SOLUTION BRIEF

LEVERAGING VENAFI TRUSTFORCE AND A10 THUNDER ADC TO SIMPLIFY CERTIFICATE MANAGEMENT

Automate Management and Security of the Entire Certificate Lifecycle Process

Challenge:

Organizations need to not only manage the lifecycle of all digital certificates but ensure that any vulnerabilities are found and automatically rectified. The difficulty of this undertaking is magnified when certificates are configured on various network infrastructure elements.

Solution:

A10 Networks Thunder ADC line of Application Delivery Controllers is fully interoperable with Venafi's Trust Protection Platform. Together, this joint solution enables control over all digital certificates present, while allowing full remediation of any anomalies.

Benefits:

- Automate management and security of the entire certificate lifecycle process
- Ensure full visibility into SSL certificate vulnerabilities with automatic remediation regardless of location
- Directly store certificates to eliminate duplication and consolidate and simplify security information
- Offload CPU-intensive processing of secure traffic and eliminate blind spots imposed by SSL encryption

Applications of all types have migrated to the web and use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption to secure user sessions. To authenticate sites, organizations rely on cryptographic keys and digital certificates to establish trust for countless business activities. Such electronic countermeasures safeguard transactions and prevent spoofed sites and snooping by malevolent hackers or other cyber criminals. Users gain confidence in such applications, allowing their use to flourish with an exponential increase in productivity.

However, the very trust that keys and certificates establish has become a source of attack. When organizations instinctively trust keys and certificates, cybercriminals can turn compromised ones against them. Worse, organizations often have limited visibility into their vulnerabilities and a restricted ability to respond to breaches. Offenders are able to successfully steal data while remaining undetected for months, or even years. These key and certificate weaknesses lead to significant security risks that demand immediate action.

Organizations must secure their key and certificate portfolio and identify their vulnerabilities. By gaining insight into the entire key and certificate inventory and by enforcing policies, IT administrators can reduce their risk exposure, both decreasing the chance of a data breach and lessening the impact if a breach does occur. Proper key and certificate management and organization based on real-time aggregated data that continuously evaluates and fortifies the security position is imperative.

Streaming and Securing Certificates with A10 and Venafi

Through its partnership with Venafi, A10 simplifies and consolidates key management, identifies key and certificate vulnerabilities, enforces enterprise policies, and detects anomalies with ongoing monitoring. Customers dramatically reduce the number of keys required by centralizing certificates for thousands of web servers at a time, rather than provisioning a certificate for each server directly. Through the Venafi TrustForce integration with A10 Networks® Thunder® ADC line of Application Delivery Controllers, customers can gain real-time visibility of all certificates, including all of those present on A10 devices in the network. Other benefits include automated renewal – installation, configuration and validation in seconds, preventing network outages, errors and reducing cost.

The A10 Networks and Venafi TrustForce Joint Solution

Venafi TrustForce

Venafi TrustForce, part of Venafi Trust Protection Platform, automates responses to trust-based attacks and remediates SSL certificate vulnerabilities before they cause complications. TrustForce secures and protects the entire key and certificate lifecycle, automatically remediating anomalies by replacing the vulnerable key or certificate. With automated integration across hundreds of applications, devices, services and certificate authorities (CAs), TrustForce ensures that the remediation process occurs seamlessly. In addition, TrustForce enables organizations to scale their cryptographic resources more quickly and securely. Its automated key and certificate operations and intelligent application-specific integration let enterprises scale to hundreds of thousands of encryption keys and certificates more quickly and securely than ever before.

Automated Key and Certificate Enforcement

TrustForce provides powerful, fully automated key and certificate control, eliminating the vulnerabilities that can arise from error-prone manual processes – errors such as accidentally copying keys or deleting certificates. TrustForce enables organizations to scale new encryption-dependent applications quickly by rapidly deploying keys and certificates to them.

Automated Key and Certificate Remediation

TrustForce delivers fully automated response capabilities by securing the distribution of keys and certificates to applications. By providing end-to-end provisioning and certificate lifecycle control of complex, load-balanced encryption environments, systems administrators can automate a wide variety of provisioning processes, including key generation, certificate signing request (CSR) generation, CSR submission, CA approval, issued certificate retrieval, certificate installation, private key backup and certificate renewal.

Fully Automated Workflows and Tracking

TrustForce enables organizations to define automated workflows to remediate key and certificate vulnerabilities, apply granular workflow processes at every stage of the certificate lifecycle, and enforce reviews and approvals for critical security operations.

A10 Thunder ADC

A10 Networks Thunder ADC line of Application Delivery Controllers solves many of the challenges facing organizations of all types including enterprises, cloud service providers, telecommunications and government. This comprehensive application delivery optimization solution helps IT administrators realize the potential of their network infrastructure investments while dramatically lowering overall costs. Thunder ADC consolidates numerous "point products" into one scalable ultra-high capacity appliance by providing application acceleration via caching, compression and TCP optimization, server availability with local and global Layer 4-7 load balancing and security with Web application and DNS firewalls, Distributed Denial of Service (DDoS) protection, authentication support, SSL offloading and SSL Insight.

