SOLUTION OVERVIEW

Dynamic Infrastructure Security Orchestration

KEY BENEFITS

Simplifies security change management
Security stack orchestration simplifies security solution changes while reducing time, cost, and impact, and eliminating downtime.

Mitigates unintentional traffic bypass
Seamlessly transfers decrypted traffic from one active security solution to another for inspection without interrupting traffic flow.

Reduces administrative costs
Monitors and scales security services and intelligently manages traffic decryption, inspection, and re-encryption across the entire security chain, efficiently utilizing existing and new security resources.

Defends against attacks from layer 2 through layer 7
F5's market-leading security solutions and services can augment or replace portions of the existing security stack.

Business is dynamic and constantly evolving—and evolution means change. Most business changes need to happen quickly for organizations to avoid quantifiable losses: lost revenue, lost opportunities, and lost business.

Some changes must happen immediately or in real-time, such as making your business more secure. If you need to increase capacity on one or several solutions in your security stack to protect your users, your sensitive intellectual property or, more important, critical customer data or personally identifiable information (PII), then you must act quickly. Move too slowly and you may be putting everything at risk.

Say your organization fails a security audit or is breached. Or maybe an attack has threatened your organization's security and you need to upgrade your protection. It's probable that you will need to either change or increase your security to pass a re-audit, or at least to lower your risk threshold to avoid being targeted again.

Like most organizations today, yours probably has amassed an array of security solutions to protect your users, applications, and data. It's also highly probable that these security point products have been manually connected, creating a daisy-chained security stack. As a result, all incoming traffic is now routed through each device in the daisy chain, with each one running security checks on the traffic for malware and other malicious payloads. So now, nearly all your incoming and outgoing traffic is encrypted. This adds a layer of complexity to daisy chaining security solutions. Each of these solutions is forced to decrypt the traffic, perform a security inspection, and re-encrypt the traffic before sending it on to the next link (solution) in the chain. And so on, and so on.

Statically configured daisy chaining of security solutions enables multiple points of failure and can also negatively impact security performance, leading to unintentional traffic bypass and breaches, compromised customer data or PII, and disastrous headlines.

So, you begin the process of changing or updating a security solution in your daisy-chained security stack. Only then do you discover that the pain induced by a bad audit or a breach is compounded by the stress and loss of business when it comes to managing a change in your static security infrastructure.

Change is never easy. That's especially true when an organization manually connects security point products inline, creating a static security stack or daisy chain. Unfortunately, many security devices are unable to perform decryption at scale when placed inline. Complex daisy-chained security stacks not only lack adaptability, induce latency, and negatively impact user experience and security performance, they also lead to long delays in making security changes that your business desperately needs now.

KEY FEATURES

Orchestrates the security stack
Shortens time-consuming security change management processes, simplifying equipment changes and mitigating any detrimental impacts.

Routes traffic based on context and policy
Contextual classification engine increases administrative efficacy by utilizing security resources more efficiently.

Scales security services
Scaling existing or new security services with high-availability and failover protection, achieving enhanced utilization and service availability, even during security stack changes.

Dynamic service chaining
Creates dynamic, logical security service chains based on the type of incoming traffic leveraging existing security solutions.

Intelligent traffic bypass
Efficiently addresses layer 2 and layer 3 security service insertions.

THE TIME INVOLVED IN SIMPLY SWAPPING OUT, UPGRADING, OR CHANGING A SECURITY SOLUTION CAN INCREASE YOUR OPERATIONAL AND BUSINESS COSTS.

Making necessary equipment changes or swaps in statically configured security stacks is difficult and time-consuming. Change windows can involve hundreds of people verifying that critical business flows function as expected. Stress-filled change windows can lead to the loss of many hundreds of human hours, followed by testing and more testing, until verification is complete.

The time involved in simply swapping out, upgrading, or changing a security solution can increase your operational and business costs. Your organization can lose business and revenue. It can also cost your business growth opportunities. The cost and complexity of security change management can even create unintended encrypted traffic bypasses, leading to more breaches and infections, which is exactly what you're trying to protect against.

Your organization needs to make changes to your security stack not just quickly, but at the speed of business.

Dynamic Orchestration: Driving Security Changes at the Speed of Business

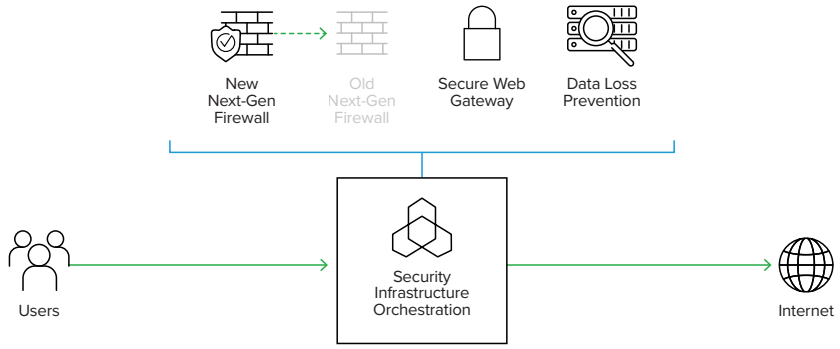
Your business can't wait for the most convenient time to hold a conference call or meeting with hundreds of SecOps, NetOps, and other interested parties; for hundreds of hours of change management calls; and for days of testing, retesting, and, finally, validation. Your organization needs to be able to move at the speed of business.

