E-BOOK

Meeting the NIST Cyber Security Whitepaper 20 (CSWP 20) Zero Trust Planning Requirements with iboss

iboss®

Table of Contents

Overview

The Zero Trust Architecture presented in the NIST 800-207 publication provides a detailed framework of Zero Trust which includes definitions of core concepts and deployment designs. The NIST 800-207 Zero Trust Architecture (ZTA) fits directly into the NIST Risk Management Framework which is a robust strategy to reduce cyber risk within organizations of all types and sizes. There are many detailed concepts and requirements within the NIST 800-207 publication that must be understood to properly implement a robust and foundationally sound Zero Trust design within an organization which will greatly reduce risks resulting from breaches and data loss.

NIST released a follow-on guide, "Planning for a Zero Trust Architecture," under the NIST label Cyber Security Whitepaper 20 (CSWP 20). This planning guide serves a few primary purposes which include showing how the NIST Risk Management Framework (RMF) can be applied when implementing a Zero Trust Architecture according to the NIST 800-207 and providing additional clarity for key requirements defined in the NIST 800-207. The additional context for concepts defined in the NIST 800-207 publication is critical as missing these requirements will have a severe long-term impact on any Zero Trust Architecture implementation.

The iboss Zero Trust Edge implements all the core concepts of the NIST 800-207 Zero Trust Architecture. In addition, it meets all additional details defined within the NIST CSWP 20 planning guide. This iboss eBook provides a companion to the NIST CSWP 20 Zero Trust planning guide designed to map the requirements outlined by the NIST CSWP 20 planning guide to the iboss Zero Trust Edge.

The NIST 800-207 Zero Trust Architecture can be found at the following URL

The NIST CSWP 20 can be found at the following URL

Zero Trust Overview

The CSWP 20 planning guide begins by baselining Zero Trust with the definition according to NIST:

> **"Zero trust provides a collection of concepts designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as contested."**

The key point of this definition is that the access decision to each resource must be performed "per-request," meaning for each and every request. An access decision includes leveraging authentication, or "knowing who the person is," and authorization, which grants the user privilege to interact with the resource. The "per-request" concept is often missed or misinterpreted to mean access decisions made at the point of login is adequate. Granting authorization only at the point of login leaves most transactions between a user and a resource completely unmonitored which results in the lack of security and visibility during the most critical interactions that result in data breaches and data loss.

Implementing a Zero Trust Architecture requires people, process, and technology. The iboss Zero Trust Edge implements the NIST 800-207 concepts serving as the technology component to enable people to run consistent processes when implementing a Zero Trust Architecture. The iboss Zero Trust Edge is designed to make a Zero Trust Architecture implementation possible in a simple and straightforward way.

The CSWP 20 planning guide shows the key logic components of Zero Trust that were originally presented in the NIST 800-207, with the heart of the Zero Trust logic components being the Policy Enforcement Point (PEP) and Policy Decision Point (PDP). The iboss Zero Trust Edge serves as the PEP and PDP which is the center of the NIST 800-207 Zero Trust Architecture.

