imperva
a Thales company

CASE STUDY

Vnetrix helps SMEs protect online presence from security attacks with Imperva Cloud WAF

Company overview

Vnetrix has been an IT Managed Services Provider since 2002. As a trusted partner, Vnetrix specialises in offering IT managed services and hosting infrastructure solutions, allowing businesses to direct their attention towards what truly matters – their core operations. With an impressive track record spanning over two decades, Vnetrix is proud to feature a dedicated and expert team that seamlessly integrates with client organisations.

VNETRIX

Company: **Vnetrix**

Industry: **Managed Services Provider (MSP)**

Website: **www.vnetrix.com**

Challenges

Helping clients protect web data from security threats

Security is top of the agenda for most enterprise organisations, but it's not just large companies that are vulnerable to security threats. "SMEs are increasingly targeted by attacks, and they don't always have the scale and resources to make investments to protect themselves" comments Rob Norman, Founder and CEO at Vnetrix.

Data exposure or loss – particularly of customer data – can have a significant impact on a company's reputation, customer trust, and revenues. With ever tighter regulations and legislation to comply with, organisations can also find themselves subject to financial penalties.

In its role as a trusted advisor to its clients, Vnetrix is always looking for scalable, efficient, and intuitive solutions to help protect them from the risk of security attacks that could expose their data.

Deployment

A flexible, scalable and reliable WAF solution

Having worked with Imperva, a leader in protecting applications and APIs at scale, since 2015, Vnetrix recognised the opportunity to make the enterprise-grade Imperva Cloud WAF (Web Application Firewall) accessible and cost-effective for its SME clients. "We've

carefully selected a group of world-class suppliers for the solutions that we deliver for our clients," comments Norman, "and as a global leader, Imperva is our choice for Cloud WAF deployment, as well as a broader range of functionalities, such as its Content Delivery Network (CDN) and DDoS Protection."

Vnetrix now offers Imperva Cloud WAF for both existing hosting clients and as a stand-alone solution for new customers. "To provide SMEs with the flexibility they need, we can either act as a reseller or manage the solution on our clients behalf, billing on a subscription basis." explains Norman.

Blocking 1,000s of attack attempts within a week

Imperva Cloud WAF has swiftly solidified its role as a pivotal element in protecting the infrastructure of numerous Vnetrix clients. An illustrative example can be found in Vnetrix's hosting services for a prominent customer with a high-profile website. In the challenging environment of a busy, multi-server infrastructure, this website experiences millions of visitors during peak periods. Recognising the importance of safeguarding such a valuable digital asset, Vnetrix recommended the deployment of Imperva Cloud WAF.

Within the first week of implementation, Imperva Cloud WAF successfully blocked 1,000s of potential security breaches, underscoring its crucial role in safeguarding the client's digital defences. This demonstrates the tangible value that Imperva Cloud WAF brings to its users.

Clients can benefit from a live view of their digital security through the user-friendly Imperva Cloud WAF portal. This transparency keeps them informed of evolving threats and allows them to easily view security statistics in real time.

A partnership that enables a first-class service

Imperva Cloud WAF operates as a self-managing solution, tirelessly blocking attacks round the clock for Vnetrix's clients, all with minimal intervention. Norman elaborates, "We've established well-documented, repeatable processes for deploying the solution, enabling us to efficiently onboard new clients in a matter of hours."

However, for Vnetrix, the commitment goes beyond merely offering a scalable and dependable security product. The collaboration between Vnetrix and Imperva is founded on a strong partnership approach, designed to provide clients with a top-tier service. "We've received exceptional support from Imperva" confirms Norman. "The Imperva support team has always been able to resolve any issues promptly, and we work closely with the pre-sales team to identify the right products for clients that require more extensive protection."

Results

Improving security for SMEs while growing the business

By deploying the Imperva Cloud WAF with Vnetrix, SMEs can protect their websites from a growing volume of security threats, simplify compliance with legislative and

regulatory requirements, and demonstrate their commitment to security to customers, shareholders, and employees.

Norman emphasises, “In today’s data-driven landscape, Imperva Cloud WAF stands as an indispensable tool. That’s why we’ve made the decision to integrate it as a standard component in our hosting solutions. When we offer recommendations to our clients, our reputation is at stake, but our trust in Imperva WAF and its robust security capabilities is unwavering.”

While the Imperva Cloud WAF is helping improve security for Vnetrix’s clients, it’s also helping the MSP grow its business. “With our Imperva partnership, we’re able to provide stronger security services for our existing clients, and have conversations with potential clients about what we can offer them” comments Norman. “This helps us boost sales and enhances our competitive advantage.”

> “Imperva Cloud WAF is an essential tool in today’s data-driven world. With our Imperva partnership, we’re able to provide stronger security services for our existing clients, and have conversations with new clients about what we can offer them to boost sales and enhance our competitive advantage.”
>
> **Rob Norman,**
> Founder and CEO, Vnetrix.

imperva

Cloud Web Application Firewall

DATASHEET

THALES
Building a future we can all trust

CYBERSECURITY

Application security from the cloud

Modern web applications have become mission-critical for major Fortune 500 organizations that rely on their applications to drive revenue, develop a desired brand image and cultivate customer relationships. Yet they face global threats from all parts of the world. Cybercriminals seek to exploit an organization's digital presence to establish a foothold into their IT environments and gain access to valuable corporate data. Further, the move of web application software towards agile development practices often means that software has not been thoroughly tested, and may be released with critical vulnerabilities that can be exploited by a cybercriminal. Organizations are looking for web security solutions that not only provide comprehensive security protection but also the flexibility to scale for their users around the world.

