

Michael Rosenberg

Writer / Editor / Content Strategist

Resume & Work Samples

Prepared for:



Michael Rosenberg

Tech-Loving Writer / Editor / Content Strategist

(831) 818-2758 | michael@strategic6.com
linkedin.com/in/michaelrosenberg

PROFILE

Passionate storyteller, skilled content strategist, engaging writer, and highly effective editor with a portfolio that reflects my expertise as a technology marketer. Writing team leader/editor who has beaten impossible deadlines while exceeding client expectations. Quick study, able to grasp complex concepts quickly and communicate them clearly and persuasively to target audiences. Expert marketing writer with experience across diverse vertical markets and all media and social channels.

EXPERIENCE: EXAMPLE ENGAGEMENTS

Self-Employed Freelance / Contract Communications Consultant 2010-Present

Intel

Senior Writer

Defined the common language to be used for all communications, advertorials and web content as lead writer for the Intel IoT Group's messaging "Storybook." Writer for advertorials, collateral, web hub, event, and product pages.

StorageCraft

Editorial Director

Increasing the reach and SEO strength of the company blog through ongoing development of posts relevant to the company's global target audiences. Develop and manage the editorial calendar, lead writer, and manager/editor for outside contract writers.

Google Cloud Platform

Content Development / Writing

Lead writer for eBooks, digital flipbooks, white papers, solutions briefs, and demand gen programs including email campaigns, animations, display ads, and landing pages for Google Cloud Platform and its channel partners.

Pure Storage

Senior Writer

Writer for all marketing materials for the joint relaunch of Cisco/Pure FlashStack converged infrastructure and Pure Storage products including web, blogs, white papers, solutions briefs, sales deck.

McAfee

Multiple Roles

Led the research and development of McAfee's messaging platform working closely with senior marketing management, ensuring consistent communication of the company's positioning for each of its target audiences (consumer, SOHO, SMB, enterprise).

Drove content development for a massive website overhaul under extremely tight deadlines as managing editor and writer, leading a team of writers (including myself) in producing hundreds of pages of high-quality corporate and product content in just six weeks, one week ahead of schedule.

Wove the company positioning and messaging into a compelling brand narrative as writer for McAfee's corporate brochure.

Sonicwall

Content Consultant / Writer

Distilled Dell SonicWall's core positioning into key messages that served as the foundation for the company's thought-leadership campaign, employing a methodical process that included interviews with senior executives. Wrote the CEO-bylined article that kicked off the campaign, cementing the company's premier position in digital security.

Siemens Technology-to-Business Group (TTB)

Communications Consultant

Increased TTB's visibility both within Siemens and globally by developing compelling communications that told TTB's unique innovation story. Produced critical presentations, including a major presentation for the GM's appearance on China State TV; case study videos shot in the U.S., Europe, and China; and feature articles, digital content, and collateral.

CORE COMPETENCIES:

Writing and editing expertise in all media and communications formats:

- Blogs
- Email Campaigns
- Web
- Social
- Collateral
- Press Releases
- Animations / Videos
- White papers
- Advertising

Company/product messaging development

Content strategy, research and development

PREVIOUS MARKETING LEADERSHIP EXPERIENCE

X2 Biosystems

Contract Vice President of Marketing / Vice President of Marketing

May 2015-October 2016

Built the X2 brand from the ground up, initially as an outside consultant, then as a member of the executive team. Drove company and product positioning and messaging, visual branding, and communications from prototype to initial market entry for this early stage biotech device company.

WindSpring Software

Contract Vice President, Communications

January 2014-April 2015

Rebranded the company and developed all communications, then recruited as contract VP to reposition WindSpring as it pivoted to IoT. Fostered engagement with key influencers, analysts, and customers by developing new company and product messaging. Expanded the company's digital footprint to drive lead generation, prospect qualification, and engagement, writing press releases, product and company presentations, website, white papers, feature articles, and technology briefs.



Role (current):

Senior Writer / Message Content Developer (Contract through Lauchlan Agency, Boston)

Responsibilities:

- Lead writer for joint Google Cloud / AMD Confidential Computing launch campaign
- Banner ads
- eBook
- Solutions Briefs
- Landing Page
- Email Campaign
- Lead writer for multiple verticals for Google Cloud partner marketing programs

Build bold

Google Cloud and AMD bring you N2D and Confidential VMs powered by second-gen AMD EPYC™ processors that deliver:

- 39% better processing performance
- 13% better memory bandwidth

Secure Confidential Computing from Google Cloud and AMD

AMD EPYC™ processors bring Secure Encrypted Virtualization to Google Cloud confidential VMs

Helping secure the cloud

AMD EPYC™ processors bring Secure Encrypted Virtualization to Google Cloud confidential VMs

Breakthrough cloud security gives you the confidence to build bold

Powered by second-gen AMD EPYC™ processors, Google Cloud Confidential Computing gives you the confidence to build bold.

