



*50 Years of Growth, Innovation and Leadership*

## Server Security Lies Deep in Hardware

Windows Server 2008 End-of-Support is an Additional Catalyst for Change

An Executive Brief Sponsored by

  
Hewlett Packard  
Enterprise



Stratecast

FROST & SULLIVAN

Introduction . . . . . **3**

Implications of Remaining with Aging Servers running  
Windows Server 2008, including the “R2” Successor. . . . . **4**

Migration to the Cloud is Not Always the Optimal Choice . . . . **6**

Recommended Secure Server Features. . . . . **8**

Reasons to prioritize HPE ProLiant Gen10  
for server modernization . . . . . **9**

Stratecast: The Last Word . . . . . **10**

# INTRODUCTION

Replacing servers is often delayed. Confronted with competing business priorities, limited budgets and personnel, and a sense of comfort as current servers reliably hum along, delay is easy to rationalize. Yet, delays are not without risk and trade-offs. Cases in point are two circumstances that small and midsized enterprises (SMEs) should seriously consider and, in our opinion, initiate action now.

Those circumstances are:

- **A new era of cyber warfare aimed at exploiting hardware vulnerabilities is emerging**—A sample of scholarly articles listed below clearly demonstrates the existence of server hardware vulnerabilities and a growing number of attack variants. For SMEs with susceptible servers, their cyber and associated business risks are increasing.
  - January 2018: Spectre and Meltdown vulnerabilities reported<sup>1</sup>
  - August 2018: Foreshadow<sup>2</sup> and Foreshadow-NG<sup>3</sup> vulnerabilities reported
  - November 2018: Five new attack variants on Spectre and two new attack variants on Meltdown revealed<sup>4</sup>
  - January 2019: Baseband Management Controller (BMC) vulnerability reported<sup>5</sup>
- **End-of-Support (EoS) for Windows Server 2008/2008 R2 is fast approaching**—Reaching EoS on January 14, 2020, SMEs still relying on this server operating system (OS) face a perilous and expensive trade-off, namely:
  - **Complimentary provisioning of security updates ends**—Complimentary security updates to newly discovered vulnerabilities stop being released through Windows Update.

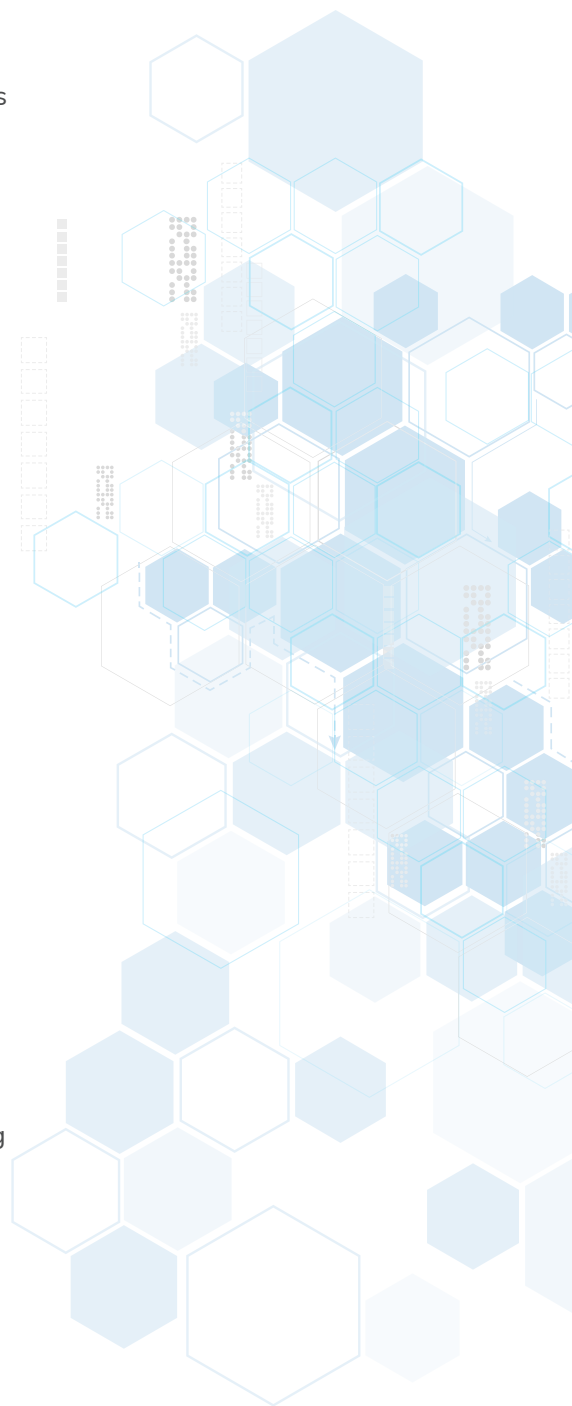
1 U.S. Department of Homeland Security, Alert (TA18-004A)—Meltdown and Spectre Side-Channel Vulnerability Guidance, Original release date: January 3, 2018