Imperva Cloud WAF

Imperva Cloud WAF offers the industry's leading web application security firewall, providing enterprise-class protection against the most sophisticated security threats. Whether your websites and applications are hosted in the public cloud or on-premises, Cloud WAF ensures your critical assets are always protected against any type of application layer hacking attempt.

Cloud WAF is part of an integrated, defense in depth suite of application security and delivery services including CDN, DDoS Protection, Advanced Bot Protection, API Security, and Load Balancing at every single one of our global points of presence. All components share intelligence so that security and delivery logic can be applied right from the edge, as soon as the request hits our network. The solution integrates with leading SIEMs, and Imperva Attack Analytics uses artificial intelligence (AI) to distill thousands of Cloud WAF events into distinct narratives, significantly improving security operations center (SOC) efficiency and reducing risk.

KEY CAPABILITIES

- Best-in-class, PCI-certified WAF
- Out of the box, automated protection
- Deploys in blocking mode with near-zero false positives
- Terraform integration enables automated DevOps provisioning
- Backed by security experts at Imperva Research Labs who de-risk use of third party code
- Self-service custom rules
- 24/7 Security Operations and Support Team
- Part of comprehensive cloud application security and delivery
- Delivers threat information for actionable insights in Attack Analytics

Figure 1: Cloud WAF inspects every request, filtering out malicious activity

Defending against web threats

Always-on protection

An advanced identification engine profiles all incoming traffic at the edge in real time, accurately distinguishing between legitimate and malicious clients long before they reach a web application. This automated security process means not only increased web security, lower web-server utilization and reduced bandwidth consumption but also less reliance on in-house security experts and the decrease in accuracy that comes with manual controls. It's no wonder that the vast majority of Imperva Cloud WAF customers deploy in blocking mode out of the box, as the solution allows legitimate traffic through with near-zero false positives.

Beyond OWASP Top 10 protection

Imperva Cloud WAF protects against OWASP Top 10 security threats like cross-site scripting, illegal resource access, and remote file inclusion, blocking attacks in real time. The solution works in conjunction with the Imperva Application Security solution stack, utilizing the different mitigation capabilities that different attacks require - whether it's a DDoS attack or a bot utilizing a SQL injection to attack your API. Moreover, the team at Imperva Research Labs actively discovers emerging threats to provide the up-to-date security protection you need in today's fast-changing attack landscape. Security experts monitor external sources like new vulnerability disclosures and help you reduce the risk of third party code. The team analyzes all traffic going through Imperva via crowdsourced intelligence, automatically vetting then propagating new mitigation rules to all our customers. New security signatures that defend against recently discovered threats are added daily.

Easy to use and scale

Imperva Cloud WAF is configurable through an easy-to-use web interface, protected via two-factor authentication. A simple GUI allows for configuration of custom security rules to optimally enforce security policies within unique environments. With DevOps automation provisioning through our Terraform provider, policy propagation of tens of thousands of rules can happen in seconds. A high-level Cloud WAF dashboard provides a summary overview of the overall threat landscape for your organization, and management is centralized alongside other functionality like API Security, DDoS Protection, and more.

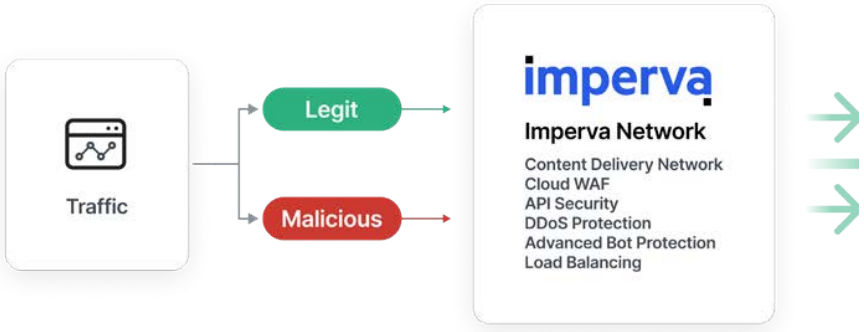

Figure 1: Cloud WAF inspects every request, filtering out malicious activity

About Thales

Thales is a global leader in cybersecurity, helping the most trusted companies and organizations around the world protect critical applications, sensitive data, and identities anywhere at scale. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

IMPERVA APPLICATION SECURITY

Cloud WAF is a key component of Imperva Application Security, which reduces risk while providing an optimal user experience. The solution safeguards applications on-premises and in the cloud by:

- Providing actionable security insights
- Providing WAF protection
- Protecting against DDoS attacks
- Mitigating botnet attacks
- Blocking cyber-attacks that target APIs
- Enabling RASP protection
- Ensuring optimal content delivery

Imperva is an analyst-recognized, cybersecurity leader championing the fight to secure data and applications wherever they reside.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us