Want to Cut Risks to Your Business?
Go Zombie Hunting
**Zombies Are Everywhere**

Would you think it inefficient, or downright crazy, for an airline to fly one out of every four of its planes without passengers, all the time? That’s what’s happening in enterprise compute infrastructure...with zombies.

“Zombies” is the term given to compute assets — virtual machines (VMs), data storage and physical servers — no longer doing useful work. At one time, these assets had a purpose and value. Then people or processes stopped using them and they were forgotten but never shut down.

In aggregate, organizations are incurring high financial costs to maintain hidden zombies. Because zombies are unmonitored and unmanaged, they also likely have significant security vulnerabilities. And the wasted energy and associated carbon emissions create substantial sustainability impacts.

What is your organization doing to find and remove hidden zombies?

**Three Ways to Reduce Business Risk**

1. Lower costs
2. Strengthen security
3. Improve sustainability
Are Zombies Really a Problem?

Discovering zombies isn’t part of anyone’s job description. Typically, their hunter is a lone champion who recognizes the business cost of their existence and is willing to take on the effort, and risk, to remediate.

Studies over the past decade show zombies exist in enterprises at levels from 15–45%.

In 2017, Stanford University and Anthesis Group found zombies in 25% of all physical servers and 30% of all VMs, across 16,000 virtualized and non-virtualized servers in 10 data centers and multiple companies. The study also identified security vulnerabilities posed by zombies. The zombie threshold for this study was zero CPU, I/O, memory, user and connectivity activity over six months.

Years before, the Uptime Institute’s “Server Roundup” contests and McKinsey & Company’s 2008 study looked for zombies in the physical server population. They discovered more than 50,000 servers (over three years and seven companies) in non-productive operation, ranging from 29–45% of the IT infrastructure. Removing zombies resulted in cost savings ranging from $9,000 per year for the smallest project to more than $10 million dollars for AOL’s three projects over three years. AOL estimated a carbon emissions savings of almost 70,000 metric tons.

---

2 Decommissioning as a Discipline: Server Roundup Winners Share Success, Uptime Institute Journal (2013); Visa and AOL Take Top Honors in the Fourth Annual Uptime Institute Server Roundup Competition, Cision PRWeb (2015)
How and Why Zombie Discovery Matters

Two events force an organization to expose zombies: a server refresh project and a data center move. Both require discovery of the owners and purpose of all compute assets. This is a laborious, although necessary process.

When VMware migrated data centers as part of a server refresh initiative in 2019, we discovered 47% of our VMs were zombies. That eliminated the need to transition them.

Because it’s so time-consuming and potentially risky to find zombies, no organization wants to repeat the process until the next move or refresh. This gives zombies an opportunity to rise again, a situation no business wants to be in because zombies lead to:

**Higher Costs**

The zombie problem is significant for many organizations, which makes it costly. Zombie VMs and storage consumption require enterprises to incur licensing costs for compute assets reserved, but not used. For physical zombies, there are operational costs from data center operations and space; licensing and maintenance fees; and capital expenses from the procurement of more servers than actually needed. Depending on the size of the organization, these costs can range from hundreds of thousands to millions of dollars annually; money that could be put to more productive use.

**Security Vulnerabilities**

Zombies are unused, so most often are also unmanaged and unmonitored. They’re more likely to have old operating systems and out-of-date patches, making them prime targets for cyberattacks. Zombies are an invitation to intruders. With the average cost of a data breach rising to nearly $4 million in 2019, catching security vulnerabilities and stopping attackers is a top business priority.

**Negative Sustainability Impact**

Because of their large numbers, zombies adversely affect sustainability. They continuously waste energy and add to carbon emissions. It’s not just the zombies themselves that add to data center power costs, but also the cooling associated with hosting them. Sustainability impacts are of growing concern for companies. During a recent data center consolidation project in a Singapore operation, 66% of non-utilized host machines were decommissioned. This reduction in infrastructure and associated data center operations saved the organization 325 kilowatts of power and 1,300 metric tons of carbon emissions.

Why Do Zombies Continue to Exist?

If the costs and impacts to an organization are so high, why do zombies continue to exist? Zombies thrive in most on-premises, corporate IT, DevOps and production environments, for two reasons:

“Not a real problem”
Most teams don’t believe the zombie problem is extensive or costly, so there isn’t a rigorous process in place to find and prevent them. However, unless teams go hunting regularly or integrate a prevention process, then zombie populations will grow over time.

“Difficult and risky”
It’s difficult and risky to find zombies with no holistic solution to provide visibility into the extent of the problem and to facilitate low-risk remediation. It’s easy to create an asset, but hard to track ownership and purpose over its lifecycle. When an asset loses its owner, usually because the owner leaves the organization, it’s rare that a new owner is assigned. Similarly, when a project’s purpose comes to an end, most owners move on without repurposing or decommissioning compute assets. Furthermore, an asset can look active without doing any useful work. Automatic patch updates, virus scans, or random polling activity can look useful even when they’re not. There may be no discernable activity, but who wants to test it by deleting the VM or data, or unplugging the server? Few get promoted for such moves. Better to leave it alone, just in case.
Achieve Sustainability Goals

Eliminating zombies that are wasting 20–50% of a company’s computing resources can result in dramatic and ongoing electricity consumption and associated carbon emissions reductions. A proactive effort can be a valuable contribution to the company’s sustainability goals.