2 Proceedings of the 27th USENIX Security Symposium, Foreshadow: Extracting the Keys to the {Intel SGX} Kingdom with Transient Out-of-Order Execution, August 2018

3 Technical report, Foreshadow-NG: Breaking the Virtual Memory Abstraction with Transient Out-of-Order Execution, August 13, 2018 (Revision 1.0)

4 ZDNet, Researchers discover seven new Meltdown and Spectre attacks, November 14, 2018

5 The Register, The BMC in OpenBMC stands for 'Burglarize My Computer'—thanks to irritating security flaw, January 24, 2019



- **Extra spending becomes the new standard**—Security updates are available for three more years after Windows Server 2008/2008 R2 exits its “Extended Support” phase in January 2020, but for a significant extra fee and a three-year commitment. Also, the updates are limited to security issues rated critical or important. With the industrialized state of cyber warfare, attackers systematically prey on the weak and vulnerable. Not doling out dollars for even the limited security updates moves your servers closer to the target’s bullseye.

There is a favorable path forward. This path is framed by servers purpose-built to withstand this new era of hardware attacks, and optimized with the latest operating systems to deliver the agility and performance SMEs need to succeed in an increasingly digitized competitive climate.

In this white paper we dive into the implications of not replacing aging servers, as well as important feature considerations in making a qualified server replacements decision. Also, with workload migration to the cloud being an often considered alternative to on-premises servers, we share Frost & Sullivan’s latest IT decision-maker views on the cloud journey; a journey that includes occasions of hesitation and regret. Finally, given their tight restraints on time, talent, and budget, we shaped our perspectives in the context of SMEs.

## IMPLICATIONS OF REMAINING WITH AGING SERVERS RUNNING WINDOWS SERVER 2008, INCLUDING THE “R2” SUCCESSOR

Although the implications of continuing with aging servers and server OS will vary by company, there are several implications that broadly apply. This section is devoted to those.

### As no layer is immune, expect higher IT operating costs

Historically, exploitable vulnerabilities were concentrated at the host operating system and above software layers. Hardware vulnerabilities and attack variants, as previously summarized, are a more recent development, but growing in number. Consequently, IT operating costs are poised to increase as additional patching of operating systems and hypervisors will be required to offset chipset vulnerabilities (e.g., with Meltdown); and/or servers will need to be pulled offline to return chipsets to original factory specifications (e.g., with BMC).

For SMEs, merely staying abreast on current server and OS inventory and their vulnerabilities; assessing cyber, compliance, and business risks; and then devising and executing prioritized remediation is already a challenging set of tasks. Adding hardware vulnerabilities and remediation further stretches an already thin staff.

### Cost of data breaches and security incidents continues to rise

Whether calculated based on average total cost or cost per lost or stolen record, the average cost of data breaches rose from the previous year, according to Ponemon Institute (now at \$3.86 million average total cost, and \$148 cost per record).<sup>6</sup> Moreover, the likelihood of one or more material data breaches within the next 24 months has risen to 27.9%; a demonstration that data-exfiltrating

6 Ponemon Institute LLC, 2018 Cost of a Data Breach Study: Global Overview

attackers return. Placed into the broader context of all incidents (those that resulted in a data breach and those that did not), retargeting is common. FireEye calculated that nearly two-thirds of its incident response clients were retargeted by the same or similarly motivated attack group within a 19-month period.<sup>7</sup> Bottom line, the cost of a data breach is rising and seldom limited to a single incident. And, with hardware vulnerabilities adding to the overall attack surface, incidents and severity of data breaches are poised to increase.

