BANYAN SECURITY

SOLUTION BRIEF

Elevate Security with Device Trust

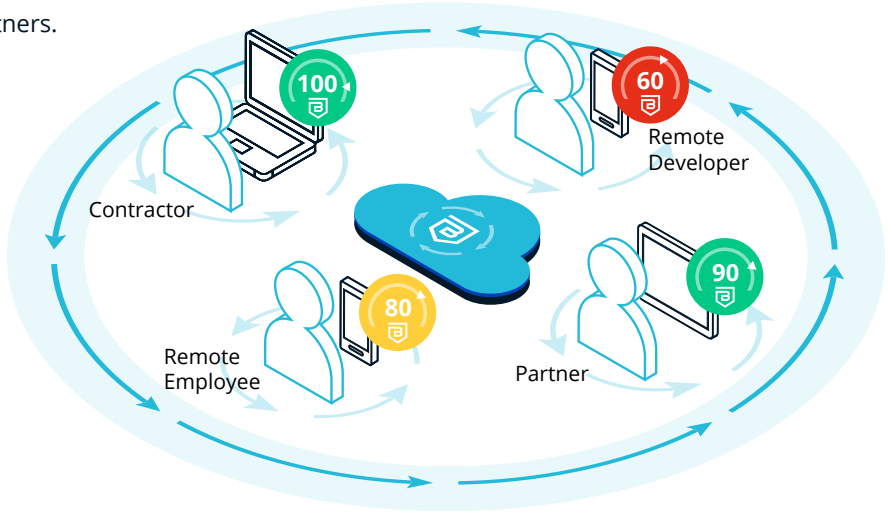
Banyan Device Trust

Achieve Device Trust Across Managed and Unmanaged Endpoints

Most organizations would say the user is the weakest link in their security chain, but they are typically lumping in devices as part of the user problem, especially when they are unmanaged or BYOD. Relying on users to follow and obey device requirements or policies as a condition for access but not have a cost-effective, user-friendly option for verification puts sensitive applications and services at risk.

Fundamentally, Zero Trust requires all users, regardless of physical location, network, and type of employment, to be authenticated and authorized before being granted access to resources, applications, and data. Further, Zero Trust requires the continuous validation of users and continuous validation of the security posture of the devices they use.

Work now occurs anywhere with a mix of employees, contractors, interns, and partners. There has not been an easy way to bridge the gap of what the business assumes and what IT and security can enforce. The principle of least privilege access applies to users but what about their devices? Banyan Device Trust continually looks at the validity of the device and its security posture. Policies can be easily created with the sophistication needed so the full spectrum of security risks based on user, resource, and current device status can be assessed before authorizing access.



Banyan Security makes it easy to achieve real-time device trust, a critical component for comprehensive zero trust access

Support for All Types of Devices and Users

Banyan Device Trust provides two critical functions that other solutions cannot address consistently across the myriad of endpoints, servers, mobile devices, and operating systems for both managed and unmanaged (and BYOD) devices.

1. Certified unique device identification and validation of authorized devices
2. Real-time assessment and validation of the device's security posture

A cryptographic certificate uniquely identifies every device. The certificate is automatically created when the Banyan app is installed, or is obtained through integration with a deployed MDM, EDR, or UEM solution. This certificate provides the first element of Banyan Device Trust – identification. Unlike MDM solutions that can invasively control or erase a device, this lightweight app simply provides information for device identification and security status reporting. If a device is lost or stolen organizations can immediately invalidate this certificate and block further access but does not alter the device. There is no additional cost when users interact with your organization on multiple devices. Their mobile devices, laptops, and even Linux systems will be uniquely registered and continuously validated without causing end user friction or requiring the organization to bear the cost of providing managed devices.

Device Trust Use Cases

Real-time verification of user *and* device trust *and* device security posture is required to grant and maintain access.

Passwordless access enables trusted devices to access applications and resources without relying on credentials that can be lost, stolen, or hacked, making it a seamless solution for users and IT alike.

