BUDGET FOR NEXT GENERATION TRUST PROTECTION

DEFEND YOUR BUSINESS AGAINST TRUST-BASED ATTACKS
BY PROTECTING KEYS AND CERTIFICATES
Executive Summary

Targeted cyberattacks are steadily increasing, and business executives face challenges with trust exploits. While organizations adopt cloud computing and allow BYOD onto the network, the challenge of securing company data everywhere increases exponentially. Cybercriminals are constantly on the lookout for new targets that will give them a foothold in the enterprise to reach their target’s most valuable assets—from trade secrets and intellectual property to customer lists, PII, and other valuable data.

As CISOs approach 2015 budget cycles they should allocate budget for one of the most important problems and highest areas of risk: protecting the trust established by keys and certificates.

Attacking the Foundation of Security: Trust

Keys and certificates ensure trust in digital communications. But when these foundational elements of security are compromised, there are often devastating consequences: without trust, organizations cannot operate.

• The good cannot be differentiated from the malicious
• Security systems are blind to attacks
• Critical security control are undermined
• Blind spots open doors to compromise

Why Attackers Want Trusted Status

Cybercriminals want to be authenticated and evade detection, keeping their actions cloaked. Attacking the assets you use to establish trust—the tens of thousands of keys and certificates in your business—are a prime target in achieving this goal.

Consequences of Failing to Protect Trust

• Stolen Intellectual Property
  Cybercriminals cloak their activities and trick analytics to leverage IP spoofing and trick users into providing sensitive data

• Breach of Customer Privacy
  Compromised keys and certificates are used in man-in-the-middle attacks to eavesdrop on encrypted communications

• Damaged Reputation
  Spoofing trusted sites provides attackers a powerful weapon and damages your brand

• Failed Audit
  Increasing trust-based attacks and vulnerabilities, like Heartbleed, focus audit attention where few businesses are prepared to defend

How Venafi Helps

Venafi secures and protects keys and certificates in the datacenter, on desktops, on mobile devices, and in the cloud so they cannot be used by criminals in cyberattacks. With complete visibility into your key and certificate inventory, Venafi detects new vulnerabilities and fixes them fast to eliminate threats.

Act Now with Next Generation Trust Protection

Contact Venafi for a customized quote and assistance with 2015 budget planning for key and certificate security.
Protect the Trust on Which Your Business Depends

Action Required Now
After Heartbleed, CISOs are budgeting to protect cryptographic keys and digital certificates to preserve the trust these assets establish. Heartbleed showed how a single vulnerability can leave keys and certificates open to compromise and eliminate the trust we have in our communications with web servers, clouds, and devices. Without this trust, organizations cannot operate. And we can only expect more vulnerabilities like Heartbleed and must ensure we have the right security in place to defend our businesses.

Enterprises rely on thousands of keys and certificates as the foundation of trust for their websites, virtual machines, mobile devices, and cloud servers. Yet it is this very trust that cyber criminals want to use, not only to evade detection, but to achieve authentication and trusted status that bypasses other security controls and allows their actions to remain hidden. If only one of your critical keys or certificates is compromised, the digital trust you have established is eliminated. Your business then returns to the pre-Internet and eCommerce age, which cannot be sustained in today’s market.

100% of Organizations Compromised
Attacks on keys and certificates are no longer a theoretical threat. In 2013—before Heartbleed was discovered—an analysis of over 2000 large, global enterprises showed that ALL had experienced and responded to an attack on keys and certificates in the previous 24 months. In this study, IT security professionals estimated the impact of an attack on trust would total almost $400 million.¹

CISO Response: Budgeting for Next Generation Trust Protection
CISOs are budgeting to make sure vulnerabilities are remediated and high-priority projects are successful. With the growth and devastating impact of attacks on keys and certificates, this includes budgeting for Next Generation Trust Protection in 2015, or addressing these issues even sooner with remaining funds in 2014.
Why, Like Your Peers, You Should Budget for Next Generation Trust Protection

Don’t Undermine Your Investment in Critical Security Controls

Organizations layer security controls to create a defense-in-depth approach to protecting their business. But a lack of key and certificate security undermines a minimum of 40% of the Critical Security Controls (CSCs) listed by the SANS Institute.²

For example, according to Gartner, 25% to 50% of all traffic in organizations is encrypted.³ Most security controls, like malware, boundary defenses, and data protection, do not decrypt data, but instead rely on keys and certificates to determine trust.

Here are a few examples of security projects that are being prioritized by CISOs, but are being weakened by a lack of protection for keys and certificates used to establish trust:

- **Data Security**: Unprotected keys and certificates provide an open door for spoofing and man-in-the-middle attacks which steal data.
- **Strong Authentication**: Using self-signed, unauthorized Certificate Authorities (CA) or weak cryptography fails to provide strong authentication.
- **Mobility Management**: Without mobile certificate security, cybercriminals can gain unauthorized network access using WIFI and VPN connections with unknown, untracked certificates.
- **SSL Inspection / Decryption and Threat Detection**: Other security controls are blind to trusted and encrypted SSL traffic because of the inability to access all keys and certificates securely.
- **Network Access Control**: Unauthorized network access can be gained from unknown, untracked certificates.
- **Privileged Access**: Unknown use of keys can compromise the most important applications and data.

