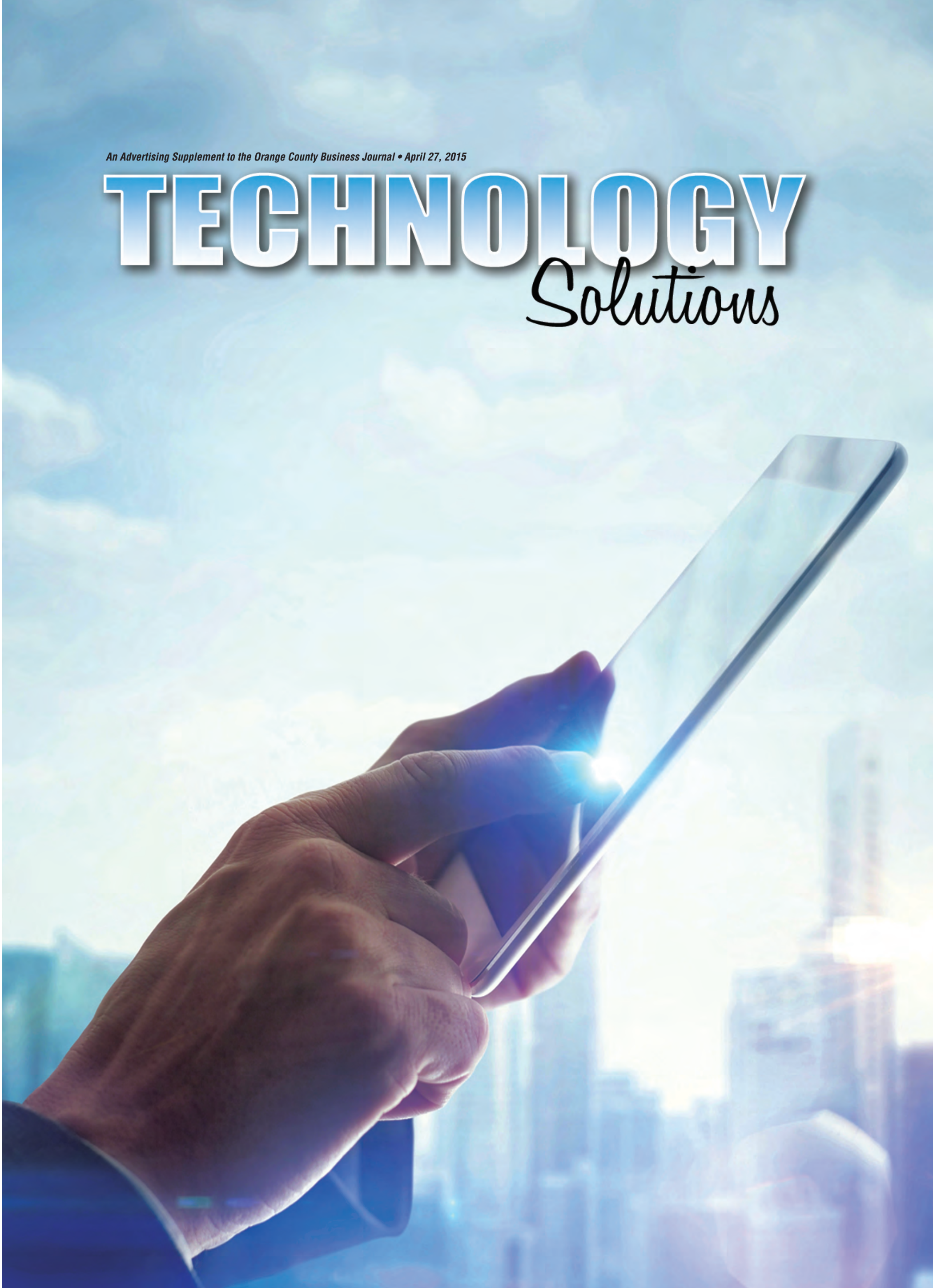
*An Advertising Supplement to the Orange County Business Journal • April 27, 2015*

# TECHNOLOGY *Solutions*



# Understanding The Evil Hacker Mentality, and Defending Against It

*by James McMurry, CEO and Founder, Milton Security Group*

The 17th century epic poem, ***Paradise Lost*** by John Milton, contains 10,000 lines of verse divided into 10 books. It tells the story of the fall of man through the two narrative arcs of the temptation of Adam and Eve, as well as one about Lucifer's fall and eventual banishment to Tartarus (Hell).

