WP engine™

The Keys to *Agency* Security

Protecting client data isn't just good business—it's essential for trust and risk prevention.

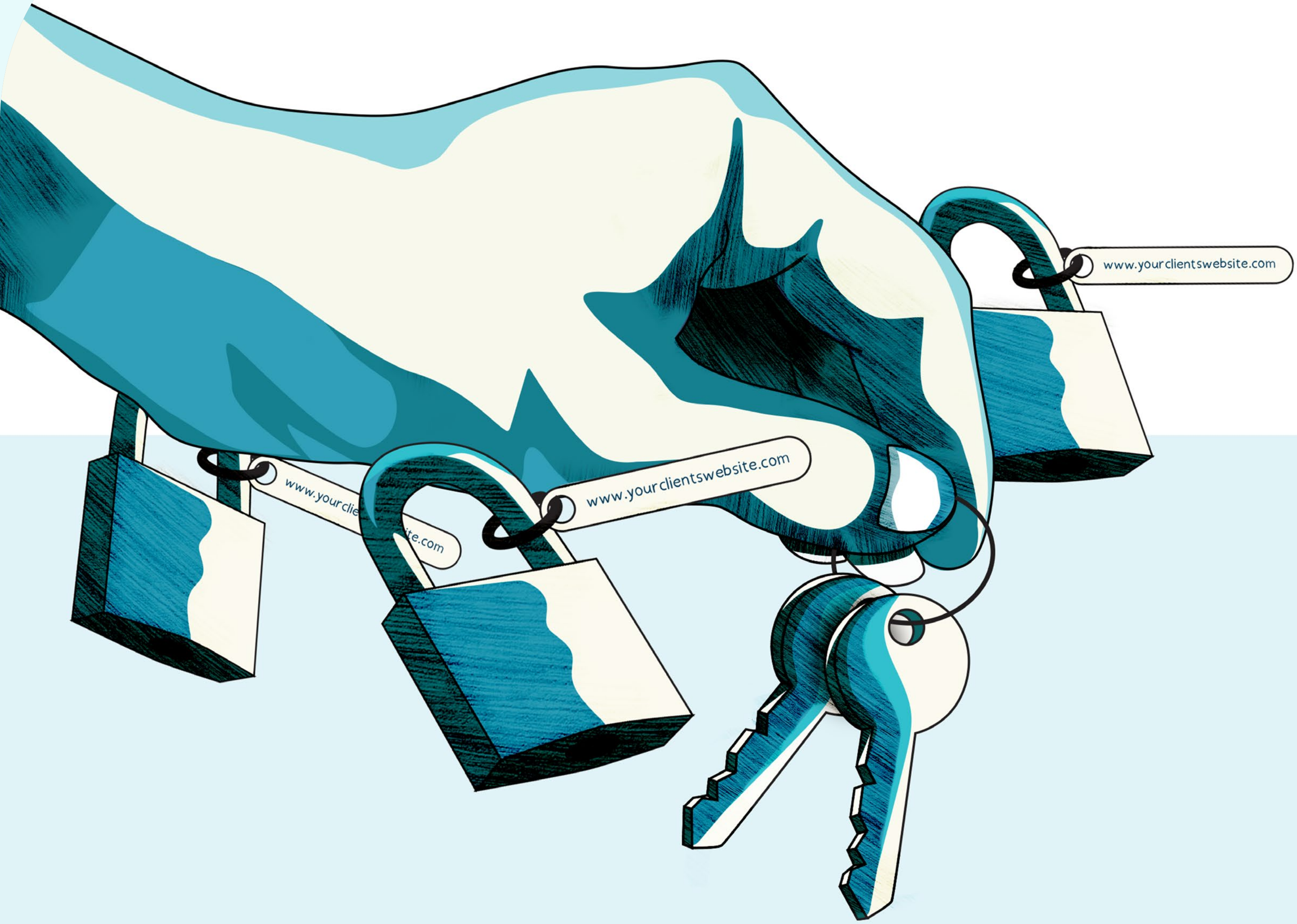
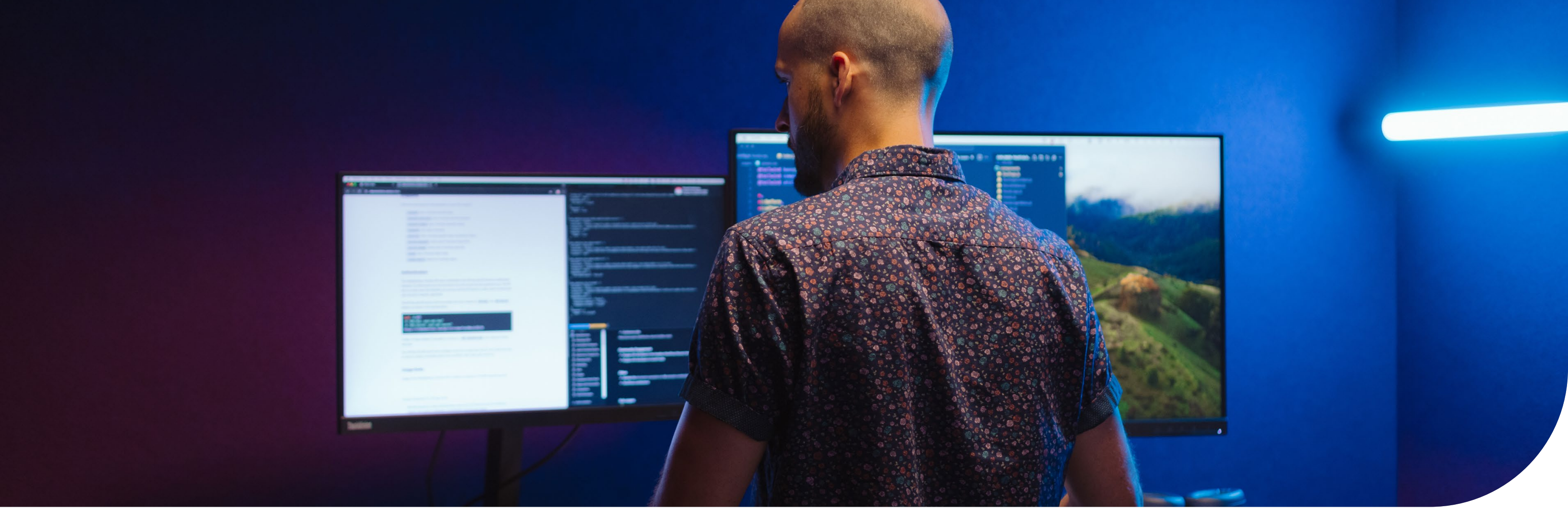