Request your cloud discovery call. Get a CONFIDENTIAL marketing.

Get break-through cloud security and performance

Explore Confidential VMs from Google Cloud and AMD.

Find out how

1 Better performance at a lower cost
Get up to 39% better processing performance and memory bandwidth for intensive workloads—and savings of up to 13% over comparable N-series instances—with Google Cloud Platform's N2D instances running on second-generation AMD EPYC processors.

2 Flexible resource options
Choose from a wide range of compute and memory configurations that can handle both general-purpose workloads that require a balance of compute and memory, and big compute workloads driven by memory bandwidth.

3 Enhanced data security
Google Cloud Confidential Computing with AMD Secure Encrypted Virtualization (SEV) encrypts sensitive data in the cloud while it's being processed, making it simple for everyone to seamlessly lift and shift workloads without requiring code changes.

4 Wide range of use cases

- Reduce costs with data center consolidation and simplification.
- Use AI and machine learning for enhanced insights and experiences.
- Handle heavy workloads like predictive analytics, modeling, and anomaly detection.
- Enhance security for sensitive data.
- Automate quality control processes in manufacturing and business workflows.
- Modernize your applications across on-prem and cloud with Anthos.
- Ensure flexible use of resources to support analytics.

Building, price, performance, and security

Big

Small

Small

Small



Managing Mountains of Data

Why you need a data-centric, intelligent, and adaptable storage infrastructure



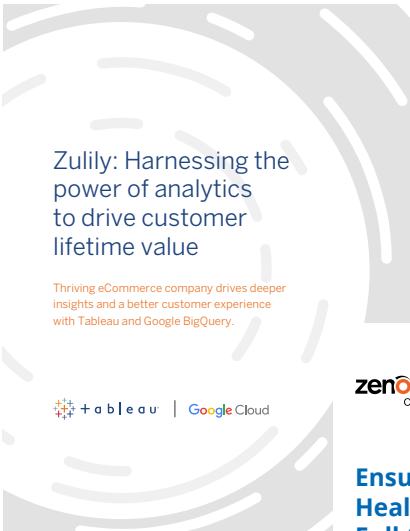
Unlocking more value from industrial data management and analytics

How data contextualization delivers smarter grid and generation operations





The Future of Dev+Ops Is Clouded with Complexity

Why Application Performance Monitoring and Observability Matters in a Multi-Cloud World



Zulily: Harnessing the power of analytics to drive customer lifetime value

Thriving eCommerce company drives deeper insights and a better customer experience with Tableau and Google BigQuery.



