dimension data

accelerate your ambition

Predictive ransomware protection

Keeping your business one step ahead of cybersecurity threats

Ransomware is a pragmatic and instantaneous attack against your entire organisation and all your data. *Make your digital business resilient with our complete ransomware solution that secures your entire infrastructure and workplace, and helps you prevent costly downtime.*

Ransomware is aggressive and attacks the entire digital business

Ransomware is a type of malware which holds information or entire devices hostage. Data from your entire digital business such as your desktop and laptop fleet, or servers, may be held ransom. Attacks are surging because of the interconnectedness of our world, which allows attacks on a much larger scale.

Many organisations are vulnerable because they haven't improved their security practices. They don't have the latest vulnerability patching in place, and the situation worsens when employees work remotely and/or on their personal devices.

Ransomware is also highly accessible to cyber criminals nowadays, even if they don't have the skills to program ransomware. Cybercriminals pay the operators of Ransomware-as-a-Service platforms to launch attacks, which can lead to mass attacks against entire industries.

The top targeted industries in terms of ransomware attacks are business/professional services (28%), government (19%), healthcare (15%) and retail (15%), according to NTT Security's 2017 Global Threat Intelligence Report.

With poor cybersecurity practices and the inability to patch and prevent malware from infecting and spreading, and without a backup and recovery system, organisations pay up to have their files back for use. Attackers are seldom prosecuted as they demand payment in cryptocurrencies which ensures their anonymity.

Ransomware has without doubt become one of the most successful revenue-generating malware types for cybercriminals. No business sector or industry is safe.

Ransomware destroys and devastates

- production lines are halted in manufacturing resulting in operating losses
- downtime across all industries leads to a loss of man-hours
- Point-of-Sales systems can't process payment transactions, resulting in customer dissatisfaction and revenue losses for retailers
- hospitals have to redirect patients to other hospitals, including critical cases, as their computer systems are not operable

Ransomware disrupts all areas of your digital business

Digital infrastructure

Hybrid cloud

Digital workplace

Cybersecurity

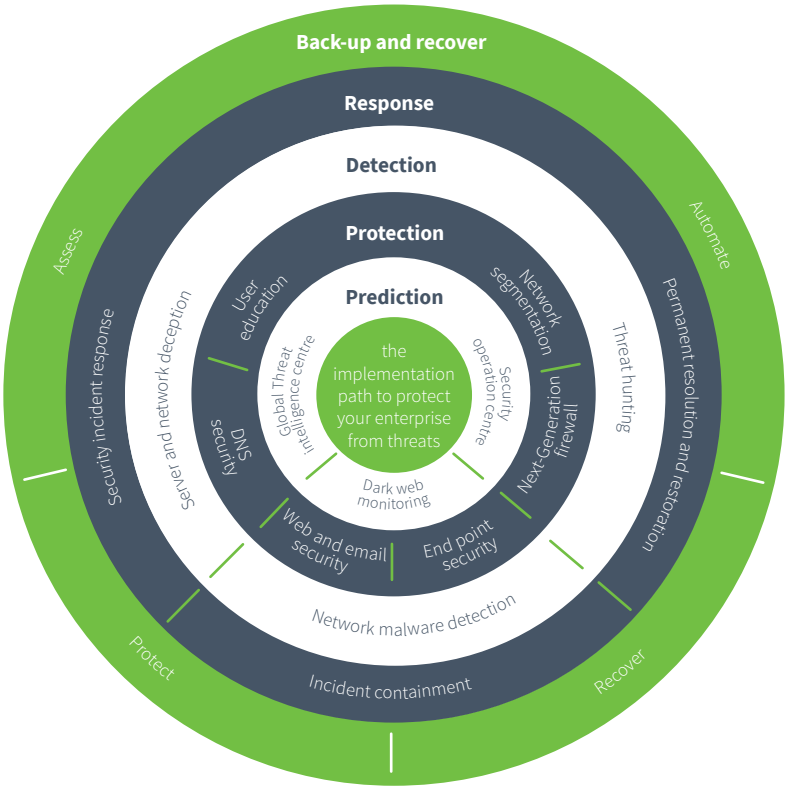
Customer experience

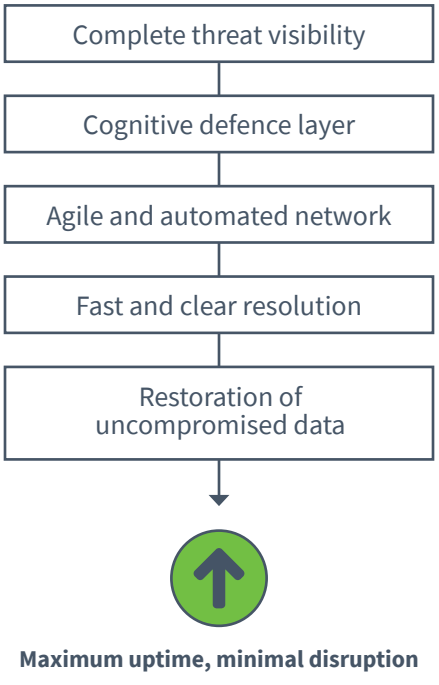
‘Ransomware is now the most *common malware discovered* in client environments.’

