PARTNER CASE STUDY

Zero Trust at Work in European Bank

Continuous visibility and policy enforcement to reduce operational and security risk

A European-based global bank found itself now challenged by greater risk exposure to cyber threats like malware, ransomware, and nation-state attacks as a result of a poorly controlled IT environment caused in part by a proliferation of siloed technologies. The bank also needed to respond to regulators who were asking how they planned to meet increased regulatory requirements including new SWIFT compliance mandates.

The bank sought to apply Zero Trust security principles to verify user access to every application. But first, they needed to create continuous visibility capabilities to discover and control the relationships that existed among its myriad applications.

The bank engaged with vArmour and technology partner, Tanium, to create a multiphase solution to:

- Provide more complete visibility into two global data centers & numerous regional sites
- Increased capabilities to segment and isolate critical applications

vArmour provided multi-environment visibility, observability, policy creation and governance capabilities. Technology partner, Tanium, is a standard platform for segmentation and isolation and delivers per-workload telemetry. By ingesting existing telemetry from Tanium, vArmour was able to accelerate the time to realizable value to weeks, instead of months or years.

The vArmour-Tanium solution enabled the bank to:

- Reduce its attack surface and security risks rapidly. 8,000 workloads were protected within a four-week period.
- Reduce the cost of compliance through full automation of flow modeling and segmentation enforcement, instead of using time-consuming and error-prone manual processes.
- Reduce overall time-to-value. It took just weeks to gain visibility across the entire IT environment by leveraging the bank's existing investments.

Joint Value

Together, vArmour and Tanium empower enterprises to secure applications and workloads across the IT estate with enterprise-wide visibility and automated policy management to:

- Reduce Operational & Security Risk
- Improve Application Resiliency
- Simplify Compliance
- Accelerate Incident Response & Enable Zero Trust
- Deploy Security Policies & Segmentation

The Integrated Solution

vArmour leverages Tanium endpoints to ingest and transform real-time, disparate telemetry data into an easy-to-understand view of applications and their relationships. vArmour then computes security policies for all applications, and automatically orchestrates the policies back to Tanium endpoint systems, providing native enforcement in any environment. Together, the solution computes appropriate Zero Trust microsegmentation policy and identifies any friction that would result in an outage; and accelerates NIST 800-207 Zero Trust asset and workflow mapping.

Find out more about vArmour

 | 650.564.5100 | info@varmour.com | 270 3rd Street, Los Altos, CA 94022