F5 Shape DeviceID+

Real-time intelligence about each device visiting web and mobile websites
F5 Shape DeviceID+ is a real-time, high-precision device identifier that utilizes advanced signal collection and proven machine learning algorithms to assign a unique identifier to each device visiting your site. Deployment is simple, with immediate benefits for the security, networking, fraud, and digital teams. Never has understanding the unique devices visiting your applications been so easy.

Benefits of Using DeviceID+

Strengthen Application Security
Strengthen your attack detection and mitigation analysis through accurate device identification. Recognize returning devices that your security systems have already flagged as suspicious.

Optimize Traffic Management
Incorporate a unique device identifier into routing logic to better manage and optimize network traffic. Identify devices even when malicious actors manipulate Layer 7 data.

Mitigate Fraud and Risk
Monitor customer behavior across new account creation, user authentication, e-commerce checkout, and financial transactions to keep customers safe.

Personalize and Accelerate Online Experiences
Make login, checkout, and authentication seamless for known returning users and devices. Shape has demonstrated through A/B testing that reducing security friction increases revenue, and device identification is an important element in any strategy for friction reduction.

How DeviceID+ Works

When each user visits your website, DeviceID+ leverages JavaScript to collect information about the browser, device’s OS, hardware, and network configuration. These attributes feed into Shape’s DeviceID+ service built on Shape’s industry-recognized AI and machine learning capabilities. The data is processed in real time, and a unique identifier is assigned to the device, unless it is already a known device. For returning devices, behavior, actions, and other properties can be recorded, learned, and studied to facilitate the reduction of fraud and a smooth experience for known good users.
Why Shape Security’s DeviceID+ is Unique

Figure 1: Business Use Cases Enabled by Unique Device Identification

Figure 2: Real-time Unique Device Identification through AI-Optimized Signals
Laser Focus on Device Identification
As the industry leader in anti-bot mitigation, defending the world’s largest financial institutions and retailers, Shape is laser focused on distinguishing human traffic from bot traffic, a challenge that depends in part upon effectively identifying devices. Based on Shape’s years of experience battling the world’s most advanced attacks against our financial and commercial infrastructure, Shape has developed the most effective set of signals—uniquely based on a combination of application-level JavaScript and network-level data—to effectively distinguish devices.

Tamper-Proof
Device identification, like so many aspects of security, depends upon integrity and confidentiality, which means preventing attackers from seeing and manipulating the signal collection. To attain this level of security, Shape has gone above and beyond anything previously seen in the industry. Shape has developed the industry’s most sophisticated obfuscation technology relying on a JavaScript-based virtual machine and regularly randomized op codes. Shape’s JavaScript code appears not in its traditional form, but as byte code that executes on the VM. With frequent randomizations to the VM’s opcodes, it is computationally infeasible to crack the obfuscation. This technological advantage results in a device identification resistant to attacker manipulation.

Uniquely Identifying Devices
The key to successful device identification is the capability of uniquely identifying devices, so that no more than one device receives the same identifier. To do this as effectively as possible, Shape’s team of domain experts, including contributing members of JavaScript specification committee TC-39 and specialists in data science, have spent years developing and refining device identification signals, discovering distinguishing features of browser instances through subtle variations in the implementations of JavaScript engines and browser APIs, browser configurations, and the distinctive characteristics of hardware, OS, and network configurations.

Machine Learning Driven Enhancements
Shape develops and refines its signals to identify devices through rich artificial intelligence capabilities grounded in the unique attributes of its data—its volume, comprehensiveness, and its accuracy. As the bot defender for the world’s largest financial and e-commerce enterprises, Shape processes 730 billion transactions per year, creating a massive volume of data. This voluminous data is also comprehensive, including layer 7, network layer, and Shape’s rich JavaScript application-layer signals. Most importantly, because Shape can filter out bot traffic and prevent signal tampering, its dataset is far more accurate than that available to any other provider of device identification, and clean data is essential to the quality of AI.
Get Started with F5 Shape DeviceID+ Today

Deploying DeviceID+ is as simple as adding a JavaScript tag to your website.

There are many easy ways to add a script tag. F5 BIG-IP customers may use a freely provided iApp. Shape Enterprise Defense™ and Silverline customers may reach out to their managed service team to add the tag through configuration. Users of content management systems or tag managers may use these tools to add the tag. And that’s it. You’re up and running.

With the tag inline, you can gain the benefits by consuming the identifier via a cookie or HTTP header. You can integrate the identifier into your application’s real-time behavior or log it to your SIEM for richer analysis.

Please talk to your Shape or F5 account rep or email DeviceIDPlus@groups.f5.com to get started with DeviceID+ today.