As the world experiences accelerating climate change impacts, the messages of IT efficiency and optimization are resonating. The Forbes Global CIO 2025 report\(^6\) – with insights from more than 650 CIOs worldwide at companies with revenues of $1 billion or more – reveals 70% of CIOs believe they will have a responsibility to use technology for the greater social good, and 64% say “fighting climate change” is important for the CIO to help meet the company’s corporate goals.

Organizations, believe zombies are a threat to society. Jean-Pascal Tricoire, Chairman and CEO at Schneider Electric recently declared,

“Climate change is the single biggest threat to the health and well-being of our society. We must work together to reduce our carbon emissions and halt the rise in temperature. At Schneider Electric, our commitment to carbon neutrality is weaved into our business decisions and governance, but we need to do more and faster. Not only are we stepping up our carbon commitments and moving up our timeline, but also calling on others to take bolder actions to reduce carbon emissions and establish more sustainable business practices that will help set the stage for a post-carbon world.”

To date, 750 companies worldwide, including VMware, have set science-based targets to reduce absolute carbon emissions throughout internal operations and supply chains. And we are all looking for solutions to help achieve these aggressive targets. For many, IT operations represent a relevant fraction of internal carbon emissions. That’s why finding and eliminating zombies will make a real and meaningful dent.

How to Prevent Zombies

To prevent zombies, organizations need to manage three aspects of an asset over its lifecycle to ensure it doesn’t turn into a zombie:

1. Define an owner
   Every asset should have an owner over its lifespan. If that owner leaves the organization, a new owner should be assigned, or the asset should be released to reduce the risk of it becoming a zombie.

2. Understand the purpose
   Every asset should have a purpose, the reason for its existence, and an associated end date to that purpose, or at least a date to recheck the need for its existence.

3. Monitor activity
   The activity of every asset should be monitored over its lifespan. This is important because if activity changes dramatically from initial activity, especially a significant decrease or sustained increase, it could be a sign the asset has been abandoned. Beyond compute resources, activity can also include an asset’s interaction and interdependencies with other assets. Who does the asset communicate with and how often? For physical assets, signals like the age of the asset or OS; out-of-date licenses and patches; blue screens; and last logins can be zombie flags.
Trust Proven Technology to Find Zombies

VMware vRealize® technologies can help manage your VM and storage assets to ensure they’re productively utilized. VMware vRealize® Automation™ confirms each VM and storage asset has an owner while VMware vRealize® Operations™ monitors VM activity and can flag wasted resources, along with the monthly cost of each of the following:

- Powered-off VMs – VMs that have been powered off for x number of days
- Idle VMs – VMs that are powered on but have consumed no more than 100 MHz of CPU for x number of days
- Snapshots – VM snapshots that have existed for more than x number of days
- Orphaned disks – Virtual disks that no longer appear to be associated with any VMs for the past x number of days

vRealize Operations features a reclaim capability
Zombie VMs aren’t the only things that misuse resources, so vRealize solutions also identify oversized VMs. Oversized VMs potentially cause performance issues for other VMs, which can lead to unnecessary hardware purchases.

Complementing VMware software operations and automation capabilities, VMware vRealize® Log Insight™ tracks VM logins. By installing the vRealize Log Insight Agent on your VMs, you can collect OS logs and events to see who, if anyone, has logged into the VM over the course of the past week, month or even longer.

Moreover, with VMware vRealize® Network Insight™ you can analyze traffic flows to and from your virtual machines and quickly identify VMs with little to no network traffic.
Self-Driving Operations from VMware

Your organization has valid reasons for wanting to find and eliminate zombies, from cost savings and strengthening security to improving sustainability. With self-driving operations from vRealize Operations, you can achieve all these goals, easily.

Self-driving operations give you a simple, yet powerful strategy for automating and simplifying operations management. It incorporates Artificial Intelligence (AI) to help your IT team be more proactive and agile.

As your data center grows in scale and complexity, your team can confidently work hands-off and hassle-free—from apps to infrastructure, and across hybrid clouds and multi-clouds—to discover and remediate zombies. Unlike traditional tools, AI-driven vRealize Operations provides:

- Comprehensive data and policy-based control across your entire infrastructure, wherever you choose to run workloads
- A way to optimize observable conditions against business key performance indicators (KPIs)
- Proactive, real-time, reliable optimization, remediation and compliance that leverages advanced analytics with AI intelligence

Deploy VMware vRealize® technologies for operations, automation, logging, and network insights—in your data center or as a service—to reduce your business risk.

Learn more at https://www.vmware.com/products/vrealize-suite.html or https://cloud.vmware.com