Table of Contents



The importance of *agency security*

It's fairly safe to assume at this point that anyone who works with websites, or spends time on computers, knows the importance of cybersecurity. But whether you're just forming your agency or you've been creating unique digital experiences for a couple decades, it never hurts to step back and make sure you're thinking about agency security from the right perspective. And just in case there's an agency out there whose official security policy is "don't do anything stupid," let's re-examine the current state of cybersecurity and how agencies can keep their business and their clients secure.

The state of cybersecurity

It seems like every year bad actors—whether state-sponsored groups, criminal organizations, or lone threats—increase the sophistication and breadth of their attacks. And if recent security reports from industry experts are any indication, this trend won't be changing any time soon. **Crowdstrike reports** that cloud environment intrusions increased 75% year over year. Meanwhile, **Forrester predicts** that the global cost of cybercrime in 2025 will hit $12 TRILLION (with a T).

Unsurprisingly, **IMB notes** that phishing and stolen or compromised credentials remain the two primary vectors for most attacks, while **Verizon's data shows** that 68% of intrusions involve a non-malicious human element. This means that up-to-date processes, policies, and education are critical to keeping your agency from becoming another statistic. But it's more than just your company at risk. In that same report, Verizon notes that 15% of all breaches involve a third-party vendor in the software supply chain (an alarming rise of 68% over the previous year's 9%).