***Paradise Lost*** is not a short, or even an easy, read, but it has an interesting parallel to security both in terms of motivations for the players involved, as well as the results of their actions.

**The Fall: "*Better to reign in Hell than serve in Heaven*."**

You've probably heard this famous ***Paradise Lost*** quote in everything from films like *Star Trek II: The Wrath of Khan* and *The Devil's Advocate* to the Eminem album, *Rap God*. This quote is interesting because it epitomizes the mentality that some malicious hackers have at creating chaos as a means of expression. Much like bad graffiti artists drawing annoying gang symbols on walls and freeway signs, malicious hackers have a similar idea about how to make their mark. Forgoing authority to make personal statements, rebelling against existing business and social structures, and seeking to create a community where they can feel like they are in common company, are all examples of reasons why malicious hackers do the kinds of things they do. And this is not even talking about Nation-States and their alleged "Cyber Armies."

The hacker mentality has existed before our current day malicious hackers though. Tales of hubris pepper human history. Some people break into places they shouldn't be purely for the challenge. Before computer networks linked everyone's PC together, there were underground "cracking" networks that took disk-based software and removed copy protection from it. An underground trading economy emerged from this activity, which led to great distress for software developers. All sorts of protection techniques were tried, ranging from codes printed on darkened paper to special disks with un-writeable regions. As networking emerged, so did network hacking. The stakes have become higher as networks allowed malicious hackers to coordinate activities. Tracking was difficult because of the primitive monitoring techniques of the time. There was also a certain innocence as the overall scale of networked system usage was relatively small compared to today. Malicious hackers used this trusting nature to take advantage of the lack of security at the time.

**The Battle in a Digital Underworld**

In ***Paradise Lost***, Lucifer's motivation is built on arrogance. Charismatic and confident, Lucifer leads his followers into a war with God, the ultimate authority. The result of his actions is banishment to Tartarus. Even with that outcome, Lucifer utters his now renowned phrase, "Better to reign in Hell than serve in Heaven," proclaiming his contempt for the status quo.

As security measures for modern systems have increased, malicious hackers, much like Lucifer, have been banished to working in a subversive way. Using all sorts of tricks like back doors into commercial products, spoofed IPs, compromised computer systems and all sorts of other elements of a digital underworld, malicious hackers are able to attack their unprotected targets quite brazenly.

With the introduction of high-speed networks and tightly connected devices, we face an even bigger threat from the criminal hacker underworld than ever. The stakes are higher today with actual money and valuable information on the line, and the challenge of disrupting large company operations is tantalizing to say the least.

**Understanding Temptation**

You can see examples of non-monetary assaults in the form of takedowns of gaming networks (like Sony Playstation Network) or the half-hour DoS attack on Facebook recently. To malicious hackers, doing these sorts of things is a way to gain fame within their community. Their actions cause millions of dollars of damage, not only by removing a profit channel, but also by threatening the jobs of those charged to run those systems.

Understanding why people do things is a good first step in preparing for the negative consequences. While it seems difficult to accept, there are people out there who use their intellect purely for malicious disruption of your company's operation. There are still others who seek to steal your company's confidential data and sell it on the black market. These are all risks, which have evolved from exactly the same motivations people have had in other industries in the past. Indeed, as we see through the similarities with Milton's epic poem, the motivations about why these things happen have been seen many times before.

