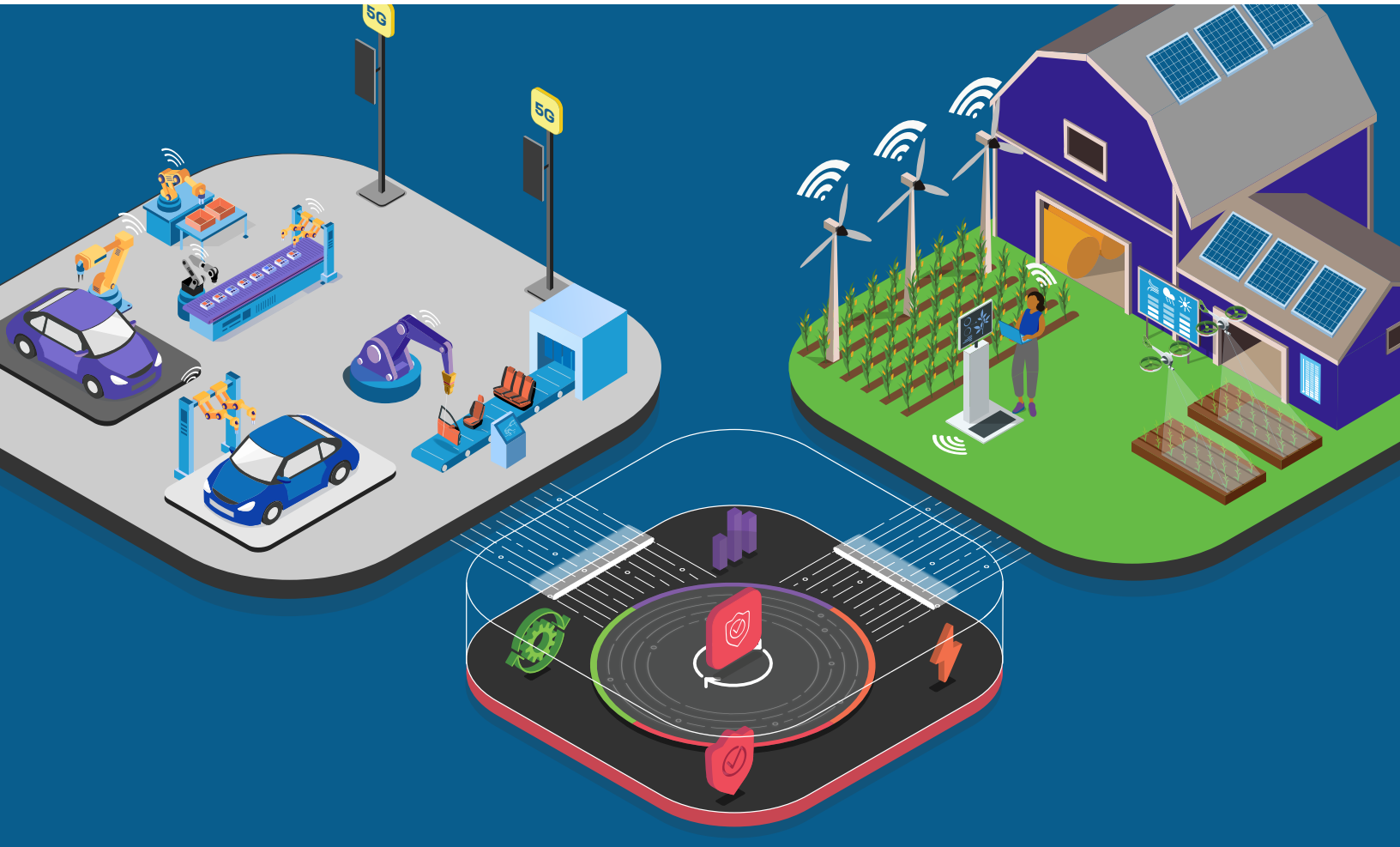
Volterra
Part of F5

SOLUTION OVERVIEW

Optimizing Your Edge Security

The edge brings data and processing power closer to the user. This expands the attack surface and makes it harder to assess and thwart increasingly sophisticated cybercriminals.



KEY BENEFITS

Securely manage APIs
A comprehensive and flexible solution to securely manage APIs and safeguard the edge.

Protect applications and data
Application security solutions speed innovation and increase application development velocity.

Mitigation of IoT threats
A secure IoT solution with the scale and performance required to handle sophisticated and emerging threats.

Secure and optimize N6/SGi-LAN
Reduce TCO by 60% by consolidating your security functions on your N6/SGi-LAN.

Deliver reliable, secure, and scalable services
Implement your edge cloud platform without sacrificing security.

