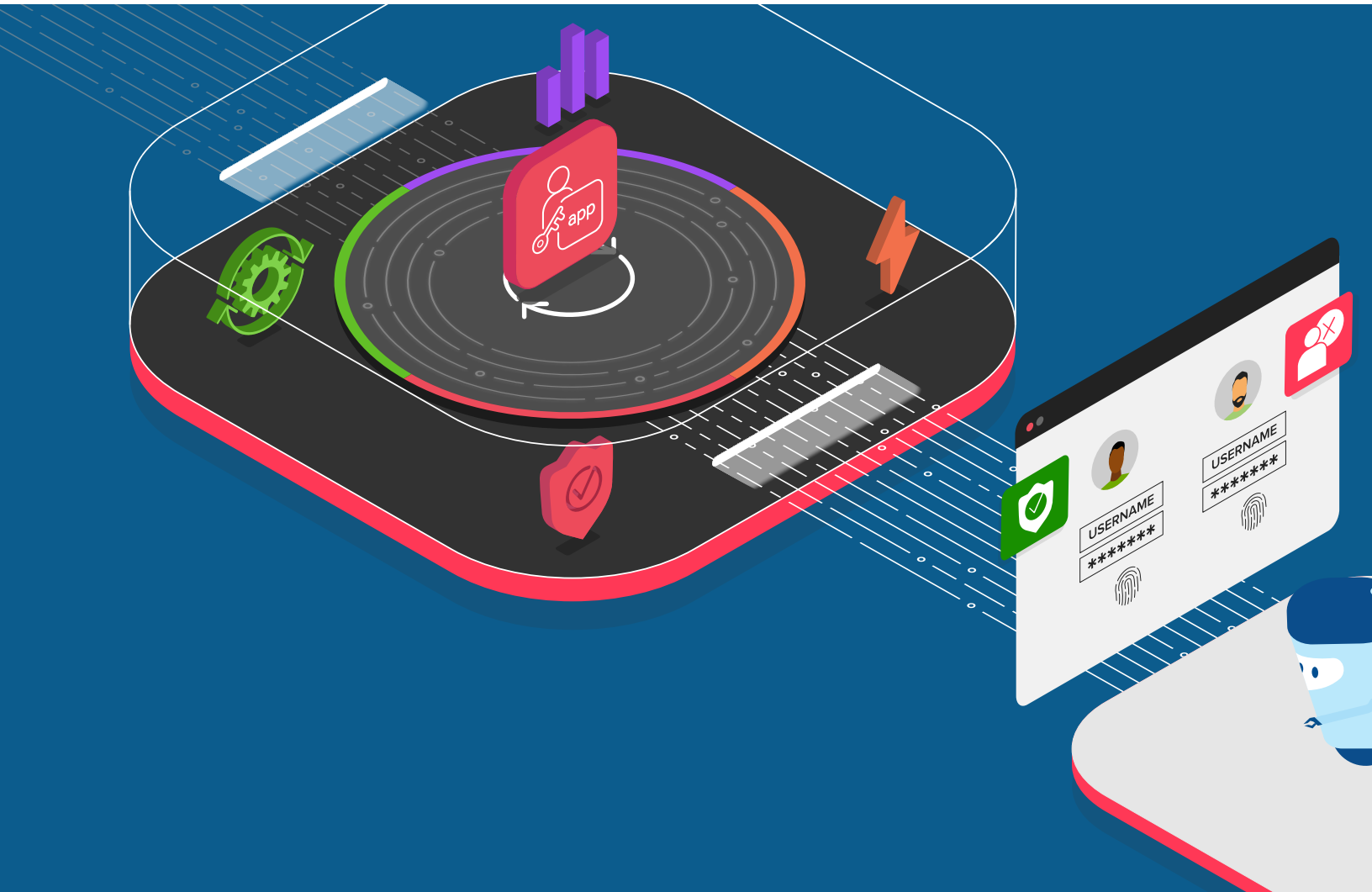
SOLUTION OVERVIEW

Implement Zero Trust

Increase efficiency and security by starting your zero trust journey.



KEY BENEFITS

Secure Application Access
Modern authentication and centralized access and control for all applications.

Identity Service
Leverage existing identity providers for source of truth, including on-premises or Identity as a Service (IDaaS).

Application Infrastructure Security
Get better visibility into attacks targeting the threat surface within your network.

Application Layer Security
Protect against common vulnerabilities and exploits, denial-of-service attacks, and automated attacks that cause fraud through credential theft and abuse.

Securely managing access to corporate applications is critical to preventing data breaches. Doing it well also can increase efficiencies in business processes and user productivity. A zero trust security model can deliver this business value, but zero trust is not a product. Rather, it is an approach—and a maxim—that translates into secure network and application architectures, where an ecosystem of solutions work together to deliver safe, appropriate access management, regardless of user location or device and wherever the network or applications reside.

Challenge

Create common security and performance policies across your application portfolio to decrease risk and improve customer experiences.

