A new beginning for endpoint security

Introduction to the Cybersecurity Innovation Series

Creating and maintaining a resilient cybersecurity architecture – an architecture that is responsive to continual business change, the demands of evolving compliance and a sophisticated and hostile threat landscape – allows organisations to take advantage of new opportunities without compromise.

No business can afford to stand still and effective cybersecurity is no different. Understanding new approaches and evaluating, implementing and maintaining the latest innovative technology solutions can be difficult, time consuming and expensive.

Use the papers in our Cybersecurity Innovation Series to guide you through the latest advances in cyber approaches and technology, to focus your investments and build capability in the right areas for your business.

A new beginning for endpoint security

Everything has its cycle – the economy, hairstyles and flared jeans. The current focus on advanced endpoint security is no exception.

Until the network became central to security controls and investment, protecting the endpoint was what information security was all about. But that was back when security professionals did not have to worry about laptops, smartphones and tablets, let alone the explosion of connected devices from tills to printers to SCADA systems. How and where we now work, coupled with our insatiable use of endpoint devices has all but eroded network perimeters – turning industry attention back to managing the risk of the endpoint. As we reach this tipping point in investment, however, it is vital to learn the lessons of the past, avoiding reactive, fashion-based purchases of technology that will create more noise and less insight.

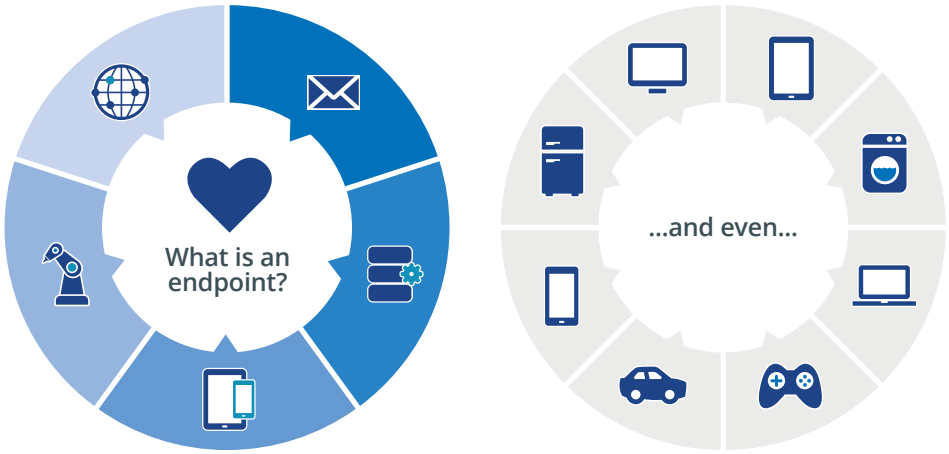
By selecting the right endpoint security solutions, organisations do not just increase their capability to protect data and devices and detect malicious activity and malware. Integrating network and endpoint security helps businesses establish greater visibility over the entire threat landscape and examine the risks in context. Organisations that have this insight are empowered to respond in real-time and use a correlated view of behavioural and geo-locational data to enhance their predictive capabilities.

There is no end to endpoints

The average smartphone or tablet has more computing power than the technology that put the first men on the moon. Mobile devices are an integral part of every connected business – used for data input, analysis, collaboration and customer insight. And with the implementation of Bring Your Own Device (BYOD) the perimeter is now permanently in our pockets – the endpoint at which our business and personal lives co-exist and sometimes collide.

Information security teams must create and enforce policies for an increasing

Figure 1 The growth of the endpoint. The ever-increasing number of connected devices creates points of risk.



number of endpoints. These range from point of sale devices, automated plant equipment, ATMs, network printers and video surveillance cameras, to a host of innovative handheld devices in industries such as healthcare, transportation, field service and retail. In addition to these challenges, IT departments are also attempting to assess the information security impact of the internet of Things (IoT) with IDC forecasting that there will be 32 billion connected things by 2020.[1]

The diversity, rapid development and demand for IP-enabled devices has created new challenges in managing network connectivity, application access, data residency and protection. Organisations need proof that the relevant controls are in place to manage the security risks of devices for a host of regulatory requirements such as data protection and PCI – and also that the appropriate encryption is consistently applied to comply with enterprise insurance policies.

In just ten years, data that almost exclusively resided on file servers is now held on endpoint hard drives or in the cloud. Our threat intelligence[2] shows that attacks pointed at users are usually gateway attacks – compromising devices to gain access to the wider network. There is recognition that traditional network security controls and anti-virus software are no longer sufficient. The demand for real-time visibility to monitor, record and report on what every endpoint is being used for and deploy this intelligence to detect malicious behaviour, is seen as critical to containing, disrupting and remediating attacks.

