WHITE PAPER

Kollective

STATE OF SOFTWARE DISTRIBUTION

How enterprises patch and secure their systems

2018

INTRODUCTION

Over the last five years, we have seen cyberattacks hit the world's largest organizations. From data breaches at Verifone, TalkTalk and DocuSign, to ransomware attacks on FedEx, Honda and the UK's National Health Service, it's becoming increasingly clear that businesses at the top of chain are just as vulnerable to cyberattacks as those at the bottom.

But are these attacks the result of poor security systems, or do they stem from something far more fundamental to an organization's core IT infrastructure? In the case of last year's WannaCry attack, the devastating breaches were not the result of ineffective security patches, but rather the inability to deploy those patches in a timely and effective manner.

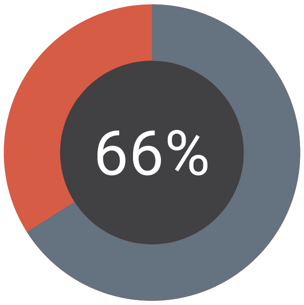
For large enterprises with increasingly distributed workforces, the ability to distribute and ensure the latest software, operating systems and patches are installed is especially challenging. Without the bandwidth or infrastructure to effectively distribute these updates in a timely manner, these organizations are left at serious risk of cyberattack - and many don't even know it.

It is this issue that the following report sets out to explore and address, offering comprehensive insights into the impact that network bandwidth, update infrastructure and software delivery practices are having on the modern enterprise. Drawing upon Kollective's extensive work in this field, this report provides expert insights into how enterprise IT professionals can use a Software-Defined Enterprise Content Delivery Network to keep their systems current and secure.

— Dan Vetras, **CEO, Kollective**

METHODOLOGY

As more business technologies become IP-based, This report incorporates research from 260 IT decision makers from the UK and US. Commissioned by Kollective and conducted by independent research agency Censuswide, all data was collected from a combination of online and phone surveys. Survey respondents were then broken down by company size, with a focus on the number of computer end points used throughout their organizations.



The percentage of organizations that are unable to automate their update/ software distribution.

THE STATE OF SOFTWARE DISTRIBUTION

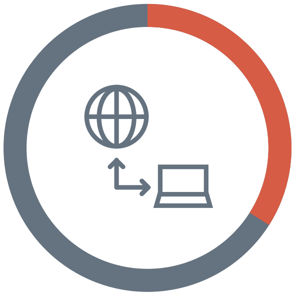
In reviewing the current state of enterprise IT, it's clear that software distribution remains a key challenge.

For the most part, these struggles come down to an ungainly update infrastructure, with many IT managers using a combination of Windows Server Update Service (WSUS), Microsoft System Center Configuration Manager (SCCM) and manually installed updates to keep pace and overcome bandwidth limitations.

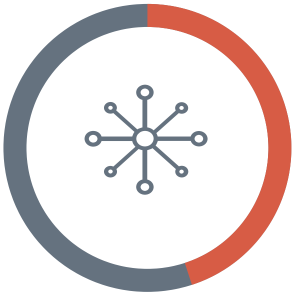
This complex combination of tools is not only making it difficult for IT teams to distribute updates but is also making it harder to guarantee that those updates are being installed.

Faced with this difficulty, **13% of large businesses have given up on managing software distribution and are instead passively requesting employees update their own systems.**

This ad-hoc approach means many IT teams don't know if all endpoints are secure and compliant – creating a security minefield within their own enterprises.

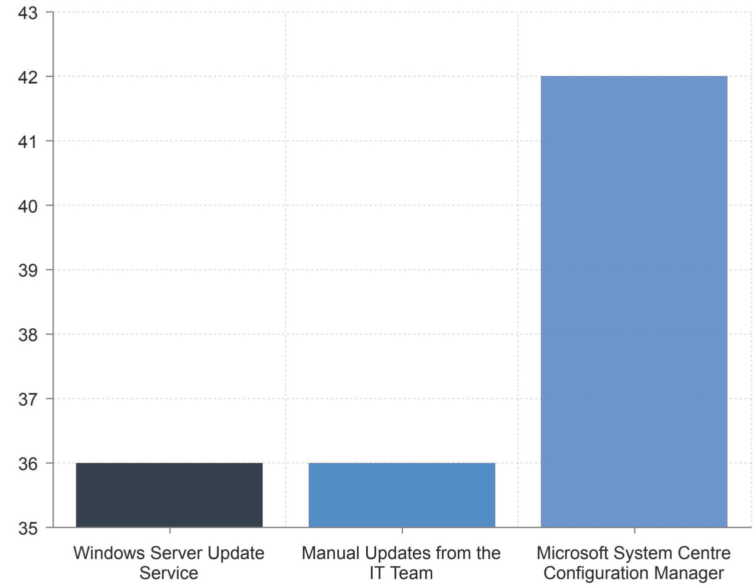


As it stands, 34% of large businesses struggle to distribute content, files and updates across their networks.



