How Endpoint Security Management platforms, and the right partner, can mitigate the security risk of increasing numbers of unmanaged and unseen endpoints
Digital transformation has ushered in a new era of greater business agility, innovative customer experiences and improved productivity. These changes have been great for users and businesses overall, but they have created new challenges for IT security. In creating those new digital experiences and efficiencies, digital transformation has put power in the hands of mobile users both inside and outside the network perimeter and increased IT’s reliance on cloud services and the Internet of Things. The resulting lack of visibility and control can make it difficult for the CISO and their team to identify and manage security gaps, something that is exacerbated by the current need for mass remote working. The endpoint visibility gap in particular challenges IT teams to definitively state that they both know where their assets are and whether or not they are protected.

CISOs also worry about finding employees with the skills necessary to address these risks. Whilst there are shortages in general security skills across the industry, there are specific skill shortages that become apparent as soon as organisations begin seriously evaluating how to secure the new digitally transformed endpoint estate. CISOs might look to specialist endpoint management toolsets and technologies to help them, but these are complex solutions. By choosing a powerful endpoint security and management platform, cybersecurity buyers have certainly gone a long way to addressing the challenge of security visibility gaps, but they may find it difficult to manage and optimise their investment.

This is where third-party expertise and resources can really help. Outsourced and out-tasked support, management and operation of both Endpoint Management platforms and endpoint security services, such as applying patches, allow the CISO and their team to concentrate resources on more strategic and technical activity. Also, by taking on the risks of staff recruitment, training and retention, third parties help organisations benefit from levels of scale and flexibility that are difficult to achieve with in-house teams alone.
THE CUSTOMER CHALLENGE

IT functions in large organisations have always fought hard to gain the insight they need to effectively manage risk across the enterprise. But with the combination of digital transformation, rising threat levels and the current distributed workforce this has become a much more challenging battle. With more and more endpoints entering the workplace, there is now a much bigger threat surface for security teams to patrol. The need to identify endpoints and their locations, assess endpoint security and respond quickly in the event of a compromise, has never been more pressing. Unfortunately, this critical work is made more difficult by the following:

IT BLIND SPOTS LIMITING EFFECTIVE RISK MANAGEMENT

Ninety-four percent of global CIOs surveyed by a leading Endpoint Security Management vendor revealed they were regularly discovering endpoints in their organisation that they were previously unaware of, and nearly three-quarters (70%) were doing so on a daily or weekly basis.¹

What’s causing these visibility gaps? Contributing factors cited by respondents included:

**Siloed IT operations** and security teams – often stemming from long-standing cultural/organisational issues – reduce IT visibility and agility. With no single owner of endpoint security, blind spots can easily emerge.

**Limitations in resources** make it difficult to effectively manage the security of the IT estate. Competing priorities, complex tooling operation and support requirements and increasing compliance all contribute to a lack of consistent visibility and control of the endpoint estate.

**Legacy systems** are often operated outside of formal customer processes because of difficulties in integrating them. Lack of process automation can result in a lack of visibility and awareness of vulnerabilities, plus a lack of resource to keep legacy systems at the right level of security.

**Shadow IT** practices prevail, including end users introducing endpoints without the usual corporate governance required for proper asset management, rendering these devices invisible to endpoint security teams and tooling.

**Tool overlap**, stemming partly from a lack of integration or optimisation of existing endpoint security and management solutions, often creates a confused or inconsistent picture of the security status of endpoints.

Without consistent visibility into the status of their laptops, servers, virtual machines, containers, cloud infrastructure and other digital assets, IT teams don’t know where these endpoints are, how many there are, and which are vulnerable at a specific moment in time. This in turn means it’s difficult to apply patches quickly when a critical vulnerability is published or take pre-emptive action to improve cyber resilience.

Lack of visibility also exposes organisations to the potential of regulatory investigations if they can’t provide detailed information fast in the event of a serious breach.

ENDPOINT SECURITY SKILLS GAP

Whilst skills shortages and gaps are unprecedented across the security industry in general – there are now over four million unfilled security positions globally, including 291,000 in Europe, according to some estimates – the biggest gaps appear to be in security operations and security administration.² These gaps are most pressing in organisations over 5,000 seats in size. As management of endpoint security typically falls within these functions, many organisations are considering accounting for their lack of human resources by investing in unified endpoint management platforms engineered to detect risk automatically.

However such an investment raises the question of whether organisations need to seek external support to help with the challenges of deploying, managing, and maintaining such complex platforms. Even where organisations do have the in-house support and expertise they need, it is often a challenge for these skilled employees to find time for monitoring, managing, and optimising these platforms, while also attending to their other day-to-day duties in the IT organisation.