A growing battle to balance speed and security

The range and number of endpoints that organisations manage has created a large attack surface for those with malicious intent. Fast becoming the easiest route into a network for attackers, endpoints are places where even the most basic malware can dupe innocent end users and bypass centralised controls. An increase in the number of devices also presents information security teams with a growing patch management workload as they try to comprehensively download all the appropriate patch executables to remediate endpoint vulnerabilities and verify successful patch deployment.

The industrialisation of malware, often with just tiny adaptions to previously seen attacks such as changing the file's hash – means that malware can evade many forms of detection. Endpoint security used to be synonymous with a single product category – antivirus software. Fast forward just a few years and APTs, sophisticated malware, targeted attacks, and zero-day exploits are changing the endpoint security landscape. Growing volumes of SSL traffic are also causing concern. The reduction in visibility significantly affects the effectiveness of existing network controls, and the correct tools to decrypt the traffic can cause performance issues if not architected correctly.

Information security professionals are constantly under pressure to balance performance and availability against the need to examine traffic, using anti-malware or sandboxing solutions. User pressure has also led to some organisations compromising on simple network access controls such as least privilege, granting excessive privileges to meet demand. In some cases, even the use of central controls such as application whitelisting, that block certain unrecognised applications as 'bad', have brought security and users into conflict. And to avoid conflict, tech-savvy users are increasingly purchasing, controlling and provisioning their own services and solutions. This widespread use of applications that are not sanctioned or managed by IT is called Shadow IT. With Gartner predicting that by 2020, 90% of expenditure on IT will happen outside of the Corporate IT budget[3], this trend is gathering pace.

It is unsurprising then, that with all these pressures to support users, InfoSec professionals are eager to understand, evaluate and implement innovative endpoint protection tools. As much of this emerging technology is relatively new, we want to share a brief perspective on the different approaches as you begin to consider the right solutions for your business.

Example Case Study: Large industrial manufacturer

Challenge:

An internal security incident prompted a full review of this manufacturer's entire security strategy. As part of this, the client's existing signature-based endpoint product was deemed ineffective.

Solution:

- Reviewed the existing environment
- Chose a signature-less solution that would integrate with the network access control system
- The evaluation detected and mitigated both deliberately planted and inadvertently downloaded malware
- After the successful evaluation, the new solution rolled out in phases to all company endpoints

Business value of the solution:

The client saved time and resources at the same time as increasing security, due to not having to remediate malware issues. The integrated solution provides better threat intelligence, enabling automatic response to threats in real time. All the client's endpoints are protected against future threats, without needing to wait for patches to be released by the software vendors.

1. IDC's Worldwide Internet of Things Taxonomy, 2015, Worldwide Internet of Things Forecast, 2015–2020 2. NTT Group Security Global Threat Intelligence Report 3. Gartner

A new age of signature-less controls

The three emerging technologies below have one thing in common: whilst they use similar techniques to detect 'known bad', they do not use signatures.

1. **Innovation – Block Exploits**

   The first emerging exploit detection and prevention technique we have been evaluating blocking specific exploit techniques. Every threat report, including our GTIR, highlights the almost unimaginable number of malware types that exist. And this number is perpetually growing. Analysis shows, however, that this vast sea of malware can be boiled down to just a handful of core exploit techniques. Vendors install software on the endpoint that detects if any of these techniques are being executed, even as a chain and blocks the attempt. These solutions then notify the administrator and the user. A full forensics report is then generated which can feed into an organisation's predictive and protective capability through its Security Information and Event Management (SIEM) system, and its Security Operations Centre (SOC).

2. **Innovation – Micro-Virtualisation**

   The second emerging endpoint technology that organisations are evaluating is based on virtualisation. Whether users are working on or off the network, these solutions isolate user tasks or processes such as that click upon a website, document or email and runs them within a separate environment (a micro virtual machine). This type of containment prevents any detected malware from infecting the network as well as keeping users productive as it allows a user to complete a task before an infected document for example is discarded. These solutions also provide real-time alerts with comprehensive forensic intelligence for each attack allowing an organisation to quickly detect and contain any attempted breach whilst it is in progress.

