Nanitor

VALITOR

CASE STUDY

# VALITOR

Valitor is an international payment solutions company helping merchants, partners, and consumers make buying and selling easy through face-to-face and online payment solutions for small and medium-sized companies. Their payment solution operates under one roof with the latest card payment technology, merchant accounts, e-commerce, and short-term hire of card machines. Customers of Valitor continually benefit from reliable payment technology, friendly customer support, and tailored pricing with no hidden costs.

The Valitor IT infrastructure is predominantly run on a Windows environment; hosting information about client accounts, payments and transactions, and wider buying and selling activities collating customer data.

## Valitor Security Obstacles

A primary business concern for Valitor was ensuring the company always met the Payment Card Industry Data Security Standard (PCI DSS) framework requirements in real-time. This ensured information security, network security, cardholder data protection, vulnerability management, access control, and network monitoring and testing standards were retained to protect vital company and customer data.

Valitor IT staff recognised that in order to continuously meet the PCI DSS framework requirements, they'd have to address their largest concerns when it came to cybersecurity:

01

### PCI DSS Requirements

It is essential that Valitor continually complies with the twelve requirements of the PCI DSS regulatory framework to ensure secure ongoing business operations. Failure to comply would lead to failed audits and a depletion in company trust, or even restricted operations.

02

### Operational Downtime and Reputational Risk

As an international payment's solutions company, it is imperative for business success that Valitor ensures they are effectively managing vulnerabilities to mitigate any operational downtime. The risks of such could directly impact company revenue alongside substantial reputational damage.

03

### Reporting Efficiencies and Auditing

With ongoing requirements to supply auditing reports and cross-system status updates, Valitor required a system to support effective asset-centric vulnerability management.

# Selecting the Right Solution

After identifying the primary security concerns of the organization, we focused on how to address them effectively. It was clear that Valitor required a simple tool to identify and monitor risks in real-time both quickly and efficiently. Easy access to reporting documentation is critical for auditing purposes. This allows for mitigating the threats posed by operational downtime and protecting customer data.

## Providing a Clear Overview of all Systems

Having a clear overview of the health of all operating systems and platforms was also essential to support Valitor's broad IT environment. It was imperative that Valitor was able to consolidate all issues and risks across their full suite of systems and platforms, whilst identifying each specifically to its environment and device.

## An Efficient System to Provide Clear Remediation Prioritization

Valitor also required the ability to integrate a robust vulnerability management solution with ease, as well as being able to prioritize risks to their organization. This was to ensure that remediation efforts were focused on the most pressing issues to leverage the efficiency of resources.

## Supporting PCI DSS Requirements

Valitor's primary concern was to ensure they were able to meet the requirements of the PCI DSS regulatory framework for compliance purposes. Thus, it was imperative that the system they implemented supported their ability to identify, monitor, and remediate risks affecting their entire IT infrastructure in a timely and efficient manner.

## Ability to Provide Up-to-date Reporting in Real-Time for Auditing Purposes

To ensure Valitor were able to meet regular auditing requirements they needed the ability to provide simple overview reports on the health of their cybersecurity environment. Having the ability to render reports quickly, simply, and accurately, covering information across all devices was a core requirement.

# Tackling the Security Obstacles

After a successful implementation of Nanitor in their environment, Valitor's IT staff quickly recognized how Nanitor would effectively help them to protect their environment and address their primary concerns. Through the support of Nanitor's customer success team, Valitor has been able to consistently meet PCI DSS regulatory framework requirements, have a clear overview of all systems and devices, provide timely reporting for in-house and auditing purposes, and prioritize remediation actions effectively.

Nanitor

VALITOR

Nanitor is a powerful cybersecurity management platform focusing on hardening security fundamentals across your global IT infrastructure. The platform provides unique visibility and control of your security challenges that stakeholders can trust, at a fraction of the cost and time of alternatives.

**Learn more at: www.nanitor.com**
**Email: sales@nanitor.com**
**+354 571 9080**