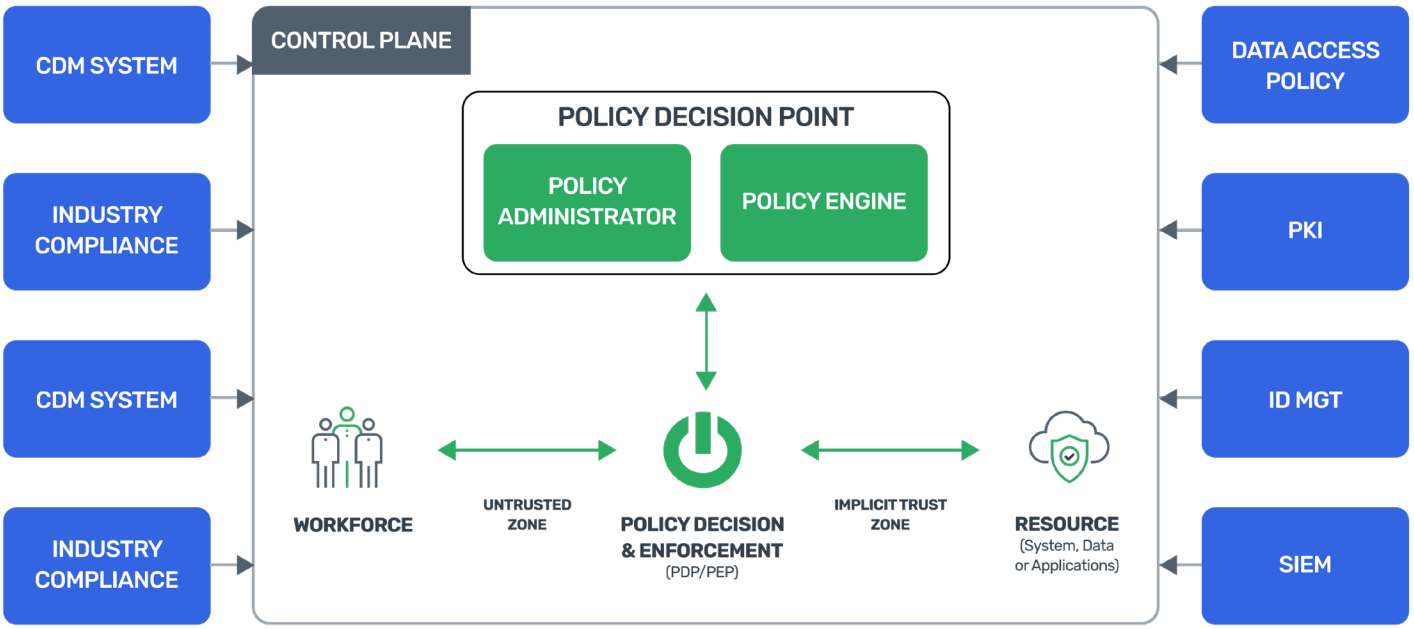

Figure 1- Core Zero Trust Logical Components

Understanding the NIST Zero Trust Definition of a Connection

Understanding what is meant by a connection is vital as this term can be misinterpreted and is often confused. For example, when using VPN technology, the VPN will connect to a network once the user is authenticated and authorized. After the VPN connection is established, the user is free to transact with resources without additional authentication and authorization verifications. This in turn means that data exchanges between the user and resources are automatically authorized resulting in no security, no inspection, and no logging visibility which result in substantially reduced security. The CSWP 20 planning guide realizes this and has a footnote to the bottom of page two as shown below.

"The unit of "session" can be nebulous and differ depending on tools, architecture, etc. The basic definition in a zero trust context is a connection to one resource utilizing one network identity and one privilege for that identity (e.g. read, write, delete, etc.) or even a single operation (similar to an API call). This would be the ideal case, but implementations may not allow this fine grain of control and may define sessions as broadly as "connection to a resource by a network identity with set privileges for a period of time" with reauthentication and reauthorization needed for increased privilege, after a set time period, or an operational change is detected."

Notice that a "session" according to NIST is a single operation performed between a user and a resource. In contrast with a VPN or technologies that mimic VPNs, a connection represents the entire VPN session after the VPN connection is established. In this legacy approach, an enormous number of operations are performed through the VPN connection without any further authentication or authorization. With a strong Zero Trust implementation, each transaction will be authenticated and authorized.

Alternative Connection Model Deficiencies in Meeting NIST 800-207 Zero Trust Connection Principles

Foundationally, the inability to authenticate and authorize each request to a resource, including the ability to apply security and log the transaction, will result in failure to meet NIST 800-207 Zero Trust Architecture principles. The goal of Zero Trust is to provide "least privilege, per-request access decisions" to reduce risk of breach and data loss. Although the legacy VPN model is the furthest from meeting the NIST 800-207 core principles, many alternative connection models are only slightly better but ultimately lack the ability to meet the core connection requirements of the NIST 800-207 concepts.

Legacy VPN Connections

The traditional VPN model lacks the ability to meet per-request authentication and authorization because authentication and authorization occur only at the time the VPN is enabled by the end user. Once the VPN session is established, users can interact with protected resources without logging and without per-request authentication and authorization that is required. A user can cause damage, via infection or insider threat, once connected to the network via the VPN because none of the connections are inspected, authenticated, authorized, or secured.

Solutions that Leverage Single Packet Authorization (SPA)

Although this model is an enhancement to the traditional VPN model, it lacks the ability to meet NIST 800-207 Zero Trust principles. To understand why, the process by which SPA connects users to resources is described below.

1. The end user connects to a Policy Decision Point (PDP) which authenticates and authorizes a request by a user to access resources. The PDP issues a token to the end user which contains the authorizations to the resources which the user can access.

2. The user presents the authorization token to a Policy Enforcement Point (PEP) that is responsible for connecting the user to the protected resources. The PEP reviews the token and opens the ports and protocols to the user based on this "pre-authorized" token.

