Understanding the Ransomware Threat
and How to Protect Your Organization

SUMMARY

Ransomware is now the number one form of crimeware. Even more worrying is the rise in the sophistication of attacks and a burgeoning cottage industry committed to propagating the distribution of ransomware.

Ransomware can be devastating for organizations causing downtime and untold financial damage. A form of malware, ransomware encrypts files, operating systems, and even file servers. Attackers then demand a sum of money in return for the release of your files and systems. Failure to meet those demands can result in the loss of data or the potential release of that data to the public. In this whitepaper, we discuss:

- **Types of ransomware and the damage they cause**
- **How the threat has evolved and why businesses and organizations are now in the bullseye**
- **Why traditional perimeter defenses can't protect you against ransomware**
- **Steps you can take to defend your organization**

WHAT IS RANSOMWARE?

Ransomware is the latest menace of the internet. Ransomware is designed to block access to computer systems or files until a sum of money is paid.

In just two years, it has jumped from being the 22nd most common variety of malware to the fifth most common and is now the number one form of crimeware. Why such a leap in popularity? Ransomware has been around for many years. But, fueled by the success of early attacks and digital innovation, the ransomware industry has undergone aggressive transformation – both in terms of technology and extortion methods.

In just two years, ransomware has jumped from being the 22nd most common variety of malware to the fifth most common.

Ransomware authors can now encrypt entire disks, steal credentials to spread the attack throughout the organization, delay encryption to infect as many machines as possible without detection, and create new code that targets corporate servers, as well as individual user devices. Securing ransom without detection by law enforcement has also become easier thanks to the Bitcoin, a digital currency that defies tracing. Perhaps the most worrying development in the evolution of ransomware is ransomware-as-a-service (RaaS). Designed to make cybercrime accessible to anyone, no matter how limited their mastery of code, advanced cyber criminals can now create pre-baked ransomware code and make it available for anyone to download and use for malicious intent.

RANSOMWARE'S NEW TARGET: YOU

For a long time, cyber criminals used ransomware to make money out of individuals. Unwitting victims would click a link in a spam email or activate a macro in a malicious document and within seconds their photos, files, and music collection would be encrypted. Victims would be given a deadline of a few days to get their data back or risk losing it forever.

Healthcare institutions, police departments, financial service companies, and even manufacturers are at risk for **enterprise-scale ransomware attacks.**

It didn't take long for cyber criminals to realize that companies and organizations are a much more lucrative target than individual users. In the past few years, healthcare institutions, police departments, financial service companies, and even manufacturers have found themselves under siege from enterprise-scale ransomware attacks.

Although ransom demands in themselves can be detrimental to any bottom line, the truer impact comes in terms of operational downtime. Lost revenue, logistical disruption, inability to invoice, and loss of consumer trust are just some of the devastating impacts. The results are there to see in the headlines each week, culminating in the biggest ever cyberattack in internet history – the WannaCry ransomware attack of 2017.

The WannaCry attack exploited a vulnerability in the Microsoft Windows operating system. Public administration organizations, financial services companies, and healthcare organizations, such as the UK's National Health Service (NHS), were hit hard. The NHS was locked out of 70,000 devices, including computers, MRI scanners, theater equipment, and more.

It took just one day for WannaCry to infect more than 230,000 computers in over 150 countries. Experts advised against paying the ransom due to reports that organizations weren't getting their data back. Paying the ransom also fuels the ransomware economy fueling further and possibly repeat attacks. All told, WannaCry hackers made less than $70,000 from the attack, however the wider business impact sent shockwaves around the world.

HOW TO GET INFECTED

Ransomware has several known attack vectors. 99% of malware comes through either your mail (as phishing) or web server (where malware code exploits specific vulnerabilities in browsers or other software). Once delivered, ransomware wastes very little time in seeking out and encrypting files. This form of ransomware is known as encrypting ransomware. Another form is locker ransomware, in which a victim is locked out of their operating system completely, although individual files remain unencrypted. Once encryption is complete and files are inaccessible, a ransomware note is generated notifying the user of what happened and demanding a ransom.

