The Futurum Group

Micro-segmentation Keeps Sensitive Mainframe Data in Compliance

AUTHOR **Steven Dickens**
VP and Practice Lead | The Futurum Group

Dave Raffo
Senior Analyst | The Futurum Group

IN PARTNERSHIP WITH

VERTALI

NOVEMBER 2023

Executive Summary

Mainframes hold an organization's most critical and sensitive business data, making it crucial to ensure that data is secure and meets the strictest privacy regulations.

Controlling access through network micro-segmentation is an effective way to protect sensitive data on mainframes by isolating applications or devices. Such isolation is required in heavily regulated industries with compliance standards such as the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and General Data Protection Regulation (GDPR).

Micro-segmentation is an important step toward achieving Zero Trust security. Micro-segmentation can isolate each application into its own network segment. That gives organizations the ability to limit application access to specific network segments or specific devices, providing an additional layer of security beyond user authentication.

Isolating card payment processing applications to specific network segments can greatly reduce the scope, cost, and time of PCI DSS compliance assessments. Although segmenting the cardholder data environment (CDE) from the rest of an organization's network is not a PCI DSS requirement, it is highly recommended by the PCI Security Standards Council. By consolidating data into fewer locations that have more control over that data, segmentation reduces the risk to an organization's payment account data.

The PCI Security Standards Council says that any assets that store, process, or transmit payment card data are "in scope"—meaning they must be assessed for PCI compliance. Thus, the entire network is in scope without proper segmentation. The wider the scope, the longer and more costly the PCI compliance problem becomes.

Network segmentation that isolates the card handling applications reduces the PCI review to that specific area rather than an entire network, which can span hundreds of thousands of devices. Reducing the scope of the PCI DSS assessment also reduces the cost and difficulty of implementing PCI DSS controls. It also mitigates risk to an organization by consolidating cardholder data into fewer locations with greater control.

Introduction – Benefits and Challenges of Micro-segmentation

Segmentation divides a network into segments to make them easier to secure and manage. Micro-segmentation goes beyond that, carving out a segment for each application, isolating and containing the traffic within that micro segment.

The benefits of micro-segmentation include:

- Improves network access control to protect systems by limiting application access to a specific network segment or device.
- Happens at the application level (unlike firewalls) and can protect specific applications.
- Detects new or unsuspected network activity to and from a mainframe computer and blocks unauthorized users from connecting to an application. This approach ensures access only for authorized users and denies everyone else, a zero trust mandate.
- Reduces the potential risk should a network exposure occur.

Inherent mainframe characteristics make these goals difficult to achieve, however.

Traffic in and out of the z/OS mainframe uses Transmission Control Protocol/Internet Protocol (TCP/IP), which was designed to allow any-to-any connectivity with minimal configuration. This setup conflicts with security policies aimed at limiting connectivity to authorized users. The z/OS Communications Server includes controls in the System Authorization Facility (SAF), but the default for many sites is to allow all connections. TCP ports can be protected by SAF so that only permitted applications can open them, but furthermore complex controls are required to secure access to and from remote devices. Controlling tens of thousands of connection combinations can become an impossible task.

Many mainframe sites lack an up-to-date and accurate picture of real-life network activity, such as which network devices are connected to specific applications and what is encrypted.

Most security mechanisms look at inbound TCP connections, but few look at controlling outbound connections. Any user can often initiate an outbound connection to a remote system, and hackers use outbound connections as a backdoor to mainframe services. User Datagram Protocol (UDP) activity is typically unsecured and unmanaged.

There are tools built into z/OS, but they can be difficult to configure and manage at large scale:

- IBM Policy Agent, part of Communications Server inside z/OS, can filter mainframe packets at the application level to provide segmentation but the process can be complicated, especially for organizations with thousands of connections.

- IBM z/OS Management Facility (z/OSMF) provides a graphical user interface (UI) that can be used to define policy agent filtering rules, but this requires time consuming manual data entry and knowledge of IP addresses and port numbers to add filters. As with Policy Agent, IBM z/OSMF does not easily scale for large organizations.

As a result, there is often a lack of understanding of what needs to be configured because application owners, network administrators, and security teams do not always have a complete picture. Among these groups, there can also be confusion over who is responsible for compliance such as PCI/DSS.

Dozens of applications running card data across hundreds of logical partitions (LPARs) could result in tens of thousands of network devices. All those devices become part of the PCI assessment scope unless card data applications can be segmented.

Solving these problems often requires a third-party tool that helps organizations understand what to configure, makes the configuration easy, and assigns configurations to the right group.