Numbers *don't lie*

With access to data and systems for multiple clients, agencies are likely popular targets for cybercriminals. So, what's a security-minded agency to do? There are three high-level categories that agencies should be mindful of when assessing their security posture: the security of the infrastructure they use, the security of the code they write, and the security of their people and processes. Before we dive into each of these categories, let's level-set on an agency's role in client security.

Clearly defined roles, responsibilities, and liabilities

Because of the nature of agency work, you're never just concerned with keeping your company safe. You are, at least in some capacity, responsible for your clients' security as well. That responsibility also implies liability, making it crucial to have clearly, contractually - defined roles, responsibilities, and liabilities. This should include definitions for intellectual property ownership, responsibility for privacy and terms of service agreements, agreement on data storage and system access, and much more.

Obviously your contracts and statements of work should outline these appropriately. And as this article is not legal advice, you'll definitely want these documents and agreements reviewed by your legal counsel.

This is also a good time to test assumptions about other third-party providers with security responsibilities and clarify how you're expected to work with them. This could include infrastructure providers, specialized security services, and additional software that will integrate with the sites you're building.

Regulatory *Requirements*

It's also important to understand which regulatory frameworks will impact each digital property, and how your agency will ensure it remains compliant. **Note:** This may also require regular reporting to a relevant regulatory body.Depending on their industry or the regions they do business in, your clients may require compliance with any of these regulatory schemes (or others):

- **General Data Protection Regulation (GDPR)**
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
- **National Institute of Standards and Technology Cybersecurity Framework (NIST)**
- **Payment Card Industry Data Security Standard (PCI DSS)**
- **National Cyber Security Centre (NCSC)**
- **Information Security Registered Assessors Program (IRAP)**
- **International Organization for Standardization /International Electrotechnical Commission (ISO/IEC 27001)**

The three big buckets of agency security

Infrastructure security

Unless your agency has aspirations for a major business pivot, it's unlikely that you're DIYing your hosting infrastructure. That said, depending on your choice in host you may be spending a good chunk of your time ensuring your environments are secure.

But there are other options. WP Engine offers **managed hosting for WordPress®** that includes **comprehensive infrastructure security.** This includes advanced encryption, **Global Edge Security,** automated threat response, and a premium managed Web Application Firewall (WAF)—all backed by deep expertise in keeping WordPress secure. This means you're free to focus on your code and processes. In fact, automation like our **Smart Plugin Manager** can help make sure some of those processes are handled as well.

Writing secure code

Application security is a critical component of your agency's cybersecurity posture, but it's also a deep, nuanced subject that would require a multi-part course to explain in full. That said, reviewing the Open Worldwide Application Security Project's (OWASP) **secure coding quick-reference guide** never hurt anyone, right?

Whether your dev team uses the OWASP standards or has opted to follow a different standard is less important than the decision to choose a standard and commit to it. Your developers are doing that, right? If not, add it to the ole security to-do list, as adopting a secure coding standard will not only help your sites and applications be more secure, it'll create efficiencies across your developers.

Security policy and processes

As mentioned above, phishing, credentials, and the human factor have an outsized impact on data breaches. Because of this, your agency's security policies—the ways you choose to work—along with regular training and refresher courses could be the difference between keeping your business and clients secure or winding up as a cautionary tale.

Beyond risk mitigation, building a reputation as a security-forward agency is just good business, as it not only changes how the market sees your company, but helps foster trust with existing clients (or even opens doors to pitching new ones).

As these processes touch on every aspect of your business and involve every agency employee, we're going to spend the rest of this ebook breaking this bucket down.

[1] WP Engine is a proud member and supporter of the community of WordPress® users. The WordPress® trademarks are the intellectual property of the WordPress Foundation, and the Woo® and WooCommerce® trademarks are the intellectual property of WooCommerce, Inc. Uses of the WordPress®, Woo®, and WooCommerce® trademarks in this website are for identification purposes only and do not imply an endorsement by WordPress Foundation or WooCommerce, Inc. WP Engine is not endorsed or owned by, or affiliated with, the WordPress Foundation or WooCommerce, Inc.

