RECAST SOFTWARE

How to Manage the Invisible

Bringing Clarity to Distributed Endpoint Infrastructure

Introduction

The proliferation of endpoints within organizations—laptops, smartphones, IoT devices, servers, and more—is not just a trend but a modern reality. With employees connecting from every corner of the globe, the challenges have never been greater or more complex. How do you track, secure, and optimize these myriad devices, each potentially with its own operating system, functions, and vulnerabilities? How do you safeguard your network when the threats are evolving as rapidly as the technology itself?

Within the following pages, you'll explore the multifaceted environment that IT professionals navigate daily. From the intricacies of various hardware to the hidden threats posed by shadow IT, you'll be guided through each layer of complexity. We'll also delve into the critical importance of endpoint security, and the challenges and opportunities presented by the cloud transition.

In addition to outlining core challenges, this white paper provides actionable insights and techniques to enhance your organization's visibility over its IT environment. With expertise backed by research and real-world experience, this guide aims to empower IT teams and decision-makers to grab hold of their elusive visibility goals. Whether you are an experienced SysAdmin, a security expert, or a concerned executive, this report will equip you with the knowledge and tools to better manage the invisible.

Welcome to the future of endpoint management.

The Proliferation and Diversity of Endpoints

The number of endpoints in an organization's environment is constantly growing, making it difficult to track them all effectively. This is especially true in organizations that allow employees to bring their own devices (BYOD) to work. As companies integrate more cloud-based services and IoT devices into their networks, environments become more complex to manage.

Endpoints come in all shapes and sizes, from laptops and desktops to smartphones and tablets. Each type of endpoint has its own unique operating system and software, which can make it difficult to manage them all with a single solution. Plus, hardware extends beyond personal devices to servers, monitors, docking stations, cables, webcams, and more.

Many of you have thousands of devices to manage, a multitude of OEMs (Original Equipment Manufacturers) within your environment, and dozens or even hundreds of software titles deployed. Based on our recent report*, many organizations struggle to holistically and actively manage their endpoints, software, and peripheral hardware. Hardware management, for instance, continues to reside on internal spreadsheets for too many organizations.

With the endless diversity and growth in endpoints, the natural progression leads to another pressing concern: the complexity of securing them. Let's delve into this crucial challenge.

Many organizations struggle to holistically and actively manage their endpoints, software, and peripheral hardware

* The State of System Administration White Paper

The Complexity of Endpoint Security

Many organizations use a variety of software tools for endpoint management, each providing control of and visibility into different aspects of the environment. However, these tools often don't integrate well with each other, creating silos of information that can be hard to consolidate. Effective management and decision-making can suffer as a result.

The cloud transition, for instance, brings promise and excitement. But how do organizations transition significant on-prem architecture, physical resources, and management platforms to the cloud? Are cloud management capabilities ready for all aspects of on-premises infrastructure management? Some organizations are calculating the expense of a successful, secure cloud transition and the following cloud-state management. After reviewing the numbers, some of these organizations are considering different states for different types of endpoints or collections to more cost-effectively and securely manage their environments.

IT environments are also dynamic, with devices constantly coming online, going offline, and changing status. Keeping up to date in real-time challenges many organizations, especially when the consequences of delays can result in blind spots and increased security risks.

The risks of unpatched software, including third-party titles, demands attention as well. In 2021, software vulnerabilities became the leading cause of the costliest breaches, outpacing phishing for the first time. 54% of SysAdmins polled by Recast Software* either patch software internally or do not actively manage software updates.

The intricacies of endpoint security are further compounded by hidden threats within organizations. Shadow IT represents one such lurking danger that needs attention.

54% of SysAdmins polled by Recast Software either patch software internally or do not actively manage software updates

* The State of System Administration White Paper

Shadow IT Lurking in the Darkness

Shadow IT is the use of unauthorized IT resources by employees. This can include personal devices, cloud-based applications, and unapproved software. Because shadow IT is not officially sanctioned, these devices and systems often go unmonitored, reducing overall visibility.

Understanding the hidden risks of Shadow IT sets the stage for our next critical discussion: how to grab hold of those elusive visibility goals. Here, we will explore actionable strategies for achieving clarity within your infrastructure.

How to Grab Hold of Elusive Visibility Goals

Engineer for Clarity

In the labyrinth of today's digital landscape, visibility within your IT environment rises high as both a critical challenge and a central goal. From monitoring and tracking activity to managing software to ensuring encryption, the ability to see and control your environment is paramount. Unveil strategies, tools, and best practices to engineer for clarity within your system, allowing you to detect, protect, and respond effectively. When you're seeking to optimize compliance and minimize threat exposure, a comprehensive visibility approach serves as a guiding beacon.

Shadow IT can include personal devices, cloud-based applications, and unapproved software

Monitor and Track Activity

Your team needs to see the details of all activities within your environment and on your endpoints. What processes get executed? Where were they executed? By whom? What files were accessed? These are but a few of the essential visibility needs for modern IT teams.

