Privileged account management done right from the start.

Whitepaper:
StrongNet Secure Admin

Table of Contents

1 Threats Are Increasing 2

2 Know the Enemy 2

3 You Need a Plan 3

4 The Weakest Link in Data Security 4

5 How to Stop Network Credential Theft 4

6 Better Enterprise Data Defense 5

7 StrongNet Solution Overview 6

8 StrongNet Attestation Protocol 10

9 Threats and Mitigations 11

10 Conclusion 11

11 Appendix: Secure Admin Deployment 12

12 Appendix: Relationship with Existing Solutions 12

13 Appendix: Kerberos Integration 13

14 Appendix: References 14

StrongNet™ featuring MEASUREMENT BOUND Keys™

1 Threats Are Increasing

We've all read about huge data breaches in the last couple of years—Target, Sony, Anthem, the US Office of Personnel Management, and others. You have probably received notice from at least one corporation or government entity informing you that your data may have been compromised. As sensational as the headlines were during the periods following those high-profile data breaches, we now know that the impacts were even more dramatic and expensive over time. What started as weaknesses in enterprise IT security defenses resulted in massive remediation and IT costs, the replacements of CxOs and senior-level managers, tarnished reputations, and permanent damage to multibillion-dollar brands.

In the Sony case, it wasn't just that the attackers exposed embarrassing internal conversations. According to security researcher Kurt Stammberger, "Sony was not just hacked; this is a company that was essentially nuked from the inside." The disruption of internal data services was so complete that Sony personnel couldn't respond, both with respect to internal employee communications and external investor and public relations. Reuters reported that the Sony breach cost up to $100 million, plus unquantifiable losses due to exposure of trade secrets, marketing plans, and contracts, and damage to personal and professional relationships through exposure of all those emails. How did this happen? It is believed that an insider with stolen sysadmin credentials provided access to a host of sensitive systems.

Anthem, the second largest health insurer in the US, was struck through the stolen credentials of at least five employees according to the AP. Hackers may have used a phishing scheme to gain credentials and were able to mine company systems for possibly six weeks before being detected, compromising the sensitive data of up to 80 million customers. The cost of this breach is expected to far exceed the $100 million in insurance coverage Anthem had, with some estimates reaching into the billions.

JW Secure, a Seattle-based company with a proven, ten-year track record of developing innovative security solutions, introduces our StrongNet Secure Admin solution. StrongNet Secure Admin protects high-privilege network accounts from credential theft by focusing on the security of your network endpoints. What are we doing in endpoint security that hasn't already been done, you ask? Endpoints are still the weakest link in data security, and yet recent generations of enterprise-class hardware have defensive capabilities that aren't being used. StrongNet hardens endpoints by seamlessly integrating hardware security enforcement into existing standard authentication protocols.

2 Know the Enemy

According to the Verizon 2015 Data Breach Investigations Report, phishing campaigns of as few as ten emails yield a greater than 90 percent chance that at least one user will click. Once a user computer has been compromised, the attacker installs Command and Control (C2) malware that calls out to a remote server for instructions. To perimeter defenses, this looks like a legitimate outbound user web query. The C2 server returns instructions, such as: Create an archive of all Outlook emails received by the user during the past week and copy that archive to a remote website. If the attacker uses HTTPS, the outbound traffic is difficult to distinguish from legitimate behavior from the perspective of IT perimeter defense and data loss prevention solutions.

These tactics can be used by all manner of organizations, including groups that are sophisticated and state-sponsored. The Mandiant APT1 report details the sustained efforts of the Chinese military to penetrate firms in intellectual property–intensive industries. Prime targets include Manufacturing, Information Technology, and Professional Services. The attackers' goal is data exfiltration, and their success has been staggering. Evidence points to terabytes of valuable data stolen over periods of months, and even years, from compromised firms.

The success of the APT1 attacks highlights the challenges that enterprise IT security teams face in mitigating sophisticated, well-funded, remote adversaries. Slow software patching cycles allow known vulnerabilities to be exploited using "watering hole" and phishing strategies. By compromising a frequently visited industry-specific website, and/or sending convincing-looking emails with malicious web links and attachments, persistent attackers are highly likely to gain a foothold in the targeted enterprise.

While the APT1 report is frightening enough, it's important to remember that the Chinese military is only one of many remote adversaries that employ similar measures to target overseas companies. Dozens of recent headlines cite organized crime groups in Russia and the Eastern Bloc as culprits in data theft from Fortune 500 companies and even the IRS.

