Think ZTN doesn't work or is too hard to deploy? Think different.

dataendure™

Traditional network-based segmentation is an age-old network security practice that isolates network traffic to reduce the attack surface. The network is segmented into VLANs so that the traffic to each segment can be monitored and controlled. This has been a reasonable approach when there is a distinct edge with information and users inside that can be protected.

In contrast, micro-segmentation has a similar objective, but works at a much more granular level. As organizations (users and data) become more distributed, there is no longer an edge to serve as the critical protective barrier – thus rendering the traditional network security practice obsolete. The purpose of micro-segmentation is to reduce the attack surface to a minimum while ensuring the prevention of any unauthorized lateral movement.

In a land of no networks, servers have to be as portable as workstations

Security engineers have the ability to create secure zones to isolate environments, data centers, applications, and workloads across on-premises, cloud, and hybrid network environments. Micro-segmentation itself has three approaches: Network-based, hypervisor-based, and host-based micro-segmentation.

- **Network-based** approaches run into many of the same challenges as network segmentation does and are challenging to manage. The segmentation approach is to apply traditional North/South access control methodologies to what is effectively East/West traffic. This approach leverages firewall rules and perimeter firewalls or mezzanine cards to manage and enforce the policies outside the servers or hypervisors. Because of this, the configurations get very large and difficult to manage and maintain, requiring specialization.

THE PURPOSE OF MICRO-SEGMENTATION IS TO REDUCE THE ATTACK SURFACE TO A MINIMUM WHILE ENSURING THE PREVENTION OF ANY UNAUTHORIZED LATERAL MOVEMENT.

- **Hypervisor-based** approaches seem to be the easier path to take because most modern data centers are virtualized, and more and more NFV (Network Function Virtualization) functionality is becoming native to the underlying hypervisors. This approach is much more manageable as modern virtualizations environments have enabled programmable overlays to apply networking and policies to the guests that run on the hypervisors. The disadvantages to this approach stem from the proprietary nature of each hypervisor manufacturer and the inability to extend the micro-segmentation to other hypervisors or physical infrastructure, creating a multi-tool management headache to address cloud, physical and virtual workloads. Additionally, this approach runs natively on each hypervisor stack and taxes the compute resources of that stack.

- **Host-based** micro-segmentation solves all of these pitfalls by being agnostic to the underlying network, hypervisor, or physical hardware your applications run on. Host-based solutions allow you to set policies based on how you think of your business applications rather than how they connect to the network. Because these systems are entirely independent of the network and underlying infrastructure, they work across cloud, on-premises, physical or virtual systems. Host-based segmentation gives you the granularity to create a micro-segment consisting of a single system, if you were so inclined, reducing the attack surface to the minimal number of hosts required to communicate in an application stack. The only drawback that most people see in this approach is installing an agent on each host. While this does require an initial deployment, an agent-based solution gives you much more granular visibility of the traffic in and out of each host, allowing you to understand your network flows and dependencies better.

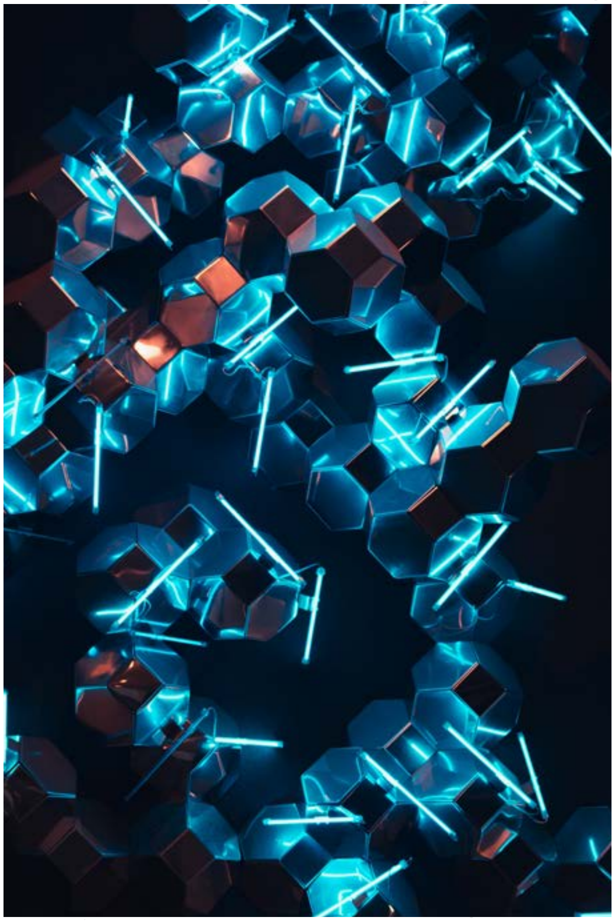
Understand Your Dependencies: Your Micro-segmentation Project Depends on It!

Dependency mapping is a critical first step in any IT project but imperative to deploying a successful and manageable micro-segmentation project. This step is where most micro-segmentation projects fail. Application dependency mapping is not easy and can be daunting. Still, host-based micro-segmentation solutions benefit from understanding individual flows to and from each host in a very granular model. This level of granularity can be challenging if you don't have a solid understanding of your applications and their dependency maps.

So, the assumptive leap at this point is, why would you do anything but host-based micro-segmentation? The answer is not that simple, and not all host-based micro-segmentation solutions are built the same or have equal footing. While most do capture and understand the flows to and from each host, they have done little to map these flows and visualize them so you can fine-tune the automated dependency mappings.

The DataEndure Difference

DataEndure's ZTN Offering is a SaaS-based, managed solution to micro-segmentation. Our ZTN (Zero Trust Networking) solution offers application discovery, dependency mapping, policies, visualization, monitoring, control, security, and portability. Regardless of the underlying infrastructures hosts run on, you have the freedom to move them into and between clouds and hypervisors while maintaining the micro-segmentation policies applied to a given host. Full application stacks, or individual hosts, can be moved into and between any infrastructure or location. There is no need to constantly plan segmentation into your data center moves or migrations to the cloud. And best of all, the added benefit of Application Discovery & Dependency Mapping addresses the most challenging part of moves, migrations, or segmentation.



Get started today.

Help your security keep up with the speed of business.

DataEndure addresses your security and compliance challenges in a cost- and time-effective manner, so that you can focus on growing your company without spending precious time thwarting potential threats. Serving as an invested security advocate with the latest technology and deep expertise, DataEndure can help your organization become less reactive and more resilient in an ever-evolving threat landscape, without draining IT resources and budget. Help your security keep up with the speed of business with DataEndure as your trusted partner.

Get started today with a complimentary Security Heath Check

Our complimentary Security Health Check helps ensure your security tools and controls are working and can detect threats and respond to incidents no matter where you are operating. And our 30-day "Go Live" Guarantee gives you the time advantage, ensuring your service is up and running quickly and your security posture fortified.

About DataEndure

DataEndure is in the business of successful outcomes, helping customers achieve and maintain digital resilience for more than 35 years. We have grown up with the industry, which gives us unique expertise and perspective that we use to help your business bypass traditional data challenges, zoning straight in for what really will or won't work for you. We bring together the gold standard of technological insight and capabilities with a comprehensive solutions portfolio and innovative managed security services that help our clients better manage their IT risks, respond well when assets are threatened, and protect and access critical information wherever it resides. Our managed security services support and secure customers across 23 countries and 4 continents. What can we do for you?

Learn more at www.dataendure.com.

dataendure™