DDI UNCOVERED

Solution Overview

efficient iP® *for*

Zero Trust Security

In today's interconnected environments, where workers access networks and applications from diverse locations and clouds, enforcing security policies requires a fundamental shift. The Zero Trust approach, which prioritizes strict "never trust, always verify" principles, replaces traditional network perimeter-based models that are no longer viable. To implement this framework effectively, organizations need precise, contextual data and intelligent enforcement mechanisms.

DDI (DNS-DHCP-IPAM) and DNS Security solutions are pivotal to Zero Trust success. Acting as a foundational Network Source of Truth (NSoT), IPAM centralizes critical network-related data, providing a single-pane-of-glass view of what is connected to networks. As the first service touched in any communication, DNS provides unparalleled visibility and contextual insights into traffic. EfficientIP's advanced DNS Security leverages this visibility for DNS-centric intelligence, granular DNS filtering policies for advanced application access control, continuous monitoring of DNS traffic for behavioral threat detection, and real-time risk mitigation. By combining IPAM's centralized management with DNS's ability to filter and secure communications, organizations can implement Zero Trust strategies with confidence, ensuring robust protection across hybrid and multicloud infrastructures.

Solution Benefits

SIMPLIFIED NETWORK SEGMENTATION	leveraging comprehensive, consistent IP data from IPAM
ENHANCED ACCESS CONTROL	highly granular user-based DNS filtering policies and network segmentation enabling application zoning and ensuring least-privilege access
BETTER NETWORK AND SECURITY COLLABORATION	DNS monitoring and analytics for proactive anomaly identification, investigation, and integration with security tools
ENHANCED THREAT DETECTION	real-time in-depth DNS transaction inspection combined with user behavioral analysis and AI-driven threat detection algorithms
INCREASED OPERATIONAL EFFICIENCY	effective threat handling from prevention to response and automation of security workflows
IMPROVED NETWORK RESILIENCE	protective DNS security for continuous verification, real-time DNS analytics and monitoring, and adaptive response

Business Challenges

Improving security for users, applications, and data requires moving beyond the traditional fortress model. The approach of protecting the network perimeter while treating everything inside as trustworthy is no longer effective in today's diverse and distributed environments. Instead, Zero Trust treats every user, device, and application as untrustworthy by default and enforces the «deny all traffic» rule as the baseline security policy. This paradigm shift raises the global security level and provides a more resilient framework for modern organizations.

But, the journey toward Zero Trust is fraught with challenges, particularly in increasingly complex and interconnected environments. Implementing Zero Trust security across hybrid and multicloud setups, maintaining visibility, and ensuring scalability are just a few of the hurdles that demand robust and granular tools, integration with existing infrastructure and systems, and collaboration between network and security teams. According to the latest EMA Zero Trust Networking Survey, the top challenges organizations face are difficulty integrating with existing infrastructure, lack of network visibility and interoperability, and difficulty scaling Zero Trust initiatives to meet growing demands.

Granting access across diverse networks is especially challenging as traditional perimeter controls fall short. Effective security must be multi-layered and focus on user identity or application signatures rather than technical attributes such as IP addresses or port numbers. Controlling access to internal applications —whether hosted in private clouds or relying on distributed cloud resources— is further complicated because traditional firewalls may not be sufficient for comprehensive filtering.

EfficientIP's SOLIDserver DDI and advanced DNS Security solutions address these challenges by providing comprehensive visibility, highly granular user-based DNS filtering policies for continuous access control and application zoning, real-time DNS transaction inspection, and automated response with the ecosystem. This empowers network and security teams to design, implement, and manage Zero Trust architectures without overhauling their entire IT and network infrastructure, enabling seamless integration and scalable security in complex environments.

Key SOLIDserver DDI and DNS Security Capabilities

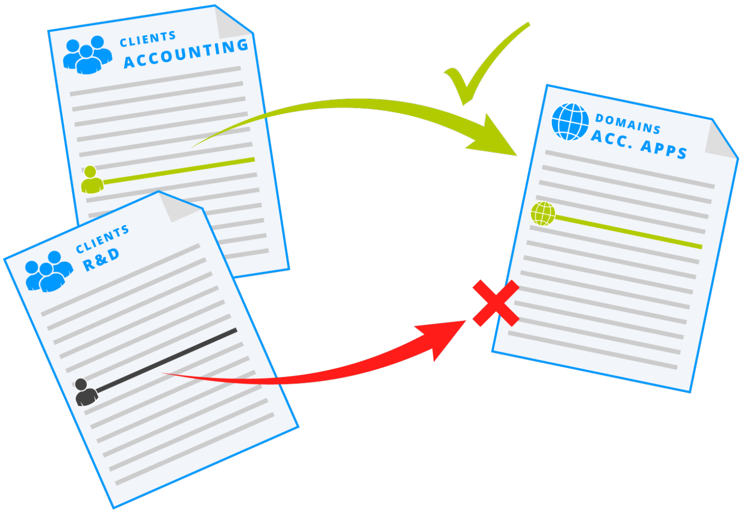
IP Address Management (IPAM) as an extended NSoT

Any IT evolution relies on an IP network, which is used to route traffic between devices through interconnected subnets. To maintain this fundamental layer of any IT system, a structured IP address plan is essential. As a central, comprehensive, and authoritative repository for all IP-related data and metadata, and extending this to data about endpoints, applications, or security zones, IPAM can play a critical role in building a Network Source of Truth (NSoT), providing visibility into what is connected across networks, and playing a central role in security and Zero Trust. Information about every connected device and IP address used on the network can be leveraged by other security components to enforce defined policies and protect the organization's infrastructure, applications and data.