3. The user can interact with the ports and protocols that have been opened by the PEP and no other ports on the network.

This model has several problems. First, authentication and authorization must occur on every request to the resource. With the SPA model, the authorization occurs once within the first step, but once the user is connected to the authorized ports, the user is free to send as many requests as possible to those ports without additional authentication or authorization checks. This results in free interaction with these authorized ports with a single authentication and authorization occurring at only at the first step of the process.

The reason for per-request authentication and authorization is important as shown in the following example. In this scenario,

a user receives an authorization token to access ports and protocols during the first step of SPA. If this token is hijacked, by a user in Russia for example, the attacker can connect to those ports and hijack data or cause damage to the resource. Using per-request authentication and authorization, if the session was hijacked, the request would be rejected by running it through a trust algorithm that denies requests originating from Russia.

SPA is like a VPN and lacks the deep security inspection and logging capabilities required by NIST 800-207 for each request. Once the client is connected, the transaction is not logged, and the data is not inspected (CASB, Malware Defense, DLP). While a VPN connects a user to an entire network, SPA connects a user to a port on the network. Zero Trust is about connecting users to resources, not networks.

An example will make this point clear. Many services may run on the same port. For example, with an Apache webserver, there may be many websites running on the same port which is typically TCP port 443. With a SPA approach, once the user is authenticated and authorized, they are connected to the TCP port 443 which means they have access to every website on that server. Using a true NIST 800-207 approach, the user would not have access to all services on TCP port 443 on that server but instead each website request would be analyzed, authenticated and either authorized or denied every time a user make a request to the resource.

This per-request ability is present within the iboss Zero Trust Edge. Even in the scenario described above where an Apache server may be serving multiple websites from the same TCP port, the iboss Zero Trust Edge will only authorize connections to specifically the resource (or website) the user has access to. Every request is authenticated and authorized by the iboss Zero Trust Edge.

Cloud Security with Multiple Service Edges

Many solutions have multiple service edges to connect users to resources. Unfortunately, the differences in the ability to authenticate and authorize every request depending on what server edge is traversed by the user is common in many models designed in this nature. For example, with some vendor implementations, data traversing a “private access” edge has no data inspection. This means there is no ability to authenticate or authorize a request, let alone apply security and provide logging visibility for the request. In addition, part of the tenets of NIST 800-207 Zero Trust, as will be expanded on later, indicate that authentication includes environmental factors. This includes determining whether the device the user is accessing a resource with has an acceptable posture, such as having the firewall enabled and antimalware running. With solutions that leverage multiple service edges, it is commonplace that one service edge applies posture checks while the other does not. This in turn results in a different level of authentication and authorization capability purely based on where a resource is located.

The iboss Zero Trust Edge is a single global security service edge that can provide the same level of authentication and authorization for each request, regardless of where the resource is located. It ensures that security and logging occur for each transaction and that the principles of Zero Trust apply in all circumstances.

Tenets of Zero Trust

The NIST 800-207 Zero Trust Architecture publication provides a set of nuanced tenets with critical implications that are easy to miss. These are baseline core concepts and requirements that set the foundation for everything else that is built on top of the architecture. While the NIST 800-207 provides a unified list of core Zero Trust concepts, the CSWP 20 planning guide takes this a step further by providing detailed clarity for the tenets defined within the NIST 800-207. To do this, the CSWP 20 planning guide breaks the tenet concepts into three categories which include the actors involved in a Zero Trust exchange: the user, the asset, and the flows to the protected resources. This is critical because it is easy to miss the nuances of the tenets which are clearly listed in the NIST 800-207 publication. By providing this level of detail broken down by category, it ensures that administrators and implementors do not miss key foundational concepts which will have long term implications on architecture that is built which will result in less security, less visibility, and a reduced potential to maximize the value of Zero Trust into the future.

The following will list each tenet described, within each category, and provide additional context and clarity to avoid common pitfalls. It will also describe how the iboss Zero Trust Edge fulfills these requirements in their entirety.

Tenets that Deal with Network Identity Governance

These tenets deal with authentication and understanding which user and asset want access to a protected resource.

Tenet - All resource authentication and authorization are dynamic and strictly enforced before access is allowed

This tenet mandates that authentication and authorization occur before access is allowed. Key points mentioned in this tenet:

1. "Some end users may have multiple identities" – The iboss Zero Trust Edge supports connecting and associating multiple Identity Providers with appropriate protected resources.

