location on or relative to the enterprise network. Verification that authorized entities are always doing only what they're allowed to do also is no longer optional in a Zero Trust model: It's now mandatory.

These changes imply the following needs:

- The need to establish trust boundaries that effectively compartmentalize the various segments of the internal computing environment. The general idea is to move security functionality closer to the pockets of resources that require protection. In this way, security can always be enforced regardless of the point of origin of associated communications traffic.
- The need for trust boundaries to do more than just initial authorization and access control enforcement. To "always verify" also requires ongoing monitoring and inspection of associated communications traffic for subversive activities (such as threats).

Benefits of implementing a Zero Trust network include:

- Clearly improved effectiveness in mitigating data loss with visibility and safe enablement of applications, and detection and prevention of cyberthreats
- Greater efficiency for achieving and maintaining compliance with security and privacy mandates, using trust boundaries to segment sensitive applications, systems, and data
- Improved ability to securely enable transformative IT initiatives, such as user mobility, bring your own device (BYOD) and bring your own access (BYOA), infrastructure virtualization, and cloud computing
- Lower total cost of ownership (TCO) with a consolidated and fully integrated security operating platform, rather than a disparate array of siloed, purpose-built security point products

### *Core Zero Trust design principles*

The core Zero Trust principles that define the operational objectives of a Zero Trust implementation include:

**Ensure that all resources are accessed securely, regardless of location.** This principle suggests not only the need for multiple trust boundaries but also increased use of secure access for communication to or from resources, even when sessions are confined to the "internal" network. It also means ensuring that the only devices allowed access to the network have the correct status and settings, have an approved VPN client and proper passcodes, and are not running malware.

**Adopt a *least privilege* strategy and strictly enforce access control.** The goal is to minimize allowed access to resources as a means to reduce the pathways available for malware and attackers to gain unauthorized access – and subsequently to spread laterally and/or infiltrate sensitive data.

**Inspect and log all traffic.** This principle reiterates the need to "always verify" while also reinforcing that adequate protection requires more than just strict enforcement of access control. Close and continuous attention must also be given to exactly what "allowed" applications are actually doing, and the only way to accomplish these goals is to inspect the content for threats.

**Key Terms**

The principle of *least privilege* in network security requires that only the permission or access rights necessary to perform an authorized task are granted.

An attack surface is any area where breaches and exploits may occur and is comprised of an organization's entire digital footprint.

A *protect surface* consists of the most critical and valuable *data, assets, applications, and services* (DAAS) on a network.