REMOTE WORKING

The current need for mass remote working has added further complexity to the IT environment, creating new endpoint blind spots and infrastructure challenges. A separate study by Tanium found that two of the top challenges for UK organisations during the pandemic were: identifying new personal computing devices on the network (28%) and overwhelmed IT capacity due to increased usage of VPN (22%) by remote workers. The same study also found that nearly all (92%) of organisations surveyed had also shifted to a distributed security workforce during the pandemic and had delayed or cancelled key security projects.³

An additional impact: more remote working, challenges in keeping track of endpoints outside of the traditional corporate perimeter and more strains on security resources and process has made the management and security of endpoints much more challenging to undertake.
**Selecting the right Endpoint Security Management solution**

Ideally organisations should be looking to unify endpoint management and security capabilities in a single platform to solve their most complex endpoint security challenges at speed and scale. Security teams need information instantly, so they can identify and qualify security issues quickly and remediate at scale to deploy patches, install software and make complex configuration changes reliably.

Traditionally it has taken days or weeks to accomplish demanding security and operations tasks. But with the right tools, your organisation could accelerate this work to mere seconds, to deliver real-time visibility and control of the entire endpoint environment. There are many solutions on the market that can help to better manage and secure endpoints.

To implement the most effective endpoint security, organisations should look for providers that offer:

<table>
<thead>
<tr>
<th>Visibility and control</th>
<th>Speed and scale</th>
<th>A single platform and agent</th>
<th>Integration with ecosystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>of endpoints to discover, manage and secure endpoints across the estate. Reduce the attack surface, fortify endpoints and identify and react rapidly to emerging threats with EDR, vulnerability and configuration management</td>
<td>supported by an underlying architecture that enables teams to gain rapid visibility and control across thousands or millions of assets.</td>
<td>to improve coverage and streamline work. Multiple tools can create confusion and security gaps. Consolidating onto a single platform means a single version of the truth to unify security and operations teams around. In addition, the smaller the footprint of the platform the easier it is to manage and support.</td>
<td>of leading CMDB, SCCM and SIEM providers such as ServiceNow, Salesforce, Splunk and Microsoft to drive down TCO, increase ROI and add value.</td>
</tr>
</tbody>
</table>

Choosing the right Endpoint Security Management tool is challenging given the size of the vendor marketplace and the number of competing solutions. Many organisations will do this in-house using procurement teams to drive the selection process. Whilst this is a perfectly acceptable approach, the complexity and specialism of Endpoint Security Management solutions could mean that involving a partner with specific knowledge could be more effective.
Finding the right partner

For most organisations, an effective strategy for endpoint security includes finding the right partner – that is, finding a partner who can ensure that a chosen Endpoint Security Management tool is deployed in the most effective way and who can provide the key skills needed for supporting the tool, running day-to-day operations and road-mapping future changes and optimisations.

There are several third-party organisations who will be able to help here. However, the most effective engagement is with partners who can sit across all areas, offering a fully packaged service that covers everything from tooling assessment and selection, procurement of product licensing, and design, build and implementation of the security platform, through to ongoing platform management with overlaid security services, and insight as to how to further leverage the technology for future optimisation.

Look for partners that can add value in three key areas:

**SOURCE**

Engaging with the vendor and chosen distributors to source the most appropriate licensing model for each customer. Provides guidance and advice on best use cases, how to build ROI and module selection and pricing. Getting the right price is important, but getting the right product is more so. Organisations that understand the security market and have relationships with all key security vendors is essential, as is the ability to procure at scale and speed.

Choosing a partner that can do all of this, one that understands the marketplace for Managed Endpoint Security and who can help organisations to choose the right tool at the right price will help to ensure any investment is worthwhile.

**TRANSFORM**

Access to highly skilled professional services teams to help design, build and implement the solution is advisable. Given the challenges with complex tooling configuration and design, it is important that an experienced partner offer professional services to help implement the selected Endpoint Security Management solution. Partners should be able to help in the following ways:

**Strategy and advisory services**

Helping to understand business requirements, aligning investments to customers’ strategic priorities and understanding any impact on current state.

- Partners should have a detailed understanding of the endpoint security marketplace
- The ability to assess and critique different vendor offerings, providing insight into product feature sets and functionality in the context of customer challenges
- Partners should be able to offer proof of concept (POC) or proof of value (POV) services at very low/zero cost to the customer to help demonstrate value and support business case development

**Design and build services**

Ensuring that any endpoint security tooling design and implementation is undertaken in a structured way that includes the following high-level activities:

- Technical Initiation Workshops with key customer stakeholders from both business and IT
- Production and the development of both high-level and low-level designs
- Impact assessment and deployment plan
- Design for integration with aligned systems and tools
- Configuration of base-agreed rules and discovery queries

**Handover into Business as Usual (BAU) support**

Ensuring that once the platform is implemented, the customer is fully prepared to support it. At a minimum, any partner should evidence experience in the following areas:

- Training operational teams
- Documenting processes and creating operation run-books
- Creation of implementation guides and documentation of build architecture and design
- Documentation of support processes between the customer and the vendor

**Product optimisation and development**

A truly effective partner will want to remain engaged post implementation to continue to advise customers on how to optimise their deployment. The partner should offer:

- Access to vendor product roadmaps and planned releases and upgrades
- Professional services to provide resource to manage version upgrades, integrations and major releases
- Support to turn on additional features and functionality
- Support of the development of business cases for further investment and optimisation, integration or automation
MANAGE

With many businesses looking for help from endpoint management tooling solutions, the promise of greater control, more visibility and opportunities for consolidation and automation, tooling solutions would seem the perfect answer. However, for organisations wanting to realise these benefits of these technologies, there are the following considerations:

• Do they have the required knowledge and experience to support and operate such technologies?
• Given the importance of such tools, and the resultant business expectations for high availability, can in-house teams scale to meet 24x7 SLAs?
• Do they have an ability to utilise the full range of platform capabilities and ensure their deployment is at the optimal level required to deliver real benefit?

