FORTINET SECURITY FABRIC: EMPOWERING SECURE DIGITAL TRANSFORMATION

In today's rapidly evolving digital landscape, organizations face numerous challenges securing their networks and protecting sensitive data. As cyber threats become increasingly automated and innovative, a new approach is needed to ensure a secure and high-performing connection between users and applications. Fortinet, a leading provider of cybersecurity solutions, offers the advanced Fortinet Security Fabric.

Gartner recognizes the importance of cybersecurity mesh architecture (CSMA) in combating the expanding threat landscape, identifying it as a top strategic technology trend. Incorporating CSMA can significantly reduce financial losses from cyber-attacks. Fortinet has been at the forefront of providing this type of protection for over a decade through its Security Fabric.

At the core of the Fortinet Security Fabric lies FortiOS, the industry's highest-performing cybersecurity mesh platform. It provides self-healing security and networking capabilities to safeguard devices, data, and applications across the extended digital attack surface. The Fortinet Security Fabric offers comprehensive real-time cybersecurity protection from users to applications by combining convergence and consolidation.

The Fabric's Cybersecurity Mesh Architecture enables organizations to respond swiftly to newly discovered threats across expanding attack surfaces. This broad, integrated, and automated approach delivers cohesive defense measures and enhances protection against evolving cyber threats.

Key Attributes

Built on three key attributes, the Fortinet Security Fabric safeguards digital environments effectively. It enables threat detection and security enforcement everywhere, offering high-performing connectivity and real-time threat detection and policy enforcement across the entire digital attack surface and lifecycle.

The Fortinet Security Fabric aims to close security gaps and reduce complexity by integrating best-of-breed technologies with AI-powered analysis and automated prevention. This ensures consistent security measures and simplifies operations across different technologies, locations, and deployments.

Leveraging a context-aware, self-healing network and security posture, the Fabric enables faster time-to-prevention and efficient operations. Through cloud-scale capabilities and advanced AI, it automatically delivers near-real-time, user-to-application coordinated protection across the entire infrastructure, allowing IT teams to focus on innovation.

Key Pillars

Supported by key pillars, the Fortinet Security Fabric provides a solid foundation for comprehensive security. With a single operating system, organizations can deploy the Fabric across various environments, including physical, virtual, cloud, and X-as-a-Service, supporting a wide range of use cases.

FortiGuard AI-Powered Security plays a critical role within the Fortinet Security Fabric. It offers native integration of FortiGuard security services, enabling fast and coordinated detection and enforcement measures across the entire attack surface. Powered by machine learning and AI models, informed by unified data sets and industry collaboration, FortiGuard services provide robust protection.

Fortinet Secure Networking tightly integrates network infrastructure with advanced security to address the challenges of digital acceleration. This integration ensures consistent policies and superior user experience, particularly for hybrid workforces.

User and Device Security is another vital component of the Fortinet Security Fabric. It protects both users and devices, securing endpoints and providing safe access to resources. With signature-based and behavior-based endpoint protections, organizations can remediate the effects of an attack. User and Device Security also provides zero-trust controls for secure user identification and authentication.

Fortinet Cloud Security solutions deliver visibility and control across cloud infrastructures. By securing applications and connectivity in the data center and cloud resources, organizations can maximize the benefits of cloud computing while ensuring a high level of security. The Fabric's context-aware policy extends into these environments, providing coordinated threat response through integration with FortiGuard AI-powered security services.

To simplify network operations, the Fortinet Security Fabric includes the Fabric Management Center - NOC (Network Operations Center). This center automates network operations, reducing human error and unburdening NOC teams.

For advanced threat detection, response capabilities, and centralized security monitoring and optimization, the Fabric Management Center - SOC (Security Operations Center) is an invaluable component. It enhances security posture across the entire Fabric seamlessly.

The Fortinet Security Fabric's capabilities can be extended through seamless integration with diverse Fabric-Ready Partner solutions, thanks to its open ecosystem. Minimizing gaps in enterprise security architectures maximizes the return on investment and enables efficient administration of security infrastructure using a single management console.

Conclusion

In conclusion, as organizations undergo digital acceleration and face increasingly sophisticated cyber threats, the Fortinet Security Fabric offers a broad, integrated, and automated approach to cybersecurity. Leveraging its key attributes, pillars, and comprehensive ecosystem, organizations can achieve a secure, high-performing user-to-application connection while simplifying operations and reducing risks. The Fortinet Security Fabric empowers organizations to navigate the ever-evolving threat landscape with confidence, ensuring the protection of their valuable assets in an increasingly digital world. IBSCY is a partner of Fortinet in Cyprus and can help businesses of all kinds and sizes to safeguard their sensitive data and operations.

Source