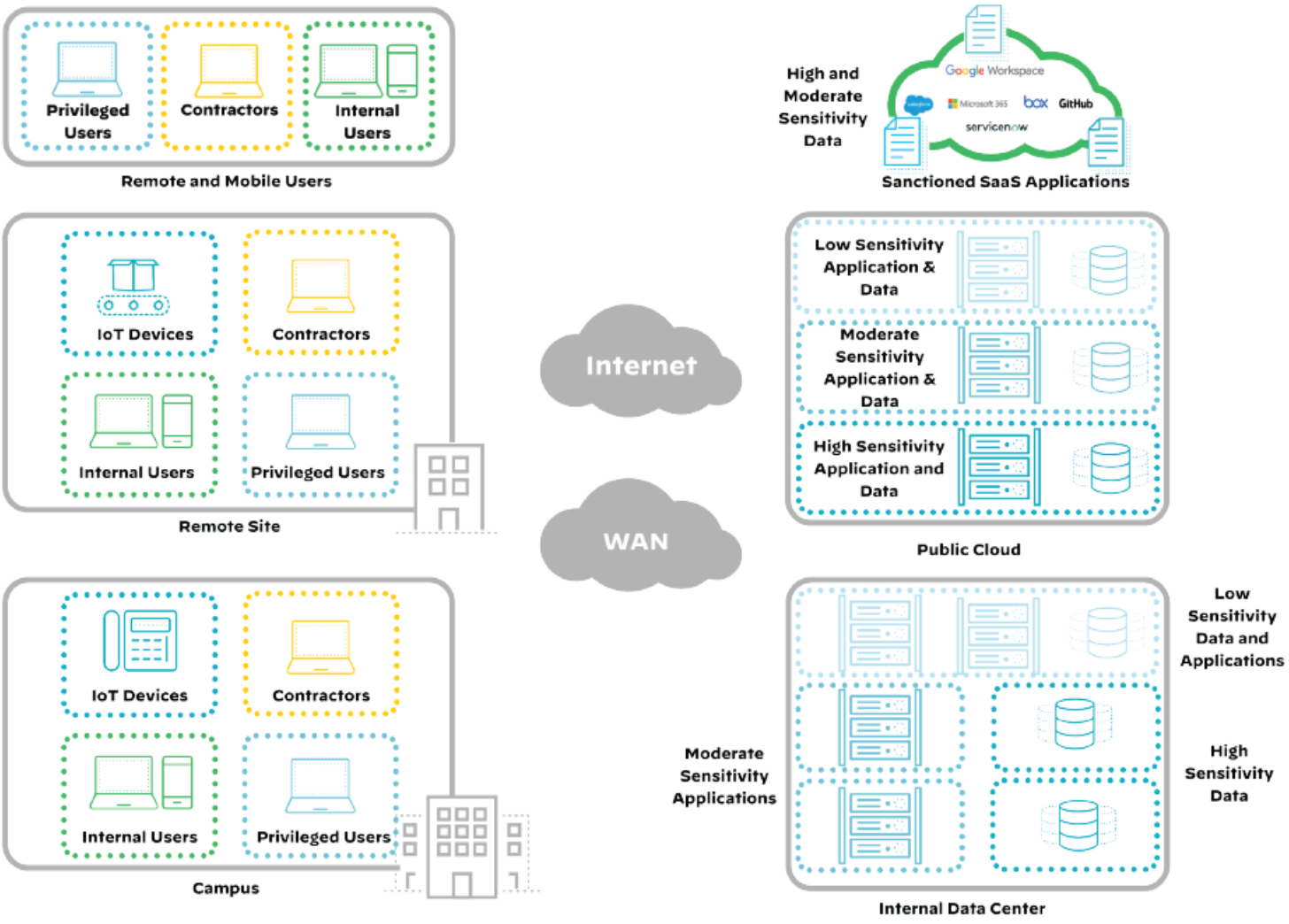
### *Zero Trust conceptual architecture*

Traditional security models identify areas where breaches and exploits may occur, the *attack surface*, and you attempt to secure the entire surface. Unfortunately, it is often difficult to identify the entire attack surface. Unauthorized applications, devices, and misconfigured infrastructure can expand that attack surface without your knowledge.

In Zero Trust, you identify a *protect surface*. The protect surface is made up of the network's most critical and valuable data, assets, applications, and services (DAAS). Protect surfaces are unique to each organization. Because it contains only what's most critical to an organization's operations, the protect surface is orders of magnitude smaller than the attack surface, and it is always knowable.

With the protect surface identified, you can identify how traffic moves across the organization in relation to the protect surface. Understanding who the users are, which applications they are using, and how they are connecting is the only way to determine and enforce policy that ensures secure access to your data. With an understanding of the interdependencies between the DAAS, infrastructure, services, and users, you should put controls in place as close to the protect surface as possible, creating a micro-perimeter around it. This micro-perimeter moves with the protect surface, wherever it goes.

**Figure 1-7** *Zero Trust protect surface*



In the Zero Trust model, only known and permitted traffic is granted access to the protect surface. A segmentation gateway, typically a next-generation firewall, controls this access. The segmentation gateway provides visibility into the traffic and users attempting to access the protect surface, enforces access control, and provides additional layers of inspection.

Zero Trust policies provide granular control of the protect surface, making sure that users have access to the data and applications they need to perform their tasks but nothing more. This is known as least privilege access.

Additionally, to implement a Zero Trust least privilege access model in the network, the firewall must:

**Have visibility of and control over the applications and their functionality in the traffic.** Traditional security infrastructure describes applications through ports and protocols. Zero Trust's least privilege access model requires precise control over application use that a port and protocol definition cannot achieve.

**Be able to allow specific applications and block everything else.** Allowing a specific set of applications through an allow-list and denying everything else significantly reduces the number of ways an organization can be attacked.

**Dynamically define access to sensitive applications and data based on a user's group membership.** Many traditional security policies define access based on the location of the endpoint in the network. Even if enterprise mobility didn't blur the traditional network boundaries, network location is a poor identifier for a user and their assigned privileges.

