A Frost & Sullivan White Paper

Ensuring Business Continuity: Certificate Lifecycle Management is a Necessity for Modern Businesses

Powering clients to a future shaped by growth

FROST & SULLIVAN

UNDERSTANDING THE CRITICAL NEED FOR CERTIFICATE LIFECYCLE MANAGEMENT

In December 2018, mobile networks in the United Kingdom and Japan experienced major outages that affected millions of customers. The following month, several major US government websites went offline, including those of the Department of Justice and NASA. Neither incident was the result of a cybercrime or natural disaster, but an overlooked deadline: IT teams had missed the renewal of critical Transport Layer Security (TLS) certificates, which caused aspects of both public- and private-facing systems to be interrupted. In the US government case, the oversight was a consequence of a federal shutdown from December 2018 to January 2019, during which the teams responsible for managing digital certificate expirations were furloughed. Within a short amount of time, at least 80 certificates used by the government websites went unnoticed and expired, and undoubtedly more followed.

These are extreme (and relatively rare) examples, but they are not unique. As recently as February 2020, Microsoft experienced a similar situation when its Microsoft Teams system went down for a few hours because of an expired certificate, showing that even tech giants can be victims of their own oversights.

With the societal restrictions put in place globally to slow the spread of COVID-19, many businesses have had to reduce operations and institute work-from-home policies. This means even more people, data, and devices are connecting remotely, but at the same time, fewer people may be available to confirm whether certificates are being renewed as needed.

Digital certificates are a necessity for modern businesses and organizations of all types. The data encryption that certificates provide is encouraged or mandated by numerous regulations and standards. Even more critically, digital certificates protect businesses, organizations, and even individuals against data breaches on connected devices and systems across the enterprise. As cybercrime is on the rise, digital certificates are an important data encryption-based solution for protecting against man-in-the-middle attacks as well as email- or web-based phishing.

Connected Internet of Things (IoT) devices, remote work tools such as virtual private networks (VPNs), and websites require digital certificates to communicate information securely with internal and external endpoints and applications. The number of applications for certificates is staggering: an estimated 547,000 new websites are being added every day[1], and Frost & Sullivan research shows that the number of IoT devices will grow from 22 billion in 2019 to more than 58 billion by 2025.

“As cybercrime is on the rise, digital certificates are an important data encryption-based solution for protecting against man-in-the-middle attacks as well as email- or web-based phishing.

While some of these IoT devices will be related to consumer products, most will be owned and operated by businesses or governments. For example, by 2025, over 10 billion IoT devices will be used for factory and industrial automation. Another 2.5 billion will be used in the energy space. Every IoT device may need multiple certificates; hence, the number of certificates needed by a business leveraging IoT devices will expand exponentially. The number, importance, and diversity of digital certificates will continue to increase as industries undergo digital transformations. This is in addition to a business’s web presence and subdomains. Geographic expansion adds to the complexity: as businesses enter new markets, they have to learn and adopt regional regulatory policies and guidelines that influence the use of certificates across their sites, devices, and applications.

Businesses need to manage a growing number of certificates and multiple types of certificates with varying renewal cycles. The maximum term for public TLS certificates has, in the past few years, shrunk from three years to, as of September 1, 2020, 13 months, but businesses can choose shorter terms. For traditional server architecture, many elect 90-day terms, and for DevOps and some IoT use cases, they may choose a day or less. At the same time, other public certificate types such as S/MIME and Code Signing can be valid for as long as three years, and for some other IoT use cases, they need to last considerably longer.

1 https://www.millforbusiness.com/how-many-websites-are-there/

Challenges with Manual vs. Automated CLM

These challenges put undue pressure on businesses because many still rely on spreadsheets: managing thousands of certificates manually is bound to result in errors and oversights. Businesses are better served with teams focusing on their core competencies rather than policing hundreds or thousands of line items on a spreadsheet. Automation simplifies certificate lifecycle management (CLM) in several ways:

- Certificates are renewed before expiring, regardless of the term. Industry-leading solutions will ensure this even when renewal times change from one generation of certificates to the next.
- Precious (expensive and increasingly rare) IT department resources will be deployed where they have the most value rather than on manual and error-prone legacy certificate renewal processes.
- Businesses can easily ramp up across countries and markets, add websites, create new applications, and expand their endpoints without worrying about how to manage the certificates for each of these changes.
- Business continuity and brand reputation are preserved when there is virtually no risk of a site or endpoint suddenly going offline during normal operations or emergencies.

