IDC ANALYST CONNECTION

**_Phil Hochmuth_**
*Program Director, Enterprise Mobility and Endpoint Device Management*

# Endpoint Management: New Challenges Posed by Today's Cyberthreats and Security Threats

*August 2018*

*Endpoint management, while broad from a technology standpoint, is moving in a definitive direction — the ability to centrally discover, provision, deploy, update, and troubleshoot endpoint devices within an organization. The proliferation of laptops, desktops, and more will propel the worldwide market for unified endpoint management software to grow from $3 billion in 2017 to $4.5 billion by 2022.*

The following questions were posed by LogMeIn to Phil Hochmuth, program director for IDC's Enterprise Mobility and Endpoint Device Management practice, on behalf of LogMeIn's customers.

**Q. What are the key trends around endpoint management and the latest cyberattack methods?**

A. The biggest themes around endpoint management and threats are the diversity and proliferation of endpoints and the breadth of attack vectors this proliferation provides. In the past, IT professionals had a finite number of endpoints to manage and secure, and these endpoints were under their direct control. However, in the past several years, bring your own device (BYOD) and the remote workforce have changed the way people work, causing IT teams to rethink how they manage and secure endpoints and their company's network. Changes in the workforce, work styles, and the device market are contributing to this current hyperalert and high-risk state.

Attacks on end-user devices are also becoming more targeted. We're seeing increasingly sophisticated attacks, with malware, ransomware, and data breaches topping the list of concerns for IT professionals. The majority of IT teams are attempting to tackle these security risks, but much more progress needs to be made to secure the endpoint infrastructure.

**Q. How are IT teams set up to handle sophisticated attacks?**

A. The platforms that infrastructure management teams use are still quite segmented, and there are a lot of overly complex solutions in the market to choose from. The use of separate tools by disparate groups leads to inconsistent policies and limited visibility into threats. On top of the separate and complicated options available, IT teams tend to wear a lot of hats, and they simply don't have the time to waste on implementing a multitude of software solutions to secure their endpoint infrastructure. The majority of IT teams are not set up well to handle these attacks because they spend a lot of their time managing recurring/remedial tasks and manual processes as opposed to focusing on strategic tactics to improve security. This means IT teams are implementing a reactive approach and playing on the defensive when handling risks; therefore, it's only a matter of time until a data breach occurs.

**Q. What are the biggest mistakes internal IT organizations can make in terms of endpoint management?**

A. One of the biggest mistakes IT organizations make around endpoint management is to not have "eyes" on large groups of connected devices. Lack of visibility into or unawareness of IT assets can extend beyond physical devices to cloud services and applications. Seventy percent of successful breaches originate at the endpoint, so given this compelling data, it's both crucial and urgent for IT professionals to consider scanning their endpoints to spot and remediate vulnerabilities.

Another mistake IT organizations can make around endpoint management is spending too much time on manual tasks. There are powerful tools that enable IT professionals to remotely deploy and automate routine IT tasks and take back their time. They need to use them!

Implementing a reactive approach to security is another big mistake. The shift from a reactive approach to a proactive approach is absolutely necessary because it allows IT teams to address security threats before issues and breaches occur. To be proactive, IT organizations need to have a single pane of glass view into the endpoint infrastructure and the ability to remotely access any endpoint at any time, so best-in-class unattended remote access capability becomes simply a table-stake, must-have feature.

**Q. What is the cost of making mistakes around endpoint management?**

A. Companies are paying prohibitive costs as a result of each successful attack.

Compliance violations are also major concerns for most organizations with regard to endpoint security device monitoring. According to IDC's 2018 *Enterprise Mobility Survey,* IT professionals cited compliance violations as their top concern and the problem they experienced most frequently.

Data loss is another top challenge. This risk increases if endpoints are left unchecked, unmanaged, or undermanaged from a security and configuration standpoint. With multiple, hyperconnected devices used in an organization, it's easy for data to move quickly to insecure or untrusted locations. Fines for data breaches and lost customer information, or even the presence of certain data types on noncompliant devices, can reach the $500,000 range in industries such as healthcare and financial services. The new GDPR rules in the European Union — which affect any firm operating or doing business in the region — add another level of potential compliance risk.

Companies can get dinged, even hit hard, by fines and penalties for noncompliance due to poor endpoint device management. Worker productivity can be impacted as well. Business productivity drops if workers can't access new applications, IT resources, or other tools to do their jobs because of misconfiguration of systems, outdated versions of operating systems or client software packages. The problem becomes more acute as workers access business software platforms from a broader range of devices and device types. The rapid update cycles of applications and modern operating systems are also a factor in end-user productivity. IT needs to ensure the tools deployed to users are 100% accessible and usable. To that end, ensuring up-to-date software — in terms of the latest versions as well as patches — is paramount.

**Q. What are mission-critical capabilities that organizations should look for when evaluating an endpoint management solution?**

A. Endpoint visibility and support capabilities are critical. This could be either a single platform or a collection of interconnected or interoperable platforms that provide common reporting and visibility (at minimum). Optimally, the endpoint management platform should allow IT to push common tasks and critical software updates across all endpoints (e.g., patch management, proactive alerts to monitor computer health, self-healing processes, antivirus capabilities, and automated task management asset management).

Another key criterion is openness, in terms of technical interoperability and from a supported partner perspective. Organizations should look for platforms with open API support for standard interoperability with other platforms. (This can get you closer to the interconnected "system of systems" approach to converged endpoint management and security.) The last key piece to look for is simplicity. The opportunity to implement a solution with an intuitive and user-friendly interface that shortens training and streamlines support should not be overlooked.

## ABOUT THIS ANALYST

*Phil Hochmuth is the program director on IDC's Enterprise Mobility team. His research provides insights into how enterprises deploy mobile devices and applications as well as management and security platforms. Key markets he covers include enterprise mobility management (EMM) and enterprise mobile security, including mobile data and threat protection and mobile device security technologies.*

## ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

## COPYRIGHT AND RESTRICTIONS

For more information on IDC, visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com