Organized attackers

While the trend towards remote and mobile work delivers tremendous efficiency gains to most organizations, it has also turned your endpoints—from laptops and smartphones to Internet of Things (IoT) devices—into your weakest security link. In addition to launching ransomware and increasingly sophisticated malware attacks, cybercriminals have also begun targeting endpoints with "file-less" attacks that can't be detected by traditional anti-virus technologies. The threat to organizations of all sizes, in all sectors, is consequently growing—while the financial repercussions spiral out of control. Today, the total average cost of a successful endpoint attack is over $5 million in lost productivity, system downtime, data theft, damage to the IT infrastructure, brand damage, and fines.

Disorganized responses

Although endpoint security continues to evolve, most existing solutions lack comprehensive coverage or lack effective configuration or operational processes, requiring organizations to adopt disparate products with overlapping features and functionality. As a result, organizations end up with disjointed and duplicate technologies, integration challenges that limit access to shared intelligence, and difficulty creating a customized environment—especially when implementing off-the-shelf solutions. Worse still, these incompatible security solutions can leave gaps in protection that attackers can exploit.

Limited resources

As the technology infrastructure becomes more complex, organizations are struggling to find the expertise and resources necessary to monitor and manage endpoint risk. Competition for qualified security experts is fierce and hampered by serious budget constraints. The need to do more with less also means IT teams tend to focus on core essential tasks rather than making sure all technology remains up-to-date.

Charting the challenge

What types of threats do organizations face? Where are you most vulnerable to attack? And how can you effectively defend your networks and respond in the event of a breach? Here's a high-level look at the threat landscape—as well as strategic steps you can take to help gain an edge on cyberattackers.

Threats
Who's coming for you?

The threats to your endpoint security can be external or internal.

External

- Phishing, spearphishing, and whaling
- Malware/ransomware
- Distributed denial of service (DDoS)
- Advanced persistent threats (APTs)
- Botnet attacks
- Attacks that use macros and scripts rather than malicious executable files

Internal

- Compromised internal users, contractors, or third parties
- Accidental misuse or disclosure by employees
- Partners, joint ventures, etc.
- Service providers and system/application vendors

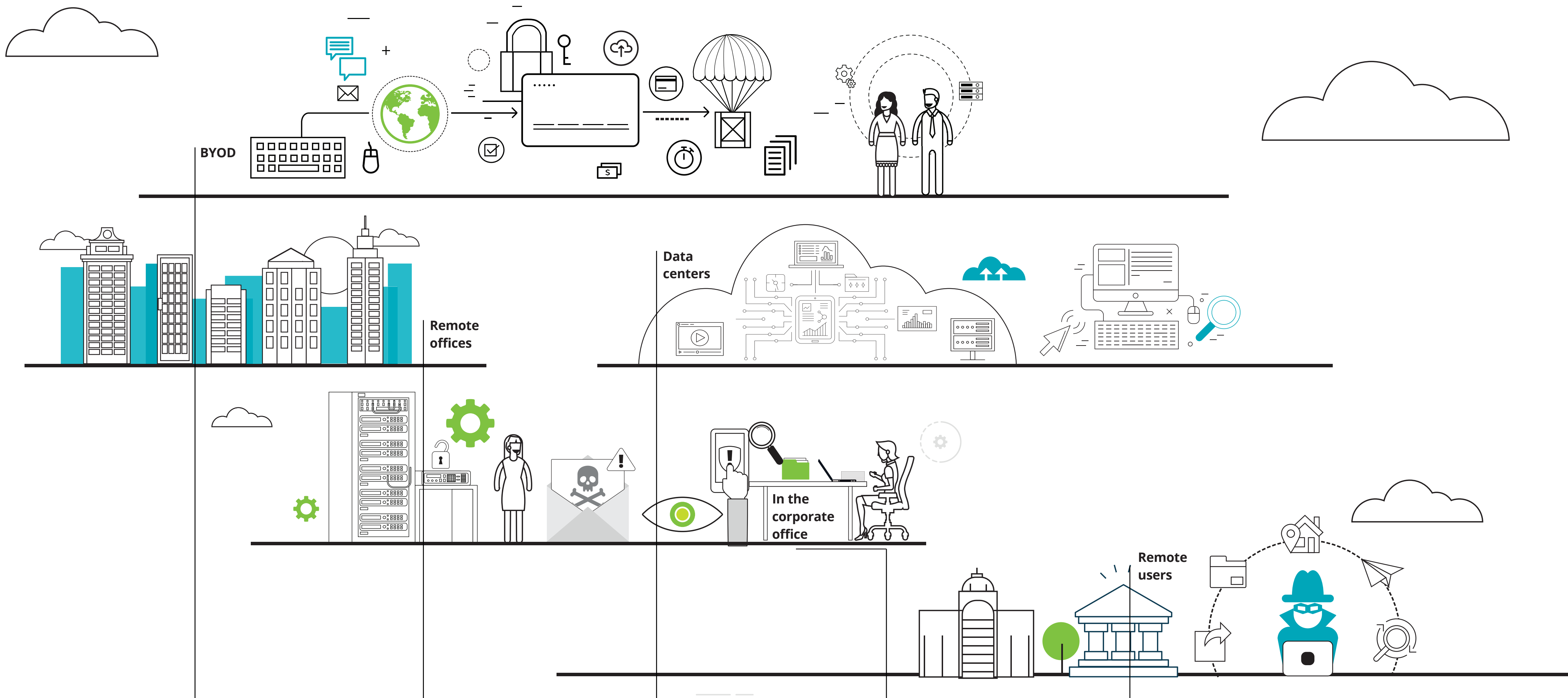
Vulnerabilities
What increases your vulnerability?

