Organized attackers
While the trend towards remote and mobile work delivers tremendous efficiency gains to most organizations, it also turned your endpoints—from laptops and smartphones to internet of Things (IoT) devises—into your weakest security link. In addition to launching pharming and increasingly sophisticated malware attacks, cyber criminals 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 fundamentals of protection are 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 disjointed products with conflicting 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 because companies implement drastically lower budgets, IT teams don’t have the personnel necessary to monitor and manage endpoint security across multi-cloud, multi-data center, multi-device environments. This puts pressure on IT teams to find ways to do more with less also means IT teams tend to focus on core essential tasks rather than making sure all technology resources necessary to monitor and manage endpoint security technologies can’t keep up with endpoint security remains under-resourced.

Charting the challenge
What type 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.

Disorganized responses
At some point, organizations will need to shift their thinking and adapt to the changing semiconductor landscape. As the cyber threat landscape evolves, traditional endpoint tools are becoming less effective. Too often, these tools are not optimally configured, or core technology updates are delayed, meaning that, without a robust endpoint detection and response solution, it’s getting harder to protect your systems online.

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 because companies implement drastically lower budgets, IT teams don’t have the personnel necessary to monitor and manage endpoint security technologies can’t keep up with endpoint security remains under-resourced.

Charting the challenge
What type 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.
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.

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 Moorman
Senior Manager, Cyber Risk Services
rmoorman@deloitte.ca

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