Ensuring Application Health with AI-Driven Full-Stack Monitoring

A guide to optimizing application performance in any environment





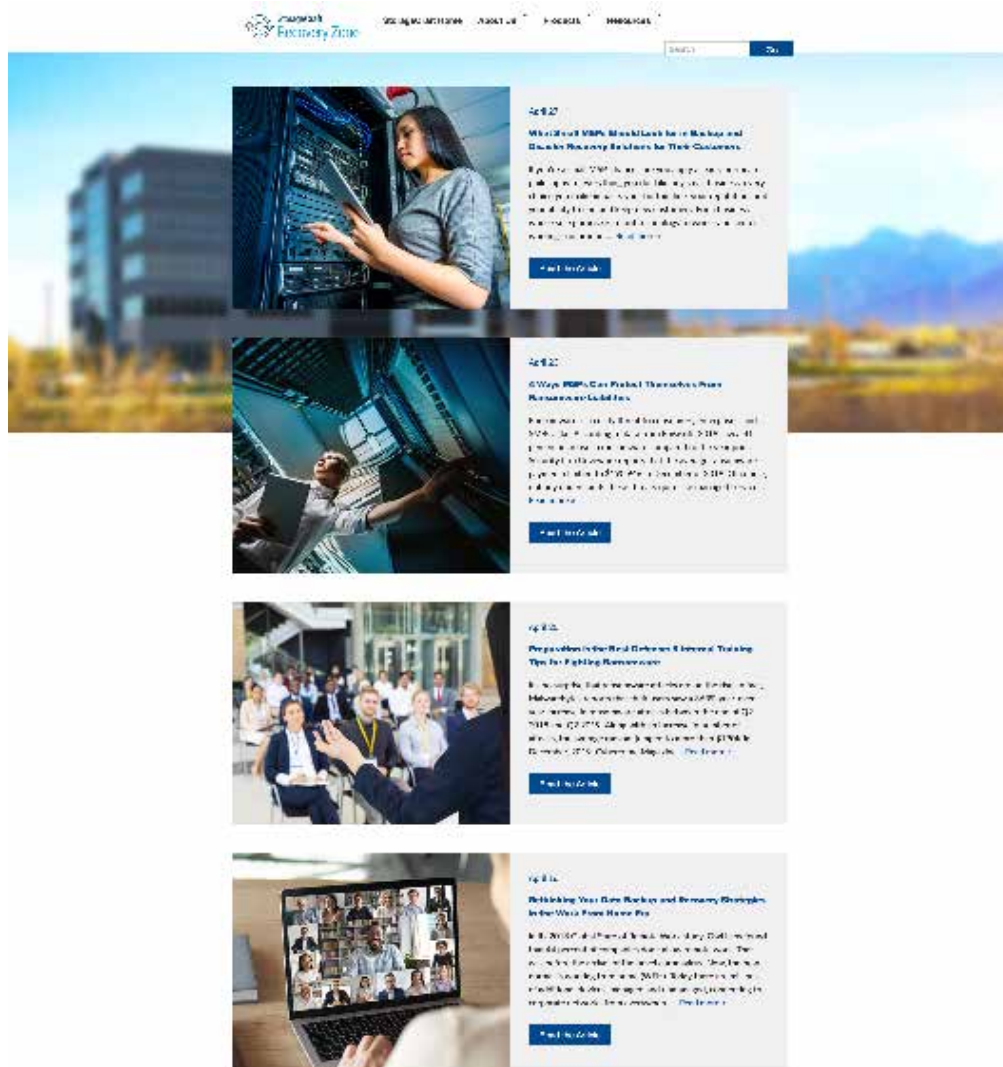
Role (current):
Editorial Director (Contract)

Responsibilities:

- Develop and execute quarterly blog editorial calendar based on marketing plan and objectives
- Research and write posts
- Manage and edit posts by outside contractors
- Interview customers and SMEs, develop and write case studies
- Collaborate with demand generation team in developing campaign themes and funnel strategy; writer for email outreach and landing pages

Work Examples:

- <https://blog.storagecraft.com>
- Example case study following page





Role (current):

Senior Writer / Message Content Developer (Contract through CMD Agency, Portland)

Responsibilities:

- Currently developing core messaging (called a Storybook) for Intel IoT Group segmented by business and technical audiences with separate Storybooks for industrial, health and science, smart cities, and retail / banking / hospitality verticals
- Currently writing series of advertorials for the Intel vPro Platform



Advertisement

PC PROTECTION THAT STARTS AT THE HARDWARE LEVEL

PCs are your company's lifeblood—the linchpin for keeping things running. But, with cybersecurity threats rampant, PCs can also be a big security problem. How big? Stolen credentials or phishing attacks are behind 61 percent of data breaches,¹ and, often, an unprotected PC is the entry point. A successful attack can spread through your organization like wildfire, wreaking havoc in terms of downtime and lost productivity. The Intel vPro® platform's hardware-enhanced protection is the solution.

Increase protection right out of the box

Security decisions start at the PC. That's why the Intel vPro platform is architected with innovative, hardware-based security that minimizes threats from the start. In fact, 75 percent of IT managers surveyed reported that Intel vPro platform-based devices are more secure,² providing protection against attacks from below the OS, minimizing malicious code-injection risks, enabling your OS to enforce security policies, and making remote management and remediation easy so your users can get back to work fast.

Proven, proactive security

Want to turn your PCs into strategic assets against security threats? The Intel vPro platform does just that, working with existing security applications, and adding additional, powerful protections that proactively secure your company's PCs at the hardware level. The result: reduced downtime and increased productivity.

Ready to put a more secure PC platform in place?

Then select the platform built for business: the Intel vPro platform.



1. Data Breach Investigation Report, Verizon 2019.

2. The Total Economic Impact™ of the Intel vPro Platform, Forrester, December 2018. A study commissioned by Intel and conducted by Forrester Consulting that surveyed 256 IT managers at mid-sized organizations (100 to 1,000 employees) using Intel vPro platforms in the US, the UK, Germany, Japan, and China. Seventy-five percent either "agreed" or "strongly agreed" with the statement that computers with Intel® Core™ vPro® processors and Windows 10 are more secure than before. Read the study at intel.com/vProPlatformTEI.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.



Advertisement

READY TO DRIVE INCREASED PRODUCTIVITY WITH FASTER PC PERFORMANCE?

