Infosys®
Navigate your next

VIEWPOINT

HOW AUTOMATION SITS WITH DEMOCRATIZATION OF CYBERSECURITY

Cybersecurity relies on many layers working together, from highly automated processes to understanding the role of humans.

Infosys® | Knowledge Institute

Companies are increasingly turning to highly automated processes to do the heavy lifting of managing the organization's IT estate, from patching laptops and checking compliance to scanning remotely for vulnerabilities and configuration drift.

This relies on processes such as network discovery tools and tools deployed on devices to take regular snapshots of users' devices and their current patch status. Given the old adage that humans are the weakest endpoints in any organization, these tools mostly take humans out of the loop, only delegating decisions about how long to defer a patch for so that it doesn't interrupt their workflow.

However, there is a tension between this automation and the trend towards democratization of security.

The latter puts individuals at the heart of security, aiming to make them understand their crucial role in keeping the organization safe. Vishal Salvi, Chief Information Security Officer at Infosys, is very clear about the role individuals play in cybersecurity, saying that businesses need to "build a security culture where everyone takes pride and ownership in execution. Cybersecurity can no longer scale and be effective if it's only left to the cybersecurity teams to implement and execute."

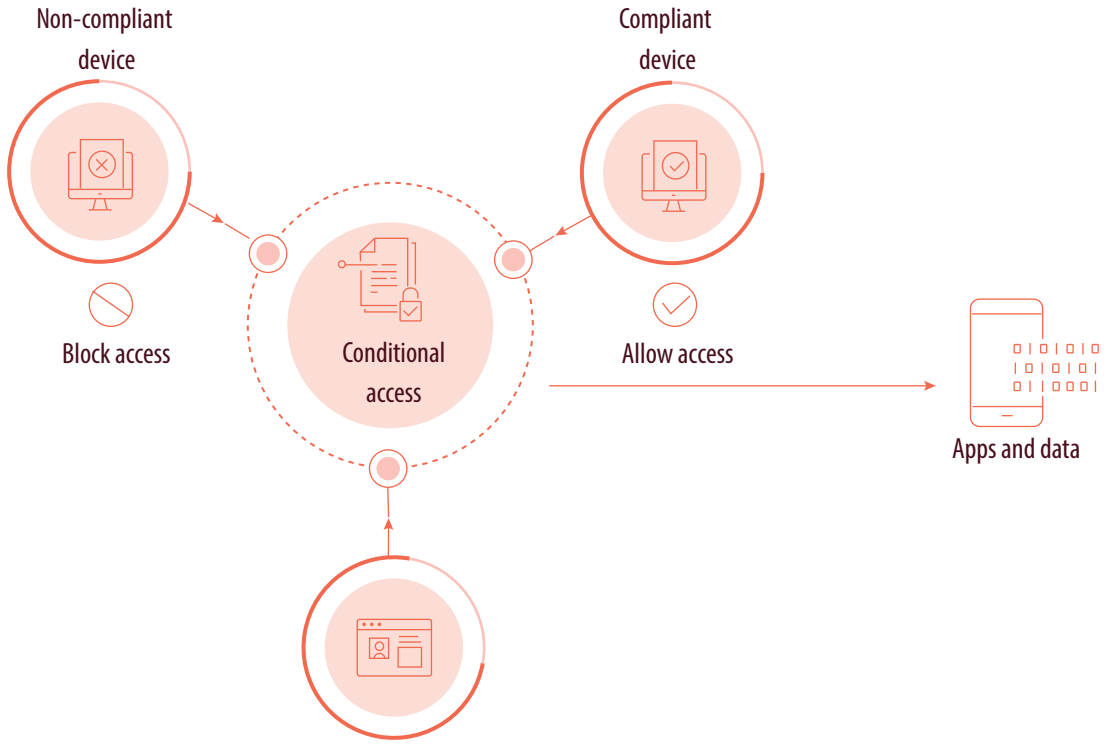
This approach, of giving responsibility to individuals within the organization, demands leadership from the top so that everyone in the business understands that there are no exemptions. Leadership from the top means everything from advocating for budget for training and making sure that training is delivered, to leading by example. That means setting clear examples by actions such as always wearing a lanyard if it's required, not insisting on inappropriate levels of admin access on devices, and making sure that all guests are signed in and that the leader is not bypassing those and other requirements that are enforced among junior colleagues.

So how does this model, of trusting employees to take responsibility for security, sit with the move towards increasing automation and a zero-trust environment?

> A zero-trust organization quashes the idea that everything inside the perimeter is safe. All access is challenged and verified.

