REPORT

Best Practices For Zero Trust Microsegmentation

Apply Zero Trust In The Network With These Best Practices For Microsegmentation

June 27, 2022

David Holmes

with Joseph Blankenship, Andras Cser, Heath Mullins, Alexis Bouffard, Peggy Dostie

Summary

The on-premises network has always been the hardest operational domain to secure. Microsegmentation solutions emerged to apply the core principles of Zero Trust. Yet, most microsegmentation projects fail due to inventory opacity, overoptimistic planning, and improper execution. Security and risk professionals can use this report to understand the many microsegmentation pitfalls that exist and learn best practices for deploying a successful Zero Trust network microsegmentation solution.

Topics

Ransomware And Data Thef... | Zero Trust In The Network ... | Follow Forrester's Best Pra...

Ransomware And Data Theft Flourishes Where Network Security Fails

Forrester clients regularly tell us that their private networks are insecure. They were not properly designed, grew organically, and were never secured. Organizations tried to rectify the situation with rudimentary segmentation, by fielding a NAC solution, or buying into the delirious visions of an infrastructure vendor that promised software-defined, intent-based access. Yet these approaches have been largely unsuccessful. In our recent report, The Forrester New Wave™: Microsegmentation, Q1 2022, 11 out of 14 customer references tried one of these approaches and did not achieve their desired security outcome. To make matters worse, malicious attackers have stumbled onto the perfect monetization strategy, ransomware. After using the payload du jour to get into a network, their malware spreads throughout, encrypting data for later ransom. The ransom further funds the adversary; as we noted in our report The State Of Ransomware Attacks And Defenses, over half a billion dollars of ransoms were paid in just the first six months of 2021. In this hazardous environment, security pros must:

- **Get serious about data classification and visibility.** The CIO of a regional utility recently told Forrester, "To be honest, we should have been more disciplined about classification." His organization had little ability to discover new or complex data, and while its categorization and classification policies were defined, they were not enforced. Similar organizations (of which there are many) need to get serious about data classification and use it as a dependency for other Zero Trust projects, lest they fail to understand what it is they are even trying to protect.
- **Implement microsegmentation as the primary security control for local networks.** Zero Trust is ultimately about the data and implementing security controls that protect it. Reducing the implicit trust that allows lateral movement within a network is a core principle of Zero Trust. Microsegmentation, by applying least privilege access at layer 4, makes it the marquee Zero Trust technology for network security.
- **Embrace Zero Trust as the larger cybersecurity strategy.** While the threat of ransomware compels organizations to bolster both their endpoint and network security, security pros can go bigger by embracing a fuller maturity of Zero Trust as a strategic initiative. Zero Trust stops ransomware propagation by segmenting the infrastructure from the internal data sources outward to the edges of the perimeter. Forrester's Mitigating Ransomware With Zero Trust report details how Zero Trust principles bolster defenses against ransomware.