3 You Need a Plan

How can you mitigate these threats? Protecting high-value data requires defense in depth and a higher level of sophistication than, for example, your public website. Sensitive data should be classified as such, so that only a specific group of users are authorized to access those servers, only for specific purposes, only for limited periods of time, and only with high-strength credentials. If you really care about those servers, you can and should enforce what client hardware that limited set of sysadmins is allowed to use, and through what set of hardware security policies, in order to mitigate credential theft risk.

Creating, maintaining, and applying an effective set of data security policies is difficult. Actually enforcing those policies in a way that is both meaningful in the face of determined adversaries as well as transparent to your users is beyond the capability of current solutions. This is the gap filled by StrongNet.

Investment in IT security is a requirement for every company that is in possession of valuable data. Security is a moving target, and if you're not proactively tracking it, you will get hacked and your data will get stolen. According to Ponemon Institute's 2015 Global Cost of Data Breach Study, the average consolidated total cost of a data breach is now $3.8 million. And Gartner predicted worldwide information security spending would reach $75.4 billion in 2015.

Tools used by hackers are becoming cheaper, more abundant, and more automated, giving hackers an asymmetric advantage over cybersecurity professionals trying to keep databases safe, as illustrated in a review of a federal data breach.

StrongNet works by integrating with enterprise PKI.

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

4 The Weakest Link in Data Security

4.1 Credentials

Credential theft is the result of almost every successful remote attack on your network. Why? To a remote attacker, network credentials, in particular credentials for highly privileged accounts such as a senior managers and system administrators, are the equivalent of continued access to all of your valuable corporate data. In other words, as long as the attacker can continue to authenticate as a trusted user, he or she can continue to steal data undetected.

Unfortunately, stealing credentials is only as hard as gaining unauthorized remote access to a single computer. This is because successful remote attacks tend to result in the compromise of an application or operating system component that has sufficient privilege on the host computer to allow the attacker access to other data, including cached passwords and configuration files. For example, a common default configuration calls for web applications to listen for remote calls using a computer account with full local administrator (i.e., root) privilege. In addition, a user with sysadmin privileges has inevitably logged in to the web server computer at least once in order to deploy or manage the web app. If an attacker can compromise the app, he or she now has access to the previously cached sysadmin credentials. Thus, the fall of a simple web server results in the compromise of the full network.

4.2 Session state

It's not just cached passwords that are vulnerable to exfiltration and replay. Security protocol session state, stored in the computer main memory or on disk, is vulnerable too. Session state includes Kerberos tickets, web app cookies, software cryptographic keys, and the stored data of any app or protocol that doesn't constantly reauthenticate users with a hardware token plus some human-initiated action. Session state is a critical consideration because (a) the whole Internet runs on standardized protocols with behaviors that take years to evolve, and (b) session state threats aren't solved by Privileged Account Management (PAM) and Multifactor Authentication (MFA) solutions (since the problem isn't the user credential; it's the protocol and the attack surface of the endpoint).

Protecting access to high-privilege accounts is critical to the IT mission. But, as you can see, it's a multi-faceted problem. Defense in depth is required: harden endpoints, don't run as admin, shorten password lifetimes, reduce privilege, and, most importantly, make privileged access contingent on security policy compliance.

5 How to Stop Network Credential Theft

The solution to mitigating the risk of credential theft is hardware root of trust combined with defense in depth and policy enforcement. Packaging the "raw materials" of effective credential protection has, until now, been the exclusive domain of advanced government research. JW Secure StrongNet Secure Admin is timely because it bridges that gap for the typical Active Directory–based enterprise environment.

By binding user and device identity, and enforcing boot integrity and hardware root of trust for every high-value transaction, StrongNet greatly limits hackers' ability to (a) steal credentials in the first place, and (b) use stolen credentials to penetrate deeper into the network. StrongNet combines enforcement of policies such as:

- **CredGuard:** This Windows 10 feature reduces the exposure of in-memory credentials by storing them within a hypervisor. This provides a layer of hardware protection against tools such as mimikatz.
- **Device Guard:** This Windows 10 feature allows whitelist enforcement of all executable binaries. By restricting what can be run on the host to vetted software, it is more difficult for attack tools to be used.