SSL Offloading

The widespread use of SSL encrypted data strains security infrastructure such as intrusion prevention systems and firewalls that must terminate SSL connections. Decentralizing SSL key management to each of these solutions further complicates security management and potentially reduces certificate visibility. A10 Thunder ADC leverages SSL Insight with high performance SSL encryption and decryption capabilities to offload CPU-intensive SSL traffic processing and enable security devices to inspect all traffic, not just clear text.

Thunder ADC's SSL Offload capabilities enable organizations to:

- Scale SSL performance to meet current and future requirements. With SSL bandwidth demands growing exponentially, Thunder ADC provides the capacity to handle high volume SSL traffic with 1024-, 2048- or 4096-bit certificates. Sustainable throughput can exceed 40 Gbps and over 170,000 new SSL connections per second (with 2048-bit certificates).
- Satisfy the most stringent security requirements. A10 products have obtained certifications for FIPS 140-2 Level 3 compliance, Common Criteria and Joint Interoperability Command (JITS). These designations confirm that the cryptographic modules are "production-grade" and include role-based administration and physical tamper evidence.

Centralized Key Management

Thunder ADC appliances streamline SSL key management and lower certificate overhead. Certificates are stored on the Thunder ADC appliance with its hardened operating system to enhance security, reduce the expense of costly duplication of certificates on the application servers and minimize management complexity. Administrators avoid procuring and handling SSL certificates for each individual server. A10 also supports the creation of self-signed certificates for simplification. In the event of an SSL vulnerability outbreak such as Heartbleed, administrators can avoid patching countless web servers. Organizations provision an SSL certificate automatically or manually to prevent users from seeing an "untrusted root" error typically generated from an internal untrusted certificate server.

Simplify Certificate Management with Venafi TrustAuthority and Thunder ADC

Venafi's TrustForce demonstrates proven interoperability with A10 Thunder ADC, providing customers with a consolidated and simplified method for managing critical security information such as the location of certificates, key sizes, ciphers used and validity dates. Combining these two solutions provides a complete view of an organizations' digital certificates and keys for efficient operations.

The Venafi platform provides the necessary visibility and reporting to ensure that Thunder ADC is using the latest standards supported via the aXAPI integration and programmability. Emerging standards in SSL/TLS supported include:

- Perfect Forward Secrecy (PFS) and Elliptic Curve Diffie–Hellman Exchange (ECDHE)
- Key size migration status compliance from 1024- to 2048-bit keys
- Emerging use case of 4096-bit keys, where usage can top twenty percent

Together, Venafi TrustForce and Thunder ADC overcome the pitfalls of SSL certificate management. IT administrators can be confident that their online data communications are protected. By combining these tools, the following benefits can be realized:

- Automate management and security of the entire certificate lifecycle process, including end-to-end provisioning, key

generation, certificate signing request (CSR) generation and submission, CA approval, issued certificate retrieval and installation, private key backup, and certificate renewal – all within a load-balanced encryption environment
- Ensure full visibility into SSL certificate vulnerabilities with automatic remediation regardless of location
- Simplified discovery of all certificates throughout the network, including all those installed on A10 Thunder networking and security devices
- Efficient tracking of thousands of SSL certificates from multiple providers with up-to-date knowledge of critical parameters including expiration times; ensures that websites are protected and visitors safeguarded from hacking
- Managed self-signed certificates, preventing them from being unaccounted for and ensuring that no violation of organizational policy has occurred
- Guaranteed correct installation of SSL certificates and business continuity; eliminates browser popup warnings when users try to access the site
- Use A10 SSL Insight to offload CPU-intensive processing of secure traffic and eliminate blind spots imposed by SSL encryption
- Deploy A10 Networks aXAPI® REST-based API to support the integration and programmability of Venafi's TrustForce to ensure compatibility

Next Steps

To learn more about how this Venalfi-A10 Networks joint solution can benefit your organization, please contact your A10 Networks representative.

About Venafi

Venafi is the market leading cybersecurity company in Next-Generation Trust Protection. Venafi delivered the first trust protection platform to secure cryptographic keys and digital certificates that every business and government depend on for secure communications, commerce, computing and mobility. Venafi TrustAuthority identifies key and certificate vulnerabilities, enforces corporate policies and monitors for anomalies. Venafi TrustForce automates responses to trust-based attacks and remediates vulnerabilities before they cause problems. It secures and protects the entire key and certificate lifecycle, automatically curing anomalies by replacing vulnerable trust assets before attackers can compromise them.

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-SB-19137-EN-01
Mar 2015

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com

Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
Hong Kong
HongKong@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.