Real-world Example: Leading Legal Software Innovator Averts Risk with Advanced CLM

Lighthouse Global, a major player in the legal software and service market, is a great example of a business that benefited from automating its certificate management. Its process was costly and cumbersome, with more than 10,000 certificates to update. When Lighthouse upgraded its software and data systems, it realized that its certificate management restrained its process, efficiency, and security goals. It considered creating an in-house solution but determined that industry-leading CLM provider Sectigo could rapidly automate the system. What would have taken more than a year of sifting and sorting to uncover, categorize, and update thousands of certificates was accomplished in a matter of weeks. The resulting automated system provides Lighthouse IT and corporate management with a clear and helpful dashboard that allows the management of all certificates from one place.

As Lighthouse's example clearly shows, by adopting automated CLM, a company could avert operational risk and challenges, as well as lower costs. These benefits extend to virtually any business of any size, as well as governments, non-governmental organizations (NGOs), educational institutes and other organizations. To better ensure continued operation of any connected system and device, avert certificate-related failures, and control costs, businesses and other organizations should consider the advantages of an automated CLM solution. Partnering with a provider of advanced solutions, such as Sectigo, mitigates the risk and much of the time and costs that come with manual certificate management, averting challenges stemming from rogue certificate expiry and human error.

AUTOMATED CERTIFICATE LIFECYCLE MANAGEMENT AND THE HIDDEN COSTS OF MANUAL CERTIFICATE PROCESSES

Despite our increasingly digitized and connected world, Frost & Sullivan research shows that many businesses still rely on archaic ways of keeping digital certificates up to date and accurate. Excel-based certificate tracking and other manual processes have clear disadvantages:

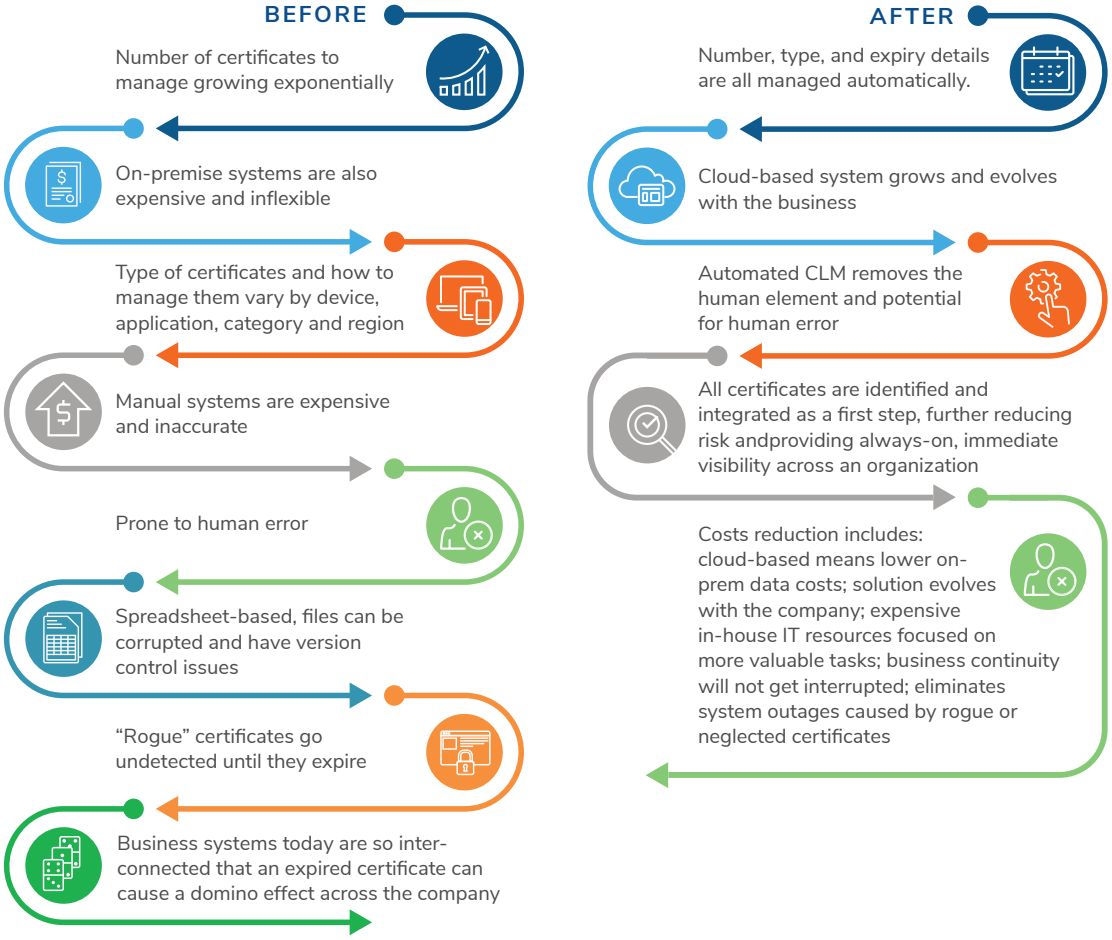
- Errors are bound to occur in any process that relies on people to enter and update information in a timely manner and to store files in a way that is secure and immune to version control issues.
- Manual certificate installation can have as many as nine steps, each of which has to be timely and precise to keep certificates up to date. These steps are also costly in terms of time, personnel expenses, and the high risk of human error.