- **Early-boot component whitelisting:** Kernel-mode drivers are an insidious source of vulnerabilities, since they run with high privilege and tend to come from a variety of third-party hardware manufacturers. Further, modern operating system architecture is such that some third-party drivers must initialize prior to antivirus/antimalware startup, creating a window for attacks that are otherwise impossible to detect. Remote platform attestation allows the presence of unknown and untrusted early-boot drivers to be detected by a trusted remote server.
- **Disk encryption:** This is an important mitigation for offline attacks.
- **Hardware root of trust:** StrongNet uses the Trusted Platform Module for nonexportable cryptographic key storage and host integrity assurance.

We've got a best-in-class solution for blocking the bad guys.

6 Better Enterprise Data Defense

6.1 The best defense is defense in depth

The purpose of StrongNet Secure Admin is to protect high-privilege accounts, such as system administrators and DevOps, against unauthorized use. We do that using a defense in depth approach that includes credential theft mitigation and hardening the computers where those high-privilege accounts are used.

The first line of defense is to protect the network from computers that are infected by rootkits. This is a critical step for a few reasons. First, a rootkit undermines the efficacy of any security policy implemented by the computer operating system. Second, rootkits are very difficult for even tech-savvy users to detect and eliminate. Third, a rootkit renders the client device untrustworthy from the perspective of other devices on the network.

StrongNet protects the network from rootkits by enforcing:

- **UEFI Secure Boot:** This is a feature of UEFI by which OEMs can control what boot images can be executed. Secure boot includes support for both whitelisting and blacklisting of code signing keys as well as of boot loader binaries.
- **TPM Measured Boot:** This is a boot loader and operating system kernel feature that uses the TPM to keep a record of early-boot components as they load.
- **Remote Platform Attestation:** This is another TPM-based feature, allowing a measured boot log to be evaluated by a remote server and for trust and policy decisions to be made based on the contents of that log.

Granular boot policy enforcement allows us to isolate devices with unrecognized components in their boot stack.

The second line of defense is to protect against offline attacks. This is important because, in addition to obvious examples of intellectual property such as documents and email, computers retain traces of user authentication information such as passwords and session state even after they've been shut down. Plus, a stolen device can have its hard drive removed, have its boot data modified, or be subjected to I/O port and DMA attacks.

What is StrongNet?

StrongNet software includes the following components:

StrongNet Attestation Service to perform a cryptographic challenge-response protocol.

StrongNet Policy Module to ensure that certain X.509 certificate templates are only issued to computers that are compliant.

StrongNet Secure Endpoint Service to provide security compliance status notifications to the end user.

StrongNet Key Storage Provider to support the Attestation Service.

See full component descriptions in 7.3 below.

StrongNet protects against offline attacks by enforcing BitLocker disk encryption and a boot PIN. As a result, data can't be recovered from stolen drives, and I/O attacks can't be initiated without knowledge of the PIN to boot the system.

The third line of defense is to protect against attacks on the running system. This is important because, even if the system started securely, the user will inevitably need to run a variety of applications, and access a variety of network locations, in order to be productive. StrongNet monitors antivirus and patching systems to ensure that the host stays protected and up to date. If the host falls out of compliance, StrongNet immediately flushes all cached credentials and authenticated sessions.

As part of every StrongNet deployment, JW Secure works with the customer to define what applications the high-privilege user requires. We create AppLocker policies to ensure that only those applications can be run. We also create web proxy, network policy, and browser settings in order to enable safe use of any must-have line of business web apps.

The fourth line of defense is to bind the user credential to all of the above policies in real time. The user can authenticate only when the host device is compliant with security policy; there is no lag in enforcement. As soon as the device falls out of compliance, access to the authentication credential is lost.

StrongNet provides real-time enforcement of security policy using our proprietary Measurement Bound Keys. The key, a component of the Secure Admin computer credential, is encrypted ("sealed") to a specific TPM security chip, on a specific device, in a specific state. The key cannot be exported or used from another device. And, whenever the device boot state changes, or when the device simply reboots, the device must be reauthorized by a trusted remote server before the key can be used again.

The fifth line of defense is ease of integration. Security technologies that are difficult to use end up getting disabled and ignored. StrongNet can protect any Active Directory or PKI-aware application or service. This includes simultaneous enforcement of multifactor authentication both of the user and of the host device.

6.2 Build a Stronghold

The JW Secure Stronghold model calls for defense in depth by placing the most business-critical assets inside layers of security. The government intelligence community uses the same approach by compartmentalizing, both physically and logically, its most sensitive data. Consistent with the NIST BIOS Integrity Measurements Guidelines and the NSA Mobility Program, StrongNet brings the highest level of enterprise network credential protection to the private sector.