2. "Authorized operations are performed…only when the identity has properly authenticated itself" – The iboss Zero Trust Edge can enforce minimum authentication requirements, including forcing authentication step via SAML or OIDC and via any Identity Provider (Azure AD, Okta, Ping, etc.). The iboss Zero Trust Edge checks every transaction to ensure that the authentication and authorization levels are met. The iboss Zero Trust Edge can force modern authentication is performed even if the resource being accessed is legacy and does not support modern authentication.

3. "Dynamic enforcement means that other factors such as endpoint and environmental factors impact authentication and authorization policies" – The iboss Zero Trust Edge supports an extensive Trust Algorithm which ensures endpoint and environmental factors are met before access is allowed. This includes endpoint posture checks such as ensuring the endpoint has its firewall enabled, antimalware is enabled, and critical OS patches installed. The Trust algorithm can also determine if the endpoint is currently infected and deny access immediately on the very next request.

A key point for this tenet category is that authentication goes beyond username and password, including going beyond Multi-Factor Authentication (MFA). The endpoint and environmental factors must also be considered to properly perform authentication and authorization.

Tenets that Deal with Endpoints

These tenets are centered around the endpoint and provide additional details for meeting those requirements.

Tenet - All data sources and computing services are considered resources

Key points of this tenet:

1. "An enterprise relies on different resources to perform its mission" - An enterprise-owned resource needs to be protected and falls under the Zero Trust umbrella. This includes cloud applications (SaaS), on-prem applications, legacy application, devices, and assets – The iboss Zero Trust Edge is delivered via a single unified security service edge that protects all resources with all security capabilities and visibility applied equally across the enterprise. This is unlike competing solutions which provide various levels of security and visibility simply based on where a resource is located. For example, for some alternative solutions that have an Internet edge and a private edge, inspection is only performed on the Internet edge and not the private edge. This means no security or visibility is possible for some resources depending on which edge is used to access the resource.
2. "If the resource lacks certain security capabilities, the enterprise may need to add a PEP component to provide that functionality" – The iboss Zero Trust Edge forces modern authentication before access to legacy applications which do not support modern authentication natively. This is an example where the PEP provides mitigating control for a resource that lacks the capabilities to meet Zero Trust requirements.

Tenet - The enterprise monitors and measures the integrity and security posture of all owned and associated resources

Key points of this tenet:

1. "This tenet deals with the aspects of cyber hygiene for both enterprise-owned resources and those that may not be owned but used in an enterprise workflow" – The iboss Zero Trust Edge provides Zero Trust Resource policies that can be applied to enterprise-owned and non-enterprise-owned resources designed to prevent leakage from enterprise-owned resources to non-enterprise owned resources. Full endpoint posture checking is included and continuously performed to ensure the health of the assets as they interact with resources.
2. "The state of resources should be monitored, and appropriate action taken when new information such as a new vulnerability or attack is reported or observed." – The iboss Zero Trust Edge includes Trust Algorithms that include endpoint posture (firewall is on, antimalware is on, critical patches are installed) as well as endpoint health (is the device infected). If the Trust Algorithm detects a failure for the endpoint to comply with the minimum requirements, it automatically responds and cuts access from the endpoint to all critical resources.

Tenets that Apply to Data Flows

These tenets apply to interactions between the first two tenet categories (users and endpoints) and protected resources.

Tenet - All communication is secured regardless of network location

Key point of this tenet:

1. "Appropriate safeguards should be in place to protect the confidentiality and integrity of data in transit." - In zero trust, the network is always considered contested. The network the user, endpoint or resource is connected to is always considered untrusted. The network includes corporate networks and non-corporate networks, such as the user's home. Location is irrelevant and the connection is always considered hostile. The iboss Zero Trust Edge encrypts ALL communication between the endpoint and the Zero Trust security service edge using industry standard TLS encryption. It encrypts data targeting enterprise-owned resources but also encrypts data traversing to non-enterprise-owned destinations. The connection the endpoint is connected to is completely untrusted. In addition, the iboss Zero Trust Edge encrypts DNS using the DoH standard (DNS over encrypted HTTPS). This ensures no attacker can snoop or modify communication between end users and resources regardless of location. Encrypting data in transit includes resources that do not support encrypted communications. The iboss Zero Trust Edge will encrypt the communication between a resource and a user, from end to end using TLS.

Tenet - Access to individual enterprise resources is granted on a per-session basis.