Vertali zTrust Manages Micro-segmentation

Vertali zTrust for Networks manages micro-segmentation using IBM z/OS tools. Based on zTrust's network discovery capabilities, zTrust provides an understanding of network and traffic patterns, building a complete map of network connections to facilitate the micro-segmentation process. It works alongside controls managed by IBM z/OS such as user access, multifactor authentication (MFA) and encryption, providing a valuable additional layer of security.

zTrust gives security teams the ability to control access by permitting network segments to access applications through standard SAF controls and commands. It can detect new or unexpected network activity to and from the mainframe and confirm that the micro-segmentation settings are correct and working. zTrust automatically generates policy agent access control lists (ACLs) directly from SAF resources managed by standard External Security Manager (ESM) commands such as those provided with RACF, Access Control Facility 2 (ACF2) or Top Secret Security (TSS).

zTrust detects all traffic on an LPAR and builds a knowledge base of every mainframe connection. The first time zTrust detects an IP address connecting to an application, it records that in the knowledge base, together with the encryption status of that connection.

zTrust uses the knowledge base to build a complete set of External Security Manager (ESM) resources and access lists based on current network traffic. Security teams can review access lists to ensure only permitted network segments and devices are accessing key applications and access controls can limit access to encrypted network connections.

After analyzing the ESM profiles, zTrust builds IBM Policy Agent profiles that permit or block network traffic. zTrust makes segmentation simpler by managing ESM resources by name rather than IP addresses and port levels. It continuously monitors network activity to ensure the ESM policies defined are correctly implemented and to highlight any network changes that may require additional policies.

Over a short period of time, the knowledge base will provide a complete map of network activity by recording every unique connection. zTrust generates an alert when it detects an IP address connected to an application on the network for the first time. Filtering options are provided to whitelist resources to reduce alert volumes. zTrust alerts can be routed to offboard security information and event management (SIEM) solutions such as QRadar or Splunk via the Syslog Daemon.

zTrust documents all activity in audit logs and can generate periodic reports that confirm network micro-segmentation policies are implemented and a valuable resource to prove micro-segmentation is indeed in place and working.

zTrust also ensures connections are encrypted by differentiating between clear and encrypted network connections. It identifies applications that are permanently or temporarily accepting inbound non-encrypted or inbound encrypted connections and applications that are making outbound non-encrypted or outbound encrypted connections.

5 Stages of zTrust Software:

Stage 1 Network Discovery: A unique tool to build your network knowledge base and continuously monitor for new network activity.

Stage 2 ESM Resource Generation: Automatically generate ESM resource definitions and access lists for RACF, TSS or ACF2.

Stage 3 Build Security Profiles: Build policy agent profiles from ESM resources

Stage 4 Managed Implementation of new policies with rollback option

Stage 5 Monitor and Manage Complexity: Monitor network activity and alert on policy violations

At any stage, reports can be produced to provide details on the SAF resources defined, permitted access lists for each application, the network connection maps and the live filters currently loaded into TCPIP.

Conclusion

Micro-segmentation makes it possible to logically divide networks into separate security segments at the level of specific workloads. By allowing organizations to define security controls and restrict access to each segment, micro-segmentation is an important step toward achieving Zero Trust. This security is crucial for financial institutions and others that hold sensitive customer information, often on mainframe computers.

Although micro-segmentation adds to the security of mainframe data, it is difficult to accomplish at scale. Large companies with thousands of network devices and applications might struggle to isolate all their resources without helpful third-party tools. Vertali zTrust works by using standard IBM mainframe tools and interfaces. It adds management, implementation, and monitoring controls to isolate systems with different security needs. This approach reduces the number of systems in PCI DSS compliance scope and empowers the Cyber/Security teams to implement segmentation via their ESM. It also saves organizations time and money from performing these tasks manually.

zTrust blocks unwanted traffic and puts mainframe security where it belongs—in the hands of an organization's security team. It controls access by permitting network segments to access specific applications through standard SAF controls and commands. That provides micro-segmentation rather than blocking or enabling access to the entire mainframe.

Important Information About this Report

CONTRIBUTORS

Steven Dickens
VP and Practice Lead | The Futurum Group

Dave Raffo
Senior Analyst | The Futurum Group

PUBLISHER

Daniel Newman
CEO | The Futurum Group

INQUIRIES

Contact us if you would like to discuss this report and The Futurum Group will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title, and "The Futurum Group." Non-press and non-analysts must receive prior written permission by The Futurum Group for any citations.

LICENSING

DISCLOSURES

The Futurum Group provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

ABOUT VERTALI

Headquartered in the UK, Vertali has a long and distinctive pedigree providing IBM mainframe skills, resources and software to organizations in the UK and around the world. Totally focused on IBM mainframe infrastructure, clients benefit from our experience, expertise and resources.here.

ABOUT THE FUTURUM GROUP

The Futurum Group is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.

CONTACT INFORMATION

The Futurum Group LLC | futurumgroup.com | (833) 722-5337