Ransomware attacks present another cost parallel, as servers are second to laptops/PCs as device types most targeted by ransomware attacks.<sup>8,9</sup> According to SentinelOne's survey of ransomware victims, the total cost of a ransomware attack averaged over \$750,000. Additionally, the suffering is not limited to the targeted company, as 40% of ransomware-attacked companies stated their suppliers and partners also suffered downtime. For some, the cost of a ransomware attack reached into the millions (e.g., \$10 million for Erie County Medical Center, and \$5 million for the City of Atlanta<sup>10</sup>). Also of note, nearly three in four SentinelOne survey responders agree that organizations are turning to cyber insurance to mitigate the cost of potential General Data Protection Regulation (GDPR) fines. Considering that the cost of cyber insurance factors in IT assets and their risk of compromise, one can rightly conclude that older servers with known and unpatched vulnerabilities, which store or process sensitive data, add to the cost of cyber insurance; versus newer servers and server OS with advanced, built-in security.

### Breach detection remains significantly slower than attackers' ability to succeed

According to FireEye, the good news is that the time to detect a breach after initial compromise (i.e., dwell time) has fallen precipitously from 416 days in 2011 to 78 days in 2018 (for comparison, Ponemon pegs the mean time to identify a data breach at 197 days). While laudable progress, the bad news is that attackers are typically more than 10x faster. According to Nuix, professional penetration testers and incident responders (groups that approximate criminal hackers in expertise and effectiveness) stated they overcame perimeter defenses, identified valuable data, and exfiltrated that data in less than two days in 80% of their attempts.<sup>11</sup> For additional comparison, 85% of the data breaches investigated by FireEye had dwell times that were considerably longer than two days: a minimum of one week and up to several years. Now, considering the relative newness of hardware vulnerabilities and attack variants, indicators of compromise (IoC) may not be as well-known or identifiable (the clues will likely be more elusive). These circumstances add to dwell time and the business implications of data breaches and other security incidents.

7 FireEye, *M-Trends 2019*

8 SentinelOne, *SentinelOne: Global Ransomware Study 2018*

9 Sophos provides a different perspective on attack targets, and reports in *7 Uncomfortable Truths of Endpoint Security* (March 2019) that servers (36.7%) are the locations where organizations found or discovered their most significant cyberattacks. Networks are a very close second (36.6%), distantly followed by endpoints (16.9%) and mobile devices (9.7%).

10 CSO, *What does a ransomware attack cost? Beware the hidden expenses—The ransom is only a tiny portion of the total cost of a ransomware attack. Consider these associated costs when estimating the total damage.*, May 29, 2018

11 Nuix, *The Black Report 2018—Decoding the Minds of Hackers*

## Downtime is costly and back-up potentially risky

Server hardware vulnerabilities inject unknowns into whether aging servers can remain online, powering business without exposing the business to intolerable risk. Unknowns include:

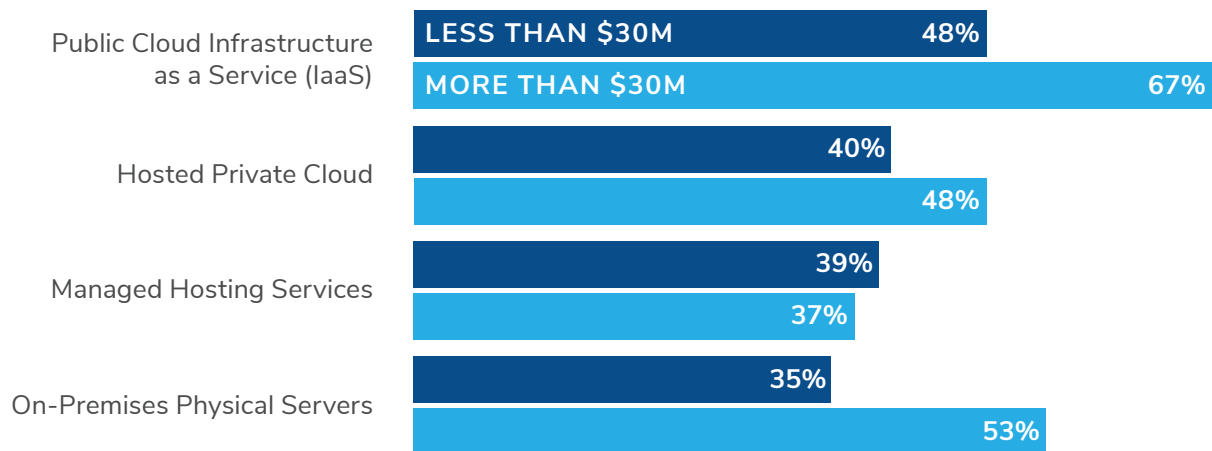
- How quickly and comprehensively will hardware vulnerabilities be identified?
- Can identified vulnerabilities be remediated with software patches?
- How quickly will software patches become available?
- Will IT staff will be available to apply remediation?
- And more disconcerting with hardware vulnerabilities, will on-site remediation even be possible?

