Privileged account management done right from the start.

StrongNet™ Secure Admin

Make security choiceless.

Threats are increasing

Ask yourself: How many people at your enterprise have system administrator access to your critical systems? How many devices do they use to exercise that access? Are you confident that every one of those devices is hardened against determined remote, online and offline attacks?

Bring Your Own Device (BYOD) and cloud computing trends have exponentially increased enterprise connectedness. At the same time, the DevOps movement has expanded the number of accounts with system administrator access to servers and data. With all of these entry points, the increasing sophistication of Internet attackers and the potential for insider threats seriously threaten enterprise data security.

Compliance isn't enough

Faced with a porous network perimeter, a heterogeneous computing environment, and hard-to-secure unmanaged devices, IT must raise the bar. Internal and external compliance is key, but focusing solely on compliance pressures too often results in unrealized security potential, without hardened endpoints.

Mitigating risks is difficult because:

- Static passwords are the norm, but best practices include strong authentication plus device verification
- Unmanaged devices are difficult to secure
- High-value credentials and devices can be compromised using rootkits and pass-the-hash techniques

StrongNet integrates with enterprise PKI to give you:

- Certificate issuance and usage that's gated on security compliance, as defined by your IT admin, using our proprietary Measurement Bound Keys.
- Device integrity that's enforced using TPM remote platform attestation. Our attestation protocol is standard-based and uses strong cryptography.
- A high-assurance endpoint security solution that integrates with all PKI scenarios out of the box.

Endpoints are the weakest link in security

While compliance solutions like Privilege Account Management (PAM) and Multifactor Authentication (MFA) help reduce the exposure of sensitive accounts and lessen credential exposure, they do not protect network endpoints from direct attack. In today's environment, authorization of system administrators must be based on real-time device security compliance, strong identity and hardware root of trust. Endpoint security is an important complement to PAM.

StrongNet software hardens workstations

The best way to administer your IT infrastructure is from locked-down, hardened workstations that enforce encryption, device-to-user association and strong authentication. StrongNet uses hardware root of trust to deliver high-integrity user and computer credentials. Our proprietary Measurement Bound Keys ensure that credentials will not be accepted unless the device complies with security policy.

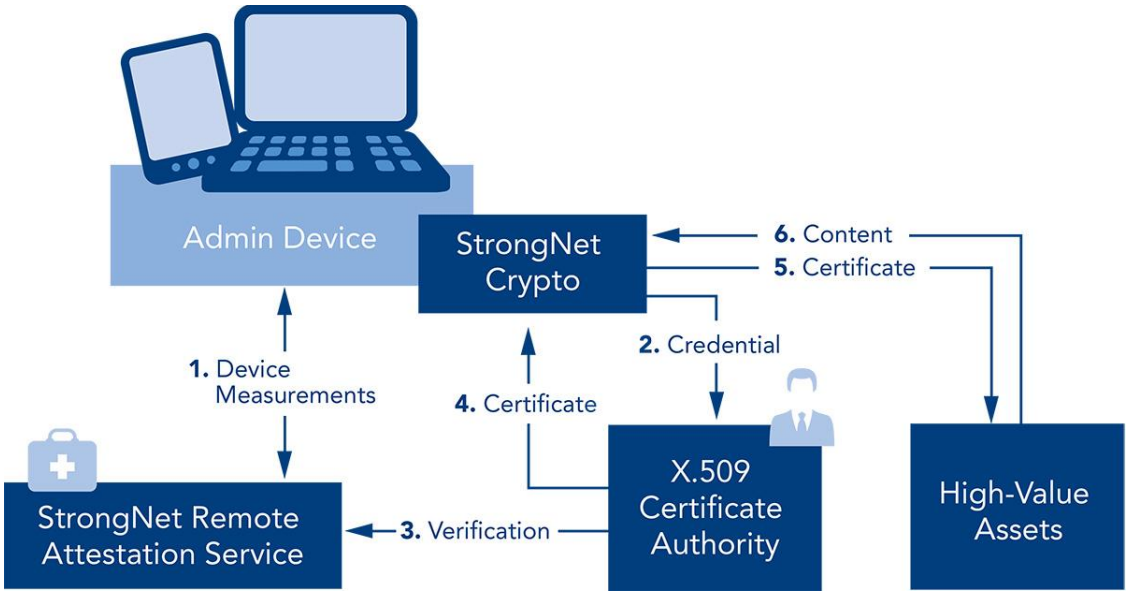
With StrongNet Secure Admin software, you can:

- **Block sophisticated attacks,** including rootkits and pass the hash, a hacking technique that allows an attacker to steal user credentials
- **Enforce remote lock** and encryption to mitigate the risk of stolen or lost hardware, protecting all data by converting it into unreadable code
- **Manage device integrity** though interoperable, standards-based secure boot and device attestation to prevent malware from infecting the boot process and to validate the integrity of the device

It's compatible, reliable and secure

StrongNet with Measurement Bound Keys protects system administrator workstations and other devices by enforcing both user identity and device integrity. With StrongNet, every network resource that supports public key cryptography or public key infrastructure (PKI) is protected.

The following diagram depicts the StrongNet Secure Admin solution components in the context of the data flows involved in granting HVA access to an admin device.



StrongNet provides seamless secure access for a variety of system administrator scenarios, both on premise and in the cloud. Interoperability with multiple identity and authorization technologies means you can lock down any line-of-business scenario.

Request a demo today

Protect privileged accounts with a proven solution. To see StrongNet in action, or to learn more, email **sales@jwsecure.com.**

About JW Secure

Founded in 2006, JW Secure provides architectural and development services to companies that need customized security solutions. Our customers include Alstom, Microsoft and the United States Department of Defense.

StrongNet™ featuring MEASUREMENT BOUND Keys™

JW secure

Privileged account management done right from the start.