Your organization needs to seamlessly move traffic from one active security solution to another, and then change or update the first security solution. All without interrupting traffic flow or allowing encrypted traffic to bypass without a security check. To swap out a security solution, you may need to bypass that solution entirely. If you're updating a security solution, you many only want to bypass the solution temporarily without interrupting the traffic flow, traffic decryption, and inspection for the rest of the solutions in your security stack. You may even want to direct traffic streams to new security solutions in a dynamic service chain to try them out.

To achieve all this flexibility, you will need to orchestrate your security stack. Security stack orchestration will simplify your security solution changes while reducing time, cost, and impact. It also alleviates potential traffic bypass and potential exploitation.

By orchestrating your security stack, you will also simplify and shorten the typically cumbersome and time-consuming security change-management process, alleviating potential time consuming negative impacts.

Figure 1: F5 orchestrates existing security solutions and simplifies security change management.



Orchestrating security stacks with F5

F5 orchestrates your existing security solutions with F5 SSL Orchestrator, optimizing and maximizing your security investments. By leveraging F5's best-in-class load balancing, health monitoring, and SSL offload capabilities, your organization will be able to scale security services with high availability.

F5 SOLUTIONS FLEXIBLY INTEGRATE INTO EVEN THE MOST COMPLEX ARCHITECTURES, HANDLING HIGH-SCALE ENVIRONMENTS EFFICIENTLY WHILE PROVIDING FULL SECURITY AGAINST ATTACKS AT ALL LAYERS OF YOUR NETWORK.

F5 solutions flexibly integrate into even the most complex architectures, handling high-scale environments efficiently while providing full security against attacks at all layers of your network.

A contextual classification engine allows F5 solutions to dynamically and logically chain your existing security solutions based on the type of incoming traffic. Traffic steering centered on context-based policies also increases administrative efficiency. F5 independently monitors and scales your security services and intelligently manages traffic decryption, inspection, and re-encryption across your entire security chain, reducing administrative costs while delivering efficient utilization of your existing and new security resources.

Through its dynamic service chaining and intelligent bypass capabilities, F5 allows you to simplify security change management. Using F5's intelligent bypass, your business will be able to address layer 2 and layer 3 security service insertions. Your organization can make changes to the security stack at minimal risk of unintentional traffic bypass, eliminate downtime, and ensure consistent security and inspection of all encrypted and unencrypted traffic.

In addition, F5 can augment or replace portions of your existing security stack. F5 offers market-leading security products and services that defend your organization from attacks from layer 2 through layer 7, including:

- Automated distributed denial of service (DDoS) protection
- World-class web application firewalls (WAF)
- Centralized traffic encryption and decryption
- Management and distribution of the latest encryption protocols and ciphers
- Zero Trust Application Access
- Carrier-grade network address translation (NAT) and access control lists (ACL)

F5 can keep your business safe and compliant with machine learning-based automated threat detection and mitigation with centralized visibility. Machine learning-based traffic baselining at layer 3, layer 4, and layer 7—with automated stress controls, anomaly detection, and attack mitigation with the ability to defend against fast morphing attacks—also protects your business environment and traffic. Further, the ability to centralize configuration of your F5 security services enhances the administrative experience, requiring less time and people power, and significantly lowers ongoing management and maintenance time.

F5 also has built and continues to expand a robust partner ecosystem, enabling a deep breadth of integration with market- and segment-leading security offerings. F5 and its partners can provide an array of services—security assessment, solution design, ongoing evolution, and compliance auditing and reporting—to help your organization orchestrate the security stack simply, quickly, and with great efficacy.

F5 DRIVES YOUR ORGANIZATION'S SECURITY—AND THE CHANGES TO IT—AT THE SPEED OF BUSINESS.

F5 drives your organization's security—and the changes to it—at the speed of business.

Conclusion

Orchestrating security infrastructure drives shorter change management windows for security solutions and is more efficient and less costly than traditional security delivery. F5's security stack orchestration, leveraging F5 SSL Orchestrator, drives security solution changes at the speed of business, greatly reducing the risk, costs, and productivity and revenue losses typically associated with traditional security change management processes.

Learn more about Orchestrating Infrastructure Security—how it saves time, cost, and human power, and drives evolving security at the speed of business.