The traditional network perimeter style of defense has always resulted in a cat and mouse game between security teams and lurking attackers. A secure perimeter proved to keep out most attackers, but the determined, sophisticated, and sometimes just plain lucky attacker who broke through defenses typically gained relatively easy access to everything on the internal network. This resulted in an increased risk of exposure to data breaches, malware, and ransomware attacks.

But now the castle and moat style of network perimeter is even less secure. Users today frequently operate outside of the office walls, in various locations with various devices, and they connect to applications that may reside on-premises or in various cloud providers. “Trust, but verify,” a philosophy that has been based on correct credentials and a user and device connecting from a trusted (usually internal) network, is now obsolete.

Besides additional risk exposure, attempting to maintain a traditional perimeter with these new ways of working makes for a poor user experience that impacts productivity. Friction increases when users are expected to remember multiple account credentials for different applications inside or outside the corporate network, or are required to use a VPN to access applications. This can result in users being locked out and unable to work, increases the load on the IT help desk or the organization’s identity and access management team, and can lead to increased credential attacks or misuse.

Corporate users and devices have moved outside the traditional perimeter.

New processes and applications driven by digital transformation increase risk exposure.

Traditional perimeters mixed with new controls for securing assets outside the perimeter are too complex to manage.

Solution: Start Your Zero Trust Journey

THE FOCUS IS NO LONGER ON SOLELY PROTECTING THE NETWORK, BUT RATHER ON THE COMPREHENSIVE SET OF CONTROLS FOR THE PEOPLE AND DEVICES THAT CONNECT TO YOUR APPLICATIONS AND NETWORKS.

This shift in the ways of working and the resulting security landscape gave rise to the zero trust architecture. In it, the focus is no longer on solely protecting the network, but rather on the comprehensive set of controls for the people and devices that connect to your applications and networks.

From F5's perspective, these are the four control points that you need to secure:

- For endpoints accessing applications, F5's **trusted app access** solutions provide modern authentication and centralized access and control for all applications.
- For the **identity service**, we have deep partnerships with Microsoft, Okta, and Ping. By integrating our trusted app access solutions with these Identity as a Service (IDaaS) providers, F5 helps you bridge the identity and authentication gap between native cloud and SaaS apps, and mission-critical classic and custom applications, enabling a unified, secure access experience for all users to any application.
- For your network infrastructure, F5's **application infrastructure security** solutions help protect your network from attack and intrusions.
- For your applications, F5 offers **application layer security** solutions delivering security at or near the application and protecting your application stack from layer 4 through 7.

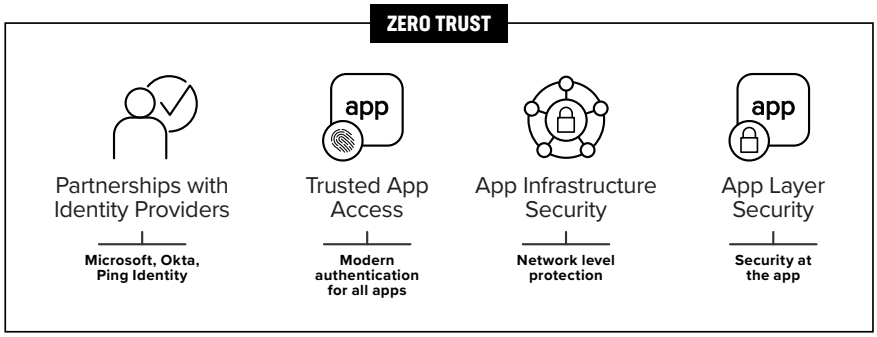


Figure 1: F5 and its partnerships help you secure all four control points in the zero trust model.

TRUSTED APPLICATION ACCESS

F5's identity aware proxy (IAP) capabilities can play a central role in your zero trust architecture. It focuses on identity and access at the application layer rather than the network layer, while centralizing authentication and authorization controls.