Zero Trust In The Network Equals Microsegmentation

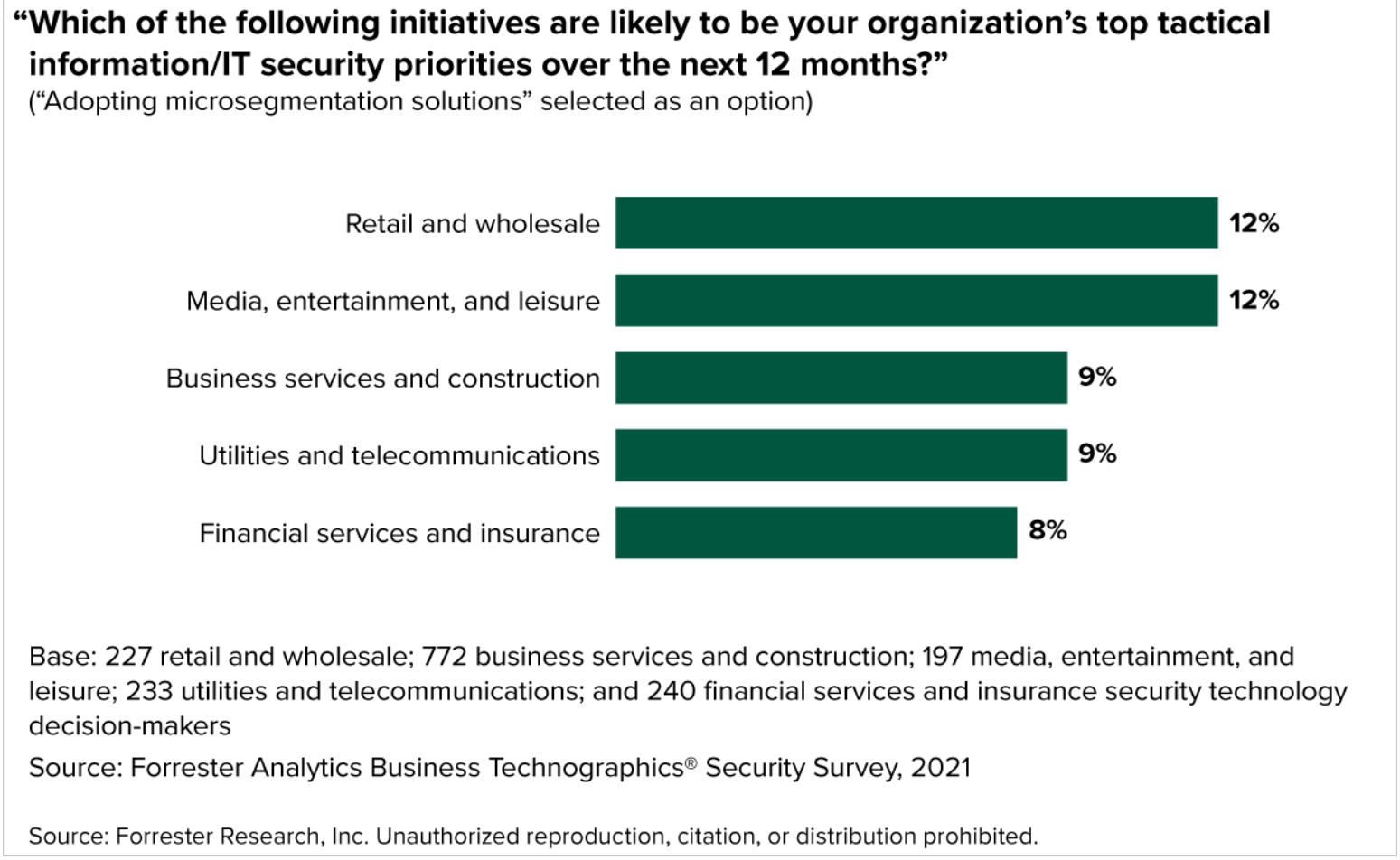
A typical greenfield IP network oozes implicit trust everywhere. It allows any device to talk to any other device in the same subnet and, when connected to switches and routers, any other device on the wide area network. Add in DHCP for easy connectivity, and then any random (unmanaged, unsanctioned) device can join the network and wreak havoc. Microsegmentation reduces the implicit trust in the network by allowing only connectivity explicitly defined by policy, thereby enforcing least privilege access across applications for machine-to-machine traffic. While these capabilities map to Zero Trust, making microsegmentation sound like the holy grail of network security, significant challenges must be overcome to make implementation successful.

Organizations in verticals with on-premises estates that can't be easily moved to the cloud are now prioritizing microsegmentation solution adoption as part of their security strategy (see Figure 1). Many of these organizations find that a manual approach to advanced network segmentation to be beyond their capability. Many have a limited

told us that they attempted to manually map how each component of their applications communicated with each other. After 18 months, he had completed mapping 10 applications — his organization has more than 200. For most firms, it is impossible to justify manually segmenting and firewalling applications; no one has that kind of time, and adding dozens or hundreds of so-called next-generation firewalls between all the VLANs is prohibitively expensive.

