TANIUM

The inside-out enterprise: Redefining SecOps for today's remote-first workplace

With change comes opportunity.

The inside-out enterprise: redefining SecOps for today's remote-first workplace

The pandemic changed enterprise IT forever. The rapid switch to a work-from-home (WFH) model forced IT organizations to make supporting remote employees the default. IT security and operations processes that assumed employees would always be on premises suddenly became obsolete.

Now enterprise IT teams are adapting to a new IT landscape with a workforce mostly or entirely remote indefinitely. More applications and storage are moving to the cloud. And cybercriminals, watching these changes unfold, are focusing their attention on new targets and new forms of attack.

Compare today's IT landscape to that of a decade ago, and you can see that traditional enterprise IT has been turned inside out. Workers are at home or in other remote locations. Once concentrated in internally managed data centers, applications and data now are distributed across multiple public and private clouds.

In this eBook, we're going to look at three challenges related to managing IT endpoints, including servers, desktops, laptops, tablets, and smartphones — in the inside-out enterprise. These challenges are:

- Asset inventory, vulnerability assessment and patch management
- Help desk responses and employee productivity
- Endpoint security

We show how the inside-out model breaks many of the tools and processes that enterprise IT organizations have relied on for decades. But at the same time, it creates opportunities for a more flexible, agile, and secure IT environment, while improving employee experience.

Asset discovery, vulnerability assessment and patch management

Before you can manage employee endpoints, you need to know how many there are and where they are. You also need to be able to catalog their hardware and software configurations so you can manage software deployments, updates and patches.

In the traditional enterprise, collecting this information wasn't difficult — theoretically. Almost all endpoints were on the internal network. You could run software that scanned the network and discovered them. You wouldn't expect a great deal of variety in endpoints since the IT department had selected and provisioned all the endpoints.

A few remote workers and salespeople might frequently be on the road and have other types of devices (such as MacBooks in an organization that otherwise mandated PCs). But these employees almost always returned to the office at some point. IT personnel could visually inspect their systems. Finding surprises was rare — or so IT organizations believed.

Unfortunately, even in this controlled environment, asset discovery often fell short. Traditional asset discovery tools often overlooked as many as 10-20% of endpoints. Those undiscovered endpoints would then be left out of software updates and patch routines. They became more vulnerable to attack and more likely to jeopardize employee performance and experience.

Today, in a WFH world, all bets are off when it comes to the location, configuration and status of endpoints. Employees use laptops and desktops provided by IT, but they probably use other portable devices, too, including their personal laptops, tablets and smartphones. They use all these devices on home networks and public Wi-Fi hotspots like those in cafes. These devices aren't on the local corporate network. Most of the time, they're not connected to a virtual private network (VPN) either.

If an IT organization wants to ensure that these devices can be cataloged, accounted for, and adequately managed, they must rely on technology that works over ordinary internet connections and doesn't require a VPN.

They need to improve the accuracy of their asset discovery tools, so they can discover and track all devices, not just 80% of them. And since the inside-out enterprise is here to stay, they need to make sure they've got tools for discovering and managing remote endpoints on an ongoing basis, not just once as part of a special, in-depth project.

Help desk support and employee productivity

Another IT function that's been disrupted by the inside-out enterprise is the help desk.

Previously, if an employee had a problem, they could call or email the help desk or service desk. To solve the problem, a help desk agent could talk to the employee, asking questions and offering advice.

If a problem was difficult, the agent could use remote access software to connect to the employee's endpoint. And if the problem proved especially difficult, the agent could walk down the hall, find the employee's office or cubicle, and work with them directly to resolve the problem.

Most of these approaches are now infeasible. Here's why:

- Remote access software usually requires a connection over a local network or a VPN, neither of which is available with today's remote workforces.
- Help desk agents can't walk to employees' desks, since employees work remotely.
- Phone access is still possible but troubleshooting over the phone is difficult. The help desk agent can't tell how the system is configured or see what processes on it are currently running.

There are two solutions to this problem.

1. Enterprises should find endpoint management solutions that allow help desk agents to connect and inspect remote endpoints without requiring a VPN connection. These solutions need to be able to connect securely over standard internet connections, so that even without a VPN, a help desk agent can explore and troubleshoot an endpoint in real time securely.
2. Enterprises should look into self-service options for remote troubleshooting and patching. For example, suppose a help desk agent works with a remote employee and discovers that by upgrading an application, the employee's endpoint performance problem can be solved. If there's a secure self-service portal for application upgrades set up, the help desk agent can simply direct the employee to that portal. The employee can perform the update when it's most convenient, and the help desk agent can return to the ticket queue and begin helping another employee who's asking for assistance.