![Figure 1. Keys and Certificates are a Hole in Your Security that, If Unprotected, Undermine and Weaken Other Critical Security Controls](image-url)

---

² [Source](https://www.sans.org)
³ [Source](https://www.gartner.com)
Example of Security Program Effectiveness: SANS 20

The SANS Institute has issued *The Critical Security Controls for Effective Cyber Defense.* This includes 20 controls that provide an actionable security framework to protect businesses. In the latest version, the SANS Critical Security Controls recognize that data protection must go beyond Data Loss Prevention (DLP) and Data Classification solutions, which cannot see encrypted traffic—creating a security gap.

An effective data protection framework must close this gap by securing cryptographic keys and digital certificates to protect the trust behind secure, authenticated, and encrypted communications. To address this need, the Critical Security Controls now include requirements for securing keys and certificates in Section 17 on Data Protection.

New Key and Certificate Security in SANS20 CSC Version 5, Requirement 17: Data Protection

- CSC 17-2: Verify that cryptographic devices and software are configured to use publicly-vetted algorithms.
- CSC-17-3: Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls.
- CSC 17-10: Only allow approved Certificate Authorities (CAs) to issue certificates within the enterprise. Review and verify each CAs Certificate Practices Statement (CPS) and Certificate Policy (CP).
- CSC 17-11: Perform an annual review of algorithms and key lengths in use for protection of sensitive data.
- CSC 17-14: Define roles and responsibilities related to management of encryption keys within the enterprise; define processes for lifecycle.

![Figure 2. SANS 20 Critical Security Controls](image-url)
Securing Your Business with Next Generation Trust Protection

Protect Your Business against Trust-based Attacks
The severity and scope of Heartbleed put a spotlight on this vulnerability that requires companies to replace all keys and certificates to fully remediate. But Heartbleed went undetected for over two years. There are undoubtedly other key and certificate compromises occurring undetected today. And this will only increase. Gartner predicts that, “50% of network attacks will use SSL by 2017.”

These threats range from exploits of accidental vulnerabilities, like Heartbleed, to advanced, persistent threats designed to circumvent and misuse keys and certificates. Failing to secure these assets using strong cryptographic policies with established expiration cycles leaves networks, data, and even your business open to attack and breach—with compromises that go undetected for extended periods.

Eliminate Vulnerabilities and Reduce Attack Surface
Most organizations rely on individual administrators to secure their keys and certificates. This leads to mistakes and errors that create vulnerabilities and no way to automatically detect anomalous keys and certificates and remediate by policy. These vulnerabilities and an evolving threatscape have led Gartner to conclude, “Certificates can no longer be blindly trusted.”

Organizations need automated security to identify all keys and certificates, enforce policy, detect anomalies, whitelisted trusted CAs, and respond and remediate quickly to security incidents and policy. The solution must track progress over time and provide actionable security intelligence.

Reduce Risk from Third-Party Compromise
Enterprises must also go beyond protecting against compromises within their own organization. Every business outsources their security to a third party—external Certificate Authorities (CAs). And enterprises must be able to quickly respond if their CA is breached. Organizations are relying more heavily on SSL to establish trust for sensitive business communications. This makes SSL certificates an attractive target for cybercriminals.

Enterprises must be able to quickly respond to trust-based attacks in their own organizations as well as CA compromises to minimize the impact to their business. Enterprises that have effectively secured their keys and certificates can respond to compromises in minutes by replacing these cryptographic assets, maintaining the trust that is critical to sustaining their business.
How to Start

Where should organizations start when deploying a Next Generation Trust Protection solution? To mitigate risks and secure the enterprise in what Gartner calls a “world without trust,” Gartner makes these recommendations:

• Survey and monitor all certificates
• Manage keys as a “top priority”
• Document and enforce policies, like revocation processes
• Monitor security feeds for compromised CAs and certificates

To accomplish these recommendations, Gartner says that enterprises must secure keys and certificates across the enterprise, on mobile devices, and in the cloud—for any key, any certificate, anywhere.

The Solution: Venafi

Venafi Trust Protection Platform™ secures and protects keys and certificates in the datacenter, on desktops, on mobile devices, and in the cloud. Venafi Trust Protection Platform enables enterprises to gain complete visibility into their key and certificate inventory, establish a baseline of normal usage, enforce enterprise policies, and respond to and remediate key and certificate anomalies. Venafi increases an organization’s security posture by reducing its attack surface and enabling a faster response when keys and certificates are compromised.

Justifying Budget for Next Generation Trust Protection

Guidance from Global 2000 CISOs

In the first half of 2014, Venafi met with over 100 CISOs in the Global 2000. They are budgeting for key and certificate security to support their investments in critical security controls and secure their businesses against trust-based attacks with a solution that delivers threat intelligence, policy enforcement, anomaly detection, and fast remediation.