**Dynamically define access from devices or device groups to sensitive applications and data and from users and user groups to specific devices.** This is important in IoT-heavy environments, where devices may access applications and data in the same way a user would. For example, medical equipment may be sending sensitive data to specific applications or repositories. Malicious or even accidental access might disrupt manufacturing equipment or industrial control systems.

**Be able to validate a user's identity through authentication.** For access to the most sensitive data, the firewall should validate user information obtained from the organization's authentication servers with another authentication method before allowing access. This ensures the traffic is coming from the expected user and not from someone impersonating them.

**Dynamically define the resources that are associated with the sensitive data or application.** Many data centers and PaaS environments dynamically allocate resources to applications. To ensure that the security posture matches the current resource allocation, the firewall needs to adjust along with the changing environment.

**Control data by file type and content.** Blocking risky file types reduces the number of ways you can be attacked and reduces the number of ways attackers can exfiltrate data.

The result is granular control that safely allows access to the right applications for the right sets of users while automatically eliminating unwanted, unauthorized, and potentially harmful interactions.

The main components of a Zero Trust conceptual architecture (shown in Figure 1-8) include:

**Zero Trust Segmentation Platform.** The Zero Trust Segmentation Platform is referred to as a network segmentation gateway by Forrester Research. It is the component used to define internal trust boundaries, meaning that the platform provides the majority of the security functionality needed to deliver on the Zero Trust operational objectives, including the ability to:

Enable secure network access

Granularly control traffic flow to and from resources

Continuously monitor allowed sessions for any threat activity

Although Figure 1-8 depicts the Zero Trust Segmentation Platform as a single component in a single physical location, in practice – due to performance, scalability, and physical limitations – an effective implementation is more likely to entail multiple instances distributed throughout an organization's network. The solution is also designated as a "platform" to reflect the fact that it is an aggregation of multiple distinct (and potentially distributed) security technologies operating as part of a holistic threat protection framework to reduce the attack surface and correlate information about threats that are found.

**Trust zones.** Forrester Research refers to a trust zone as a micro core and perimeter (MCAP). A trust zone is a distinct pocket of infrastructure where the member resources not only operate at the same trust level but also share similar functionality. Functionality such as protocols and types of transactions must be shared in order to minimize the number of allowed pathways into and out of a given zone and, in turn, to minimize the potential for malicious insiders and other types of threats to gain unauthorized access to sensitive resources.

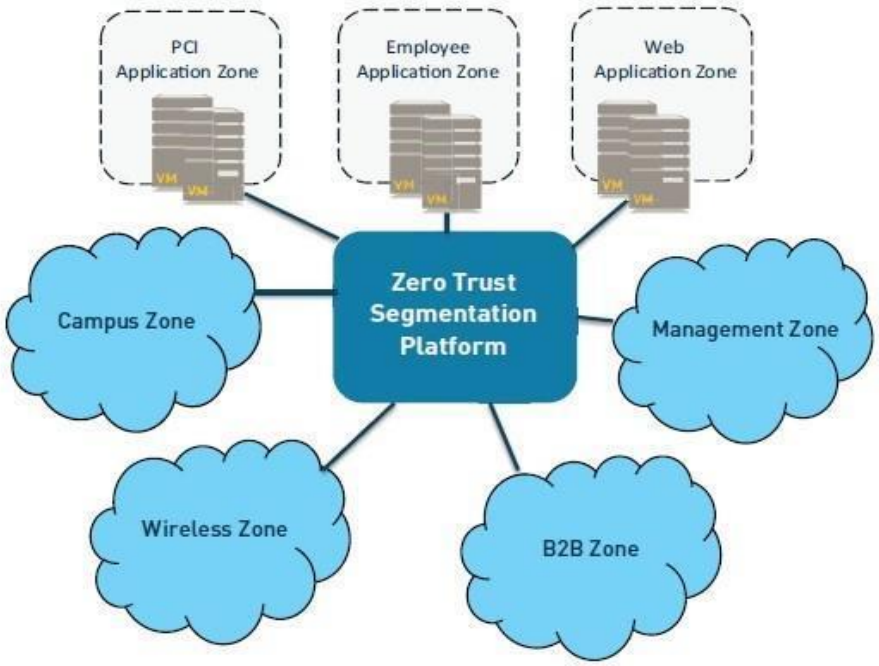
Examples of trust zones shown in Figure 1-8 include the user (or campus) zone, a wireless zone for guest access, a cardholder data zone, database and application zones for multitier services, and a zone for public-facing web applications.