Businesses cannot afford to have certificates expire. External costs associated with an outage on a customer-facing website can be immense. For significant customer-facing sites, even one hour of downtime can cost as much as $100,000 and upward of $1 million[2] for the most active sites. The resulting loss of customer confidence could affect brand equity and cause customers to migrate to a competitor. But the risk extends far beyond this. If a server's certificate expires, for example, the resulting outages can cause any number of internal connected systems to go offline and have ramifications across the enterprise. Websites, servers, IoT equipment, and VPNs for remote workers, which expanded drastically during COVID-19 shelter-in-place restrictions, could all be affected and would result in significant productivity losses if they went offline.

These problems are easily preventable. A business can turn to one of the effective automation protocols available in the market, including Simple Certificate Enrollment Protocol (SCEP); Enrollment over Secure Transport (EST), which is considered the evolution of SCEP because it uses standard TLS; and Automated Certificate Management Environment (ACME), which is a newer protocol. The ACME protocol is gaining popularity as an open-source and relatively low-cost option, helping bring down CLM total cost of ownership.

2 https://itic-corp.com/blog/2016/08/cost-of-hourly-downtime-soars-81-of-enterprises-say-it-exceeds-300k-on-average/

The Risks (and costs) of Manual Certificate Managements Before and After Automated CLM



A supplier that can provide CLM through the cloud offers an even stronger value proposition, allowing for easier scaling up or down of certificate management without taking up any on-premises resources, as well as speed and accuracy. Additional benefits include:

- Continuous conformance with current patches, security practices, and cryptographic standards. This last part falls under the rubric of crypto agility. The pace at which cryptographic algorithms require updates has accelerated. Frost & Sullivan and the industry expect this acceleration to continue, especially as advances in quantum computing inevitably change the entire cryptographic landscape.
- Discovery of rogue certificates, which can exist inside an enterprise without the knowledge of the security team or central IT. In this alarmingly common situation, at some point, the certificate expires and takes the associated critical system offline with it (with no clear reason why). This can take days to uncover and days more to re-certify and rectify, and can leave substantial damage in its wake. Businesses must understand this and implement CLMs with certificate discovery functionality that can apply to all certificate types (whether TLS, client, S/MIME, code signing, or document signing) with both public and private roots. These systems can discover rogue certificates/CAs, bring them under management, ensure that they are audited for compliance and cryptographic best practices, and automatically renew them when the time comes.
- Visibility and reporting. This is critical to an enterprise's management of certificates and its ability to enforce and demonstrate compliance with industry and regulatory standards and customer service-level agreements.