Figure 1

Vertical Adoption Plans For Microsegmentation



Most Microsegmentation Projects Fail, Too

Attempting to manually resegment the network is too expensive. You'd think that an automated microsegmentation solution would guarantee success, but you'd be wrong. In our recent report, the Forrester New Tech: Microsegmentation Solutions, Q3 2021, we surveyed more than 20 microsegmentation solutions, spread over five different functional groupings. One representative of these vendors told us, frankly, "most microsegmentation projects fail." We already knew this based on prior research and client conversations, but it was refreshing to hear it stated so baldly by a vendor in the space. Even with automation, most microsegmentation projects fail because of:

- **Analysis paralysis.** Organizations have a mix of on-premises, private cloud, and public cloud properties. Each of these individual environments has microsegmentation solutions tailored to them. Buyers looking for a single solution to fit all will not find one and will spend too much time looking. One network director told us that they were given a blanket cloud migration mandate for their applications without an associated timeline. They were also certain many of the applications could never be moved anyway.
- **Going too big too soon.** Trying to segment too much at once leads to overreach and then failure. A microsegmentation project that is initially too large will have too many stakeholders, too much segmentation with complicated policies, and will accrete so much mass that the project collapses under the collective weight of unrealistic expectations.
- **Lack of visibility.** Microsegmentation projects can go offtrack or stall because organizations are unaware of their own environment. Once they start implementing microsegmentation, they discover additional systems, networks, and applications that were not part of the original project scope. Or worse, they find or remember specialized technical environments (like mainframes), where a microsegmentation solution may not exist.
- **Enforcement anxiety.** Even after microsegmentation software gets deployed, organizations find they lack the confidence to enforce the policies for fear it will cause disruption and break valid communications. Because they don't have complete visibility, they can't simulate with live traffic to determine impact prior to enforcement. Improper enforcement creates connectivity issues and discontinuity for the business.
- **Lack of a nontechnical business driver.** In rare cases, there can be a specific business driver associated tomicrosegmentation. One firm, hired by cybersecurity insurance companies, uses microsegmentation to rebuild a victim's network after a ransomware attack. Another firm told us that due to very high security requirements around networking and data, customers wouldn't use their service unless they had microsegmentation. But these cases are outliers. In the past, most organizations struggled to find a business driver for microsegmentation (outside of cybersecurity for its own sake). However, this is changing with the increasing adoption of Zero Trust, by mandate or otherwise.

Get Tactical With Counterintuitive Prescriptions

That microsegmentation projects often fail doesn't mean they aren't the right approach. It does mean that success will require more discipline. Given the political risks in even

global solution then stalling. Get tactical, and follow these counterintuitive prescriptions:

- **Focus on a specific environment.** Rather than trying to find a solution that works across public cloud, private cloud, and on-premises workloads, choose your priority environment and the solution that fits it best. For many organizations, the physical on-prem network is the most insecure, presents the greatest risk, and offers the greatest opportunity for microsegmentation success.
- **Prioritize network constructs over user identity.** While Zero Trust emphasizes user identity, organizations need to fix the layer 3 and 4 implicit trust problems in machine-to-machine environments now. Don't be swayed by a vendor promising a mix of authentication and authorization across layers 3, 4, and 7 in complex, heterogeneous environments; the technology isn't there yet for on-premises networks.
- **Be skeptical of the microsegmentation freebie.** Be very skeptical of large-scale network infrastructure projects that promise microsegmentation as a side effect. We frequently speak with Forrester clients who are holding the bag for large-scale network infrastructure projects that went awry. Many organizations try a complex Cisco ACI or SDA project, for example, but few can implement it properly. Many organizations (sometimes the same ones!) have VMware NSX in their virtual environment but leave it to collect dust on a virtual shelf instead of using it to understand and ringfence critical applications. When a company *can* implement these giant programs, it's great, but most cannot.