For organizations with greater than 100,000 endpoints, this figure jumps to 45%.

HOW TEAMS ARE DELIVERING UPDATES ACROSS THE ENTERPRISE



DISTRIBUTION DELAYS

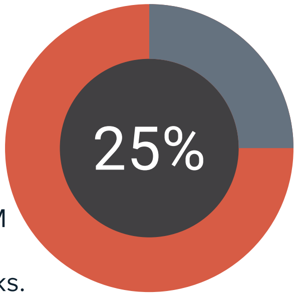
In addition to working within the constraints of their update infrastructure, one of the biggest issues facing large enterprises is the amount of time it takes to roll out new software and patches.

As it stands, 81% of IT teams are unable to deploy software updates when they first arrive. 52% of those in large enterprises must wait a minimum of **7 days before installing vital security patches.**

This delay leaves a significant window of opportunity for hackers to infiltrate unpatched systems, placing businesses at risk.

Unfortunately, application compatibility testing of updates is business critical; the testing process can result in delays IT teams are powerless to hasten.

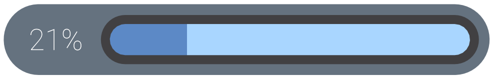
However, changes at the network and infrastructure level can improve the IT team's ability to reach all the endpoints in this shrinking window of time.



Currently, 25% of businesses delay the installation of updates due to network scaling issues.

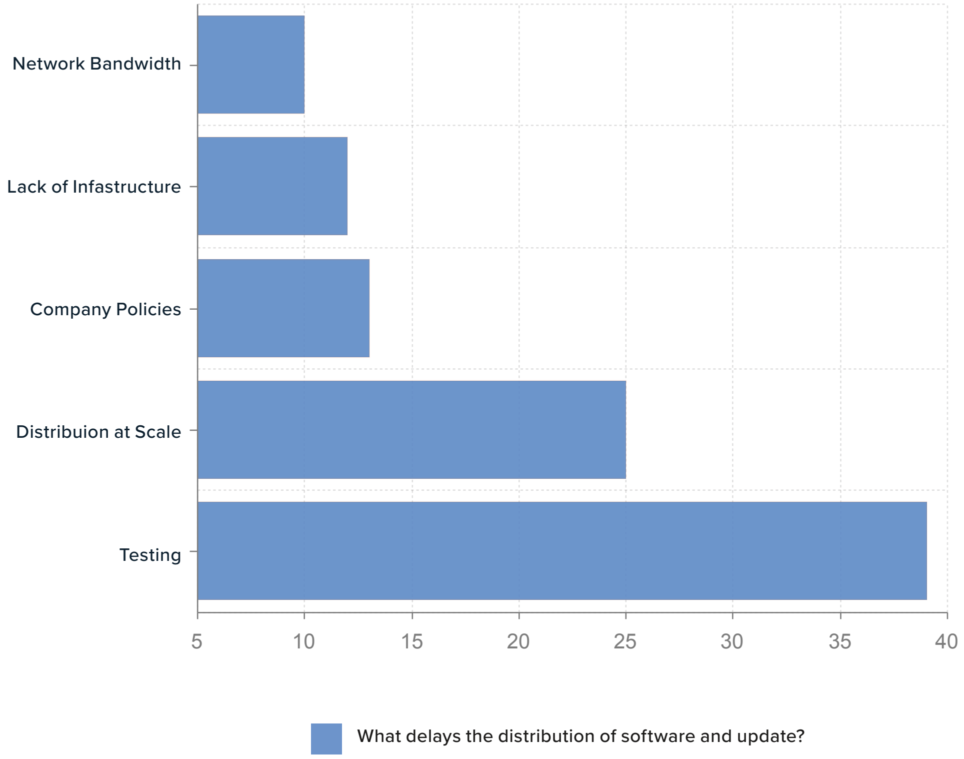
Despite bandwidth and network problems being a known cause, SCCM teams have few resources available to effectively remediate those bottlenecks.

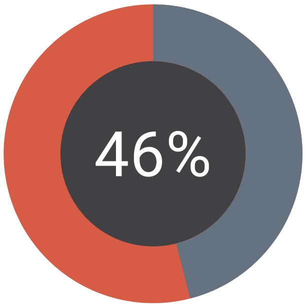
While one way to solve this would be to overhaul the company's network infrastructure, **21% of IT managers say they don't have the budget needed.**



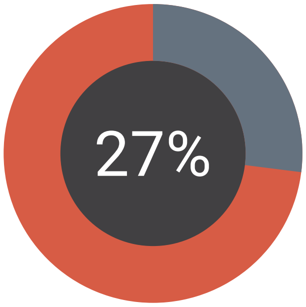
An economical option is to run a software-defined enterprise content delivery network (SD-ECDN), to help manage traffic flow and maximize bandwidth without replacing existing network hardware.

WHAT DELAYS THE DISTRIBUTION OF SOFTWARE AND UPDATES?





of businesses have no plan in place to manage WaaS updates.



of businesses wait a month before installing vital security updates.