This is typically the first point at which the user or organization becomes aware that they've been infected with ransomware.

YOU ARE VULNERABLE TO RANSOMWARE

Every organization is vulnerable to ransomware. Whether your organization is big or small, if your users rely on information technology to access data or your cyber security controls aren't as strong as they should be, you are easy prey.

Since implementing our cyber security solutions, organizations have been able to detect and prevent over 30,000 coordinated ransomware attacks from hackers across Europe, Asia, and the U.S.

Case in point. An international retail manufacturer experienced days of disruption as a result of a ransomware attack. With only traditional, signature based antivirus, network firewalls, and VPN in place to secure their network, they lacked the ability to prevent, detect, or remediate against the attack. The result was a logistical nightmare. Unable to ship their goods, invoice customers, or even guarantee that customer information wasn't at risk, the company failed to function for several days. The company approached Neovera to prevent future incidents. Since implementing our cyber security solutions, they have been able to detect and prevent over 30,000 coordinated ransomware attacks from hackers across Europe, Asia, and the U.S.

COMBAT THE RANSOMWARE THREAT 1: PREVENTION

There is no single-point solution to preventing the threat of ransomware. However, there are several best practices that organizations can adhere to combat the threat:

- **Secure backup.** Any anti-ransomware strategy starts with a solid data backup strategy. Create daily backups either to the cloud or external hard drives (although be sure to disconnect them afterwards to avoid ransomware spreading to your backups). Consider a layered approach by backing up files in different locations and on different media.
- **Patch management.** Many organizations struggle to find the time or resources to stay on top of cyber risk assessments and constant updates from software vendors. The results can be catastrophic. WannaCry, for example, exploited a vulnerability in Microsoft software. Although a patch was available two months earlier, many users failed to implement the update. Stay on top of patch management by prioritizing those that can reduce your risk.
- **Risk assessments.** Conduct regular risk assessments to identify vulnerabilities and prioritize risk remediation activities. Again, this is often overlooked. In the financial services sector, for example, the SEC found that 5% of broker-dealers and 26% of investment advisers don't conduct periodic risk assessments of critical systems.
- **User education.** Teach users how to spot and handle suspicious emails so they can help you detect ransomware or prevent it from propagating if they suspect they've opened a suspicious file attachment or visited a malicious website.
- **Restrict user privileges.** Limit the number of employees who have the authority to install software or access data they don't need.

COMBAT THE RANSOMWARE THREAT 2: ADAPTIVE SECURITY

While best practices can help your organization reduce its vulnerability to a ransomware attack, they are far from watertight. Patches get overlooked, vulnerabilities go unchecked, or users fall for a phishing email. Neither do these best practices put your regulatory woes to rest.