Key point of this tenet:

1. "In an ideal zero trust architecture, every unique operation would undergo authentication and authorization before the operation is performed. For example, a delete operation following a read operation to a database should trigger an additional authentication and authorization check." – The iboss Zero Trust Edge is built foundationally with this principle in mind. Each transaction runs through an authentication and authorization check before access is granted. This includes applying full security being applied to the transaction such as malware defense, CASB, DLP and policies.

This tenet is incredibly important and cannot be underestimated. Legacy approaches and deficient VPN replacements have serious gaps that result in this tenant not being met. For example:

1. With legacy VPN – Authentication and authorization ONLY occur at the point of login. After login to the VPN, traffic flows freely, without security, inspection, or logging. Authentication and authorization cannot be enforced before every operation is performed using a legacy VPN approach.

2. With Zscaler – There are two service edges, Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA). Depending on which edge is traversed, the transaction is either inspected or not. If traffic traverses ZIA, the data flow is inspected for security and logging. If traffic traverses ZPA, the traffic flow is NOT inspected, meaning no security including CASB, malware prevention or DLP. This is a critical capability gap because there is no way to enforce authentication and authorization before every operation if data is not inspected as it traverses ZPA.

3. With typical solutions that leverage Single Packet Authorization (SPA) – With this approach, authentication and authorization occur when a user requests permissions to access a resource from a Policy Decision Point. The PDP issues a token that contains the privileges of which resources can be accessed by the end user. This "pre-authorized" token is then presented by the endpoint to the Policy Enforcement Point for access which opens the ports and protocols

for the end user. This approach has serious flaws. First, this tenet requires authentication and authorization for every request before access is granted. If ports and protocols are opened, the user can interact and perform many requests without additional authentication and authorization checks to those ports. Secondly, since the authentication and authorization occurred once at the beginning of the transaction, authentication and authorization does NOT occur at the time of access for each request. This is like a VPN. Lastly, if the authorization token which contains privileges to access ports and protocols is stolen, an attacker could use that token to access those resources because authentication and authorization is not occurring at the time of access. These are critical flaws to this approach which eliminate it from achieving NIST Zero Trust principles.

Tenet - Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.

Key points of this tenet:

1. "In zero trust, the default behavior for all resources is to deny all connections and only accept connections that are explicitly allowed by policy." – The iboss Zero Trust Edge provides simple-to-configure Zero Trust Resource Policies that can deny access by default and only allow those users that are explicitly authorized to access a resource.

2. "Those authorized to access the resource must still authenticate themselves and prove they meet the enterprise policy to be granted the session. This may include meeting requirements such as client software versions, patch level, geolocation, historical request patterns, etc." – The iboss Zero Trust Edge uses a Trust Algorithm that is applied for each and every request between a user and a resource. The Trust Algorithm includes the ability to automatically deny based on software versions, patch level, geolocation, or request patterns, such as detecting when an endpoint is infected because it is found beaconing to a Command and Control (CnC) center.

Tenet - The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

Key points of this tenet:

1. "Zero trust adds a dynamic response factor that was typically lacking (or not possible) in previous perimeter-based architectures. This requires the enterprise to monitor all traffic to the extent feasible and restricted (or required) by policy…" – The iboss Zero Trust Edge inspects, protects, secures, and logs each transaction to protected resources. The ability to ensure every connection between every user, device, and resource traverses the same unified global Zero Trust security edge provides this critical requirement as logs are generated for each transaction. This is unlike VPNs and alternative platforms such as Zscaler or those that leverage Secure Packet Authorization, which do not inspect every transaction. Without inspecting every transaction, log events for those transactions will not be created, resulting in failing to meet this requirement.

This tenet is another key reason that leveraging an authentication provider (IdP) alone does not come near meeting Zero Trust requirements according to NIST. For example, if authentication and authorization occur only at the point of login, all further transactions with the resource occur directly between the user and resource and are completely unchecked. This means that no logs will be generated for those transactions, in addition to no security being applied, resulting in their failing to meet this requirement.

2. "A zero trust enterprise could move quickly to quarantine the affected resources until they can be patched or modified to mitigate the newly discovered vulnerability." – The iboss Zero Trust Edge includes Trust Algorithms that take automatic action based on several factors including automatically restricting access to sensitive resources if an endpoint is missing critical patches. Because the iboss Zero Trust Edge authenticates and authorizes every transaction, as soon as a signal is detected that results in an action to cut access to resources, that action occurs quickly and is applied on the very next request to a protected resource.

