DATA SHEET

Applied Network Segmentation

Restore Critical Systems Rapidly

MOXFIVE recommends network segmentation - specifically software-based microsegmentation - as part of an early-stage ransomware recovery plan to accelerate the pace at which critical business systems can be restored.

During the first 48 hours of an incident response, IT teams focus on understanding affected systems, ensuring that endpoint detection and response (EDR) tooling is deployed widely and effectively, and building a recovery plan. If ransomware was deployed, systems and the business operations they enable are likely impacted. Adding microsegmentation into the approach will enable a more rapid restoration of business-critical systems including legacy servers that EDR tools do not support.

Why Microsegmentation?

Since the early days of network security, experts have recommended segmentation as a means of reducing attack surface and containing the blast radius of successful attacks. Implementing such changes within hardware appliances introduced additional complexities, and organizations embraced only limited segmentation with networks that remained relatively flat inside.

At a high level, software-based microsegmentation enables more granular policies to be deployed with less complexity than traditional network segmentation approaches. Benefits include the ability to easily restrict “internal to internal” (“east-west”) traffic within a network, application-centric approaches that would be very difficult with traditional methods, and cost savings over complex and hardware-centric approaches.

While responding to an incident, two microsegmentation use cases provide outsize benefits relative to their level of effort to implement: legacy operating systems and business critical systems.

Legacy Operating Systems

Many organizations’ first experience with EDR tooling comes on the first day of an incident response effort. Responders need the ability to rapidly gather metadata and other artifacts across the entire environment to determine the scope and impact of the intrusion. Additionally, many EDR tools provide next-generation antivirus (NGAV) features that block known and suspected malicious activities.

Benefits of working with MOXFIVE

IT & Security Expertise On-Demand

With a deep understanding of both IT operations and security, MOXFIVE Technical Advisors can provide the expertise you need and help determine the most efficient and cost-effective solution.

Access to Experts at Scale

MOXFIVE maintains an ecosystem of the industry's best technology experts and service providers so we can quickly assemble the right team with the skills you need.

Streamlined Process

MOXFIVE manages the selection, implementation and procurement processes to keep projects on schedule and minimize disruption.

Resilient Outcomes

MOXFIVE identifies gaps between business, IT and security objectives to build a more resilient environment.

Despite legacy operating systems presenting known risks to an environment, they are a reality for many IT shops. Some servers and workstations must run old operating systems to support specialized applications that cannot be upgraded because the vendors that wrote them are no longer in business. In other cases, the upgrade path away from the outdated systems is lengthy because of the criticality of the applications and business processes they support.

Realities collide: modern EDR tooling does not often mesh well with legacy operating systems. The lack of visibility into these systems stymies the investigative team's progress, missing opportunities to manage risk (for example, having an active attacker in the environment longer than necessary) and increases the business interruption cost.

MOXFIVE has assisted clients in deploying microsegmentation software in these cases to isolate the legacy systems on which the EDR tooling was not supported. The investigative team might not have the same level of visibility but the microsegmentation tool provided a solid level of comfort that those systems were free of attacker activity.

Business Critical Systems

Ransomware can significantly interrupt business operations. In the early stages of an incident response effort, responders initiate multiple simultaneous efforts including investigation, containment, and recovery. Certain systems bubble up to the top of the recovery priority list: Active Directory, email, and file servers are usual suspects. There are also systems that support the revenue-generating processes that are the lifeblood of the business; their downtime translates clearly to dollars.

Considering their restoration can present difficult decisions in those first few days of the response. The business is hurting, but if the systems are brought back online too soon ransomware may again run rampant, setting back the recovery effort. Or the systems could contain a yet-unidentified backdoor mechanism implanted by the attacker that could permit a resurgence of activity.

Microsegmentation software can provide an additional level of comfort to quickly restore such systems. In one case MOXFIVE helped a global manufacturing client restore a small number of servers that controlled critical manufacturing process equipment. The client had limited connectivity within its WAN as part of their initial containment action, which complicated recovery. Microsegmentation enabled them to not only bring those manufacturing operations online within 48 hours, but to do so with added confidence that those servers were protected within a secure segment, while online within a network that might have still been compromised.

Other Use Cases to Consider

Beyond the incident response use cases discussed above, software microsegmentation can be leveraged for multiple other purposes including

- Aiding in implementing a Zero Trust architecture with the ability to flexibly and scalably control diverse workloads and systems.
- Moving beyond traditional Network Access Control (NAC) solutions to a more flexible and comprehensive identity-based segmentation.
- Deploying a unified network protection posture across assets that sit in multiple data centers or cloud platforms.

www.moxfive.com
(833) 568-6695
info@moxfive.com

MOXFIVE