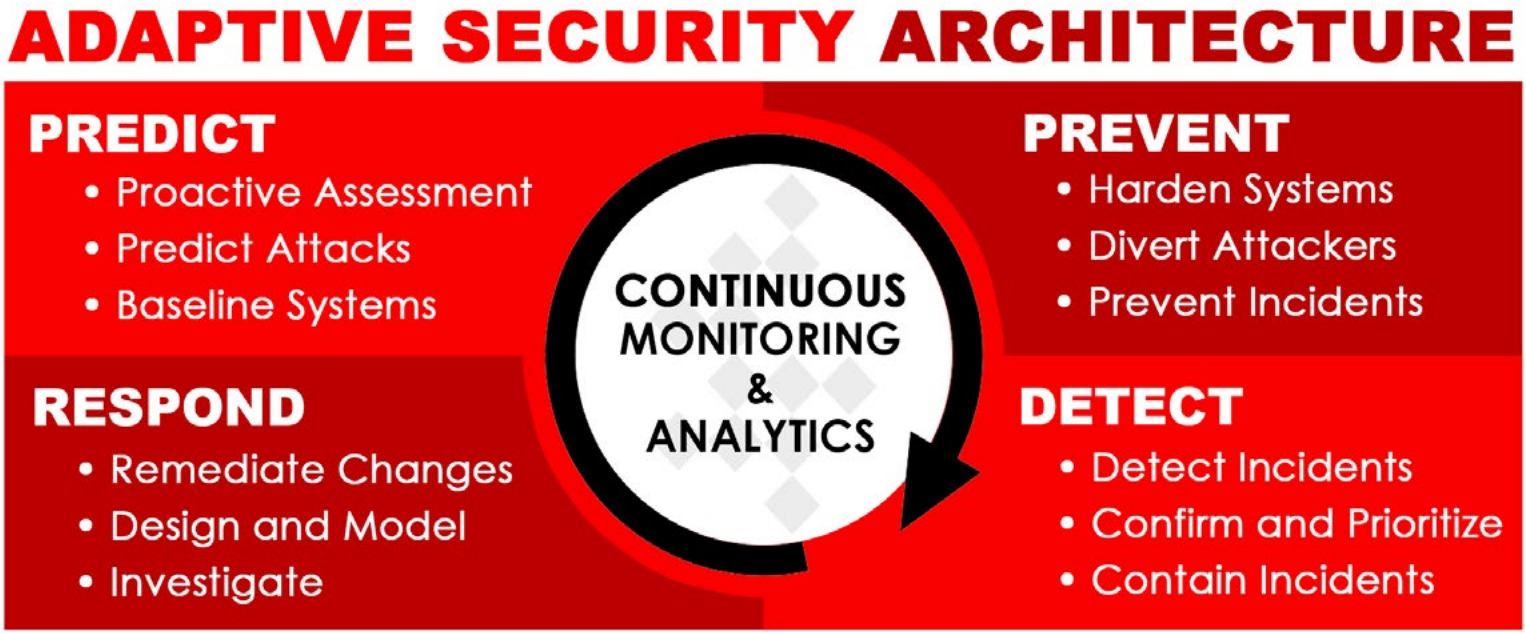
Predicting new threats and automating routine cyber security responses is key to staying ahead of rapidly emerging and changing threats – it also frees up security teams to focus on the most complex incidents.

The problem is that many of today's point solutions fall short. Policy-based controls, such as antivirus software, IDS/IPS, and firewalls won't protect you against rapidly evolving advanced ransomware threats. These prevent-and-detect perimeter defenses and rule-based security solutions are also becoming less effective as organizations move to the cloud and open APIs. In today's digital world, IT doesn't control the boundaries of the network as they used to, limiting their ability to detect and respond to ever-evolving threats.

Instead of focusing their time on preventing a cyberattack, industry experts agree that organizations' need a constant, pervasive monitoring, and visibility strategy. One in which systems are assumed to be compromised and require continuous monitoring and remediation.

Gartner calls this approach an "adaptive security architecture". "Many enterprise IT security teams spend much of their time focused on preventing a cyberattack. In doing so, they have implemented an 'incident response' mindset rather than a 'continuous response' where systems are assumed to be compromised and require continuous monitoring and remediation."

Predicting new threats and automating routine cyber security responses is key to staying ahead of rapidly emerging and changing threats – it also frees up security teams to focus on the most complex incidents.



Addressing all four pillars of Gartner's adaptive security architecture, Neovera's cyber security services deliver unprecedented defense-in-depth capabilities that can help organizations predict, prevent, detect, and respond to ransomware and advanced attack methods – thwarting them before the damage is done - both in the cloud or at your on-premises data center.

Plus, you'll get unrivalled visibility into your security infrastructure. Our client dashboard provides the intelligence and analytics you need to easily understand your risks, demonstrate compliance, and make better security decisions.

Our no-hassle solutions let you stay ahead of ransomware and other security threats with continuous monitoring, enhanced intelligence, proactive prevention, early threat recognition, rapid response, and investigation of root causes. Better knowledge means better protection when combined with comprehensive tools to defend your networks, data, devices, web traffic, applications, and more.