Back-up servers is a viable alternative. However, back-up servers with the same vintage as current servers are equally vulnerable. As previously noted, incident investigations confirmed that cyber attackers frequently retarget previous victims.

## MIGRATION TO THE CLOUD IS NOT ALWAYS THE OPTIMAL CHOICE

Migrating workloads to the public cloud (i.e., Infrastructure-as-a-Service) is a growing trend. Even so, Frost & Sullivan’s research shows that, while hosting workloads in the public cloud is one of many options that SMEs use, the cloud is not always the optimal choice. To demonstrate, the following series of survey-based findings illustrate IT decision-makers’ views on on-premises versus cloud-hosted workloads. For comparison purposes, survey responses are segmented by IT decision-makers employed at businesses with ‘Less than \$30 million’ in annual revenues (a proxy for SMEs) versus ‘More than \$30 million’.<sup>12</sup>

### WHERE WORKLOADS ARE CURRENTLY DEPLOYED—TOP FOUR CHOICES



Source: Frost & Sullivan

<sup>12</sup> All cited findings in this section are from Frost & Sullivan’s 2018 Cloud User Survey. The number of respondents in the ‘Less than \$30 million’ cohort totaled 202 versus 174 for the ‘More than \$30 million’ cohort.

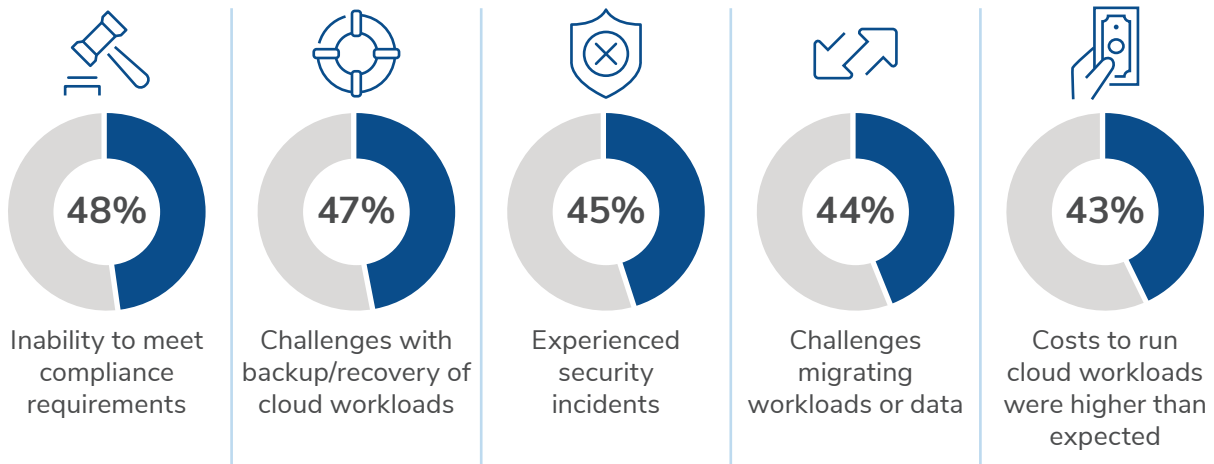
Indicative of a hybrid IT model, a variety of deployment options are currently used for hosting workloads. Additionally, workload deployment plans for the next two years foretell similar diversity. In other words, the hybrid IT model will continue to be prominent into the foreseeable future.