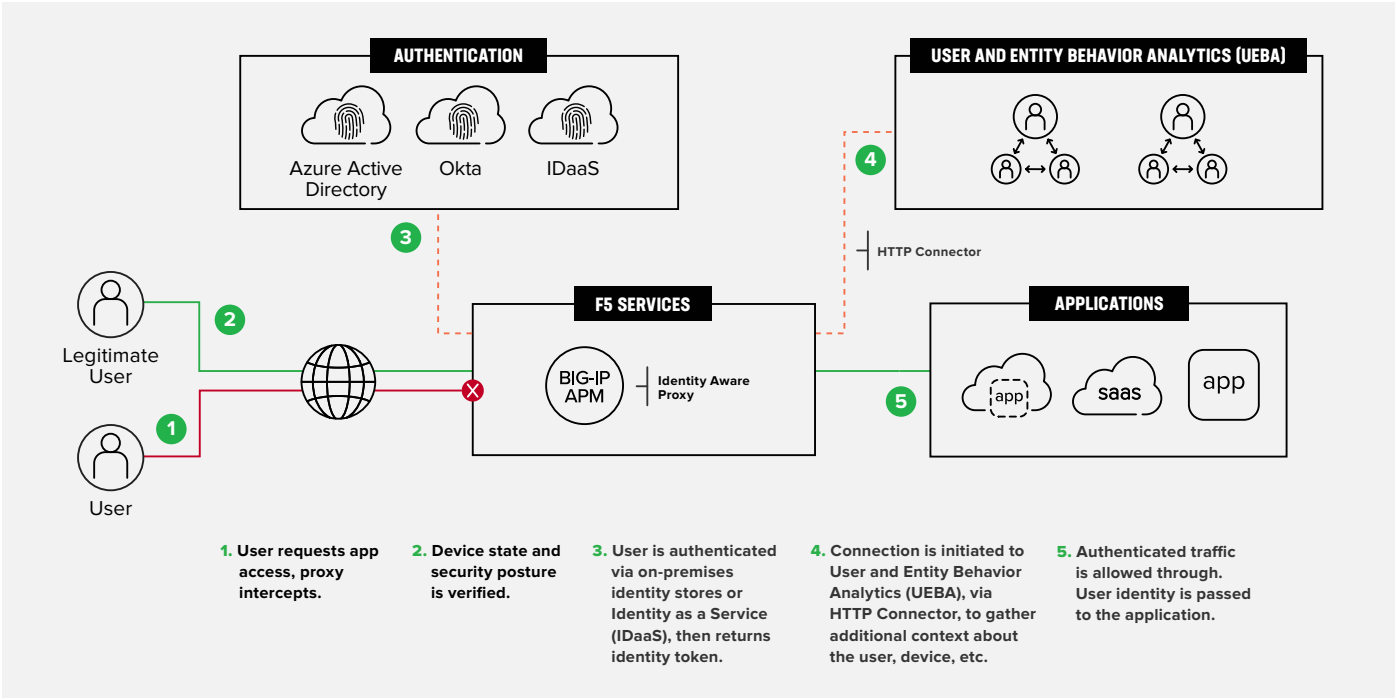


Figure 2: How an F5 identity aware proxy works to control access at the application layer

Core solution services include:

Single sign-on (SSO): Centralize authentication and authorization to provide users a one-stop login to any application, regardless of where it's hosted or resides. This centralizes and simplifies administration of user authentication and authorization, while it enables multi-factor authentication (MFA) for all applications, even those applications previously unable to support MFA, including classic and custom applications.

Device security posture checks: Interrogate a user's device to ensure it complies with corporate policy and is secure, including supported version and patch checks, before granting application access and during the entire application session.

Contextual access with multi-factor authentication: Verify user identity and grant access at the time of login and per request thereafter, based on a multitude of configurable attributes that include device security posture, time and date, user location, application sensitivity, and risk engine integration. MFA can be automated based on risk to be only presented when

necessary, which reduces friction when users log in. Furthermore, riskier login attempts can present step-up authentication—additional requirements for users to log in or be denied access.

APPLICATION INFRASTRUCTURE SECURITY

WHILE THE FOCUS ON SECURING THE NETWORK PERIMETER IS DIMINISHED, SECURITY CONTROLS ARE STILL NECESSARY.

While the focus on securing the network perimeter is diminished, security controls are still necessary. Your network infrastructure plays an important role in ensuring that your apps on-premises, in a data center, or in a private cloud remain secure and available in order to achieve zero trust. One danger that could significantly impact your network, users, and data are threats hidden in encrypted traffic.

F5's SSL/TLS visibility solution solves the encrypted traffic dangers trying to access your network. It eliminates security blind spots by exposing malware hiding in encrypted traffic and halts exfiltration of stolen data. It enables the creation of dynamic security service chains for security inspection tools like web application firewalls (WAFs), next-gen firewalls (NGFW), malware sandboxes, and more by leveraging its context-aware policy engine and policy-based traffic steering. It also intelligently bypasses decryption of sensitive data to keep you from running afoul of industry and government privacy compliance regulations. F5® SSL Orchestrator® monitors, load balances, and ensures the health of your existing security solutions. It also centralizes encryption control, saving your administrators time and energy.

APPLICATION LAYER SECURITY

Attackers know how important applications are for your enterprise and they actively try to compromise your apps, as every one of them can be a back door (or front door) to your valuable intellectual property and data. It's critical to continuously protect every facet of your applications' threat surface as part of your zero trust strategy.

F5 protects your application stack in a zero trust architecture though a suite of solutions. Our web application firewall (WAF) solution prevents common vulnerabilities and exploits, such as the OWASP Top 10 or SQL/PHP injections, as well as DoS attacks, through our behavioral analytics capability. Plus, with the growing use and reliance on APIs for application access and interconnectivity, the F5 solution ensures you can appropriately manage and protect APIs from attacks.

F5 also protects the application threat surface from ever-increasing and evolving automated credential-related attacks to prevent unauthorized access to your users' accounts. Leveraging artificial intelligence and machine learning, the F5 solution can accurately distinguish between human and non-human (bot) traffic. This protects your business from fraud and abuse that can drive up bottom-line costs.

Conclusion

There's not one magical solution that by itself delivers a zero trust architecture, but F5 provides the major pieces of the puzzle. F5's set of solutions ensures that the right people—and only those people—have access to the right applications or information at the right time. F5 can help provide the foundation for your journey into zero trust.

To learn more, explore F5's access management solutions or contact your F5 representative.