



THE SECURITY 6

According to industry experts, there are 6 primary Security Threats impacting or targeting your business today. Security matters to everyone and any one of these 6 challenges could bring your business down for good.

The it will never happen to us approach is not a Security Strategy, especially when according to US Bureau of labor Statistics, 1/3 of security positions are unfilled and SMB's cannot find or keep these skills internally much less afford Enterprise class security tools.

When you have been compromised, the ounce of prevention delayed becomes the pound of crisis that derails your business. Every business needs a strategy for these threats in place now:

1. End Point Computing

The most prevalent source of all security breaches today is the End Point you gave your End Users. Forbes reported that Locky malware was infecting as many as 100,000 PCs a day and most security experts recognize that “[A] careless worker . . . is as dangerous as a disgruntled user who maliciously leaks information to a competitor,” says Ray Potter, CEO, SafeLogic. Protecting employees from themselves, locking down End Points with best security practices can protect against weak passwords, unauthorized website visits, suspicious emails and attachments.

Nuvestack addresses this issue by protecting employees from themselves. Our proprietary End Points and Remote User App grant easy access to needed business tools while locking End User sessions down, mandating best practices for security and compliance, protect against weak passwords, unauthorized website visits and even flag suspicious emails and attachments.

2. Disgruntled Employees

Internal attacks are one of the biggest threats facing your data and systems,” states Cortney Thompson, CTO of Green House Data. “Rogue employees, especially members of the IT team with knowledge of and access to networks, data centers and admin accounts, can cause serious damage.”

NuveStack insulates your business from these threats by mandating multi-factor authentication, and providing fast User and Admin management with NuveCenter that also disallows unauthorized inbound traffic for backend servers. NuveStack's Cloud-IT strategy automates, manages and monitors optimum security and best practices for all of our Customers. We make sure the proper people access your data at proper times, making your business profile unique and secure. We monitor for bad-actor alerts and react quickly to malicious activity early in the attack cycle to mitigate threats from those who would do your business harm.

3. Mobile Devices (BYOD)

Your Employees End Points only add points of attack to mitigate. “Data theft is at high vulnerability when employees are using their mobile devices to share data, access company information, or neglect to change mobile passwords,” explains Jason Cook, CTO & VP of Security, BT Americas. “According to a BT study, mobile security breaches have affected more than two-thirds (68 percent) of global organizations in the last 12 months.”

NuveStack ensures data is never cached or stored locally on your end point. BYOD should never mean company data is stored on employee-owned devices. Before NuveStack, performance woes put mobility and security at odds with one another. No longer. NuveStack delivers superior performance for BYOD and remote employees because for the first time, the Cloud is really faster than local PCs, security does not have to be compromised for performance. If your BYOD device is lost or stolen, there's no risk of sensitive data being lost because nothing is local. NuveStack adds end-to-end traffic encryption so every Customer has the most secure, high performance computing environment in the world.

4. Ransomware

Ransomware has been in the news a lot in 2016 and we are only going to hear more about it. Online extortions threatening reputation and brand names are leveraging automated ransomware attacks that have forced several businesses to pay to avoid suffering the consequences. To make matters worse, ransomware as a service (RaaS), which makes criminal extortion incredibly easy, is now available to everyone who may want to harm your business with exploit kits and phishing emails.

NuveStack solves Ransomware. An aggressive but true statement. We proactively prevent attacks inside our Cloud with anti-phishing solutions, but even if Ransomware infects your system, NuveCenter instantly reverts your business back with our proprietary Snapshot solution. Want 7 days, 7 hours, 7 minutes of Snapshot backup and Recovery? We will deliver it. NuveStack supports unlimited snapshots and recovery; you define what your business needs and NuveCenter will automate it. Snapshot as you want without impacting storage or network resources.

5. Cloud Applications

Third Party vendors may push SaaS, but Cloud Applications present security threats that must be addressed and monitored. Elimination of end point data and computing is great, but add market leading encryption like AES 256-bit and retaining exclusivity keys “can prevent third parties from accessing data even if it resides on a public cloud,” says Pravin Kothari, founder and CEO of CipherCloud. “As many of 2014’s breaches indicate, not enough companies are using data level cloud encryption to protect sensitive information.”

NuveStack increases security for Cloud applications by ensuring End Users access Cloud Applications by a locked down, protected NuveStack session strictly designed for best practices security. If you can’t control how your End Users access Cloud Applications, you can’t secure your business. This kind of security used to mean lackluster performance; no more. Be faster and more secure with NuveStack.

6. Managing Multiple Environments

It’s all about Cloud and securing hybrid environments now, but this only means many businesses are trapped in the worst of two IT worlds: 1) managing on premises PCs, Laptops and mobile devices; and, 2) integrating them with Cloud based applications and storage. This approach doubles the risk, requires additional IT skill sets and significantly increases costs. NuveStack solves this and saves Customers money in the process.

NuveStack will migrate your entire environment to our secure Cloud for free. All of your systems are protected, isolated, and running within the same locked down high performance infrastructure. What does this mean to your business? Zero migration costs, satisfied End Users, faster access to back end Applications and Data, elimination of end point infection of backend systems, easy remote access from anywhere (without the hassles of VPN), and unmatched performance.

All of this is NuveStack’s Cloud-IT – the world’s first comprehensive Cloud-based IT Service that addresses the Security 6, improves End User satisfaction and delivers unparalleled performance. We created Cloud-IT with the security of your business in mind.

Contact NuveStack to find out more about the Security 6 or to address other threats confronting your business today.