With today's exponential data growth, mobile workforce, and demanding workloads, fast PC performance isn't an option—it's a necessity. Your employees are your most valuable asset, but did you know that lost productivity from waiting for boot up or large files to launch costs nearly \$8,000 per user, per year¹ with PCs that are as little as three years old? Add it up for your business and you'll agree that faster is better. That's where the Intel® vPro® platform comes in.

Increase productivity right out of the box

The Intel vPro platform boosts productivity from day one by delivering business-class performance that lets you handle data faster, makes connectivity simpler, and extends battery life longer. And increased productivity equals way lower costs. The Intel vPro platform even comes in lots of form factors, so your users can use the devices that fit their style.

The features you need, the headroom you demand

Built to meet the demands of business workloads, the Intel vPro platform enables Wi-Fi 6 for fast connections and makes connectivity effortless. You'll also get the most out of Windows® 10 features, including device interactions through voice, gesture, pen, touch, keyboard, or mouse.

Ready to drive higher productivity with faster PC performance?

Then select the platform built for business: the Intel vPro platform.



1. "Employees are 12% less productive on PCs that are 3+ years old, resulting in an estimated cost of \$7,794 per year, per user" is based on a 2018 web-based survey, commissioned by Intel and conducted by JGold Associates, LLC, of 3,297 respondents from small business in 16 countries (Australia, Canada, China, France, Germany, India, Italy, Japan, Mexico, Saudi Arabia, South Africa, Spain, Turkey, UAE, UK, USA), to assess the challenges and costs associated with deploying older PCs. Survey respondents estimated that for PCs more than 3 years old, employees would be up to 12.99% less productive—based on an average assumed employee's salary of USD 60,000, the lost productivity cost will amount to USD 7,794. To review this statistic, and the full report, visit intel.com/SMEStudy.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.





Role:

Thought-Leadership Writer (Contract with Dell Sonicwall prior to spinout)

Responsibilities:

- Based on interviews with senior executive management team, partners, and analysts, developed the company's thought-leadership campaign positioning, then wrote the campaign kickoff article over the CEO's byline (below and following page)

WHEN ACCESS OUTWEIGHS SECURITY, ARE YOU READY FOR THE FALLOUT?

Ambient intelligence, biometrics and the future of security

By Matt Madeiros, President and CEO, Dell SonicWALL

We love our devices. A quick glance around any business meeting and I can say with certainty you'll see colleagues with their eyes downcast, locked on a screen. Devices have become a very real extension of ourselves. In fact, IDC is predicting 686 million smartphones will be deployed this year. Then there are the countless connected tablets, laptops, desktops, and other new devices. And now many products—from cars to copiers—are connected devices, too. From a network perspective, it all adds up to a staggering number of endpoints.

Obviously, our relationship with our devices is deep, and getting deeper. But without access to data, the value of our devices is limited, if not eliminated. Whether business critical or frivolous fun, our mood quickly fades to frustration when we can't access our data (as we punch "submit" one more time when the screen doesn't instantly change).

The truth is, there's a powerful three-way relationship that exists between our devices, our data, and ourselves. But without access to data, the relationship just doesn't work. Nowhere is this more apparent than in the business world. Today, a business's productivity is inextricably linked to the ability of its employees, partners, and customers to access and exchange data. And there is a straight line between productivity and profitability.

But hackers also smell opportunity in this evolution. We've already seen attacks on connected medical devices, so we know we can expect them to come through any device, anywhere. And we can certainly expect the sophistication and complexity of the attacks to increase.

With so much at stake, ensuring secure, efficient access to data is key to productivity in our future. But where do you start?

The logical first step is to secure everything, from endpoint to data center and everything in between, from everywhere—cloud, mobile, and remote. And every aspect of network technology has to be engineered for security, throughout the product lifecycle, supply chain, and manufacturing process. Dell is already ahead of the industry curve in solving these challenges.

But how do you secure everything from everyone—especially the bad guys—without restricting access and limiting productivity? In a mobile world of evolving devices, meeting the demand for unfettered access to data by those who depend on it, and on whom you depend, without compromising security, is critical. We believe there is a simpler, smarter solution to this complex problem: build future security solutions that leverage the very things that make us human.

Think biometrics and ambient intelligence.

Biometrics are now relatively common solutions for physical security barriers. These same technologies are already being applied to devices, allowing access only after the user's identity is verified by physical evidence—a fingerprint, retina scan, or voice recognition, for example. This same strategy works at the network level, where limiting access to critical assets—manufacturing areas, servers, and network equipment—adds an additional layer of physical security.

But it's also common knowledge that the most vulnerable point on any network is the end user. What happens if a user loses a powered-up device? Or if someone does manage to slip by physical security measures?