The zero-trust model of cybersecurity was initially described in 2010, and since then it has gained popularity. In a zero-trust organization, the notion that everything inside the perimeter is safe is discarded, and instead all access is challenged and verified. That means the lowest possible level of permission to connect to networks, access information, and be allowed into sensitive areas of the building.

Figure 1: Zero-trust and access to assets



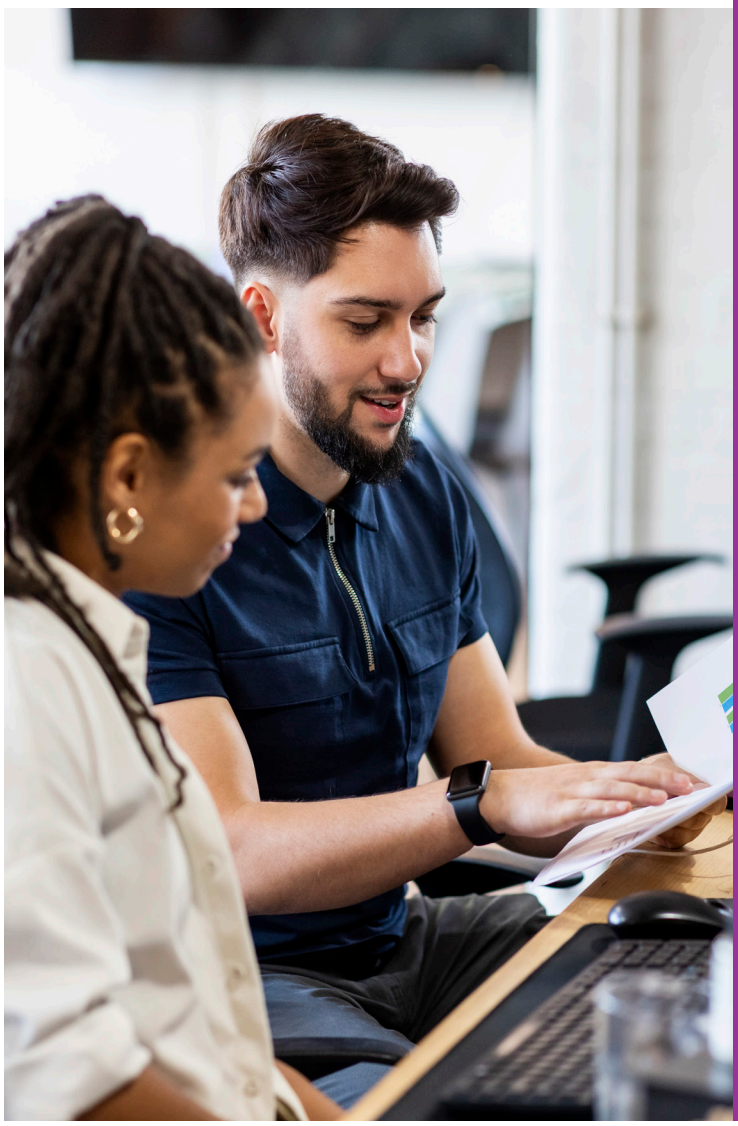
Source: Infosys

Zero trust links into highly automated processes by taking the decision to run updates on a laptop out of the user's control, for example. The only autonomy the user has in this situation is the ability to temporarily defer an update and reboot so that it doesn't interrupt their immediate work.

Even management of patching can be highly automated, turning the process into a zero-touch process for the IT team, thus removing the potential for human error.

With all the effort in cybersecurity teams to make the IT estate management as highly automated as possible, and to limit individuals' access and require them to verify themselves at every step of the way, how then does that fit in with the democratization of security approach, which relies on individuals' alertness and judgment?