Remember, too, that a trust zone is not intended to be a "pocket of trust" where systems (and therefore threats) within the zone can communicate freely and directly with each other. For a full Zero Trust implementation, the network would be configured to ensure that *all* communications traffic – including traffic between devices in the same zone – is intermediated by the corresponding Zero Trust Segmentation Platform.

**Management infrastructure.** Centralized management capabilities are crucial to enabling efficient administration and ongoing monitoring, particularly for implementations involving multiple distributed Zero Trust Segmentation Platforms. A data acquisition network also provides a convenient way to supplement the native monitoring and analysis capabilities for a Zero Trust Segmentation Platform. Session logs that have been forwarded to a data acquisition network can then be processed by any number of out-of-band analysis tools and technologies intended, for example, to further enhance network visibility, detect unknown threats, or support compliance reporting.

**Figure 1-8**

*Zero Trust conceptual architecture*




### *Key Zero Trust criteria and capabilities*

The core of any Zero Trust network security architecture is the Zero Trust Segmentation Platform, so you must choose the correct solution. Key criteria and capabilities to consider when selecting a Zero Trust Segmentation Platform include:

**Secure access.** Consistent secure IPsec and SSL VPN connectivity is provided for all employees, partners, customers, and guests wherever they're located (for example, at remote or branch offices, on the local network, or over the internet). Policies to determine which users and devices can access sensitive applications and data can be defined based on application, user, content, device, and device state.

**Inspection of all traffic.** Application identification accurately identifies and classifies all traffic, regardless of ports and protocols, and evasive tactics such as port hopping or encryption. Application identification eliminates methods that malware may use to hide from detection and provides complete context into applications, associated content, and threats.

**Least privileges access control.** The combination of application, user, and content identification delivers a positive control model that allows organizations to control interactions with resources based on an extensive range of business-relevant attributes, including the specific application and individual functions being used, user and group identity, and the specific types or pieces of data being accessed (such as credit card or Social Security numbers). The result is truly granular access control that safely enables the correct applications for the correct sets of users while automatically preventing unwanted, unauthorized, and potentially harmful traffic from gaining access to the network.

**Cyberthreat protection.** A combination of anti-malware, intrusion prevention, and cyberthreat prevention technologies provides comprehensive protection against both known and unknown threats, including threats on mobile devices. Support for a closed-loop, highly integrated defense also ensures that inline enforcement devices and other components in the threat protection framework are automatically updated.

**Coverage for all security domains.** Virtual and hardware appliances establish consistent and cost-effective trust boundaries throughout an organization's entire network, including in remote or branch offices, for mobile users, at the internet perimeter, in the cloud, at ingress points throughout the data center, and for individual areas wherever they might exist.

### *Implementing a Zero Trust design*

Implementation of a Zero Trust network security model doesn't require a major overhaul of an organization's network and security infrastructure. A Zero Trust design architecture can be implemented in a way that requires only incremental modifications to the existing network and is completely transparent to your users. Advantages of such a flexible, non-disruptive deployment approach include minimizing the potential impact on operations and being able to spread the required investment and work effort over time.

To get started, you can configure a Zero Trust Segmentation Platform in listen-only mode to obtain a detailed picture of traffic flows throughout the network, including where, when, and to what extent specific users are using specific applications and data resources.

With a detailed understanding of the network traffic flows in the environment, the next step is to define trust zones and incrementally establish corresponding trust boundaries based on relative risk and/or sensitivity of the data involved:

Deploy devices in appropriate locations to establish internal trust boundaries for defined trust zones.

Configure the appropriate enforcement and inspection policies to effectively put each trust boundary "online."

Next, you can progressively establish trust zones and boundaries for other segments of the computing environment based on their relative degree of risk. Examples of where secure trust zones can be established are:

IT management systems and networks (where a successful breach could lead to compromise of the entire network)

Partner resources and connections (business to business, or B2B)

High-profile, customer-facing resources and connections (business to consumer, or B2C)

Branch offices in risky countries or regions, followed by all other branch offices

Guest access networks (both wireless and wired)

Campus networks

Zero Trust principles and concepts must be implemented at major access points to the internet. You will have to replace or augment legacy network security devices with a Zero Trust Segmentation Platform at this deployment stage to gain all of the requisite capabilities and benefits of a Zero Trust security model.