7 StrongNet Solution Overview

7.1 Scenario integration

StrongNet integrates with enterprise PKI. Kerberos (PKINIT), VPN, TLS client authentication, 802.1x, SAML, IPSEC, and S/MIME are all supported enforcement scenarios. Use of TPM hostage keys, and careful lifecycle management of an X.509 "device health" certificate, are fundamental to reducing adoption barriers. That is, by gating certificate issuance, and binding each private key to a specific device in a specific state, we solve several problems at once:

- No modification of your existing applications is required.
- Network access keys are hardware protected and nonexportable (this is an especially important consideration in light of the credential theft risks discussed previously).
- Network access keys are only valid while the host maintains policy compliance.
- Therefore, if the network authentication attempt succeeds, you know the computer is secure.

The strategy of StrongNet is to reduce the exposure of high-value network credentials. If a sysadmin is presenting a user authentication credential on a host that isn't sufficiently protected, we block the authentication attempt. This reduces the exposure of sensitive account information, since it prevents insecure devices from connecting to high-value network assets. StrongNet thereby prevents credential theft as well as unauthorized lateral movement through the network.

7.2 Endpoint security features

StrongNet endpoint agent features include the following:

- Drive TPM remote platform attestation. Based on the TCG and NIST standards, this challenge-response protocol allows the boot integrity of the host to be securely measured by a trusted remote server.
- Monitor Windows Security Center status (client SKUs only).
  - StrongNet continuously checks the runtime security state of the host.
  - Enroll or remove the health certificate when policy compliance changes are detected.
- For Kerberos integration, refresh the computer authentication token whenever a new health certificate is received (or removed).
- Remove IPSEC security associations and Kerberos service tickets when the host is noncompliant.

StrongNet Secure Admin protects high-privilege Active Directory credentials from theft. StrongNet defends sensitive accounts in three ways:

- Ensures the integrity of the system boot environment using TPM remote platform attestation (based on NIST SP 800-155). This helps to mitigate the threat of rootkits as well as offline attacks.
- Protects the host at runtime by continuously monitoring security policy compliance.
- Enforces security policy compliance synchronously during every remote authentication attempt into your high-value assets.

StrongNet uses defense in depth, rooted in hardware, to protect your most sensitive accounts and assets. This approach offers several benefits:

- Nonadministrative tasks can always proceed. This helps to ensure user acceptance.
- The most important defensive security measures for mitigating remote attacks and data loss are combined into a single solution.
- Policy drift is prevented—if the host isn't secure, authentication into the HVA will fail.

7.3 StrongNet components

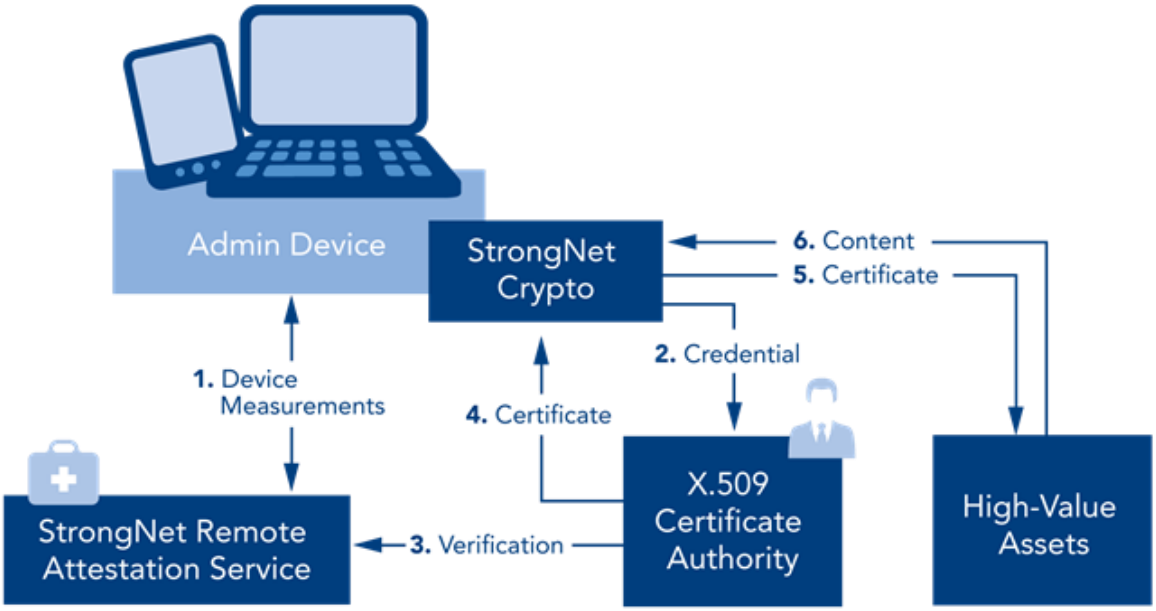
The solution includes the following components:

- **StrongNet Attestation Service:** The purpose of the Attestation Service (AS) is to perform a cryptographic challenge-response protocol in order to ensure that client computers have trustworthy BIOS, TPM, and boot software. The AS also enforces security policy and acts as a repository for client device history. See the StrongNet Remote Attestation Service item in diagram 7.3.1.
- **StrongNet Policy Module:** The purpose of the Policy Module is to ensure that certain X.509 certificate templates are only issued to computers that are compliant with security policy, as measured by the Attestation Service. The Policy Module does this by plugging in to Microsoft Windows Certificate Services (i.e., an Enterprise Certificate Authority). See the X.509 Certificate Authority item in diagram 7.3.1.

- **StrongNet Secure Endpoint Service:** The purpose of the Secure Endpoint Service is to provide security compliance status notifications to the end user. This is done using a Windows system tray icon. See the Admin Device item in diagram 7.3.1.
- **StrongNet Key Storage Provider:** The purpose of the Key Storage Provider is to interact with the Attestation Service in order to create attested cryptographic keys bound to the security policy settings of a client computer. Keys generated in this way are only usable while the client stays compliant with security policy. See the StrongNet Crypto item in diagram 7.3.1.

7.3.1 Component diagram

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.



The data flows, represented by the diagram's numbered arrows, are described in section 7.3.2.

7.3.2 Data flow

1. **Device Measurements:** The Admin Device attempts to create a StrongNet measurement-bound keyset. That is, a cryptographic key that is sealed to a specific TPM in a specific state.
2. **Credential:** The device uses the StrongNet key to sign a certificate enrollment request.
3. **Verification:** The Certificate Authority verifies that the request signer is trusted by the StrongNet Remote Attestation Service.
4. **Certificate** [granted]: If the signer is trusted, the Certificate Authority issues the requested certificate to the device.
5. **Certificate** [submitted]: The device uses the certificate for authenticated access to High-Value Assets on the network.

6. **Content** [released]: Only policy-compliant devices can reach sensitive resources.
    a. If the device deviates from security policy, authenticated access is immediately terminated.
    b. StrongNet supports optional enhanced scenario integration with Kerberos and IPSEC. For more information on those data flows, please see the Appendix.

7.4 Device health monitoring

The StrongNet AS monitors several pieces of device health, through the device registration service, which obtains health readings from the client Secure Endpoint Service, and the use of elements of the boot logs employed during TPM attestation.

7.4.1 StrongNet Secure Endpoint Service

The Secure Endpoint Service monitors the following areas, and reports them to the device health registration endpoint on the AS:

- Windows Security Center status, which includes firewall status, User Account Control state, antivirus and antispyware state, Internet settings state, and whether Windows update is enabled.
- Group Policy state.

The AS determines whether the device meets the policy requirements that have been configured by the administrator and returns a response to the Secure Endpoint Service. If the device is successfully registered and meets policy, it:

1. Enrolls for an X.509 certificate, if one isn't present. This is how remote TPM platform attestation is triggered.
    a. The certificate template to be used is expected to be compatible with Kerberos PKINIT.
    b. The certificate template must be configured to use an RSA keyset that has been generated using the StrongNet key storage provider.
2. Clears the Kerberos ticket caches.
3. Uses that certificate to do a Kerberos PKINIT logon. We recommend that the client certificate include a policy OID that is mapped to a security group that will then be included in service tickets the next time Kerberos is used. Alternatively, for federation applications, the OID may be mapped to a SAML claim.

If the device does not meet policy, the Secure Endpoint Service:

1. Deletes certificates matching the configured certificate template.
2. Purges Kerberos tickets to remove tickets containing extra security groups and device claims.
3. Removes all IPSEC security associations.