Leveraging the NIST RMF for the Zero Trust Journey

The NIST Risk Management Framework should be used to go through the NIST Zero Trust journey. NIST Zero Trust Architecture fits perfectly under the NIST RMF and follows the same general processes as implementing other controls.

The CSWP 20 planning guide points to the NIST 800-37 Revision 2 publication which is titled "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy." This is a core reference guide for the RMF. In addition, iboss provides an implementation guide which leverages the NIST 800-37 RMF as well but maps this directly to the iboss Zero Trust Edge for implementing Zero Trust.

The RMF follows steps which include categorizing resources, implementing controls, approving, and monitoring the system.

For **more information on each RMF Step,** including **Resources for Implementers** and **Supporting NIST Publications**, select the Step below.

Prepare	Essential activities to prepare the organization to manage security and privacy risks
Categorize	Categorize the system and information processed, stored, and transmitted based on an impact analysis
Select	Select the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
Implement	Implement the controls and document how controls are deployed
Assess	Assess to determine if the controls are in place, operating as intended, and producing the desired results
Authorize	Senior official makes a risk-based decision to authorize the system (to operate)
Monitor	Continuously monitor control implementation and risks to the system

A key phrase that is used here is the notion of a "protect surface." John Kindervag, creator of the term and concepts of Zero Trust, referred to the area between the Policy Enforcement Point (PEP) and protected resource as the "protect surface." The protect surface of the resource should be minimized so that eventually only the PEP can communicate with the resource. The term "protect surface" is referred to as the "implicit trust zone" in the NIST 800-207 publication. The ultimate goal that is desired with Zero Trust is the same. In an ideal situation, the front door to the resource must be minimized completely so there is no direct communication with the resource without it being authenticated and authorized by the PEP.

This is another critical concept and capability that only the iboss Zero Trust Edge can achieve for all resources, including those on-prem and those in the cloud (SaaS). Because the iboss Zero Trust Edge is built on a containerized architecture, enterprises can anchor applications, including SaaS, to the iboss Zero Trust Edge PEPs so that the only communication flow to the application is directly from the PEPs themselves. The PEPs within the iboss Zero Trust Edge have unique IP space that are associated directly to each customer and can be used to create ACLs for traffic flow between the PEP and the protected resource. This includes resources that are multi-tenant and public facing. Alternative vendors, such as Zscaler, require enterprises to backhaul traffic back to on-prem private Zscaler Enforcement Nodes (ZENs) to achieve this capability. By doing this, it violates Network Requirements from NIST 800-207 which require users to be able to access resources without having to traverse the enterprise infrastructure first. This is a requirement because if data flows are backhauled to the on-prem datacenter, costs will rise due to hosting appliances, increased bandwidth to the datacenter and increased labor costs to manage the equipment. In addition, this results in slower connections and a poor end-user experience as well as loss of productivity from the slow connections.

Conclusion

This supplemental guide provided key points when preparing to implement the NIST Zero Trust Architecture according to the NIST 800-207 Zero Trust Architecture framework. Use the iboss **Zero Trust Architecture Implementation Guide E-Book** - iboss as a companion to the CSWP 20 planning guide to implement the iboss Zero Trust Edge which will enable the enterprise to substantially reduce risk and meet compliance.

iboss®

+1 877.742.6832
sales@iboss.com

101 Federal St
Boston,MA 02110

iboss is a cloud security company that enables organizations to reduce cyber risk by delivering a Zero Trust service designed to protect resources and users in the modern distributed world. Applications, data and services have moved to the cloud and are located everywhere while users needing access to those resources are working from anywhere. Built on a containerized cloud architecture, iboss delivers security capabilities such as SWG, malware defense, browser isolation, CASB and data loss prevention to protect all resources, via the cloud, instantaneously and at scale. This shifts the focus from protecting buildings to protecting people and resources wherever they are located. Leveraging a purpose-built cloud architecture backed by 230+ issued and pending patents and more than 100 points of presence globally, iboss processes over 150 billion transactions daily, blocking 4 billion threats per day. More than 4,000 global enterprises trust the iboss Cloud Platform to support their modern workforces, including a large number of Fortune 50 companies. iboss was named one of the Top 25 Cybersecurity Companies by The Software Report, one of the 25 highest-rated Private Cloud Computing Companies to work for by Battery Ventures, and CRN's top 20 Coolest Cloud Security Companies of 2022. To learn more, visit www.iboss.com