Internal security policies for your agency

Require secure passwords and manage them safely

Secure passwords

Can you remember your first password? Likely it was simple, easy-to-remember, and one you used everywhere. Remember, cybercrime is predicted to cost our economy $12.5 trillion this year. Using simple passwords that never change ain't gonna cut it, and reusing them is right out. Make sure whatever systems your team uses require complex passwords that, preferably, they are regularly required to reset.

Safely storing and managing passwords

Take a look at your desk. Check out the bottom of your keyboard or the inside of your desk drawer. If you have a Post-it with a password stuck in a hard-to-see location, this one is for you. Those of you with complex Excel spreadsheets keeping track of passwords aren't off the hook either, so lock in for a second.

Remember how credentials are one of the primary vectors for security breaches? Using complex, unique passwords for every system including your clients' can quickly become overwhelming, leading to habits that actively harm your security positioning.

The solution? Utilizing a password manager. All the better if it can be managed at a team level so access to passwords can be revoked in case of a breach or change in employment. Some popular password managers include **NordPass, 1Password,**and **LastPass.**They each approach management differently and have different features, so do your due diligence to see which of the many options on the market would work best for your team.

> Managing passwords at the team level becomes ***especially important*** if a particular client is only providing a single login to a system.

Individual access or usernames

Speaking of sharing credentials—don't do it. Tight timelines and razor-thin margins often mean it's easier and cheaper to share software/tools or even access to client systems. But again, whenever possible, don't do this. Shared credentials make it more difficult to understand the source of a breach. It can also mean your entire agency is locked out if an intruder signs in and changes the password and/or profile information. It also becomes more difficult to remove access to employees who are reassigned or resigning. All in all, it will likely cause more headaches than it's worth, even if it does help your bottom line or mean you get to work faster with a client.

Wall off remote access

Working at an agency often means the freedom to work wherever you want— from your couch to your local coffee shop or even a South American beach that just so happens to be in the same timezone as your residence (don't worry, we're not gonna tell anyone). But each of those locations (yes, even your home office) is vulnerable to unauthorized access. Because of this, it's important to require that data, systems, and tools be accessed securely. This typically means a Virtual Private Network (VPN).

A VPN is a service that protects your privacy by routing all internet traffic to and from your device through an encrypted connection to a secure server. This hides your public IP address and allows you to use public wifi hotspots more securely. Your agency's VPN can also be set up as the only network capable of accessing specific internal systems and tools, ensuring any connections made to these systems are secure.

Popular business VPNs (that enable you to secure your systems behind the firewall and manage access) include **Nord Layer, Perimeter81, Palo Alto's GlobalProtect,** and **Cisco's AnyConnect**

Least privilege

Requiring secure passwords, individual access, and VPN usage all contribute to one of the cornerstone principles of modern cybersecurity—the **least privilege standard.**

This principle is exactly what it sounds like: users (and applications) are restricted to the least amount of access needed for them to accomplish their assigned/necessary tasks. Employing a least privilege approach can create frustration with your power users who are accustomed to wearing multiple hats, but least privilege is critical to limiting the damage from bad actors who deploy compromised credentials.

Least privilege is a key policy for your internal systems, but it's also important to insist on it when accessing client systems. While having more access to additional data or systems than is strictly necessary might sound like a good opportunity—perhaps to find additional ways to add value to the relationship with the client—it's not really all it's cracked up to be. It not only opens your agency up to additional, possibly unintentional liability, it can create new attack vectors that empower bad actors and lead to more damaging breaches.

Two aspects of least privilege include both **just-in-time (JIT)** and **just-enough access (JEA).** Just-in-time access is simply that a user (or app) only has access to the data or systems at the expected and necessary times. At all other times, access would be denied. Just-enough access is the principle of limiting access to a system to only what is strictly necessary. Of course, the key to implementing these policies efficiently is ensuring they're well-managed and flexible enough to handle agency employees, who often move between clients and projects seamlessly.

