Why a Sprawled Stack is a Vulnerable Stack

With the rise of cloud services, the number of IT tools organizations now juggle has skyrocketed. On average, companies manage more than 70 security tools!

But here's the catch: while having a robust security stack is crucial, there's a growing concern that the sprawl of these tools might actually be making organizations more vulnerable.

What is IT Tool Sprawl?

IT Tool Sprawl refers to a situation where organizations accumulate several tools, applications, and technologies over time, often resulting in a complex and disorganized IT environment.

Over time, this decentralized approach results in a complex and fragmented IT landscape, making it challenging to manage, integrate, and maintain the various tools effectively. IT tool sprawl eventually increases your Total cost of ownership (TCO).

What Causes Tool Sprawl?

IT tool sprawl isn't always caused by neglect or poor planning but rather occurs naturally as a result of various factors.

For instance, the rapid pace of technological advancements leads to the continuous emergence of new tools and solutions. As a result, businesses may feel compelled to adopt multiple tools to keep up with the latest trends or to address emerging needs.

Another reason for IT tool sprawl is the inheritance of legacy systems and applications. Over time, as technologies evolve, new tools are introduced while older ones are retained, leading to a mix of outdated and modern solutions.

IT tool sprawl also occurs as a result of shadow IT. Shadow IT refers to the use of unauthorized or unapproved technologies by employees to address their specific needs. This can happen when organizations grow, and individuals within the organization acquire or create technology that is outside the visibility and control of the IT department.

Employees often turn to familiar tools to solve problems, even if they are not officially sanctioned, leading to an increase in the number of tools in use and a lack of centralized decision-making.

Tool Sprawl Security Risks

There are several security risks associated with IT tool sprawl that organizations need to be aware of to effectively mitigate potential threats. Some of them include:

Increased Cyberattack Surface Area

Tool sprawl contributes to an expanded attack surface for cybercriminals. When you deploy multiple applications and systems without proper integration, it increases the footprint available for attackers to exploit.

These applications, particularly those with entitlements in core infrastructure and servers, can serve as entry points for attackers to gain unauthorized access within the organization's network.

Additionally, siloed applications that are not fully integrated with security controls and monitoring tools further exacerbate the risks by evading detection.

Credential Risks and User Access Management

Failure to reverse IT tool sprawl often results in applications existing outside of a universal Identity and Access Management (IAM) system, making user access management challenging. This fragmented approach to user access increases the risk of unauthorized access to IT resources.

Attackers can exploit weak or reused passwords, bypassing proper authentication measures. Additionally, the lack of integration with cloud security measures like Zero Trust leaves data and users vulnerable to compromise.

Compromised Supplier Security

Each new third-party component introduced through tool sprawl introduces a potentially compromised supplier, expanding the threat landscape for an organization. These third-party components may have poor security practices or vulnerabilities, which threat actors can exploit to gain unauthorized access or compromise the organization's systems.

Moreover, the lack of visibility and control over these components makes it difficult to assess their security posture, increasing the potential for security breaches.

Other Negative Impacts

Besides security vulnerability, IT tool sprawl is also associated with a high TCO among several other negative impacts.

First, managing a diverse and expansive IT tool stack requires significant time and effort. Each system needs to be set up, configured, and integrated with existing infrastructure. This increased management overhead can strain IT resources, diverting valuable time and attention from other critical tasks.

Secondly, the complexity introduced by IT tool sprawl can be challenging for employees to navigate. With multiple systems in place, each with its own interface, workflows, and learning curve, employees may struggle to adapt and become proficient in using the various tools. This can lead to reduced productivity, increased training needs, and frustration among the workforce.

Moreover, when multiple tools are used to perform similar functions, data gets duplicated and stored separately in each tool's database. This redundancy further exacerbates the problem of data silos, as inconsistencies and discrepancies can arise between different instances of the same data.

How to Address Tool Sprawl

Unlock the power of efficiency and streamline your IT environment by strategically addressing IT tool sprawl through the following actions.

Identify Your Core Stack

The first step in addressing IT tool sprawl is to conduct a comprehensive assessment of your IT environment. Consider your objectives, needs, and the technologies required to achieve them. Determine the platform(s) that align best with these requirements, factoring in scalability, compatibility, and integration capabilities.

Identifying your core stack can help you to strategically select solutions that meet your specific needs, reducing the need for multiple tools that perform similar functions.

Integrate Your Core Stack into Unmet Needs

Integrate your newly identified core stack into areas with unmet needs or underperforming solutions. Actively listen to user feedback and engage with stakeholders to identify pain points and areas where your existing tools fall short.

For example, if users express difficulties in managing identities, access, and devices across multiple systems, consider implementing an open directory platform like JumpCloud. It will definitely increase productivity by unifying identity, access, and device management capabilities, regardless of the authentication method or device ecosystem used by your users.

Integrate Systems Surrounding IT

Automate user provisioning and access control using attributes for authorization and smart group management for app assignment. This integration reduces manual work and improves efficiency while ensuring that users have appropriate access to the tools they need.

An open directory platform can pull information from authoritative sources such as HR systems, enabling seamless integration between HR and IT processes. By automating group memberships and leveraging automated auditing, you can establish a mature approach to entitlement management.

This approach not only reduces the likelihood of unauthorized access but also eliminates the need for separate, siloed tools that handle user provisioning and access control.

Automate the Identity Lifecycle

Eliminating identity sprawl and breaking down silos surrounding HR processes allows you to establish a more efficient and integrated approach to managing user identities.

This not only saves time but also reduces the risk of onboarding errors that could lead to security vulnerabilities or access issues.

Consolidate and Eliminate Unnecessary Tools

Evaluate the functionality and overlap of your existing tools and identify opportunities for consolidation. Consider retiring tools that have become redundant or no longer align with your current needs.

When Sapling was looking for a single solution to replace the separate systems they were using for IAM, MDM, SSO, and password vaulting, they settled on JumpCloud. Now, the company uses the time they save using JumpCloud to serve their customers better.

Solve IT Tool Sprawl With JumpCloud

Purchasing management tools without considering their integration and overall impact can make the IT environment difficult to manage. But a strategic approach that focuses on consolidating tools, implementing proper identity and access management, and actively managing the IT environment can help prevent IT tool sprawl from becoming a significant problem.

Unification helps MSPs succeed by improving productivity and control over client environments. By supporting fewer solutions and eliminating shadow IT, MSPs can streamline operations and reduce tool sprawl. JumpCloud provides a comprehensive, cloud-based directory platform that allows IT departments to consolidate and streamline their IT tools.

With JumpCloud, you can simplify user provisioning, access control, and device management, reducing the need for multiple disparate tools and enhancing overall efficiency and security. Try JumpCloud for free today.