SECURE AND COMPLIANT NETWORK INFRASTRUCTURE FOR SLASHNEXT

CASE STUDY

COMPANY OVERVIEW

SlashNext is a cybersecurity company specializing in real-time, cloud-based phishing site detection. Their solution integrates with firewalls and DNS infrastructure to provide instant, effective protection against web-based phishing attacks.

REQUIREMENT

The SlashNext team, led by experienced cybersecurity experts, prioritized building a private cloud solution for granular control over their network and infrastructure. As a startup, they aimed to focus resources on product development and customer acquisition, seeking a partner to manage their cloud platform effectively.

CHALLENGE

- Eliminate vulnerabilities with best-in-class design and practices.
- Build private cloud infrastructure aligned with FedRAMP standards.
- Host SlashNext appliances on the private cloud.
- Ensure continuous security compliance and auditing.
- Implement a robust SIEM for early threat detection and incident management.

SOLUTION (CONTD.)

- Set up a PaaS-based private cloud for SlashNext.
- Conducted OEM hardware testing for security compliance.
- Configured SIEM for early detection, traffic monitoring, and graded alerts.
- Performed penetration testing to ensure PCI DSS compliance.

BENEFITS

- Achieved 60% IT capex savings with the PaaS model and 50%+ savings through OaaS.
- Built a robust, scalable infrastructure in weeks instead of months.
- Maintained 99.999% uptime despite 1,000% infrastructure growth in 18 months.
- Gained on-demand expertise without requiring a large operations team.