NETWITNESS

DORA and NetWitness NDR

Ensuring Financial Security with Network Threat Detection

Introduction to DORA

The Digital Operational Resilience Act (DORA) represents a significant legislative framework aimed at strengthening the information and computer technology (ICT) resilience of financial entities within the European Union. Enacted in response to continuously escalating digital threats, DORA mandates stringent requirements for financial institutions to ensure their capability to withstand, respond to, and recover from all types of ICT-related disruptions.

Objectives of DORA

The primary objectives of DORA include:

- Enhancing ICT Risk Management: Financial entities must establish robust ICT risk management practices to identify, monitor, and mitigate risks effectively.
- Strengthening Incident Response: Institutions are required to implement comprehensive incident response strategies to promptly address and resolve ICT-related disruptions.
- Ensuring Operational Continuity: The act underscores the importance of maintaining operational continuity during crises, ensuring minimal impact on critical services.
- Promoting Regulatory Oversight: DORA emphasizes the role of regulatory bodies in supervising and enforcing compliance with its provisions.
- Fostering Collaboration: Encouraging cooperation among financial entities, regulatory bodies, and relevant stakeholders to enhance collective resilience.

NetWitness Network Detection and Response (NDR)

NetWitness NDR is an advanced solution designed to provide comprehensive visibility into network traffic, thereby enabling organizations to detect and respond to sophisticated cyber threats. Leveraging machine learning and threat intelligence, NetWitness NDR offers unparalleled insights into network activities, facilitating the identification of anomalies and potential security breaches, and providing tools to swiftly investigate and respond to threats.

Key Features of NetWitness NDR

NetWitness NDR distinguishes itself due to its robust features:

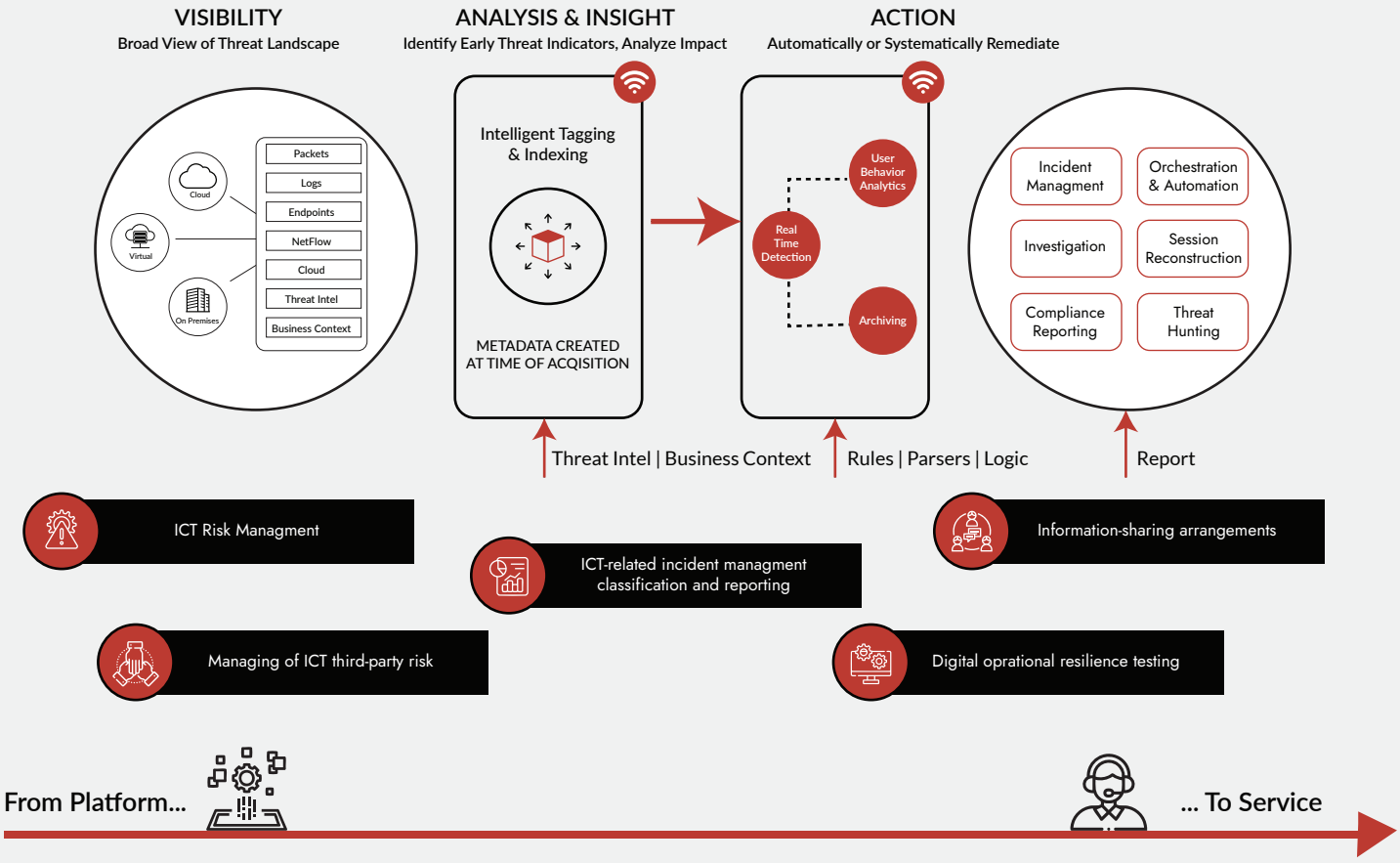
- **Deep Packet Analysis:**
  The solution captures and analyzes network packets to uncover hidden threats and gain a thorough understanding of network traffic.
- **Threat Intelligence Integration:**
  NetWitness NDR integrates its NetWitness FirstWatch as well as global threat intelligence feeds, providing real-time updates on emerging threats and vulnerabilities.
- **Behavioral Analytics:**
  Utilizing machine learning algorithms, the solution analyzes user and entity behaviors to detect anomalies that may indicate malicious activities.
- **Automated Incident Response:**
  NetWitness NDR automates responses to detected threats, ensuring swift and effective remediation.
- **Scalability:**
  The solution is designed to scale seamlessly with the growing needs of organizations, accommodating increasing network traffic and expanding threat landscapes.