3. **Innovation – Behavioural Analysis**

   Another endpoint security approach that we are helping customers to deploy is based on behavioural analysis techniques. These solutions are installed on the endpoint and are driven by a behavioural risk engine to analyse and correlate device and application activity at an operating system level, as well as information about applications and network connections. For example, these solutions will inform an administrator in real time if an application has requested excessive privileges or is leaking data. In our experience, these solutions integrate easily with existing mobility and security infrastructure such as mobile device management (MDM) to help an organisation build its predictive as well as its protective capability. For organisations that are building their maturity to make risk-based decisions, these solutions use behavioural analysis to produce a risk score of suspicious activity based on the type and severity of risk. This score can be placed in context within an organisation's policy to determine whether automatic mitigation action is required to keep a device and its data protected.

These three approaches are just some of the innovative techniques and technologies that organisations are deploying to reduce endpoint risk. We are also working with other new and interesting approaches such as real-time monitoring, endpoint stealth and machine learning. As with all technology decisions, it is vital to ensure that they meet the short- and long-term needs of the business.

But whatever approach a business decides to adopt, human behaviour remains a critical component in protecting sensitive resources and data. Endpoint policies will fail if employees are not reminded about their specific responsibilities.

In our experience, the battle between security and performance is fiercest around the endpoint. All of the successful endpoint security strategies we have seen will establish shared ownership and accountability with a cross-functional team with executive level support. This ensures that policy creation, enforcement and technology selection remain aligned with business objectives and priorities.

Advanced endpoint - NTT Security point of view

An organisation seeking to reduce the risk from its endpoints have a wide choice of new and innovative approaches. This risk not only comes from the scale and sophistication of threats and the rapidly increasing number of devices but from the realisation that anti-virus controls give insufficient protection. Information security teams also know that even if signature based solutions could give them the right level of real time insight, some endpoints are virtually un-patchable – such as systems no longer supported by vendors, or that require 100% availability.

One thing is clear: whatever advanced endpoint solutions an organisation selects, a successful investment must integrate with network security to build detection, prevention and increasingly, prediction capability. They must do this in a business context that balances a decrease in threat surface without disrupting business as usual activity. Preserving endpoint performance and user experience is key to any technology decision as employees have proven to have little tolerance for security solutions, particularly at the endpoint, that stand in the way of productivity and collaboration.

Example Case Study: Large financial institution

Challenge:

A large financial institution was targeted with malware. Gateway controls were ineffective, due to configuration issues and the existing signature-based endpoint product could not detect and alert on all malware items. A great deal of manual effort to remediate the issues was required.

Solution:

- Signature-less solution to resolve the gateway controls' configuration issues
- New solution configured to collaborate with the controls and provide correlation, augmented by threat intelligence feeds
- All known malware items picked up by the new solution, which also detected some unknown ones present on the network and endpoints

Business value of the solution:

In addition to the protection against unknown threats provided by the new endpoint solution, the business also benefitted from a more collaborative, intelligence-based security approach. The new solution had low additional impact on the endpoints thanks to the lightweight clients, as well as requiring little maintenance.

What is resilient cyber intelligence capability?

At NTT Security, we work in partnership with our clients to build resilient cybersecurity architectures, transforming a mass of point technology solutions into a sustainable cyber defence capability. Internal and external threat data sources are transformed into intelligence that can help predict and prevent future attacks, defending the business from and responding to, current threats.

Technology innovation is at the heart of the cybersecurity industry as it attempts to keep pace with those that wish to disrupt, defraud or damage our organisations. Our technology partners consistently develop solutions that make the tasks associated with cybersecurity easier and faster – but more strategic planning, business context and rigorous evaluation must be applied to investment decisions.

Look out for the rest of our Cybersecurity Innovation series where we will examine how new solutions and approaches can help to create sustainable, resilient cyber architectures - or contact us to explore how our range of innovative services can help your organisation to drive greater business value from people, processes and technology to close the cyber intelligence gap.

Our range of consulting, managed security and technology services to help our customers build a resilient cyber defence architecture include:

- Assessment services including architecture, risk, capability and compliance
- Independent technology evaluations
- End-to-end implementation experience
- Managed services to build capability such as 24/7/365 monitoring and intelligence analysis

Visit **www.nttsecurity.com** to find out more

About NTT Security

NTT Security seamlessly delivers cyber resilience by enabling organisations to build high-performing and effective security and risk management programmes, with controls that enable the increasingly connected world and digital economy to overcome constantly changing security challenges. Through the Full Security Life Cycle, we ensure that scarce resources are used effectively by providing the right mix of integrated consulting, managed, cloud, and hybrid services – delivered by local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest information and communications technology (ICT) companies in the world. For more information, visit **www.nttsecurity.com**

To learn more about NTT Security and our unique services for information security and risk management, please speak to your account representative or visit: **www.nttsecurity.com** for regional contact information.