7.4.2 Key attestation policies

In order for a key to be granted from the AS, the client device must meet the following security policy requirements. These settings are configurable:

- Trusted TPM manufacturer Endorsement Key
- Valid, contiguous boot logs for hibernate and resume sequences
- Kernel debugger is not present
- Kernel/driver test signing is disabled
- BitLocker is enabled
- BitLocker boot PIN (the "TPM and PIN" key protector) is enabled
- All boot binaries are digitally signed

- A whitelisted Early-Launch Antimalware driver (ELAM) is present
- Code Integrity is enabled
- LSA Protected Process is enabled
- UEFI Secure Boot is enabled
- Device is registered and compliant with the user-mode health policies described in the previous section
- MS15-111 is mitigated
- CredGuard is enabled
- Device Guard is enabled

If the client device does not comply with security policy, then it will not be able to create a new attested key. It will also not be able to use any key previously obtained.

Since Windows boot measurements change at every power state transition (reboot or hibernate/resume), StrongNet Measurement Bound Keys must be reverified following every reboot and hibernate/resume. Reverification is handled seamlessly by the StrongNet client components without any user interaction required. If reverification fails due to the client failing security policy checks, StrongNet keys are unusable until the client is back in compliance.

7.5 Multi-platform support

StrongNet v1 client-side components support Windows 8 and later. TPM 1.2 or 2.0 (hardware or firmware) is required. Coming in 2016, we are extending StrongNet with the following platforms and scenarios:

- High-assurance server workload integration, including physical (non-virtualized) TPM-capable hosts on Windows Server 2012 R2 and later; and virtualized hosts on Windows Server 2016
- Linux clients and server integration, offering a unified hardware-attested policy management experience
- Chromebook integration, allowing inexpensive, forward-deployed devices to be used in sensitive cloud connectivity and data access applications

8 StrongNet Attestation Protocol

The creation of a Measurement Bound Key entails the following challenge-response message exchange between the StrongNet Client Components and the AS:

1. The client requests a Nonce.
2. The client requests a TPM Attestation Identity Key (AIK) challenge. The AS challenges the binding of the Nonce, the AIK, the manufacturer Endorsement Key, and the TPM Storage Root Key.
3. The client sends its signed boot logs to the AS. The AS enforces log integrity, continuity, and boot policy.
4. If successful, the client is issued an encrypted Measurement Bound Key. Only the specific TPM challenged in step 2 can decrypt and use the key, and only until the security policy measurements change again.
5. When the boot measurements change, the client repeats steps 1–4.

9 Threats and Mitigations

9.1 Offline attacks

StrongNet implements client hibernate/resume log verification and enforces the use of BitLocker TPM-based boot volume encryption. This includes verification of the following:

- That the latest boot log is, in fact, the latest boot log. We use a Nonce for this.
- That the client has provided all logs back to, and including, the last full boot.
- That all of the logs pass all AIK signature and policy checks.

The above log chaining enforcement is critical for mitigating offline attacks against client devices that may have previously been used to access sensitive enterprise data or high-privilege network accounts. Without this protection, a possible attack would be, for example:

1. User has a compliant/attested device after a clean boot.
2. Turn off BitLocker.
3. Hibernate.
4. Boot Linux and maliciously modify one of the loaded driver images in the Windows hibernate file.
5. Resume.
6. Turn on BitLocker. Then hibernate/resume again.
7. Now, an incomplete check of the TCG log chain will make the server think that the system is still compliant, even though it's running a compromised driver image.

However, by enforcing policy—including BitLocker/TPM boot volume encryption—on all contiguous logs, we mitigate that threat.

9.2 I/O port attacks

We recommend the use of a BitLocker boot PIN in order to mitigate the risk of I/O port attacks against stolen devices. For high-risk deployments, we further recommend the use of client hardware without Direct Memory Address (DMA) accessible ports and without removable RAM.

10 Conclusion

We learn best from personal experience, but corporate Boards of Directors are no longer accepting the legal risk of waiting for a major security incident before instituting proper defenses. Mandiant, Microsoft, and Verizon have all published sobering reports that point to the importance of staying vigilant: keeping patching up to date, fixing security bugs in Internet-facing web apps, reducing the impact of phishing, slowing lateral movement of intruders on your network, and responding quickly to attacks once they occur. Using hardware root of trust and continuous monitoring, StrongNet solves those problems by ensuring that a broad range of policies are enforced at the time of authentication, thereby protecting all of your high-value network assets.

Psychological and social research show that risk assessment is something that humans tend to do poorly. Careful, considered analysis of risks and assets, and staying informed about online security, are the only ways we can effectively prioritize and mitigate those risks. Just because cyber offense has an advantage over defense doesn't mean attacks can't be stopped, or at least greatly slowed down. Don't just institute security policies—enforce them with StrongNet.