Synergy Between DORA and NetWitness NDR

The integration of DORA principles with NetWitness NDR creates a powerful synergy that enhances the operational resilience of financial entities. By aligning ICT risk management and incident response strategies with advanced threat detection capabilities, organizations can achieve a comprehensive security posture.

What makes NetWitness unique?

How does it help speed up investigations?



Enhanced ICT Risk Management

NetWitness NDR's deep packet analysis and behavioral analytics complement DORA's requirements for robust ICT risk management. Financial entities can leverage these capabilities to proactively identify and mitigate risks, ensuring compliance with DORA's mandates.

Strengthened Incident Response

DORA's emphasis on swift incident response is bolstered by NetWitness NDR's automated incident response mechanisms. Organizations can quickly detect and remediate threats, minimizing disruption and ensuring operational continuity.

NETWITNESS

Operational Continuity

NetWitness NDR's scalability ensures that financial entities can maintain operational continuity even during high-stress periods. This aligns with DORA's objective of ensuring minimal impact on critical services during crises.

Regulatory Oversight and Compliance

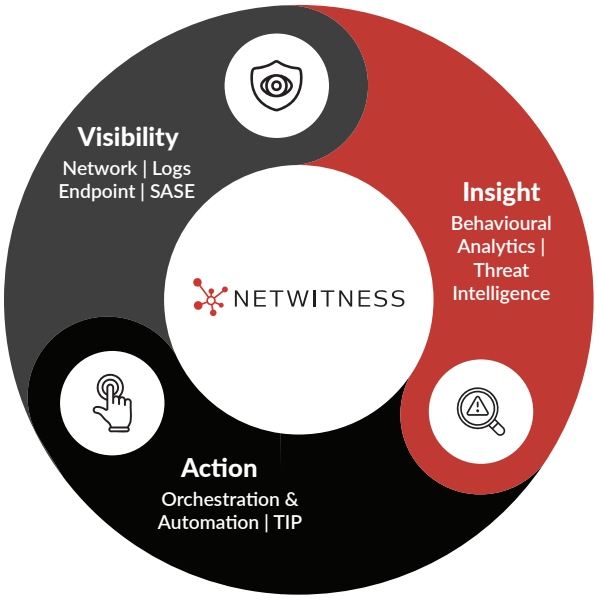
The integration of threat intelligence feeds in NetWitness NDR supports DORA's aim to promote regulatory oversight. Organizations can stay informed about emerging threats and vulnerabilities, thereby facilitating compliance with regulatory requirements.

Collaboration Among Stakeholders

NetWitness NDR fosters collaboration among financial entities, regulatory bodies, and stakeholders by providing a common platform for threat detection and response. This cooperative approach enhances collective resilience against digital threats.

Conclusion

In the face of rising digital threats, the combination of DORA's legislative framework and NetWitness NDR's advanced threat detection capabilities offers a comprehensive solution for financial entities. By embracing these tools, organizations can ensure operational resilience, robust incident response, and continuous compliance with regulatory standards, safeguarding their operations and assets in an increasingly complex cyber landscape.



Visibility

NetWitness Platform delivers unrivaled visibility into your organization's data, wherever it resides - SaaS and cloud applications, on-premises, or hybrid deployments.

Insight

NetWitness applies advanced analytics and threat intelligence to detect and correlate attacks so you can stop them before they damage your operations and reputation.

Action

NetWitness makes detections actionable with tools that block processes, isolate infected applications and endpoints, and re-image hardware.

Ready to learn more? Visit www.netwitness.com