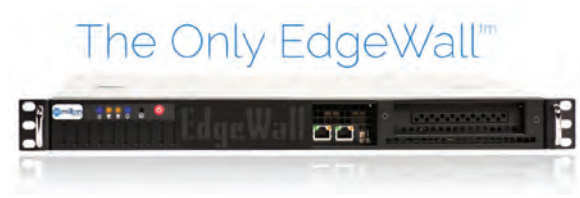
**Paradise Regained**

At Milton Security Group, we understand the malicious hacker mentality, the ways that they attack, and their goals. In fact, as a veteran-owned business, we are well-versed in the Art of War, being able to anticipate an attacker's strategies. This is why we've developed a solution that will not only keep hackers from attacking from the outside, but attacking from the inside as well.

Let's say you have an employee with a laptop at the local coffee shop. An evil hacker sneakily breaks in it via WiFi and drops malware on it. If that employee walks that laptop in to your organization, and connects to your network, are you going to be able to stop that malware from spreading? You could if you had an EdgeWall.

Let's say an evil hacker walks in to your place of business dressed as your phone service provider. They made an appointment with you and everything. Could your current security stop them from plugging a USB stick into a machine and wreaking havoc? An Edgewall could.

An EdgeWall protects you from all threats, including yourself! By controlling access to your network, monitoring all activity in real-time, and being able to launch isolation protocols, an EdgeWall has you covered from every angle.




Don't allow your company's computer network to become a footnote in your own version of ***Paradise Lost***.

We'll help make sure that the people who prefer to rule in Tartarus remain there, cut off from causing you trouble.

We will provide you providence over your security world.

*For more information, visit www.miltonsecurity.com or 888.674.9001.*

**James McMurry**

James McMurry, CEO and Founder of Milton Security Group, is an accomplished technologist with an entrepreneurial mindset with over 20 years of experience in security, information technology, telecommunication, networking, management and software development.

**About Milton Security Group Inc.**

Milton Security Group Inc., a Veteran-Owned Small Business (VOSB) was started with the basic idea to make excellent network security within reach of all businesses. From this basic principle, Milton Security Group has designed and developed a growing suite of security solutions, including the EdgeWall Network Security solution. Founded in 2007, Milton Security Group has enabled organizations, across public and private sectors, to protect their internal systems and endpoints. All solutions are tailored for the individual customer, as each network and needs are unique.

DORSEY™
DORSEY & WHITNEY LLP

# Just Say No to BYOD Policies

## *Five Reasons Why Company Owned Devices Are Your Safest Bet*

*by Gabrielle Wirth, Department Head, Labor & Employment, Southern California, and David Murphy, Department Head, Labor & Employment, Northern California, Dorsey & Whitney*

Many employees have switched to a BYOD policy and enacted reimbursement policies which pay for the increased cost incurred by employees who use their personal devices for business related calls and emails. However, due to the result in *Cochran v. Schwan's Home Service*, many are updating these policies in an attempt to factor in the cost of devices and the pro-rata percentage of business use of the monthly charges. Because of these many potential complications, many employers may forget to consider the safest approach – company provided devices for work use only.

**Background**

In August 2014, the California Court in *Cochran v. Schwan's Home Service* ruled that California employers must reimburse employees "a reasonable percentage of their cell phone bills" even if the employees cell phone plan has unlimited minutes and data. Cal. Labor Code Section 2802 requires employers to reimburse employees for expenses necessarily incurred for business to prevent employers from passing on what should be company paid operating expenses to their employees. The rationale of this ruling and Section 2802 applies to smart phones and computers used to access business data in the Cloud or on network servers.

Gabrielle Wirth

**Why Making the Switch Back Makes Most Sense**

*#1 - Cost*

BYOD policies have associated cost issues. By providing devices, employers often can cut costs by bulk purchases of electronic devices and better data plans. Additionally, BYOD reimbursements lack control over the cost of the device the employee chooses to use, and leave the employer saddled with a share of the costs of the newest smartphone, adding no true value to the company. Further, employees often end up using an employer's IT personnel for their own devices anyway, resulting in little or no cost savings there.