The next level of security must go beyond the physical attributes that make every human being unique, and include proactive strategies that recognize how our interactions with our world, and with our devices, are also unique.

These future solutions must be based on ambient intelligence, and hidden within the networks that connect our devices. Essentially, our environment, networks, and our devices must learn to recognize us, based on both our physical presence, and our virtually impossible to duplicate human behavioral patterns.

In its most basic form, simple behaviors such as how you handle a device and stroke keyboard keys are inherently unique to you as an individual. And with millions of data points available to define an individual, unauthorized access becomes virtually impossible, whether the threat is external to the network, or from any device, anywhere.

At the same time user authentication will be just about bulletproof, and access management will be much simpler and more secure when there is certainty that the person trying to connect is who they say they are. But ambient intelligence offers tremendous potential for both enhancing productivity and becoming a strategic business asset, as well. For starters, just imagine never having to remember or use a password to gain access to data again. How much time will that save over millions of users?

Then there is the biggest obstacle to our own productivity—us. Think social media, YouTube and instant messaging, for starters. How much time do we waste with these distractions (that so many of us love)?

Ambient intelligence can make it possible for us to recognize our own behaviors and their impacts on our productivity, then adjust those behaviors—whether to achieve our own goals, or to conform to established business goals. So we can decide how much time we want to spend on distractions, and our intelligent devices can suggest when it's time to get back to work.

Of course, as human beings, we'll always retain the right to ignore those suggestions. Whatever choice we make, biometrics and ambient intelligence will transform the future of security.

#



Role:

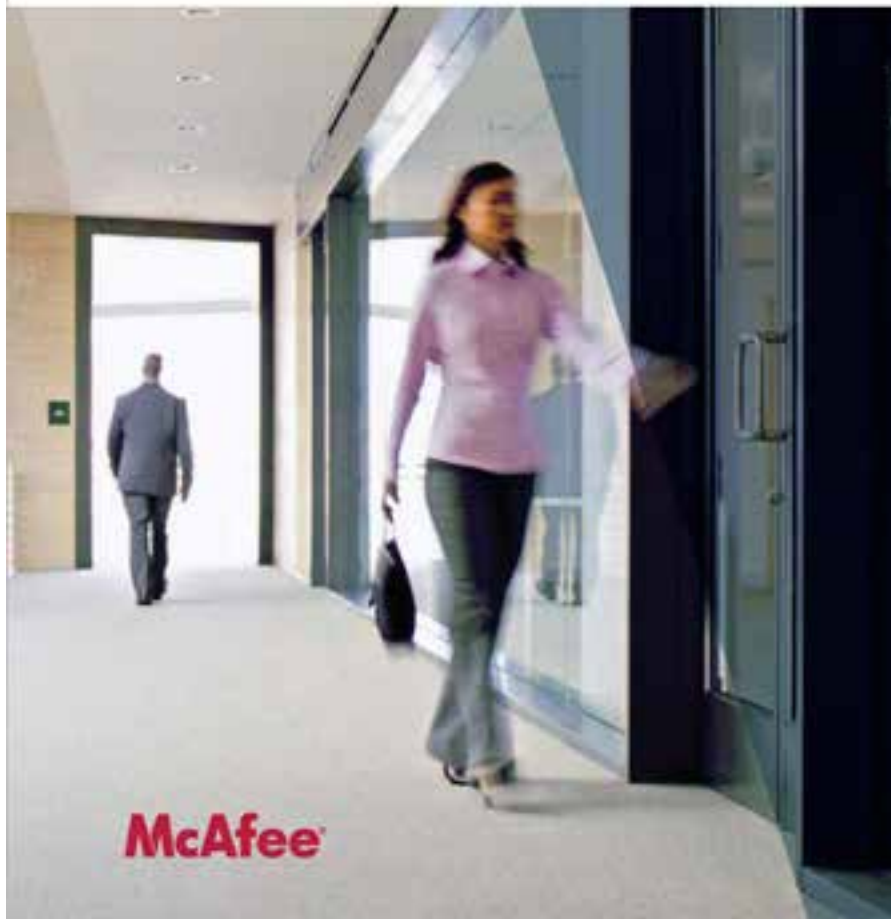
Lead Writer / Message Development (Contract)

Responsibilities:

- Developed messages for all target audiences (enterprise, SMB, SOHO, consumer) in collaboration with senior marketing management
- Managing editor and writer, leading a team of contract writers in a complete rebuild of company website; writer for white papers, company brochure, email campaigns, and other collateral

Proven Security:

Comprehensive protection for the real world



Thank you!