In short, most IT customers implementing Endpoint Security Management solutions need a minimum of two operation and support staff dedicated to their chosen security platform.

Organisations unable to provide this level of support in-house may struggle to realise the benefits of any platform they invest in. Should they instead decide to outsource this work to a partner, that partner should be able to offer the following services to support an Endpoint Security Management platform:

Incident Management and Incident Resolution
• The partner should be able to resolve incident tickets assigned to them by the customer, in their role as a technical resolver team
• Conduct incident root cause investigations
• Act as an intermediary with the vendor to co-ordinate the resolution of any level 4 technical issues
• Co-ordinate the resolution of break-fix issues

Problem Management and Problem Investigation
Contribute to problem investigations relating to the Endpoint Security Management platform.

Change Management and Change Implementation
Contribute to the customer’s change process and take responsibility for any technical aspects of a change relating to the Endpoint Security Management platform.

Request Management and Request Fulfilment
Undertake request fulfilment when they receive a request work order through the customer’s ticketing system.

Service reporting/Daily checks
Run diagnostic reporting to assess any daily performance and identify issues not picked up by the customer application monitoring.

Additional Managed Services
Operate additional overlay managed services on the customer’s instance of the Endpoint Security Management platform - for example, Patch and Vulnerability management, if requested.
CONCLUSION

IT security leaders are struggling to mitigate cyber risk effectively across their entire endpoint environment. Digital transformation and remote working trends have only increased IT complexity and gaps in endpoint visibility - and cyber-criminals have proven they're more than capable of exploiting these blind spots. As security teams, particularly those in operational and administrative security roles, become more resource-constrained, the best way for organisations to mitigate the risk of unmanaged, unseen endpoints is to invest in an Endpoint Security Management platform. A solution that can provide the visibility and control needed to help detect and thwart security attacks, overcome any internal resource shortages and provide additional integrated services for identifying risk, remediating at scale and speed, and streamlining important security tasks such as patch and vulnerability management.

The challenge for CISOs is that few have the in-house skills and resources to maximise ROI and successfully customise these Endpoint Security Management platforms to their specific SLA and availability requirements. As such identifying a partner to support the customer through vendor selection, POC, procurement, design, build and implementation and then run services ensures any investment has a more concrete return.

DELIVERING VALUE TO CISOs

Tanium offers an industry-leading way to tackle such challenges, using a unique high-speed architecture which allows customers to detect and manage their IT endpoints in real time - whether they're physical computers, virtual assets in the cloud or remote systems. Computacenter offers an end-to-end managed solution built around the Tanium product set, covering everything from sourcing to transformation to management. With decades of experience in the security market, powerful ecosystem relationships and a multi-year Tanium partnership, we have the expertise, the skills and the scale to ensure our customers always get the best outcomes.

With Endpoint Security Management, powered by Tanium, Computacenter will:

- **Take the risk** to recruit, train and retain market-scarce skills to operate and support Tanium
- **Get close to customers** through day-to-day operation of the platform, enabling us to provide advice on additional optimisation, such as customised reporting
- **Provide scalable support** and free up in-house teams to focus on strategic tasks
- **Understand** the Tanium roadmap to drive continuous value going forward
- **Leverage understanding** of other customers and how they use Tanium to improve our services for all
- **Use our ecosystem experience** to optimise integration opportunities

In short, we know the market, the vendor and our customers inside out. Managed by Computacenter, Tanium can become a key strategic value driver for the security function and the wider organisation.

SOURCES
1 - https://www.tanium.com/resources/mind-the-endpoint-visibility-gap
2 - https://www.isc2.org/Research/Workforce-Study
3 - https://world-at-home.tanium.com
ABOUT COMPUTACENTER
Computacenter is a leading independent technology partner, trusted by large corporate and public sector organisations. We help our customers to source, transform and manage their IT infrastructure to deliver digital transformation, enabling users and their business. Computacenter is a public company quoted on the London FTSE 250 (CCC.L) and employs over 16,000 people worldwide.

www.computacenter.com

LET’S TALK
To discover how Computacenter and Tanium can help you find, then close the security gaps in your endpoint estate, please contact:

COMPUTACENTER  SecurityEnquiries@computacenter.com  +44 (0) 7834 650 509

TANIUM  info@tanium.com