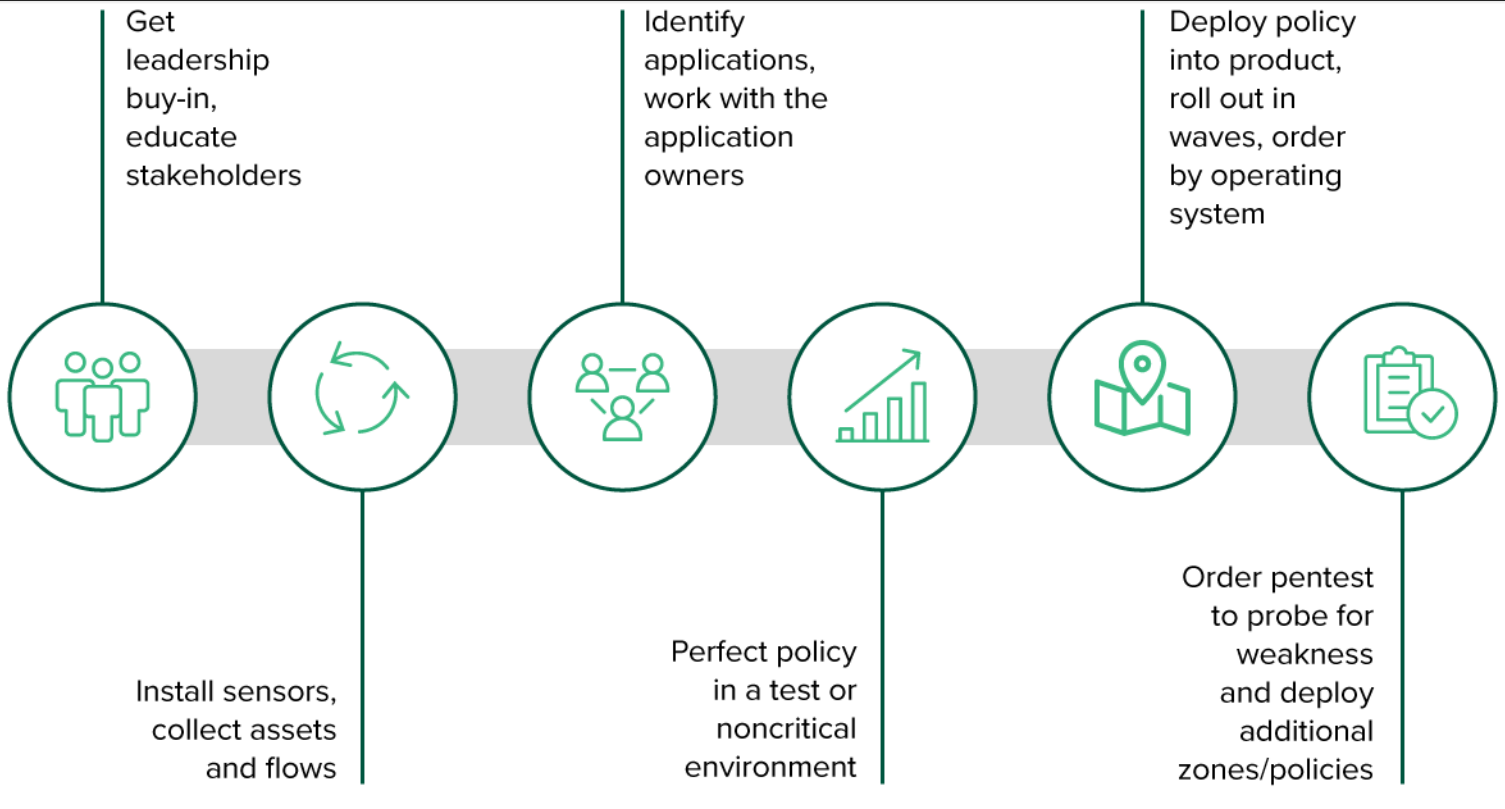
Follow Forrester's Best Practices For Microsegmentation