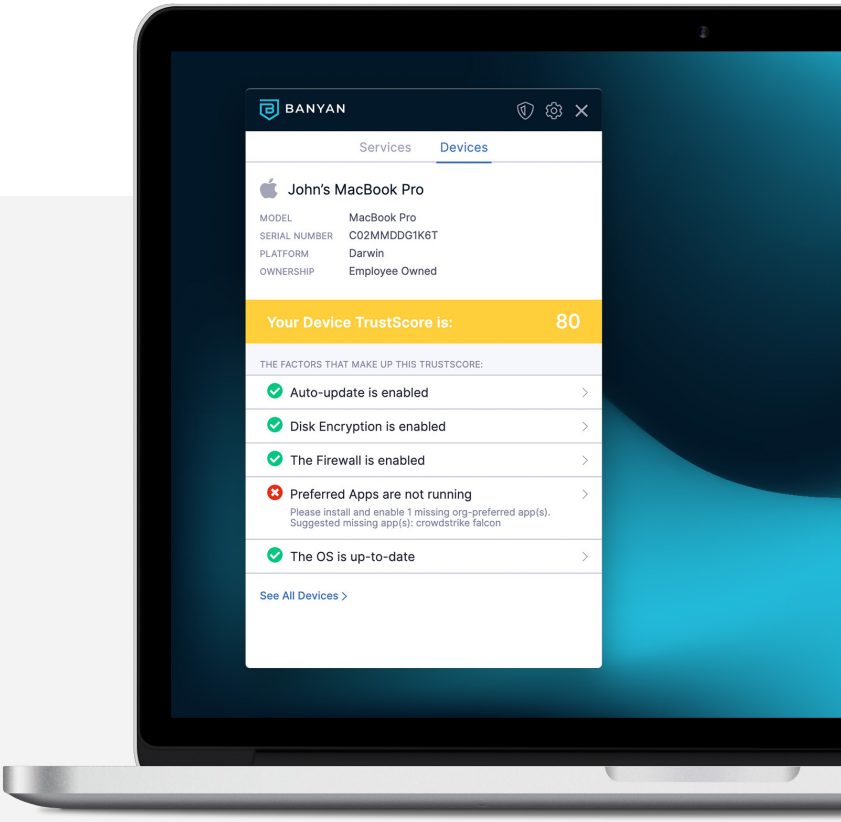
Respond to device loss and theft by invalidating a device's certificate. Active sessions are dropped, and future access blocked.

Enforce device trust even while accessing external cloud-based resources, like IaaS and SaaS applications.

Measure Trust Before Access

Banyan Device Trust solves the problem of enforcing least privilege access across all types of users (employees, contractors, temporary workers, and third parties). For example, everyone with a registered device can access the intranet cafeteria menu, but developers accessing the testing environment must have a higher device trust level by having disk encryption configured and verified security protection. The following desktop and mobile parameters are continually assessed per device and can be used in access policies.

- > Device auto-updates
- > Disk encryption
- > Firewall
- > Jailbroken status
- > Preferred apps running
- > OS is up to date



Authorization Informed by Real-time Security Context

Banyan continuously re-authorizes access based on real-time user, device, and contextual information. Administrators define security requirements for devices within policies that reflect the data sensitivity and potential business risk for individual or groups of resources. Devices not meeting these requirements or having invalid certificates will be blocked. If a policy is updated to require an additional security parameter, immediately any user missing this parameter would lose access, regardless of session length configuration. The Banyan app quickly shows the non-compliant device trust parameter, and directs them to fix their issue. Self-remediation and ease of use minimize IT helpdesk workload making this solution ideal for large organizations.

Steps for Enabling Device Trust and Continuous Authorization

1

Create Access Policy
against context of user identity, device trust, and resource sensitivity in the cloud admin console.

2

Lightweight App Installation
initiated by the user (getbanyan.app) or via a silent install supports all popular device types.

3

Device Authorization
uniquely registers all devices, regardless of platform type or device management software on the system.

4

The Banyan Trust Level
is clearly visible within the Banyan app enabling users to self-remediate device non-compliance.

5

Continuous Re-Authorization
of device trust enforces access policy requirements, immediately disconnecting when a device is no longer compliant.

About Banyan Security

Banyan Security provides secure, zero trust "work from anywhere" access to applications and resources for employees and third parties while protecting them from being phished, straying onto malicious web sites, or being exposed to ransomware. A Flexible Edge architecture enables rapid, incremental deployment on-premises or in the cloud without compromising privacy or data sovereignty. A unique device-centric approach intelligently routes traffic for optimal performance and security delivering a great end user experience. Banyan Security protects workers across multiple industries, including finance, healthcare, manufacturing, and technology. To learn more, visit www.banyansecurity.io or follow us on Twitter at @BanyanSecurity.

BANYAN SECURITY

Banyan Security, Inc. | +1 415-289-9414 | www.banyansecurity.io