Case Study: The CLM Experience in the Financial Sector

For many businesses, the point in which they realize they need an automated CLM solution may come after they have already experienced a significant and preventable system outage due to a failure of their manual certificate management process. A business may also discover the benefits of automated CLM through an assessment of processes that can be automated or through exploring ways to reduce risk.

For a multinational company in the financial sector that manages data from millions of businesses and hundreds of millions of consumers, the decision to move to an automated CLM system stemmed from the need to streamline its processes. While the company had a platform from which it could manage certificates, it was an expensive and inflexible on-premise system. As the company had grown in part through acquisitions, visibility of all the certificates from these different entities was often obscured. The company also has a presence in dozens of countries around the world.

Managing a huge number of certificates with varying requirements and limited visibility became a significant cost and risk to security and operations. The company, therefore, engaged Sectigo to provide a centralized, always-on, cloud-based certificate provisioning and management solution. Moving to the cloud reduced costs, and using Sectigo to identify and manage certificates across the organization greatly improved visibility. The automation aspect of certificate management further provided the benefits of reducing the occurrence of a certificate expiring and causing an outage that could potentially cascade across the organization. It also helped the company ensure a consistent and high-quality experience for its customers.

BUSINESS CONTINUITY CAN DEPEND ON ADVANCED CLM

Along with material costs, the risks of manual certificate management can be extensive and result in an overall interruption of business continuity. Automated CLM resolves the challenges and risks inherent in manual certificate management processes that can impede business security, stability, and growth.

Highly interdependent digital systems across modern businesses foster efficiency and productivity. However, interdependence also makes these systems vulnerable: a failure in one part of the enterprise can quickly affect related systems. Whether a certificate expiry happens on an IoT device on a manufacturing line, a backroom server, or a website subdomain, the failure is rarely contained in that single place. A business may have thousands of certificates of varying types, making it difficult to manually find the root cause (especially if the outages cascade rapidly across the business). In addition, rogue certificates that are off the radar of a manual system may come to light only once they expire, further complicating the task for in-house IT departments to find and correct the fault. Sophisticated CLM systems can find and update rogue certificates and automatically manage thousands of disparate digital certificates. Protection from enterprise-wide failures is one of the most critical benefits that CLM can bring to a business.

Along with being error-prone and inefficient, manual certificate management is time-consuming and expensive. Considering the average hourly rate of an IT professional in the United States is about $34[3], and that of a cybersecurity professional is upward of $55[4], businesses can almost immediately see benefits in pivoting expensive resources toward more valuable tasks when automating rote digital certification management. With today's shortage of nearly 3 million cybersecurity professionals globally[5] expected to increase in the coming years, these skilled positions will be more expensive in the future, making CLM even more of an imperative.

3 Salary.com
4 Payscale.com
5 https://www.cnbc.com/2019/03/06/cybersecurity-expert-shortage-may-cost-companies-hundreds-of-millions.html

Brand value is another factor that cannot be overlooked. External-facing downed websites, internal failures in operations, and other interruptions have tangible, negative effects on a company's brand equity and its value, which can extend to stock price. Automated CLM leaves virtually no room for errors that can lead to these consequences. A related aspect of brand reputation is digital trust. Both businesses and consumers need the assurance that the organizations with which they interact will protect any information shared between parties. Certificates encrypt information (whether across systems and devices or between parties in commercial transactions) and help prevent costly data breaches that hurt brand value, equity, and trust. Automated CLM ensures this is done accurately and consistently.

> **Insurers increasingly demand that their clients have strong cybersecurity programs in place. A company demonstrating cybersecurity best practices with industry-leading partners would be seen as a lower risk.**

Insurance is another cost that can be influenced by automated CLM as part of a comprehensive cybersecurity strategy. Insurers increasingly demand that their clients have strong cybersecurity programs in place. A company demonstrating cybersecurity best practices with industry-leading partners would be seen as a lower risk. Regulations come into play as well. Heavily regulated industries, such as finance and healthcare, have some of the most stringent regulations around cybersecurity, but all businesses and organizations fall within the purview of governmental, industry, and/or standards organizations that encourage, if not require, a high level of cybersecurity. Automated CLM is among the most fundamental, cost-effective, and easy-to-implement means of compliance.