“The hybrid IT model will continue to be prominent into the foreseeable future”

When asked about the business restraints on implementing cloud solutions for some or all of their workloads, the two cohorts were uniform in the top restraint, namely: **Security risks/unauthorized access to my data or applications.**

Another cloud consideration is that returning a workload from the cloud to a business-managed environment (i.e., repatriation) is common. **Forty-three percent of the ‘Less than \$30M’ cohort repatriated workloads versus 48% for the ‘More than \$30M’ cohort.** For the ‘Less than \$30M’ cohort, the reasons for workload repatriation span compliance, security, and operations (see next chart). Reflecting the higher percent of the ‘More than \$30M’ cohort having repatriated workloads and having greater IaaS adoption, this cohort’s percentages were also higher for each of the same repatriation reasons.

### REASONS WORKLOADS WERE REPATRIATED—TOP 5 REASONS FOR THE ‘LESS THAN \$30M’ COHORT



**NOTE:** Percent of Respondents choosing “Important” or “Very Important”

Source: Frost & Sullivan

Connected devices generating sensory data is another scenario that argues for retaining localized or edge computing capabilities. Cost economics, data sovereignty, and latency are leading variables in making edge-versus-cloud decisions.

This collection of findings funnels to a conclusion that an ‘all on-premises’ or ‘all cloud’ deployment model is unlikely for most SMEs. Moreover, a full migration to the cloud by SMEs with established on-premises footprints is even less likely. As previously shown, cloud migration issues and missed expectations offer a cautionary tale. Nevertheless, SMEs want choice in order to optimally match business objectives with deployment options. To that end, **we believe a hybrid IT model will continue**

to grow in prominence, with workloads shifting back and forth among hosting locations (i.e., fluidity). Supporting fluidity, OS compatibility between on-premises servers and cloud is critical and is one of the recommended server features listed in the next section.

## RECOMMENDED SECURE SERVER FEATURES

As described in the previous sections, relying on aging servers running soon-to-be EoS Windows Server 2008/2008 R2 is a certain step backwards in security. Also, migrating on-premises workloads to the cloud is not always the optimal choice. Modernizing on-premises servers and their operating systems is the logical direction. This direction, however, is not clear-cut as numerous server options are available. And considering that today's servers will support the business for many years, an unqualified server selection can be regrettable.

To assist in reaching a qualified server modernization decision, we recommend evaluating your server options based on the following built-secure features.

- **Immutable Authenticity Assurance**—A server's firmware is the base for the software layers operating above, and is also a layer that is susceptible to compromise. But how do you know the firmware is authentic? What you need is an immutable confirmation of firmware authenticity. This is where a silicon root of trust comes in. This root of trust is a fingerprint of the firmware burned into the server's silicon at the time of manufacture. Plain and simple, if the current firmware code matches the silicon fingerprint, authenticity is confirmed.
- **Authoritative Alerts**—Because this fingerprint is sealed in silicon, the fingerprint is permanent. Consequently, any fingerprint mismatches, at boot or run-time, are the real deal. By design, there are no false positives, and your IT staff is not drawn into an unproductive effort of disproving false positives.
- **Simple Recovery to Trusted State**—Knowing there is a problem is only the first step in resolving a problem. As firmware checks are transparently occurring during run-time, and the firmware fingerprint is permanent, recovering to a trusted state is straightforward—just reboot.
- **Built Compliant**—Cyber regulations guiding a digitized world to a safer existence are on the rise. Therefore, shouldn't the servers you use to power your business be built compliant versus reliance on complex and compensating means to accomplish the same outcome? We believe this is only logical, and a feature you should demand in your next set of servers.
- **Native Data-at-Rest Protection**—Sensitive data stored in your servers is honey that attracts data thieves. Using third-party technologies to protect data-at-rest is a common approach. Common, however, should not be assumed default. As silicon root-of-trust identifies and prevents compromised firmware from running, couldn't this same mechanism be an option for data protection? We believe it can be.