A self-service model benefits everyone involved. Employees get a speedy resolution to their problems and help desk agents can spend less time on the mechanics of upgrading and patching. Employees are used to installing updates on their personal mobile devices. This model simply takes that practice and applies it to corporate computing, too.

When remote employees can resolve problems more quickly, their productivity improves, and the quality of their work experience improves, too.

Endpoint security

The third area of concern is endpoint security. In the inside-out enterprise, employee endpoints are out of sight and likely out of date in their software patches. Worse, cybercriminals know that employees are more vulnerable working in their remote offices than they are on premises behind a corporate firewall. They're crafting phishing messages and other types of attacks specifically aimed at isolated employees.

Almost three-quarters of businesses in the U.S. and the U.K. have suffered some kind of data breach because of a phishing attack in the past year, according to email security company Egress.[1]

[1] https://www.itproportal.com/news/phishing-attacks-hit-a-huge-number-of-businesses-last-year/

Beyond discovering, updating, and patching remote endpoints, IT organizations need a way to:

- Scan remote endpoints for security vulnerabilities and threats
- Apply whatever patches or configuration changes are necessary to address vulnerabilities and any compliance requirements
- Configure endpoints to close ports and pathways often used by attackers for spreading malware
- Rapidly contain any attack on an endpoint once the attack is detected

Here, too, IT departments need visibility into and control over endpoints without requiring VPN connections. If an endpoint is under attack, you can't expect an employee to launch a VPN connection back to headquarters. IT teams need to be able to access the endpoint as-is — and without launching a new network connection that could potentially hasten the spread of malware.

Without requiring a VPN connection, endpoint security software should be able to:

- Scan and analyze endpoints
- Detect attacks
- Raise alerts about attacks and patch requirements
- Provide security operation center (SOC) analysts with real-time visibility into endpoint activity
- Contain attacks by instantly isolating endpoints

CASE STUDY

Containing a ransomware attack at Ring Power

The benefits of real-time, distributed endpoint management became clear recently to Ring Power Corp., a heavy-equipment dealer based in Saint Augustine, Florida.

When a manager clicked on a phishing email, the company was hit by a ransomware attack that shut down all 150 servers in the company's data center and crippled the 2,300 endpoints its employees relied on for their daily work.

Fortunately, the company had just purchased Tanium solutions for endpoint management, including modules for asset discovery and inventory, risk and compliance management, sensitive data monitoring, and threat hunting.

With help from Tanium, Kevin Bush, VP of IT, and his 10-person team were able to

completely disinfect and restore Ring Power's IT infrastructure in a matter of weeks. And they did so without paying the ransom — in fact, without ever communicating with the attackers at all.

Instead of negotiating a payment, they shut down systems, isolated their backups to ensure they weren't corrupted by malware, physically collected all endpoints from the company's 26 locations, and disinfected every system. They also installed Tanium on every endpoint. Operations resumed with cleaned and now secured endpoints.

"Tanium brings visibility to one screen for our whole team," Bush says. "If you don't have that kind of visibility, you're not going to be able to sleep at night."

Download the full **Ring Power case study here.**

Conclusion

The inside-out enterprise has forever transformed daily life for employees and the IT organizations that support them. This transformation brings challenges, but it brings opportunities, too. Specifically, it gives IT organizations the opportunity to:

- Finally, implement comprehensive asset inventory tools, so that IT organizations can find, manage and secure the 10–20% of endpoints overlooked by traditional tools.
- Gain more accurate and timely information about the status of endpoints, so that they can be patched and updated more quickly and effectively.
- Improve help desk efficiency by enabling agents to connect in real time to endpoints in any location and by empowering employees to solve their own problems quickly and easily through self-service operations.
- Provide remote employees with better endpoint security, so that they can withstand the latest forms of cyberattacks, and so that infected endpoints don't end up compromising large swaths of the corporate network.
- Improve security readiness, so that when attacks occur, they can be quickly and efficiently contained and mitigated (as Ring Power was able to do when they were attacked with ransomware).

The enterprise IT landscape has changed forever. But with the right tools and strategy for endpoint management, this change can serve as the catalyst for great things: more comprehensive and efficient IT operations, improved employee experience, and more robust IT security for employees everywhere, so that at any location on any device, employee productivity remains better than ever.

Learn how Tanium's endpoint management solution can help your organization overcome these challenges in today's inside-out enterprise.