11 Appendix: Secure Admin Deployment

11.1 Riding the Windows 10 wave

For Windows 10, the killer security feature for reducing credential theft risk is CredGuard. It's not enough just to turn on CredGuard, though. First, you must actually enforce its use. Second, you must protect the integrity of the host. StrongNet solves both problems.

The Windows 10 adoption wave presents a unique opportunity to kill two birds with one stone: increase user productivity and improve your security posture. Many organizations skipped Windows 8 and some are still running even earlier desktop versions. However, more recent versions of Windows are offering compelling security features, including CredGuard, Device Guard, Kerberos armoring, Secure Boot, and TPM platform attestation. Plus, new hardware features such as touch-based, high-resolution screens, fast disks, lightweight chassis, UEFI, and TPM 2.0 make an attractive security-plus-usability package for enterprise users. While BYOD can present an appealing option from a CapEx perspective, MDM and lightly managed devices cannot be held to the same security standard as fully managed computers without herculean effort by system administrators.

11.2 Ideal deployment

An ideal, state-of-the-art Secure Admin deployment consists of the following components:

- Windows 10 admin laptops
  - TPM 2.0
  - UEFI
- Multifactor authentication enforced for all users
- PAM deployment for Just In Time, short-term privilege elevation
- StrongNet for enforcement, protecting the HVA from noncompliant hosts

12 Appendix: Relationship with Existing Solutions

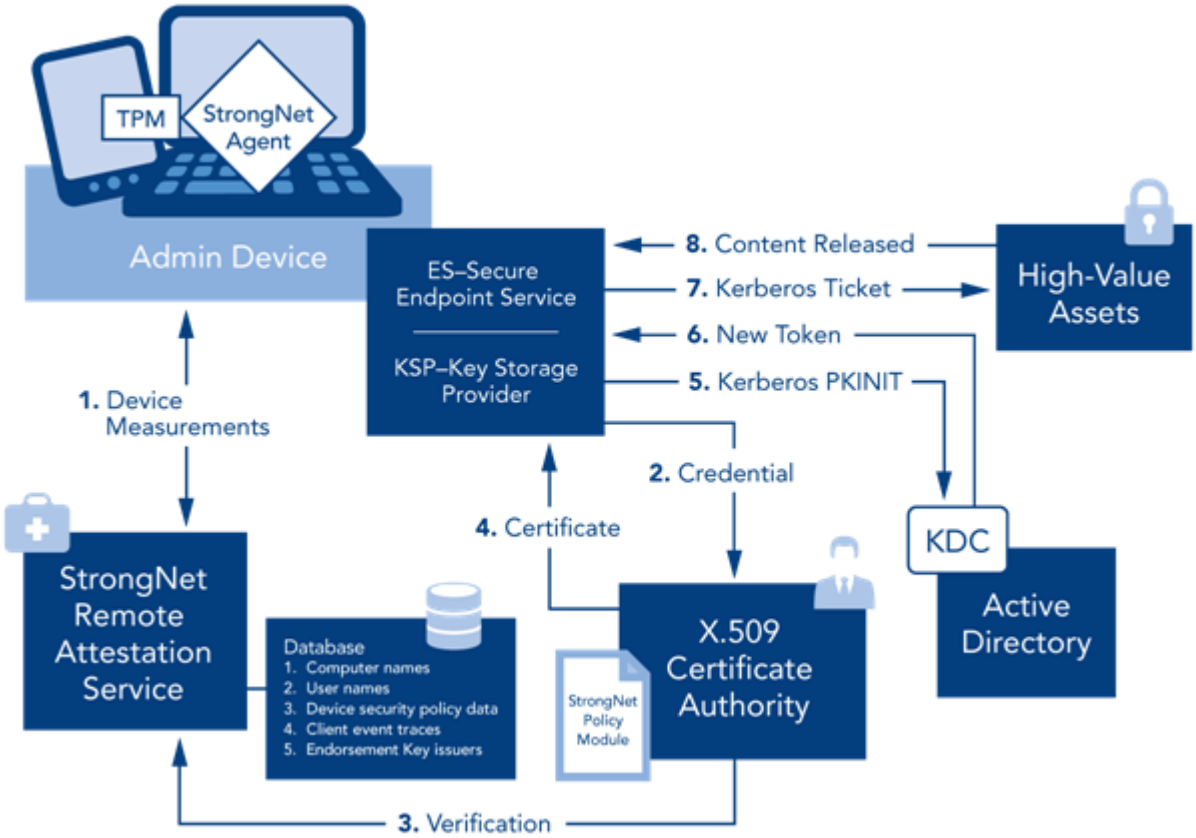
Privilege Account Management (PAM) and Multifactor Authentication (MFA) solutions help to reduce the exposure of sensitive accounts. PAM and MFA reduce credential exposure by some combination of reducing password lifetimes, reducing privilege elevation lifetimes, and increasing password complexity. However, PAM and MFA have a weakness in that they don't protect network endpoints from direct attack.