DNS serves as both an entry point and an early checkpoint for network traffic, efficiently routing users and applications while delivering real-time insights. This strategic role makes DNS a cornerstone for forming a first line of defense and enforcing Zero Trust security principles. First, DNS provides the ability to check and authorize the client to reach an application, based on specific criteria. Then, by analyzing DNS queries, it provides valuable global data on behavior and intent—capturing the who, what, and where.

Micro-Segmentation and Advanced Access Control

EfficientIP's DNS Security Solution includes Client Query Filtering (CQF), enabling precise user-based filtering and micro-segmentation to enforce least-privilege access. By grouping devices into categories—such as internal, VIP, and IoT—CQF helps segment network devices. For each group, CQF can apply tailored security policies for access to internal and external applications. It can also filter out resolution requests based on a DNS-centric threat intelligence feed such as DNS Threat Pulse or apply an «allow» filter which lists only authorized domains accessible for this set of devices or clients. This last technique can be applied to untrusted devices (e.g. IoT).



Centralized Management of Policies

EfficientIP's DNS Security provides unified and centralized management of DNS filtering policies to simplify and streamline the definition, deployment, and enforcement of consistent security policies across the enterprise. Leveraging IPAM's built-in NSoT capabilities keeps policies up-to-date and accurate. This minimizes the attack surface, mitigates lateral threat movement, and supports application zoning, ensuring Zero Trust principles are upheld while securing critical assets.

Continuous Monitoring for Advanced Threat Detection

DNS Transaction Inspection (DTI), provides granular visibility and analysis of internal DNS traffic in real-time. Combined with real-time multi-factor traffic analysis, it ensures User Behavioral Analysis to identify threat activity and anomalous traffic patterns early. Meanwhile, AI-powered technologies such as Natural Language Processing (NLP), image recognition, and Tuple Clustering, along with Suspicious Domain Behavior Analysis, improve detection of threats such as phishing, DGAs, or data exfiltration. Security teams can immediately raise alerts, save time, and make rapid decisions. This layered approach ensures proactive identification and rapid response to evolving cyber risks.

DNS-centric Intelligence and Observability

Detailed insights from the DNS Intelligence Center (DNS IC) and DDI Observability Center (DDI OC) provide full visibility into DNS traffic, enabling continuous verification —a core Zero Trust principle. By quickly identifying and effectively investigating anomalies while ensuring network operations, these tools empower SOCs to accelerate threat handling and response, while enforcing strict access controls. This granular observability minimizes blind spots, strengthens threat detection, and ensures adherence to Zero Trust strategies by maintaining ongoing network integrity checks.

Adaptive Countermeasures

Dynamic responses such as IP blocking, Quarantine Mode, and Rescue Mode mitigate threats in real time while maintaining service continuity. These measures restrict unauthorized access, accelerate remediation, and minimize operational disruption, ensuring Zero Trust security principles are enforced and threats are effectively contained.

Seamless Integration and Automation with the Ecosystem

Integration with security platforms such as SOAR, SIEM, and NAC streamlines operations by automating threat detection and remediation. This approach reduces response times and operational overhead, addressing the challenges of managing fragmented security ecosystems. Actionable DNS data and event sharing enrich the capabilities of these security tools, ensuring consistent Zero Trust enforcement while simplifying security workflows and improving SOC efficiency.

Key Takeaways

Zero Trust is critical for securing modern, interconnected environments but presents challenges like complexity, scalability, visibility gaps, and fragmented infrastructures. As the first service to establish communication, DNS is vital for enforcing Zero Trust. EfficientIP’s DDI and DNS Security play a pivotal role in Zero Trust Networking by enabling full visibility on network assets, advanced DNS filtering policies leveraging micro-segmentation for fine-grained access control, continuous DNS traffic monitoring with breakthrough and AI-driven threat detection, and observability to eliminate blind spots. Adaptive countermeasures ensure real-time risk mitigation, while seamless integration with security ecosystems enhances operational efficiency. Finally, centralized management ensures scalability and policy consistency, empowering organizations to secure critical assets across hybrid and multi-cloud environments. All for a low investment.

efficient iP®

REV: C-231226

As one of the world’s fastest growing DDI vendors, EfficientIP helps organizations drive business efficiency through agile, secure and reliable network infrastructures. Our unified management framework for DNS-DHCP-IPAM (DDI) and network configurations ensures end-to-end visibility, consistency control and advanced automation. Additionally, our unique 360° DNS security solution protects data confidentiality and application access from anywhere at any time. Companies rely on us to help control the risks and reduce the complexity of challenges they face with modern key IT initiatives such as cloud applications, virtualization, and mobility. Institutions across a variety of industries and government sectors worldwide rely on our offerings to assure business continuity, reduce operating costs and increase the management efficiency of their network and security teams.

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752