Unparalleled security and QoE
Deliver exceptional QoE to customers while protecting their critical assets.

Unlocking the Edge Is Fraught with Security Challenges

Edge computing brings unprecedented opportunities to transform a wide range of industries. IDC predicts that by 2023, over 50% of new enterprise IT infrastructure deployed will be at the edge rather than in corporate data centers, up from less than 10% today.[1] Having compute, storage and processing power close to the end user is fundamental for reaching the near real-time latency, performance, and high bandwidth required to deliver exceptional customer experiences.

Service providers are in a strong position to play a prominent role in edge computing. They are transitioning to the edge by building virtual, hybrid, and multi-cloud infrastructures, enabling them to deploy applications anywhere across their hybrid multi-cloud and edge infrastructure. In doing so, they face the daunting task of mitigating increased security complexities and, above all, ensuring unparalleled customer Quality of Experience (QoE). As networks evolve, so does the threat landscape. It is vital to gain and maintain customer trust. It is very difficult to earn but can be lost in the blink of an eye.

Service providers must understand the ever-evolving threat landscape they face to safeguard their customers' assets. The highly distributed nature of edge computing increases the security risk for service providers. The massive number of connected devices, unprecedented volumes of data generated, and the required edge infrastructure all make tempting targets for malicious actors. Let's take a closer look at five key risks introduced with edge computing:

1. Explosive growth of IoT devices. Modern applications and services will increase the number of devices connected to the Internet by an order of magnitude—all requiring instantaneous connectivity and data transfer to and from those devices.

2. Distributed edge computing increases the attack surface. The distribution of compute and storage to a greater number of edge locations or endpoints increases the attack surface and reinforces the need for security across the entire network and at every location.

3. Securing multi-cloud edge deployments. Service providers will need to rely on multiple vendors to deliver edge capabilities at scale. This will open the door to increased security threats because each hardware and software component will come with its own set of security vulnerabilities.

4. Traffic visibility and control. Edge infrastructure is built on cloud-native containerized architectures requiring new levels of visibility, control, and security to safeguard the edge.

5. API threats. APIs that are not secure or that are poorly coded can expose the core assets to cyberattacks, placing the entire network at risk.

KEY FEATURES

Extensive API security
API management, high-performance API gateways, and advanced security controls all in one solution.

Securely deploy apps across the entire network
Protect applications across hybrid multi-cloud and the edge.

Prevent threats from IoT devices
An IoT security solution provides device-aware, application-centric policies to prevent threats from the IoT devices.

Consolidated N6/SGi-LAN
The widest range of services—from CGNAT and distributed denial-of-service (DDoS) protection to TCP and video optimization—in a single, unified solution.

Secure Edge Cloud Platform
Security services such as DDoS protection, firewall, and web application firewall (WAF) to prevent malicious traffic from entering your network.

How Do You Keep Customers' Trust?

The edge revolution has created an explosion of connected devices and access points, driving a dramatic increase in network complexity. This has led to expansion of the attack surface exposed to sophisticated and malicious attacks.

F5 offers a comprehensive portfolio of seamless security solutions for hybrid, multi-cloud, and multi-tenant edge deployments. Enabling a zero-trust security model across all edge locations, F5 edge security offerings provide proven and trusted solutions for IoT, API, platform, N6/SGi-LAN, and application security.

MANAGE AND SECURE APIS

APIs are the fundamental building block of modern application development. They can speed up application development by connecting disparate systems and delivering improved user experiences. The use of APIs has decentralized the architecture of applications, making them even harder to secure. As application development moves swiftly to enable more rapid innovation, managing and securing APIs becomes an ever-evolving challenge. Sometimes security is overlooked in the design of APIs, or it is misconfigured, so it lacks security controls against common attacks. Since APIs are designed for machine-to-machine data exchange, many of them represent a direct access route to sensitive data. With applications and data deployed across hybrid multi-cloud environments and the edge, APIs pose a serious risk to organizations of any size.

F5 provides a comprehensive and flexible solution to securely manage APIs from the core data center to the edge of your network. This helps drive the velocity of the business by easing API deployment and management while protecting against API-specific threats. The F5 solution seamlessly integrates into virtually any deployment design or architecture, from any cloud to the edge, improving operational efficiency and reducing risk exposure. With API management, high-performance API gateways, and advanced security controls all in one solution, F5 provides security controls that meet security requirements of the data and API delivery platform to protect organizations against cyberattacks.

Learn more about F5 API solution.

IDC PREDICTS THAT BY 2023, OVER 50% OF NEW ENTERPRISE IT INFRASTRUCTURE DEPLOYED WILL BE AT THE EDGE RATHER THAN CORPORATE DATA CENTERS, UP FROM LESS THAN 10% TODAY.