Endpoint security is an important complement to PAM. First, PAM deployments still tend to be based on static passwords, albeit short-lived ones. Second, even with PAM, MFA solutions still have password equivalents, plus session state, for backward compatibility. Third, PAM in some ways consolidates risk, especially for local sysadmins and EA/DA.

StrongNet mitigates credential theft risk for high-privilege Active Directory accounts. We enforce a variety of security policies in real time with every network logon attempt. We use TPM remote platform attestation to enforce as many of those policies as possible, and we rely on our agent software to enforce the rest.

13 Appendix: Kerberos Integration

The following diagram shows the StrongNet Secure Admin solution in the context of our integration with the Kerberos armoring feature in Windows. While StrongNet integrates with any enterprise PKI scenario out of the box, the Kerberos scenario is particularly compelling because it allows the customer to enforce user authorization plus device policy compliance in a single security group check in existing applications. The data flow represented by the numbered arrows in the diagram is described following the image.



1. The sequence begins with an attempt to create a private key with the StrongNet Key Storage Provider (KSP) on the client.
    a. For example, key generation can be initiated by the built-in Windows certificate enrollment client and/or the StrongNet Secure Endpoint Service (ES). Either way, certificate template configuration is designated by the system administrator.
    b. The KSP drives the remote platform attestation challenge-response protocol with the StrongNet Remote Attestation Service (AS).
2. The client sends an authenticated certificate enrollment request to the Certificate Authority (CA).
3. The CA queries the AS in order to ensure that the certificate enrollment request is for a verified StrongNet private key (i.e., a hostage key, bound to the latest TPM measurements).
4. If the private key is determined to be valid, the CA issues the requested certificate. User as well as computer certificate templates are supported by StrongNet; however, the Kerberos scenario works best with a computer template.

5. Whenever the client transitions in or out of security policy, including following CPU power state transitions that are tracked by the TPM, the ES updates the computer Kerberos TGT. The ES does this by manually initiating a logon using the latest device health certificate (or a software-based certificate if the device is noncompliant).
6. The recommended Active Directory configuration for StrongNet integration with Kerberos calls for at least one mapping between a “device is compliant” certificate OID and a Security Group. Thus, the resulting token group memberships indicate whether the device is compliant. Further, by using Kerberos armoring, the combined group memberships of the client device plus the user are reflected in user tokens obtained on the device.
7. High-Value Assets are access-control restricted based on membership in the “device is compliant” SG, plus whatever user SGs are appropriate. This approach is therefore usable by all existing Kerberos-aware applications without modification.

14 Appendix: References

CACM: Passwords are always too weak:
http://cacm.acm.org/magazines/2015/7/188731-passwords-and-the-evolution-of-imperfect-authentication/abstract

Gartner: Market Guide for Privileged Account Management:
https://www.gartner.com/doc/2770418/market-guide-privileged-account-management

ISC: User multifactor authentication solutions are too expensive:
https://isc.sans.edu/forums/diary/Implementing+two+Factor+Authentication+on+the+Cheap/9580/

Mandiant APT1 report:
http://intelreport.mandiant.com/

Microsoft Security Intelligence Report:
https://www.microsoft.com/en-us/download/details.aspx?id=46928

Microsoft: What’s New in Kerberos Authentication:
https://technet.microsoft.com/en-us/library/hh831747.aspx

NIST: BIOS Integrity Measurements:
http://csrc.nist.gov/publications/drafts/800-155/draft-SP800-155_Dec2011.pdf

NIST: Software patching cycles inevitably lag vulnerability exploit release:
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

NIST SP 800-155:
http://csrc.nist.gov/publications/drafts/800-155/draft-SP800-155_Dec2011.pdf

NSA Mobility Program:
https://www.nsa.gov/ia/programs/mobility_program/

Rapid7: Mitigating Service Account Credential Theft on Windows:
https://community.rapid7.com/docs/DOC-2881

Verizon Data Breach Investigations Report 2015:
http://www.verizonenterprise.com/DBIR/2015/