WAITING ON WINDOWS

While there is no shortage of security concerns associated with existing technologies, a new challenge is rapidly appearing on the horizon – Windows as a Service (WaaS).

In January 2020, Microsoft will discontinue updates and support for Windows 7, leaving businesses with the option of upgrading to Windows 10 or pay exorbitant support fees to remain on Windows 7.

While Windows 10 comes with numerous benefits for IT teams (and enterprise security as a whole), many have been left concerned by Microsoft's new 'as a service' update model.

Rather than ask users to migrate to a new operating system after a set number of years, Microsoft is compressing that cycle down to a few months, and it continually repeats itself. Now companies will be provided a perpetual stream of updates to their Window endpoints. These large updates come at a monthly pace, with additional larger size updates on a biannual basis, leaving little time for testing and distribution.

For enterprise IT teams that take 1-2 months to roll out new patches, this represents an enormous backlog of updates, presenting a major security threat and potential entry point for future cyberattacks. **As it stands, just under half of IT teams (46%) have no plan in place to manage Windows as a Service updates**, organizations that are servicing in the WaaS model are struggling to leverage existing infrastructures to do so.

But it's not just Windows that is shifting to this update model. As ever more applications and IT service providers move to the cloud, continuous updates will rapidly become the new normal. With this inevitable disruption on the horizon, it's ever more vital that large organizations and those with distributed workforces invest in a software-defined enterprise content delivery network.

UNDERSTANDING THE REAL THREAT

Faced with distribution delays and the difficulties involved with scaling software distribution, ConfigMgr teams are extremely preceptive to the significant threat unpatched systems pose.

Over a third (37%) of IT managers see a failure to install updates as their biggest security threat in 2018. Unpatched software is perceived as a bigger threat vector than password vulnerabilities (33%), BYOD (22%), unsecured USB sticks (9%) and the use of outdated hardware (6%).

Despite understanding the threat posed by out of date and unpatched software, most SCCM infrastructures – particularly those in large enterprises – are not adequately equipped to keep endpoints up-to-date using native ConfigMgr capabilities.

Saddled with budgetary restraints and overly complex infrastructures, ConfigMgr admins tend to work nights and weekends attempting to overcome the limitations imposed on them. **The result is that 27% of enterprises spend at least a month waiting to install vital security patches, while 45% must wait a month or more.**

It's easy to blame budgetary constraints, but the reality is that many enterprises are overspending on reactive heuristics and AI based security technologies to protect their endpoints, when solving the inability to deploy content is the root cause of their security problem.

Only 18% of IT managers see the adoption of a SD ECDN (Software-Defined Enterprise Content Delivery Network) – designed to solve the issue of updating at scale - as a priority. By attaching an on premise SCCM infrastructure to the Kollective cloud platform, a peer to peer delivery mesh is logarithmically created allowing scalability and increasing reliability of software distribution.

The Kollective agent uses machine learning to discover where content is located on its peers, allowing it to shrink bandwidth usage, while maximizing payload size capabilities for SCCM.

TOP IT PRIORITIES FOR 2020

1. The Cloud
2. Windows 10
3. Machine Learning
4. AI
5. Unified Communications
6. BYOD
7. Software-defined Networking

A SOFTWARE-DEFINED SOLUTION

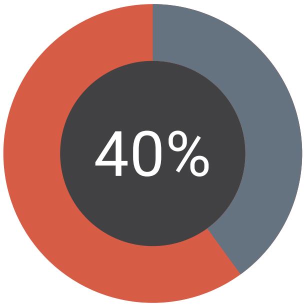
As security concerns grow and Windows as a Service steps to a quicker pace; businesses and IT teams are being thrust into a harsh, new reality of rapid-fire testing and endless features, apps and OS upgrade deployments.

For many large enterprises, a combination of outdated infrastructure and poor network speeds has convinced IT teams that – without rebuilding their network from the ground up – they simply cannot afford to run such updates at scale. Now, software-defined enterprise content delivery networks offer an intelligent, cloud-based alternative.

Software-Defined Enterprise Content Delivery Networks exponentially decrease the bandwidth load on your organization's network. The greater the number of peers across a complex distributed enterprise, the more efficient content delivery becomes – turning even legacy hardware, into intelligent edge devices.

In short, networks that couldn't hope to deliver software at scale, can now do so with ease without interruption to critical business functions.

Using the Kollective SD-ECDN, your business can increase the speed of software distribution, future proof against Windows as a Service updates by attaching SCCM to the power of the cloud and leverage the same SD-ECDN to power live video events and townhalls. This can all be achieved without a costly overhaul to the organization's IT and network infrastructure.



of businesses use a software-defined enterprise content delivery network to stream live internal video.

A single additional component could allow distribution of software and updates.

FIND OUT HOW A SOFTWARE-DEFINED ENTERPRISE CONTENT DELIVERY NETWORK CAN BE USED TO HELP KEEP YOUR BUSINESS UP-TO-DATE

LEARN MORE