APPLICATION SECURITY AT THE EDGE

Applications are some of the most valuable assets of your organization. They are the gateways to your data and your customers' data. Attackers know this better than anyone. Applications need to run everywhere across the immense distributed cloud ecosystem and be accessible from anywhere. Workloads need to be instantiated on demand and deployed across the distributed network and the edge. Distributing applications and data to a greater number of edge locations to provide better customer QoE also increases the attack surface and grows the risk to your apps and to your business.

F5 offers a range of next-generation application security capabilities, integrated into multiple different insertion points, depending on your particular app deployments and level of customer management. With F5 solutions, you can protect applications across architectures, clouds, and the edge to reduce security risk and safeguard your application and data. F5 application security solutions help speed innovation and increase application development velocity to improve time-to-market. You can rely on F5 application security to protect your critical assets from today's advanced attacks and tomorrow's emerging threats with the highest real-world security efficacy.

Learn more about F5 Application Security Solutions.

MITIGATE IOT THREATS

Whether consumer or industrial IoT, security is the biggest challenge, with far-reaching safety and legal implications. The massive volume of connected IoT devices introduces new challenges for security. Without adequate security measures, these devices are easily compromised for nefarious purposes. To handle the large number of IoT devices and support QoE requirements— such as ultra-low latency, device prioritization, and requirements for IoT applications—service providers need to deploy secure, scalable, available, and high-performance solutions across their networks.

F5 plays a critical role in ensuring that system security, reliability, and safety are preserved, and recognizes the need to provide network-centric security, focused on end-to-end protection of IoT devices.

Learn more about F5 IoT Security Solution.

ENABLING A ZERO-TRUST SECURITY MODEL ACROSS ALL EDGE LOCATIONS, F5 EDGE SECURITY OFFERINGS PROVIDE PROVEN AND TRUSTED SOLUTIONS FOR IOT, API, PLATFORM, N6/SGI-LAN, AND APPLICATION SECURITY.

SECURING AND CONSOLIDATING N6/SGI-LAN

Consolidated N6/SGi-LAN solutions enable service providers to optimize network performance and reduce costs. This interface is the gateway to the Internet and must be properly secured. Security features that are normally contained in N6 LAN are CGNAT, N6(Gi) Firewall, IoT Firewall, DDoS, Subscriber Security Services, and Secure DNS Cache. N6 LAN consolidation can also help improve customer QoE and reduce TCO.

F5 consolidated and containerized N6/SGi-LAN lets you optimize, secure, and monetize your network. With real-time, per-subscriber traffic visibility, F5 allows service providers to automate and improve operational efficiency of their network. F5 integrates with the widest range of services—from CGNAT, firewall, and DDoS protection to TCP and video optimization—into a single solution with a unified framework that dramatically simplifies service management.

Learn more about F5 N6/SGi-LAN solutions.

CLOUD-NATIVE EDGE PLATFORM SECURITY

Service providers are partnering with hyperscalers to build edge solutions that will appeal to enterprise customers. Each provider will have a different architecture, deployment plan, and timeline, but all must ensure that security is factored into every element of their network. Service providers are implementing a cloud-native, containerized infrastructure to deliver reliable, secure, and scalable services. Protecting the edge is fundamental to ensuring that valuable customer data is secure and is essential for delivering end user QoE.

F5 provides security solutions for service providers to implement cloud-native edge security. Security services such as DDoS protection, firewall, and WAF can be applied at container ingress to prevent malicious traffic from entering the cluster, ensuring that bad traffic stays out of a service provider's network. F5 edge security solutions help ensure customer QoE by providing encryption and offering SaaS-based solutions with system-wide security to consolidate and protect app clusters at the edge.

Learn more about F5 Cloud-Native Infrastructure Security Solutions.

Conclusion

The edge promises exciting new opportunities for service providers to win new customers and grow revenue. Seizing the edge also comes with vexing security challenges as the expanded attack surface creates numerous opportunities for increasingly sophisticated cybercriminals. F5 comprehensive security services provide protection from cyberattacks across hybrid multi-cloud and edge environments. Service providers can rely on proven and trusted F5 security solutions to safeguard their applications and data from ever-evolving and growing security threats.

About Volterra

Volterra provides a comprehensive SaaS platform to deploy, connect, secure and operate distributed applications and data across multi-cloud and edge sites.

To learn more, contact Volterra Technical Sales representative at sales@volterra.io, or visit volterra.io

Endnotes

1 IDC Presentation: *Extending Infrastructure to the Edge*, by Ashish Nadkarni, March 2020