When structuring the funding, many are combining Next Generation Trust Protection within broader IT and security projects:

• **Data Security:** Eliminate blind spots and security gaps by decrypting SSL traffic and ensuring protection of private keys to prevent attacks.

• **Strong Authentication:** Enforce policies and whitelisting to prevent and detect the use of self-signed certificates, unauthorized or vulnerable CAs, and weak cryptography that undermine the ability to authenticate websites.
• **Mobility Management**: Enforce policies for WiFi, VPN, and Mobile Device Management (MDM) certificates, detect anomalous certificates that provide unauthorized network access, and quickly respond with a single “kill switch” for IT security.

• **Threat Detection and SSL Inspection / Decryption**: Decrypt all SSL traffic by securely delivering and updating SSL keys and certificates to authorized SSL decryption appliances, Next Generation Firewalls (NGFW), and other security systems and services.

• **Network Access Control**: Ensure every device, user, and application possesses a unique certificate for trusted Network Access Control for WiFi and VPN access and includes a “kill switch” that immediately revokes trusted access.

• **Privileged Access**: Ensure that privileged access is granted, controlled, monitored, and audited, including protecting all SSH keys and SSL private keys.

• **Compliance**: Achieve regulatory compliance, such as with PCI DSS, and meet internal governance standards that require securing cryptographic keys and digital certificates.

### 2015 Peer Budget Example

After meeting with over 100 CISOs in the Global 2000, Venafi has created a sample budget for enterprises based on the cost of including key and certificate security within the following critical security projects.

<table>
<thead>
<tr>
<th>Projects</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security, IP Theft Prevention, Strong Authentication, and SSL Inspection/Decryption</td>
<td>$500,000</td>
</tr>
</tbody>
</table>

**Critical Component**: Venafi TrustAuthority and Venafi TrustForce find all SSL keys and certificates, protect with policy, detect anomalies, and respond and remediate automatically.

<table>
<thead>
<tr>
<th>Projects</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged Access Security, IP Theft Prevention, and Data Loss Prevention</td>
<td>$400,000</td>
</tr>
</tbody>
</table>

**Critical Component**: Venafi TrustAuthority and Venafi TrustForce find all SSH keys, protect with policy, detect anomalies, and respond and remediate automatically.

<table>
<thead>
<tr>
<th>Projects</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged Access Security, IP Theft Prevention, and Data Loss Prevention</td>
<td>$250,000</td>
</tr>
</tbody>
</table>

**Critical Component**: Venafi TrustAuthority and Venafi TrustForce identify all MDM, WiFi, and VPN certificates, detect anomalies, and respond quickly with a single kill switch.

**Total Peer Budgeting** | $1,150,000 |
This example shows how Global 2000 CISOs are now budgeting to protect the trust established by keys and certificates. This budget estimate includes a get-started-fast approach to eliminate the most critical vulnerabilities and a strategy to protect more of the enterprise over time.

Why Budget for Next Generation Trust Protection Now?

Advanced Persistent Threats (APTs) that compromise keys and certificates—including APT1, Mask, Energetic Bear, Crouching Yeti, and Zombie Zero, just to name a few—continue to damage the organization long after the malware has been removed. Cybercriminals still have access until the compromised keys and certificates are changed.

And experts agree the problem is only going to get worse:

- **McAfee Labs Threat Report for Fourth Quarter 2013** noted that malware signed with legitimate certificates more than tripled between 2012 and 2013.

- **Microsoft's Corporate VP, Scott Charney**, stated “PKI is under attack” in the beginning of 2013.

- **University of Michigan** found 99% of SSL certificates in use to be vulnerable according to the current NIST standard.

- **Heartbleed** remediation, as defined by Gartner, requires all keys and certificates be changed—Q3 2014 research shows 90% of external facing servers have not been fully remediated.

- **Netcraft** discovered dozens of spoofed SSL certificates that impersonated financial institutions, merchants, and other trusted online sources, making the companies and their customers vulnerable to man-in-middle attacks.

Without Venafi to secure and protect keys and certificates, other security controls are less effective at reducing risk and do not achieve their intended goals. Securing keys and certificates establishes a foundation of trust for an effective security program and a defense against today’s cyber threats.

Next Steps: Contact Venafi

Contact Venafi for a customized quote for your business and assistance with including key and certificate security in your 2015 budget—or even for remaining 2014 funds. With the increasing threats against keys and certificates, CEOs, Board of Directors, and auditors are expecting that a solution will be in place to provide needed protection now and in the future. Contact us to learn how Venafi can be that solution for your business.
About Venafi

Venafi is the market-leading cybersecurity company in Next Generation Trust Protection. As a Gartner-recognized Cool Vendor, Venafi delivered the first trust protection platform to secure cryptographic keys and digital certificates that every business and government depends on for secure communications, commerce, computing, and mobility. Venafi customers are among the world’s most demanding, security-conscious organizations.

References