Effective and secure management requires the ability to detect configuration changes within your environment. With edit logs, you can audit your environment to check for any drift from your established settings. Drift impacts your company’s alignment with compliance and regulatory standards and increases your threat exposure as well.

For example, someone may modify server configurations or change local firewall policies that open up the device to unnecessary and unwanted traffic. This action softens the overall security of the device and in turn the broader environment. Proper audit logging makes identifying and correcting this change simpler. Teams can also then identify and address the source of the change.

Monitoring is made more effective by gating admin rights and then tracking all access to the controlled usage of those gated rights. While simple to say, we all know IT teams spend hours deliberating and planning for admin rights control and management. In the face of obstacles like push back by end users, concerns from Help Desks, and challenges with managing privileges, organizations are served well to tackle the issue head on.

Some privileged access management (PAM) solutions require significant time and resource investments. However, other PAM solutions exist that can be implemented more quickly and managed with concise training.

Monitoring your environment’s activities and attributes is vital to securing endpoints and identifying unauthorized actions. Gaining better visibility also allows your security team to take advantage of threat intelligence, helping to identify threats and respond in a timely fashion.

Employ Comprehensive Inventory Management

Comprehensive inventory management provides a 360-degree view of all hardware and software within an organization's environment. This doesn't merely catalog what exists; it's a dynamic tool that continually updates, reflecting changes in real-time.

What sets comprehensive inventory management apart is its ability to facilitate decision-making. By centralizing data on hardware, software, versions, and usage, IT teams can optimize resources, eliminating redundancies and ensuring that essential tools are available when needed. Inventory awareness and management is a vital early step to secure your environment.

Manage Software Actively

Organizations need to quickly update operating systems and third-party software to improve their cybersecurity position and reduce risk.

Organizations have two main options:

- Invest in a robust internal team capable of monitoring, packaging, testing, and deploying patches across your entire application ecosystem. Ensure the team can monitor and patch through holidays and extended leaves.
- Utilize software that automates all aspects of patching, including the monitoring of all necessary software titles.

In-house patching teams can take on the task of patch management. This strategy requires a significant investment in FTE (Full-Time Equivalent) and mandates weekend and holiday coverage. The manual process involves piloting patches, prepping patches for preproduction, testing patches in production groups, and then pushing the patches company-wide. New patches are released regularly, often 10-20 patches per year per software title.

Third-party patching software automates the monitoring of patches across hundreds of titles, and then follows up by packaging, testing, and deploying the software patches. **Security teams find great value in automating both the monitoring and patching process, which reduces human error.** Depending upon your environment, accounting and management often also appreciate the move to an automated patching solution. Patching software tools can provide significant ROI (Return on Investment) when weighed against the FTE needed to patch effectively and the economic and reputational impact of threat exposure that results from human error in the in-house monitoring and patching process.

Learn more about patching best practices in our eBook, "Reduce your Attack Footprint."

Add Visibility Capabilities

Without thorough visibility into your assets and users, you are a BMW on the Autobahn driving with a blindfold on—you are in imminent danger. To "drive" safely, centralize your data on hardware, software, and usage. Single pane solutions enable powerful, nimble IT teams that can manage environments as they scale.

But visibility isn't only about what you have; it's also about who has access to it. Role-Based Access Control (RBAC) can assist you here. RBAC allows IT teams to define precisely who can access what within the network based on specific roles and responsibilities. RBAC adds a substantial layer to your security protocols. By ensuring that only authorized personnel have access to critical assets, RBAC helps minimize the risk of internal threats. It also aligns access controls with compliance requirements.

Finally, insights into your security and encryption tools, like LAPS and Bitlocker, confirm their implementation while allowing for functional maintenance and support. These security tools build a robust shield, encrypting critical information and fortifying your endpoints.

Seeing is Essential

As organizations manage the intricate maze of distributed endpoint infrastructure, clarity is more than desirable—it is essential. By embracing best practices and leveraging powerful strategies and tools like third-party patching software, RBAC, and comprehensive inventory management solutions, organizations can cast a bright light into the shadowy corners of their environments. The path to effective, efficient, and secure endpoint visibility is within reach.

> "The ability to evaluate inventory based on multiple options has really allowed us to refine our IT needs to specific machines instead of going to each machine to find out it's status of a program or its age. Countless people hours saved!"
>
> — Bill, Systems Operations Supervisor, Utilities Sector

Recast Software

We're obsessed with information technology and how to better manage it.

We are a dedicated group of Systems Administrators and tech-savvy product experts that love what we do and the IT community we do it with.

We empower organizations to better manage and support users and devices.

We are a rapidly growing software company with our solutions being used by thousands of enterprise organizations in more than 125 countries, impacting millions of devices and (more importantly) the people who use them. With our growing portfolio of tools, we empower IT departments at every single endpoint to do their best work.

Learn more about
Recast Software here.