PROTECTING FINANCIAL SERVICES: BEST PRACTICES FOR RESILIENT CYBERSECURITY.

In today's digital era, financial organizations face a wide range of challenges that can potentially threaten their business operations, customers, and regulatory compliance. Cybersecurity attacks and bad actors can compromise financial data, consumer trust, and hinder digital transformation initiatives. Therefore, financial organizations need to implement resilient solutions that secure their financial data, banking systems, and customers. In this article, we will discuss the best practices to protect your financial services and secure your sensitive data.

- **Consumer Trust and Compliance.** Consumer trust and regulatory compliance are crucial for any financial institution. Data breaches, identity thefts, and other cyber-attacks can damage a financial organization's reputation and cause significant financial losses. Therefore, financial organizations need to adopt proactive measures to protect their data and meet compliance requirements. One of the best ways to achieve this is to implement endpoint and network attack protection through real-time threat detection.
- **Establish Zero Trust Security.** Zero Trust Security is an approach to cybersecurity that requires all users, devices, and applications to be verified before being granted access to the network or data. Financial organizations need to manage financial personnel and consumer identities at a scale for trusted access to critical data and information. Implementing role + purpose + time-based security across your banking services environments can help to ensure that only authorized users have access to sensitive data. Moreover, financial organizations need to understand and be alert to entity behaviors to identify irregular actions by internal employees and external customers. Monitoring and analyzing user behavior can help detect any unauthorized activity and potential threats to your financial data.
- **Financial Data Protection.** Data is the lifeblood of financial organizations, and its protection is essential to maintain business operations and compliance with regulatory requirements. Financial institutions need to ingest and manage structured and unstructured financial data across their environment to eliminate risks. Additionally, discovering, and securing bank data on-premises, in the cloud, or in hybrid environments can increase awareness and enhance data protection. To meet the regulatory finance requirements of GDPR and CCPA, financial organizations should

consider implementing end-to-end encryption and hashing techniques. These techniques help to secure data in transit and at rest, ensuring that only authorized users can access sensitive data.

- **Real-Time Threat Intelligence.** To protect financial data, financial organizations need to implement next-generation SIEM (Security Information and Event Management) for end-to-end financial network and device visibility and event management. Implementing automated orchestration and response solutions with machine learning can quickly mitigate security incidents, thereby reducing the risk of data loss or damage. Furthermore, leveraging threat intelligence with entity behavior analytics can detect known and unknown threats to financial data. This helps financial institutions to stay ahead of the curve and respond proactively to potential threats.
- **Timely Threat Intelligence.** Financial organizations can improve their business performance by having a holistic view of network threats. Geographic customized insights and actionable impact reports can help financial organizations to identify threats, prioritize responses, and reduce potential damage. Global visualization by area can also help organizations to understand the threat landscape and improve their cybersecurity posture.

In conclusion, protecting financial services requires a proactive and holistic approach to cybersecurity. Financial institutions need to adopt resilient solutions that secure their financial data, banking systems, and customers. Establishing Zero Trust Security, implementing financial data protection, and leveraging real-time and timely threat intelligence are the best practices that can help financial organizations to protect their business operations, customers, and regulatory compliance. By following these practices, financial institutions can maintain consumer trust and ensure the confidentiality, integrity, and availability of their sensitive data. IBSCY is a gold partner of Micro Focus in Cyprus and offers IT security solutions to all sizes of organisations in Cyprus and the greater region.

Source