Case Study: Automated CLM Proves Critical to Healthcare Tech Innovator

Medecision, a leading software-as-a-service provider of cloud-based solutions to the healthcare industry, is representative of benefits companies recognize when moving to an automated CLM solution.

Medecision has been instrumental in helping its clients along their digital transformation journey. However, despite having highly advanced, industry-leading technical solutions, it had fallen behind in transforming its own certificate management process. The company had a manual, spreadsheet-based solution, accompanied by email alerts, to manage hundreds of certificates. These certificates allowed it to securely connect with and provide services to dozens of major HMOs and other healthcare providers. Any downtime due to certificate expiry would impact its ability to provide these solutions. The business was also concerned that it had rogue and non-compliant certificates, without a good sense of how many or where they might be. Furthermore, the company had recently moved to more frequent, one-year terms for its TLS certificates to improve its security posture and comply with current and anticipated healthcare industry data management regulations. However, the Medecision team became overwhelmed after making the certificate management process more frequent and implementing automated alerts internally to stay abreast of renewals.

This confluence of challenges put tremendous stress on Medecision's IT team and management, both in terms of keeping abreast of the certificates and by creating a looming fear of a sudden, unforeseeable outage. The company decided something had to change before an event occurred that caused significant damage to its systems and ability to deliver its cloud-based software solution.

Medecision brought in Sectigo in a tiered approach: first, to help the company understand the landscape of the situation, and second, to provide an automated solution to replace the manual one that was fraught with potential inconsistencies and version control issues.

While the company expected Sectigo to find some rogue certificates, Sectigo's results still proved to be eye-opening. For example, certain servers that were not deemed to be at risk were found to have misnamed or extraneous certificates. Either of these situations could have resulted in a server outage, which would have had the potential to reverberate across different systems. Sectigo also found non-compliant certificates, which the company had not expected. This illustrated how the current manual process was inaccurate.

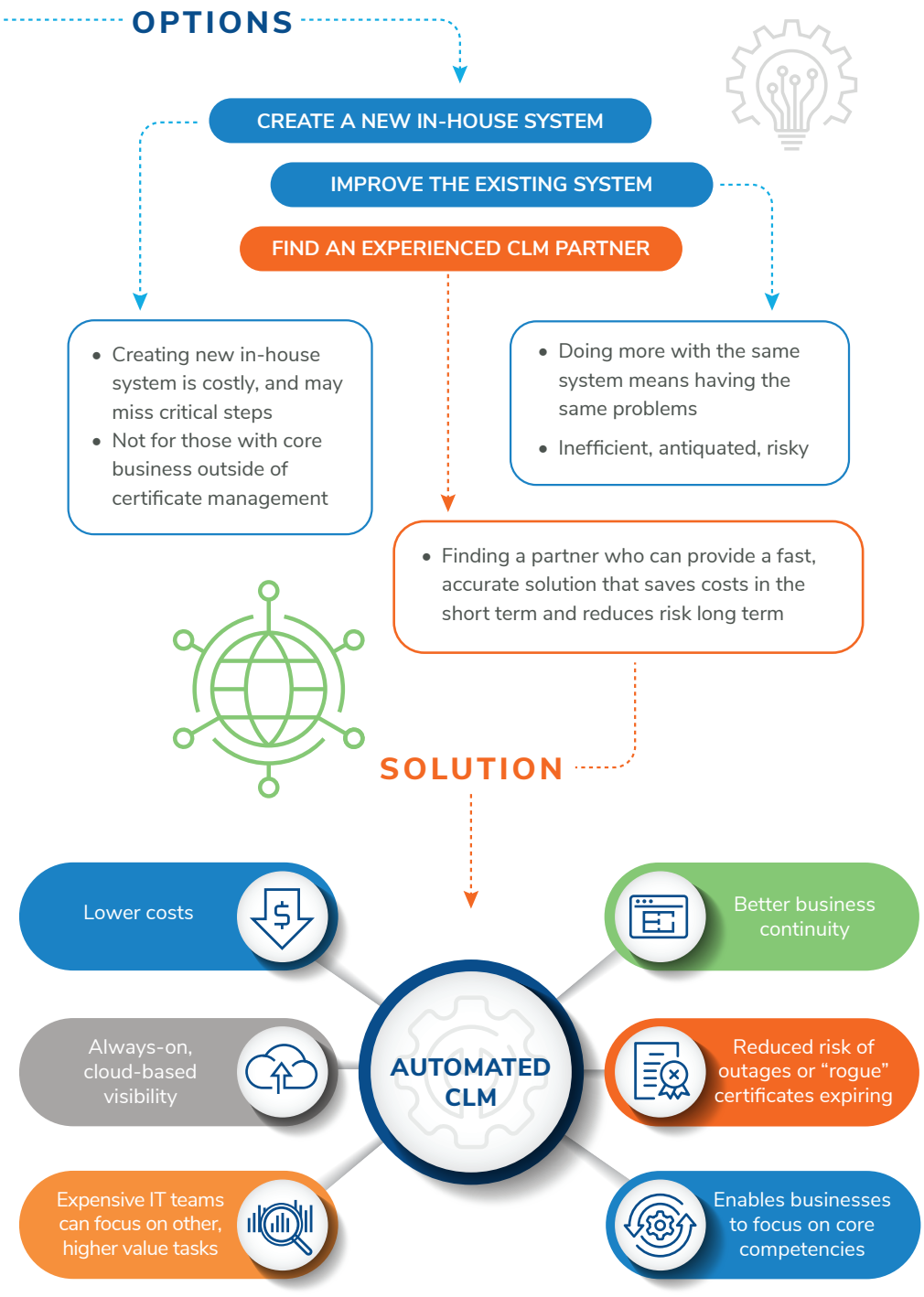
The first step of comprehensively identifying problematic certificates helped bring significant relief to Medecision, allowing it to understand the scale of its potential problem and head off any issues. To build upon these benefits, Medecision engaged Sectigo to fully automate the CLM process with a cloud-based solution. These two steps gave Medecision peace of mind that it would avert any certificate-related outages and enabled it to provide higher-quality service to its customers.