David Murphy

*#2 – Data Protection*

BYOD policies can make company data security protections far more difficult, especially for employees dealing with protected personal or commercial information. Besides risking unauthorized disclosure of this data, the incidence of actual loss of data may be greater. Data on employee owned devices is often more vulnerable to loss and damage because of more uncontrolled access to the device and less sophisticated antivirus and encryption software.

*#3 – Off the Clock Work*

Providing company owned devices only to those required to use them off-site/after hours protects the employer by avoiding the now frequent claims that the employer knew of off-the-clock work performed on these devices. These claims often arise from non-exempt employees returning after-hour phone calls/emails or completing work on personal devices after hours.

*#4 – Employer Protections*

A policy restricting data and work to the employer's systems and devices better protects trade secrets and other company confidential information. Employees can be prohibited from copying customer contacts and other confidential data, which would otherwise reside on their personal devices. This can become especially important when the employee is no longer with the company.

*#5 – Work Boundaries*

Depending on the workforce, limiting work to that performed on the employer's devices may be seen as an attractive benefit. An employer will provide state-of-the-art devices, and many employees just may not want to spend the money on such devices themselves.

Overall, and as Secretary of State Hillary Clinton recently acknowledged, it's often simply a better approach for all to keep business information on business devices only. That is the approach that not allowing BYOD use fosters, and is rooted in, common sense.

*To learn more about Dorsey's Labor and Employment lawyers and how we can help protect your business, visit: www.dorsey.com/labor_and_employment/.*

SYSPRO™
Simplifying your Success

# Enabling Better Performance for Manufacturers and Distributors

In a world of complex innovation and technology stacks that are often very difficult to comprehend, it is important to have software that simplifies how your business runs. A reliable vendor and software that delivers feature sets and capability is critical. Beyond this, best practices are an essential ingredient to optimizing success in the 21st century. Rising costs, compliance and shifts in the technological landscape have created an environment that demands businesses be more agile. This means manufacturers and distributors are placed under pressure to perform by delivering faster, at less cost with greater accuracy over inventory, financial management and retail outlets in order to meet growing customer demand. Where does this leave us today?

As we have seen innovation grow, the capability of ERP (Enterprise Resource Planning) Software has accelerated and expanded exponentially. Today, it is all about getting what you need and the ability to use it in the right way. Whether your deployment is in the cloud, mobile or on-premise, the choice should always be to meet your operational requirement. What is most important is agility and of course, having the software that will cement the operational backbone of your business.

Sophistication and depth of functionality does not have to mean complication. Having the right components/features that provide visibility, ease of operation and cost control will influence the success of every business. Keeping it simple and having the capability to do what is needed, when it's needed and how it's needed.

SYSPRO is one of those rare companies that has been acknowledged for understanding customer needs and providing service levels that can make the difference to the software investment. A full package vendor that can provide all the facilities to implement software and deliver after sale service that is truly exceptional. SYSPRO's award-winning STARS QE Implementation Methodology saves customers money, helps control their budget and offers a platform for customers to effectively work side-by-side with SYSPRO to implement an effective business model that addresses their unique needs.

So, who is SYSPRO? SYSPRO is the leading platform for mixed mode manufacturers and distributors to provide companies with all the software needed to leverage their business – on-premise, in the cloud, or from a mobile device. From single location companies to multinational corporations, SYSPRO provides the functionality to connect the entire supply chain. With one of the highest customer retention rates in the industry and a commitment to ongoing cutting edge development, SYSPRO is focused on meeting both current and future needs of its customers. An exceptional feature-rich product and a team of highly trained personnel provide the lowest risk for businesses purchasing ERP business solutions. Key industries include Food & Beverage, Medical Device, Electronics, Aerospace, Machinery, Chemicals and Automotive among many others.