Too often, security teams seeking to implement microsegmentation don't give themselves enough time to plan the project. Research interviews with many network security practitioners led us to this recommendation: Spend even more time on preparation for microsegmentation than you'd initially consider necessary. Follow this twist on an old adage: Measure twice, segment once. Follow Forrester's six-step process to increase the chances of a successful microsegmentation implementation (see Figure 2). To successfully implement microsegmentation:

- **Cultivate a C-level champion.** Your microsegmentation project will eventually need a push from a C-level champion to get over a political hurdle. Enlist leadership buy-in early and get your champion to announce, across the organization, the Zero Trust microsegmentation initiative. Perform a risk assessment that highlights the network insecurity if the champion needs convincing. When they're onboard, have them communicate the import and implications of fully deploying enforcement.
- **Classify your data.** Zero Trust isn't just about security controls; it's about your data. At the risk of oversimplifying: Some level of data classification must exist prior to microsegmentation, especially for knowing where to initially scope the project. If you must start from scratch because your organization lacks a coherent data classification program, Forrester's Five-Step Strategy For Data Discovery And Classification report recommends you aim for simplicity in your classification levels and use a combination of automated and manual processes.
- **Collect asset and flow information.** All microsegmentation solutions include sensors for collecting network traffic in monitoring mode, and these can integrate with configuration management databases (CMDB) and asset inventory tools. Utilize these wherever possible to help with tagging and annotation of network resources. Do everything possible to ensure accuracy of the CMDB and use it and IP address management (IPAM) as data sources. Collect and analyze longer than you think is necessary before promoting rules to block mode.
- **Analyze and prioritize suggested policy.** Take advantage of the automated modeling capabilities within the microsegmentation solution to test for false positives and anomalies. Some solutions, like Cisco's Secure Workload, keep up to 12 months' flow data for historical testing. Others, like Illumio, can simulate what traffic would break in a draft policy change. While these tools help, don't skip analyzing the suggested policy with a critical eye. Avoid overbroad access policy and strive to reduce implicit trust, prioritizing around the critical applications and flows you identified in the steps above.
- **Engage application owners.** Identify the owners of critical applications and work with them to reconcile the suggested segmentation policy with their understanding of the business logic of the applications. Bring reports that include applications, topologies, server inventories, and owner lists to the relevant departments, and accept their exception requests for required connections like backups, vulnerability management, scanning and administration.

Figure 2

Six Steps Of Microsegmentation



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Execute Via Iteration — Start Small And Perfect Your Process

Even after you've laid the proper groundwork, a significant challenge remains for the implementation: minimizing false positives, where the solution denies legitimate connections between hosts. Each false positive will require a manual fix and ultimately undermines confidence in the initiative as IT learns to blame microsegmentation policy for any connectivity issue, related or not. To increase your chances of success:

- **Start small.** Scope and deploy into a noncritical, nonproduction environment first and stay in monitoring mode before enforcing the policy. Move slowly, be patient, and ensure that the team knows the process and procedures backward and forward.
- **Iterate success.** After you've perfected the initial nonproduction deployment, use the knowledge gained to expand scope, including multiple production applications — but not all of them at once. Continue rolling out the policy in successive waves, ordered by the application's business value, potential outage impact, and operating system. Note each false positive as it occurs and learn to look for the same in every iteration.
- **Check the work.** When the microsegmentation policy has been designed, deployed, and living with enforcement mode for a month, consider ordering a penetration test that's scope is limited to the segmented applications to see if additional zones/policies need to be established.
- **Embed microsegmentation into your rollouts.** Once you've achieved the original project goals, embed microsegmentation into the rollout process. Draw a line in the sand: Mandate that all important rollouts must have classification and microsegmentation going forward. Building the common understanding between IT and security, that microsegmentation is part of the forward process will give leadership confidence that corporate jewels are being protected.

Supplemental Material

Companies We Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Akamai Guardicore

Avocado Systems

Check Point Software Technologies

Cisco Systems

ColorTokens

Forescout

Illumio

Intelligent Automation

Tufin

Unisys