Modular in design, Neovera's monitoring and/or manage service offerings are highly customizable to your infrastructure and business needs. Our NeoCyber security packages provide continuous security management, monitoring, and scanning across Intrusion Prevention System (IPS) and Unified Threat Management (UTM), Secure WiFi Management, NeoCyber Security Services

(Bronze, Silver, Gold, Platinum), Security Information and Event Management (SIEM), and Vunerability Scanning Solutions.

Neovera's cyber security services deliver unprecedented defense-in-depth capabilities that can help organizations predict, prevent, detect, and respond to ransomware and advanced attack methods – **thwarting them before the damage is done.**

With the NeoCyber™ Intrusion Prevention System (IPS), our team of cyber security experts manage the maintenance, administration, and monitoring of your IPS device to achieve a layer of powerful security. Or if you just need monitoring, we can do that too. With Neovera, you can extend the security of your critical information and help you stay ahead of ransomware threats with continuous monitoring, enhanced intelligence, pervasive visibility, proactive prevention, early threat recognition, rapid response, and investigation of root causes.

In addition, our Managed Unified Threat Management (UTM) service protects and thwarts ransomware and other advanced persistent threats (APTs) using a consolidated protection of intrusion prevention, antivirus, and application control. Users experience comprehensive protection and simplified security management, all without slowing the network. With Neovera, host devices can be quarantined, malicious actions are shut down before they take hold, and other measures automatically are deployed to secure your enterprise.

Plus, you'll get unrivalled visibility into your security infrastructure. Our client dashboard provides the intelligence and analytics you need to easily understand your risks, demonstrate compliance, and make better security decisions.

WE TRACK THE THREATS SO YOU DON'T HAVE TO

To improve compliance and alleviate alert fatigue, Neovera delivers unprecedented visibility into your security environment. We continuously collect, monitor, and manage logs from virtually any device capable of producing a syslog, including firewalls, IDS/IDPS, UTMs, routers/switches, and network devices. Plus, our SIEM system aggregates and correlates data from security feeds such as network discovery, vulnerability assessment, and intrusion detection systems, creating a single pane of glass, dashboard view for our security experts to monitor and protect your enterprise.

Neovera offers **24x7x365** cyber security monitoring.

Our Joint Security Operations Center (JSOC) is staffed 24x7x365 by security experts and analysts who provide an extra layer of protection between you and the security threats that threaten your business.

CHOOSE THE OPTIONS THAT WORK FOR YOU

Our adaptive security architecture approach also stresses flexibility. Choose from a range of modular service options, all of which include 24x7x365 cyber security monitoring and expert support – customized to your infrastructure and business needs. Contact us to learn more about these options.

NEOVERA
SECURE CLOUD CONNECT

PREDICT	PREVENT	DETECT	RESPOND
• Cyber Security Services (CSS) Gold Package • CSS Platinum Package • Continuous Vulnerability Scanning and Reporting	• Managed Intrusion Prevention System (IPS) • Managed UTM • CSS Gold Package • CSS Platinum Package • Managed Secure WiFi	• Managed IDS • Bronze • CSS Silver Package • CSS Gold Package • CSS Platinum Package • Managed Unified Threat Management (UTM) • Managed Secure WiFI	• Managed Threat Detection and Response (TDR) • CSS Gold Package • CSS Platinum Package

Neovera Secure Cloud Connect provides a comprehensive foundation for success including continuous security monitoring and analytics, network and application security and performance, identity security, and more.

CONCLUSION

The ransomware threat is real and pervasive. Incidents continue to escalate causing un-told damage in terms of downtime, financial costs, compliance, and reputation management. With the democratization of ransomware code and new variations entering the black market each day, traditional cyber defense mechanisms like antivirus, fail to provide the protection that organizations need. It's not a case of *if* but *when* your organization is attacked.

Stay ahead of security threats with Neovera's comprehensive approach to securing your environment. We integrate different security functions into a single solution delivering complete visibility in and around the network so that security events are thwarted before they can wreak havoc.

For information about Neovera cyber security services used by hundreds of organizations to thwart more than 600 million cyber events daily and save over $200 million in total cost savings by preventing attacks, visit **www.neovera.com**.