NTT Security’s 2017 Global Threat Intelligence Report

Our predictive cybersecurity approach to ransomware protection

Ransomware can penetrate your organisation in multiple ways – from your endpoints to your servers – requiring a complete approach, rather than a single product. Ransomware must be prevented, where possible, detected, if it gained access to systems, and contained to limit the damage. To block and stop the attack, your organisation needs a multi-faceted approach towards services and security technologies.





We work promptly on blocking malicious communication channels at the firewall or IPS, and *quarantine infected machines as soon as possible with Network Access Control* technologies.

Secure your digital business with our complete solution:

Prediction

Our continuous research on known and emerging threats, ability to monitor incoming threats in real-time coupled with the detection of dormant threats, allows us to inform you before the attack occurs.

Protection

Together with your stakeholders, we create a strategy which correctly manages IT security policies and deploys technologies to effectively detect and block external threats and malicious behaviour across your network and endpoints.

Next-generation security technologies may include:

Identity and Access Management tools	essential in identifying enterprise devices and assets
Network Access Control	allow devices with adequate security settings that adhere to your IT security policies, and detects if you're vulnerable to the latest wave of attack
End-point security	prevents exploitation of vulnerabilities across all operating systems
Email security solutions	identify inbound phishing mails from suspicious domains and remove spam

Detection

When malware has infiltrated into your endpoints or network, we have technology in place that detects anomalies in your infrastructure while preventing the spread of malware.

We watch your network around-the-clock to check for compromise and determine whether it's a security incident by using our Security Incident and Events Management tools. Network equipment helps us automate the detection before the attack worsens.

Response

Upon detection of ransomware incidents, our defined response includes isolation, eradication and forensics to determine the root cause and improve security.

We work promptly on blocking malicious communication channels at the firewall or IPS, and quarantine infected machines as soon as possible with Network Access Control technologies. Endpoint security tools eradicate malware while under quarantine. A thorough scan of the rest of your network looks for traces of ransomware in other devices, and we use endpoint forensics tools to provide the visibility.

Backup and Recovery

Backup plans were traditionally built around server failures, and laptop data risks were evaluated as a single laptop getting lost or failing. Ransomware affects all your data and devices and to protect backup data from a possible attack, we follow a proactive approach:

Step 1 Identify critical data and define your backup placement strategy

Step 2 Isolate backup and reconfigure your network

Step 3 Disaster recovery and testing to validate your data

Step 4 Detection, containment and recovery with automated tools

Examples of critical data

Healthcare	patient data, e.g. surgery schedules or patient medication schedules
Financial Services	client accounts, e.g. online payments or ATM functions
Retail	online Point of Sale systems or customer credit card accounts
Public sector	government officials' laptops

The Dimension Data advantage

	**Complete security solutions**	We provide a complete security solution. We have strong security consulting-led capabilities, architecture services, as well as a comprehensive range of Managed Security Services. We combine this with a range of technologies to accelerate your digital business, ensuring that you're able to optimise your hybrid IT environment securely.
	**Advanced security expertise**	• proven experience, 15-year track record in security solutions • security professionals who are certified to the highest levels across multiple vendors, technologies, and industry standards • more than 15,000 security engagements with clients spanning 49 countries across multiple industries
	**Global threat protection with advanced analytics**	Our Managed Security Services platform, delivered by NTT Security, offers threat insights from visibility gained from: • analysing more than 3.5 trillion logs annually • detecting and defending against 6.2 billion attacks annually • global honeypots and sandboxes in over 100 different countries • ten Security Operations Centres • seven Research and Development centres globally (over USD 2 billion spent on Research and Development annually) • monitoring 40% of global internet traffic using the NTT Global Threat Intelligence Platform. The platform provides advanced analytics: malware taint analysis, machine learning, and enhanced threat visibility, ensuring the broadest set of threat data in one view.
	**Worldwide operations and management**	With a turnover of USD 7.4 billion, offices in 49 countries, and 30,000 employees, we deliver wherever our clients are, at every stage of their technology journey. Our services are standardised globally, ensuring a consistent client experience across the world.
	**Vendor independent**	Our partnerships with leading security vendors ensure that we're vendor agnostic – we manage and support multiple technologies.