Zero trust

Perfectly paired with the principle of least privilege is having a zero trust policy. A zero trust policy is one which defaults to not trusting any device on any network without thorough verification—even behind the company firewall or VPN. While a true **zero trust policy** is an end-to-end approach to security, one big component of it includes enabling two-factor authentication (2FA) or multi-factor authentication (MFA) on every system that offers it.

Behind the scenes, a zero trust posture is continuously validating and limiting access to minimize the impact of any potential breach. When rolled out comprehensively, a zero trust policy will typically use either:

- One-time passwords (OTP) algorithmically generated by a physical token or app.
- Authentication apps or single-sign on services like **Duo** or **Okta.**

What's *the difference* between 2FA and MFA?

2FA

username + password and one other authentication option.

MFA

username + password and one **or more** additional authentication methods.

Methods include:

- Knowledge Based: PIN, security question, or similar.
- **OTP:** These can come via text, email, an authentication app, a security service, or a physical token. Some physical tokens can be sensed/scanned vs inputting the OTP directly, but are still randomly generating or automatically refreshing the authentication code. Any algorithmic-based or expiring OTP can be referred to as a **Time-Based One-Time Password** (TOTP)
- Biometrics: Often referred to as a passkey. Includes fingerprints, facial recognition, etc
- Location: Apps and services only accessible to users within a specific geographic location. (ie: on the corporate VPN)

In other words, all 2FA is MFA, but the opposite is not always true.

Additionally, MFA beyond just two factors is by necessity a more complex process, but typically provides much better protection.

Backup all the things

According to **Nuspire,** data theft extortion rose 46% in Q4 of 2024 alone and is quickly becoming one of the most common cyber attacks. While traditional ransomware practices coerce victims into paying a scammer to get their data back, data theft extortionists often go a step further, threatening to publicly release your company's private data on the dark web. Obviously, no one wants that, but part of the reason for this shift in tactics is the prevalence of backups — removing the bad actor's leverage in a straight ransomware attack.

Hopefully, that means you already know you need to back up, literally, all the things. Your site, your data, your clients sites, and your clients data (where appropriate). Make sure you regularly test your backup solutions, the data that's backed up, and processes informing your team on how to quickly restore hijacked data.

Have a plan

Speaking of informing your team, the worst thing you can do in the event of a security issue is to panic. The second worst thing you can do is to have no idea what to do.

Having a documented and communicated disaster recovery plan is essential to quickly responding when one inevitably happens.

Make sure your agency is prepared for:

- ✓ Inaccessible OTPs or OTPs sent to employees who are unable to be contacted.
- ✓ Datacenter outages.
- ✓ Hacked sites.
- ✓ Natural disasters impacting infrastructure and networking.
- ✓ Death or serious illness of a team member.

Each of these requires different responses, which is why it's important to map out the following at a minimum:

- Roles, responsibilities, and prescribed actions during an incident. This may be different depending on the type of incident.
- Emergency contact information for everyone expected to respond.
- Contact information for clients as well as how is informed.
- Login credentials for critical services including:
    - Datacenter
    - Hosting
    - DNS
    - Backup storage services
- Emergency OTPs needed to overcome 2FA/MFA in case of an emergency. ogin credentials for critical services including:

Having a plan will help your agency respond quickly and mitigate damage, but a plan is only half the battle. Make sure you test your processes and systems regularly, evaluate how effective they are, and adjust as necessary.

Ongoing training for your team

Remember our three big initial vectors? Two of them are all about the (pesky?) human factor.

Indeed, it's unfortunately easy for many folks to unintentionally slip into efficient—but less secure—ways of working. This is why providing ongoing educational opportunities for your team, as well as having annual mandatory certification, is crucial for your agency. And, unless you want to be in charge of becoming your in-house security expert and knowing what the latest security best practices are, it's probably important to outsource this to a trusted security provider.