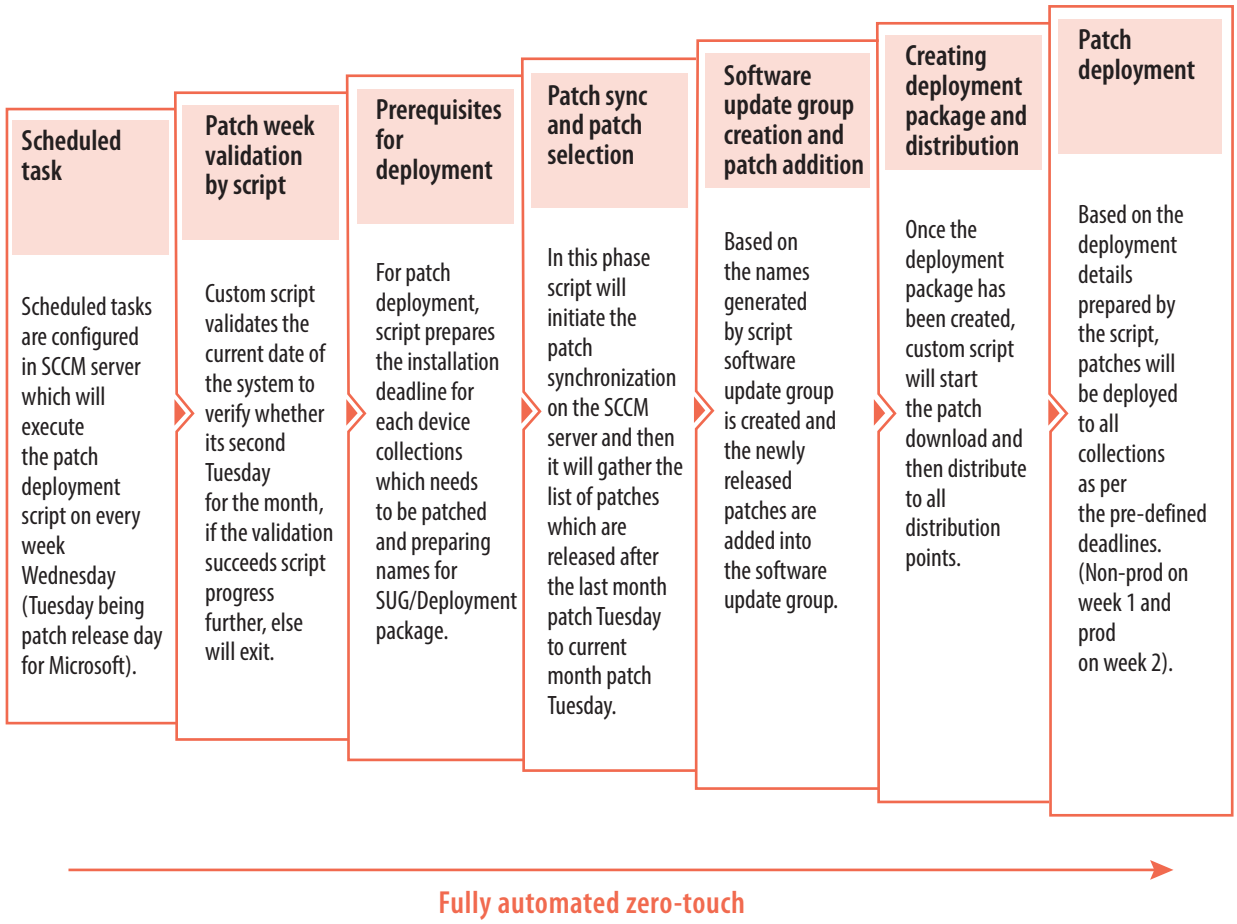
The answer is that highly automated management and zero-trust frees up the employees so that instead of, for example, having to remember to run their updates, they can be wholly focused on the important roles they play in keeping the organization secure.



Cybersecurity is often framed as a "Swiss cheese approach". Slices of Swiss cheese have holes in them, and, to extend this metaphor, a single slice, or single approach to cybersecurity, cannot on its own create a secure environment. However, if you layer several slices of Swiss cheese on top of each other, where one slice has a hole, it will be blocked by another slice that doesn't have a hole in that location on the slice.

Cybersecurity similarly depends on many layers working together. A combination of highly automated defence mechanisms, such as zero-touch patch management, which can see 85% of the business's estate being compliant on patches within a week, using automated tools to manage configuration drift in devices and platforms across the organization, quarantining devices until they are compliant, together with a zero-trust approach that verifies access and a motivated, alert workforce of employees who understand their important roles in keeping the organization secure, will work together to build an organization that is using best practice from across security strategies.

Figure 2: Fully automated zero-touch patch deployment



Source: Infosys

In short, democratization of cybersecurity fits seamlessly into an organization that takes a zero-trust, highly automated approach, and will make businesses safer.

Authors

Kate Bevan

Infosys Knowledge Institute

Sathish I Machaiah

AVP - Practice manager - IT services

Parthiban G

Associate practice manager - IT services

Kiran Bhojaraju

Associate practice manager - IT services, support and operations

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.
To view our research, visit Infosys Knowledge Institute at infosys.com/IKI or email us at iki@infosys.com.

For more information, contact askus@infosys.com

Infosys®
Navigate your next