THE SECRET LIFE OF YOUR NETWORK: 9 THREATS LURKING IN YOUR DATA CENTER

Pictur

e a place filled with threats both known and imagined. Perhaps it's a ramshackle house with creaky stairs and dusty furniture; a damp, shadowy basement with ominous shapes looming in the corners; or the deepest depths of the ocean.

Or maybe it's your data center.

Yes, even a landscape of soothing hums and flashing lights has a secret life, and it's not pretty. Your data center is ground zero for a wide range of threats to your organization's security. Some are actively malicious, some the product of carelessness or oversight, and some simply the result of a lot of people working with a lot of technology in a complex environment. Regardless of the origin of the threat, you can't protect yourself if you don't know it's there – and what to do about it.

We've identified nine risks that could be lurking in your data center at this very moment.

1. **Zombie servers.** Forget those lightweights on the Walking Dead – the real zombies to be concerned about are zombie servers. We've written of their danger before, but their power continues to grow. Zombie servers, a.k.a. servers that are unused or underutilized, number over 10 million globally. Keeping them running requires the equivalent amount of energy required to power all the homes in the city of Chicago. They suck up space as well as energy - taking up precious data center square footage that could be used for more critical assets.Zombie servers are notoriously hard to identify and destroy. Defeating them requires powerful tools that go beyond a single metric to look for servers with few network connections to other systems, then assess what software (if any) is running on those systems, and then compare those results both in real-time and as long-term trends.
2. **Malicious software.** If zombie servers are the walking dead of the data center world, malicious software is the axe-wielding murderer who is very much alive. No matter how secure your networks, new and evolving threat vectors can still manage to penetrate your walls. Withstanding malicious software threats is a battle of vigilance. The best defense is offense. With a clear view into all of your assets, you can identify which systems or applications are affected by vulnerabilities found by your security management tool.
3. **Looming outages.** Not all threats are nefarious; sometimes components of your infrastructure simply break, wear down, or overload. The key to these data center disruptors is early detection. If you know which systems are showing symptoms, you can prevent outages from impacting your business. If an outage does occur, it's helpful to have tools that pinpoint which applications are affected so you can mitigate the impact.
4. **Compliance vulnerabilities.** Like signs of a looming outage, compliance vulnerabilities are a harbinger of bad things to come. Internal and regulatory compliance requirements demand consistent and frequent assessment and documentation of your asset inventory, including each asset's business function. Without that view, you're open to threats of a different kind - including audits, fees, and sanctions.
5. **Version sprawl.** Like wayward clones, your software has a tendency to replicate itself into a resource-sucking army. You may be hosting countless versions of the same piece of software due to inconsistent upgrades or failure to address outdated versions. These clones are not necessarily evil, but they do consume a surprising amount of unnecessary space and energy that should be dedicated to more valuable assets. Version sprawl is expensive too - each software clone is costing your company unnecessary money.
6. **Servers reaching storage capacity.** Functional (non-zombie) servers must still be watched carefully to keep them safe from the dark side. Without regular assessment, servers can quickly reach capacity unbeknownst to your team, resulting in downtime and headaches that

you can't afford.

7. **Backdoor entry points.** To wreak their havoc, bad guys must be able to get in. Your data center may be hosting unlocked doors and windows just waiting to be breached. It's critical to understand where your weak points are and whether business applications are running on vulnerable systems so that you can properly secure your defenses. This may include identifying unpatched systems, locating servers that are listening on unwanted service ports, or flagging dependencies associated to vulnerabilities. When (not if) attacks or disruptions occur, you also need to be able to prioritize fixes to get your most important assets back online fast.
8. **Unauthorized software.** "Shadow IT"… it sounds sinister, and it is. Every time someone in your organization goes it alone and downloads an app, you face a potential security threat. The risks of unauthorized software has only grown with the consumerization of IT, and therefore so has the need to detect these rogue operators before they become a problem.
9. **Out-of-support operating systems.** These systems are the ghosts of the data center world: they're no longer alive, but are still stuck in our dimension. Lack of support doesn't just mean that the company won't answer your phone calls, it means that vital things like security patches no longer exist. That means that these ghosts can turn evil at any moment.

All of these threats present a real risk to your business – but they can also be vanquished. Asset discovery and application dependency mapping tools like BMC Helix Discovery combat the menaces to your data center by giving you up-to-date, holistic views of all your data center assets and the relationships between them. They give you the weapons – visibility, accuracy, speed, and insight – that you need to understand the threats to your system so that you can defeat them. Banish the cobwebs and bring on the sunshine. With BMC Helix Discovery, the secret world of your data center won't be so secret after all.

Start your free trial to see BMC Helix Discovery in action.