Enhanced security is not the sole objective in server replacement. There should also be a step-up in performance and agility. **Additionally, the relationship between the server hardware and server OS**












should deliver a synergistic “one plus one equals three” windfall. With this in mind, we recommend examining:

- The server’s ability to fine tune performance to workloads
- The server OS’s complementary features in security, storage, and virtualization
- Cloud compatibility of the server OS

## REASONS TO PRIORITIZE HPE PROLIANT GEN10 FOR SERVER MODERNIZATION

HPE ProLiant Gen10 supports SMEs with the advanced security and step-up in performance and agility they need in their next servers. In partnership with Intel and Microsoft, SMEs are also assured that their servers are built to leverage the best that these preeminent companies offer. Aligned with our recommended feature set, HPE ProLiant Gen 10 running Microsoft Server 2016 or 2019 is check marked end-to-end.

|   | FEATURE                          | REMARKS  |
|---|----------------------------------|--|
|    | Immutable Authenticity Assurance | Silicon-based Root-of-Trust pioneered by HPE   |
|   | Authoritative Alerts             | Never a false positive   |
|  | Simple Recovery to Trusted State | Malicious actors blocked from establishing a foothold. Additionally, business resilience with hardware-enhanced security included in the latest Intel® 2nd Generation Xeon® Scalable processor provides hardware mitigation for enhanced performance over software-only mitigations. |
|  | Built Compliant                  | Broad and deep compliancy: NIST, GDPR, ISO 27001, and HIPAA  |
|  | Native Data-at-Rest Protection   | Four levels of data protections available to align with SME’s specific needs: CNSA Suite, FIPS 140-2, High Security, and Production  |
|  | Jitter Smoothing                 | Valuable for applications intolerant of jitter fluctuations [exclusive to ProLiant Gen10 servers equipped with iLO 5 firmware running on Xeon Scalable processors]   |
|  | Workload Tuning                  | Configurable to produce maximum performance at the workload level  |
|  | Server OS Extra Features         | Numerous security, storage, and virtualization features not found in Windows Server 2008 R2 or 2012 R2. Examples include: Shielded VMs through Host Guardian Service, Credential Guard, Storage Replica & QoS, and Windows Containers  |
|  | Cloud Compatibility              | With Windows Server 2016 and 2019, seamless embrace of hybrid IT model between HPE ProLiant Gen 10 and Microsoft Azure   |

Source: HPE, Intel, Microsoft, and Frost & Sullivan

## STRATECAST: THE LAST WORD

Reliance on aging servers running a Windows Server 2008 generation OS is no longer a viable option. The era of hardware attacks is emerging, and EoS of Windows Server 2008 and 2008 R2 is less than a year away. As a result, the status quo is just too risky and hampers your company's ability to effectively compete in a digitally intensive world. Modernization of server and server OS is overdue.

When you examine your server options, keep in mind that the features you want now, and will need more in the future, are generationally different from those when your current servers were chosen. Time has made those servers obsolete.

Our recommendation is that you zero-in on servers with security that is not just built-in, but cutting edge. Now is not the time to scrimp on security. History has shown that cyber threats are relentless, adaptive, industrialized, and accelerating their pace of innovation. The slightest of vulnerabilities is all that threat actors need to start their sequence of exploitation. And once successful, your business will be tagged for retargeting. You must do all you can to avoid giving them an opening.

A final thought is your security readiness to engage with your suppliers and partners, and your company as a supplier or partner to others. In the web of digital interconnectivity that defines business relationships today and tomorrow, your attention to security is highly relevant. In the worst case, a relationship is disqualified because your company's attention to security is substandard. Less intense is having additional terms and conditions inserted into relationship agreements with your company, incurring additional costs or restrictions. To avoid these consequences, start with a server foundation that begins and ends with security. A weak foundation, once in place, is extremely hard to rectify.

### Michael Suby

VP of Research

Stratecast | Frost & Sullivan

## ABOUT STRATECAST

Stratecast collaborates with our clients to reach smart business decisions in the rapidly evolving and hyper-competitive Information and Communications Technology markets. Leveraging a mix of action-oriented subscription research and customized consulting engagements, Stratecast delivers knowledge and perspective that is only attainable through years of real-world experience in an industry where customers are collaborators; today's partners are tomorrow's competitors; and agility and innovation are essential elements for success. Contact your Stratecast Account Executive to engage our experience to assist you in attaining your growth objectives.

**SILICON VALLEY** | 3211 Scott Blvd, Santa Clara, CA 95054

Tel +1 650.475.4500 | Fax +1 650.475.1571

**SAN ANTONIO** | 7550 West Interstate 10, Suite 400, San Antonio, Texas 78229-5616

Tel +1 210.348.1000 | Fax +1 210.348.1003

**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**

---

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, Santa Clara, CA 95054