*For more information, visit www.syspro.com or contact Stanley Goodrich at Stanley.Goodrich@us.syspro.com or 714.437.1000.*

**About SYSPRO USA**

Located in Costa Mesa, SYSPRO USA has been leading the technological landscape in the Orange County marketplace for nearly three decades. SYSPRO is a product that can truly scale and give small, medium or large businesses the opportunity to protect their investment and growth.

milton
security

www.miltonsecurity.com

# You Think Your Network is Secure?

# It's Not.

The average cost of a data breach is is $5.5 Million and 80% of data breaches start from the inside.




## Secure Your Network, Protect Your Resources

Milton Security's EdgeWall solution is the first Adaptive Network Access Control appliance that provides identity-based access to your network. It continuously enforces policies customizable for each individual user, allowing you complete control over access and behavior on any network. Most NAC solutions watch your network from the outside and make reports on what they see. Unlike its competitors, the EdgeWall is an inline solution, meaning it sits between your network and any threats, stopping them before they can can breach your data.

## More than NAC, Adaptive Security

Tear this page out, and give to your IT/Security Team:

## Do We Have An EdgeWall?

261 E. Imperial Hwy Suite 550, Fullerton, CA 92835 Tel: 1.888.674.9001 Fax: 1.714.459.7489

# As Counterfeiting Grows, a New Necessity for IT Resellers Emerges: Verified Products

*Adding third-party testing and verification will help resellers and end users alike*

According to estimates from the Organization for Economic Co-operation and Development, the value of counterfeit IT products may cost the global economy up to a quarter of a billion dollars per year. Even more concerning for IT resellers and procurement teams is that recent industry research estimates that 10% of all IT hardware is counterfeit. Companies across all sectors are struggling not only to understand the impact that fake products have on its business and financial results but also to ensure that those products don't enter its IT infrastructure. From catastrophic security breaches to downtime, damaged business partnerships to disastrous financial and brand consequences, the stakes for fake IT hardware products entering an organization's technical infrastructure are enormous. This is why a new necessity is rapidly emerging in the IT marketplace – third-party verification.

The role of third-party testing and verification, put simply by Core 3 Technologies' Managing Partner and Founder Chris Bergen, is to "provide quick and accurate detection and identification of counterfeit and modified IT hardware." Verification companies are the bridge ensuring that IT manufacturers, resellers, and end users develop trust, reduce fear, and increase security across the supply chain.

To accomplish this job, Core 3 Technologies, a leading value-added distributor headquartered in Irvine, has invested heavily over the last five years in the ability to verify IT hardware. The company not only partnered with Verification Systems Technology (VST), an independent company that has developed the premier online test platform that enables quick and accurate authentication of network hardware, but also ensured that its new Irvine distribution facility was built around the testing and verification process. Products entering the Core 3 Technologies supply chain undergo strict testing, authentication, and verification using VST's platform before ever entering its inventory. Should products be identified as counterfeit, the company maintains a zero-tolerance policy. Core 3 engineers work aggressively with VST to quarantine these products and remove them from the marketplace.

And the results are impressive. Since its founding seven years ago, Core 3 Technologies has grown from a team of four to 35 across its headquarters and West Coast distribution center in Irvine, an East Coast distribution center in Morristown, NJ, and offices located in Los Angeles, Phoenix, San Francisco, and New Jersey. Additionally, the company was listed on the Inc. 5000 list last year and has been named among the Best Places to Work in Orange County.

As Mr. Bergen puts it, "Counterfeiting will continue to grow – we can't stop it. But what we can do is ensure that we build our client relationships around trust that not only extends within our conversations but also to the products we are selling them." And he's right. Global counterfeit trends not only indicate that counterfeiting will continue to grow but that the counterfeiters will diversify what they produce. Companies need to know that the products they are plugging into their IT infrastructure are trusted and authentic. Testing and verification can do just that.

*For more information, visit www.core3tech.com or contact Chris Bergen at 949.387.6732.*