As the cyber threat landscape evolves, traditional endpoint security technologies can't keep up. Too often, these tools are not optimally configured—or are misconfigured entirely. This means that, without a robust endpoint detection and response solution, it's getting harder to protect your systems and data.

Email, applications and devices
Burgeoning end-user reliance on smartphones, laptops, notebooks, and cloud-based apps—not to mention web-based email servers—introduces almost-endless entry points for threats.

Security protocols, processes and practices
One of the greatest dangers to endpoint security remains weak protocols, processes, and practices. Busy employees using multiple devices at once do not always exercise the highest degrees of caution before clicking on potentially suspicious links. Similarly, overworked IT teams sometimes fail to patch software regularly or find themselves relying on outdated products and tools.

Endpoint security risks are rising



Bring your own device (BYOD)
Workers can now connect to your network anytime, from anywhere—home, hotels, cafes—unsecured networks, using personal laptops, smartphones and devices that are often unpatched and are prime targets for malware attacks.

Remote office
Branch locations are often subject to hacks and breaches. Acquisition strategy introduces disparate technologies that may or may not be supported or secure. Branch offices may also be located in countries that may not use the most up-to-date security software or solutions.

Data centres
As data centres become more virtualized and adopt cloud computing to improve resource utilization, new avenues of attack open up. By targeting "weak link" servers in a data centre, cyberattackers could gain a foothold to launch attacks across multiple systems.

In the corporate office
Phishing and ransomware incidents are increasing at an unprecedented rate. Your corporate office is connected to your operations, meaning malicious activity can work its way up from any connected system or device to impact critical infrastructure.

Remote users
Do remote users have the same security measures as your corporate systems? Unmanaged systems may introduce various types of malicious activity when attackers gain access into your environment. This includes customers, employees working from home, and third parties.

How can you protect your organization?

To counter today's increasingly persistent threats, you need a robust endpoint detection and response solution—one that allows you to integrate your disparate technology solutions, leverages real-time threat intelligence and analysis, and gives you access to leading security professionals. Here are a few key first steps to get started.

Get informed

Strong endpoint security begins with a clear understanding of your asset inventory so you can assess which systems and devices pose the highest risks. By conducting a health check, you can validate your systems' performance status, review your security architecture, and identify any gaps.

Get organized

To strengthen your protection, you'll need to adopt next generation security tools, engage in continuous monitoring, sandbox your networks and applications, and take steps to integrate your endpoint solutions with your existing technologies.

Get help

In a tight talent market, getting the right help can be tough. A managed endpoint solution can give you access to comprehensive threat intelligence and analytics capabilities, the resources you need to monitor your endpoint security around the clock, the ability to keep your tools up-to-date and optimally configured, and valuable insights to help you protect your critical data and infrastructure.

Ready to get started?

Being secure, vigilant, and resilient across your entire organization requires a team that understands your business and that can deploy comprehensive solutions to enhance your endpoint security.

Deloitte brings that leading team, providing the full spectrum of services to help your organization become more cyber prepared—from strategic consulting, to technology implementation, to full management and support. Our professionals have years of experience designing, deploying, and implementing endpoint security solutions, while our strong partnerships with leading vendors give us access to proven product roadmaps. We deeply understand the risks organizations face and, as a leading Canadian managed security services provider with four Canadian Cyber Intelligence Centres and multiple locations across the globe, we can monitor, detect, and proactively respond to threats 24/7—no matter where you do business around the world.

We help you in the following areas:

Cyber Strategy

Guide investment and ongoing management of your endpoint security programs, including risk assessments, threat awareness, and implementation of GRC solutions.

Cyber Security

Establish risk-focused endpoint security controls, balancing the need to reduce risk while meeting productivity, business growth, and cost optimization objectives.

Cyber Vigilance

Leverage our deep experience with analytic and correlation technologies to develop monitoring solutions focused on critical business processes, including the integration of threat data, IT data, and business data to prioritize incident handling and investigation.

Cyber Resilience

Prepare to handle critical cyber incidents, return to normal operations, and repair damage to the business.

Let's talk

If you're ready to take the lead on endpoint security and proactively respond to the evolving threats, we're ready to talk. Contact us and let's start the conversation.

Contacts

Rocco Galletto
Cyber Risk Services Leader
rgalletto@deloitte.ca

Robert Moerman
Senior Manager, Cyber Risk Services
rmoerman@deloitte.ca

Bryan Rowland
Senior Consultant, Cyber Risk Services
browland@deloitte.ca

www.deloitte.ca

Deloitte.

About Deloitte
Deloitte provides audit & assurance, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights and service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 264,000 professionals—9,400 of whom are based in Canada—make an impact that matters, please connect with us on LinkedIn, Twitter or Facebook.

Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private companies limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte.

Endpoint security risks are rising

New approaches are required to address complex new threats