The results were transformative: to date, Medecision has not experienced any certificate-based issues. In addition, the company's IT team has been able to redirect its time to higher-value activities more in tune with the company's core value proposition, further improving its current and future services for its customers as well as relieving the IT team of a significant, and stressful, burden.

AUTOMATED CLM AND THE CUSTOMER JOURNEY

Businesses today recognize the value digitization brings; however, many have been remiss in upgrading their certificate management programs accordingly. Manual, spreadsheet-based processes are difficult and expensive to maintain and use valuable IT resources. Adopting automated CLM, such as from market leader Sectigo, nearly eliminates the risks of inaccuracy and inadvertent certificate negligence that can otherwise have dire consequences to business continuity. The charts below shows the challenges to modern certificate management and illustrates the customer journey in moving from a manual to an automated CLM system.

continued on next page



The costs from expired certificates go well beyond systems going offline. These ramifications can extend to customer loyalty, stock price value, and lack of regulatory compliance. Moving to an automated solution reduces these risks substantially, removes the uncertainty and some of the costs from human-driven manual systems, and allows a business to focus more time and efforts on higher-value, less-mundane activities. Partnering with a provider of advanced solutions, such as Sectigo, mitigates the risk and much of the time and costs that come with manual certificate management, averting challenges stemming from rogue certificate expiry and human error.

To learn more about Sectigo's Lifecycle Management solution, visit: www.Sectigo.com

NEXT STEPS

- **Schedule a meeting with our global team** to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.

- Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.

- Visit our **Digital Transformation** web page.

- Attend one of our **Growth Innovation & Leadership (GIL)** events to unearth hidden growth opportunities.

Silicon Valley
3211 Scott Blvd
Santa Clara, CA 95054
Tel 650.475.4500
Fax 650.475.1571

San Antonio
7550 West Interstate 10
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

London
Floor 3 - Building 5,
Chiswick Business Park
566 Chiswick High Road
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

myfrost@frost.com 877.GoFrost http://www.frost.com

FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
3211 Scott Blvd, Suite 203
Santa Clara, CA 95054