Stay up-to-date

The third initial intrusion, "known exploits," are vulnerabilities in software, hardware, applications, or systems that are being actively exploited for cybercrime. These account for nearly 20% of said initial vectors, with almost all of these occurring on web applications. Systems behind a VPN are inherently more secure (depending on the VPN obviously), but attacks on those are on the rise too!

All of this means a key security measure against known exploits is staying as up-to-date as possible. Obviously updates to production environments must be done with overall business continuity in mind. But having policies on when and how updates are performed will ensure systems are as protected as possible.

This can also be impacted by tech debt. If your systems, tools, or code rely on outdated, unsupported tech, you'll expose yourself to security vulnerabilities—both known and unknown—once those technologies no longer receive regular updates.

> That's why it's so important to ***regularly evaluate*** the technologies you're using while replacing or removing any that are outdated or no longer needed.

Document the process

If you've made it this far, it should be obvious that there's no easy button to securing your agency—and that's without us really touching on infrastructure or writing secure code.

Implementing the right security processes and tools for your agency and clients requires thoughtful consideration, team buy-in, and ease of implementation. That's why it's critical to document everything during the decision-making process, and not just the implemented policies. This gives you a firm foundation when you inevitably need to reevaluate a decision—helping you remember how you got where you are.

However you document, make sure it supports versioning so you've always got a comprehensive look back at your security journey. And if a particular policy is client-specific, make sure it's noted so you never miss a necessary stipulation.

Create a security culture

Along with documenting your process, it's critical that your agency's security policy is fully articulated and posted as a known resource for your team. This helps ensure everyone knows what is expected of them in nearly every situation.

But it's also important to move beyond a simple policy that can be ignored or skimmed. Weaving the principles of working securely into your team culture can foster safer working habits while helping them become second nature with your employees.

Cybersecurity is table stakes for any industry with a digital presence—potential clients will either assume you can operate securely, or they won't entertain working with you. That said, building a reputation for being a security focused agency may actually cause certain prospects to take notice or create an initial sense of trust. Of course, the proof is always in the pudding.

Where to start?

Building a security-minded focus won't happen overnight. You can't just turn on new, unevaluated policies or systems and hope for the best. On the other hand, securing your agency's and clients' data can't wait.

While building out robust disaster recovery plans and evaluating the right tools and services for your team will take time, there are ways to increase security immediately. Go ahead and multi-factor all the things. All. The. Things. If you don't have 2FA or MFA on for any of your current tools or accounts, flip that switch as soon as possible to ensure you have at least that level of protection. If you need to move to a more complex MFA or single sign-on solution down the line, you'll have already built up the muscle memory of MFA for your team.

Want to explore secure infrastructure options? Our team at WP Engine would be happy to talk through our enterprise-grade approach to keeping the hardware running your clients' sites secure. Find out more here.

Reach out to a representative today!

WP engine™

WP Engine empowers companies and agencies of all sizes to *build, power, manage, and optimize* their WordPress websites and applications with confidence.

Serving 1.5 million customers across 150+ countries, the global technology company provides premium, enterprise-grade solutions, tools, and services, including specialized platforms for WordPress, industry-tailored eCommerce and agency solution suites, and developer-centric tools like Local, Advanced Custom Fields, and more. WP Engine's innovative technology and industry-leading expertise are why 8% of the web visits a WP Engine-powered site daily. Learn more at wpengine.com.

WP Engine is a proud member and supporter of the community of WordPress® users. The WordPress® trademarks are the intellectual property of the WordPress Foundation, and the Woo® and WooCommerce® trademarks are the intellectual property of WooCommerce, Inc. Uses of the WordPress®, Woo®, and WooCommerce® trademarks in this website are for identification purposes only and do not imply an endorsement by WordPress Foundation or WooCommerce, Inc. WP Engine is not endorsed or owned by, or affiliated with, the WordPress Foundation or WooCommerce, Inc.