CYPROTECK

# Security Assessment & Ransomware Assessment

Our experienced consultants help manage your network transformation and help you reduce cybersecurity risks and overcome internal resource constraints

CYPROTECK

# Summary

Security breaches are increasing in frequency and severity. As we move more data between devices and environments through IoT and other connected technologies, we are increasing our data footprint, and thereby, increasing security risks. IT and OT leaders need to adjust their approach to security to protect data in motion - a new challenge for their business. Consider:

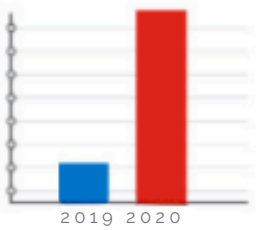
- More people and organizations that need to access data
- Increasing number of applications and APIs
- Networking east-west data flows and new network configurations.

As dependency on data to generate revenue deepens, cybercriminals have shifted focus to ransomware attacks, pervasive DDoS attacks, IoT botnets and command and control attacks.

If living and working in a connected world wasn't challenging enough, add in the global pandemic that grossly shifted how employees work. This new hybrid workforce has significantly altered the security perimeter, creating yet another challenge for IT and OT leaders who need to review security policies and procedures to minimize risks. Remote desktop protocol, bring your own PC and virtual private network vulnerabilities and misconfiguration are becoming the most common point of entry for attackers.

At Cyproteck, we build our threat intelligence from one of the world's largest internet backbones, which gives us a massive field of view when it comes to emerging and evolving cyber threats. The Black Lotus Labs* security team provides some of the most comprehensive threat intelligence in the world, routinely identifying new attack vectors and working with government agencies to take down bad actors. Cyproteck serves as a trusted service provider of Fortune 500 companies and federal agencies alike, with more than 10 years of experience in tracking and stopping emerging threats throughout the global internet. Simply put, we see more so we can stop more.

4X increase in vulnerabilities tied to ransomware




Reduce exposure to potential attacks by

30%

by patching "high" vulnerabilities

8 nation states beh

CYPROTECK

124 current trending ransomware attackers

Source: 2021 Spotlight Report "Ransomware Through the Lens of Threat and Vulnerability Management by RiskSense and Cyber Security Works

## Ransomware

Ransomware is the highest-profile type of malware attack at present, with headline grabbing events occurring seemingly weekly. From oil pipelines to healthcare and food processing. no industry is unaffected. Recent attacks have evolved from attacking individual endpoints to attacking an organization. Ransomware has evolved from the widespread attacks intended to infect a single endpoint to include more advanced techniques such as fileless malware and data exfiltration. These new strains of ransomware make prevention and planning more important to prevent ransomware attacks.

We have seen a 4x increase in the number of attacks in the past year, according to a 2021 Spotlight on Ransomware report published by RiskSense and Cyber Security Works. The average cost of downtime for a business is $274,000 and growing, and the average payment for ransomware is over $154,000 and growing. It's no wonder cyber resilience has become a board level conversation. IDC says that 35% of failed Edge proof of concepts fail due to security concerns. It's no wonder why external risks are top of mind for business leaders.

The only way to stop theft and loss of intellectual property, customer data and personal information is to conduct regular assessments of your security environment and follow-up with a comprehensive program to address your security posture and vulnerabilities.

Many businesses don't know where to begin or where they are vulnerable and unprotected. Some aren't even able to say when the last time they ran a security health check. With the number of security tools on the market, it can be difficult to move beyond managing your security tools into a more proactive security strategy Security can help you understand your risks across your network and mitigate that risk to protect company brand and shareholder value.

CYPROTECK

# Security and impact on business objectives

Security is a business problem. You need to be able to demonstrate to your executives,
the board of directors and other business leaders that you know the likelihood of a
security incident and the impact to the company's ability to do business - including
potential impact to your brand's reputation.

Align your security strategy with your business. Protect your digital assets, users and data. Protect valuable intellectual property by preventing unauthorized access
Maintain reliable customer experience that could be disrupted by malware
Meet regulatory requirements
• Safeguard sensitive data and avoid jeopardizing employee or customer privacy
Protect the corporate brand and competitive market position that could be damaged by a security incident

Ransomware attacks span multiple industries,
crippling operations and impacting local economies

Global criminals pivot from stealing data to hobbling operations and attacking infrastructure:
• JBS Foods: $11 million

Colonial Pipline: $5 million
NYC Subway and Massachusetts Ferry

> **can't do it alone. Business leaders have a** responsibility to strengthen their cyber defenses to protect the American public and our economy."
>
> - Jen Psaki
> White House press secretary

# The Cyproteck Solution

Cyproteck offers two solutions for companies looking to improve IT resilience. Backed by CyPROsecure and Cyproteck's unique position in the global network provider, we see more bad actors, so we can stop more bad actors. With organizations constantly under attack, only a reliable expert can provide lasting solutions to these problems. Cyproteck is redefining cybersecurity by working to be defenders of a clean internet

Throughout our large IP backbone, we able to see more of our pre of the internet's traffic, which then enables us to stop more attacks. Our experienced consultants help manage your network transformation and help you reduce cybersecurity risks and overcome internal resource constraints. Our mission is to make the internet safer for everyone, and safer for your business to grow.

For those organizations looking for more of a starting point, we also offer a quick Security Assessment. The Security Assessment offers a three-part vulnerability scanning service and a detailed summary of findings, with credit toward the purchase of future Cyproteck Security Services. For those looking to build out a more complete solution, a Ransomware Assessment is a 12-month program aimed at helping organizations identify their vulnerabilities, conduct routine scanning and build a long-term roadmap to close gaps in their cybersecurity strategy.

## Security Assessment

Cyproteck will provide a three-part vulnerability scanning service (Dark Web scan, technical scan and web applications scan) for one low price. Within 30 days of project kickoff, a prioritized report will be delivered showing vulnerabilities. The report also will contain recommendations for remediation and suggestions for follow-on services to strengthen the organization's security posture. This offer includes up to a $5,000 credit for the purchase of new Cyproteck Security Services.

Security Assessment capabilities
Dark Web scan: Uncover any exposed credentials on the Dark Web on your current domains (up to 5 domain names)

Technical scan: Assess network (up to 100 external IP addresses)

Web application scan: Assess applications Respond to threats before they become a crisis. (limited to 2 applications)

Assessment report: After the scans are completed, security analysts will deliver a report that summarizes the methodology, the findings and our recommendations. The assessment will be delivered within one month of project kickoff.

Security credit: Customer will be eligible to receive up to a $5,000 credit toward any future Cyproteck Security products and services.

Cyproteck can provide a security risk assessment within a short amount of time to provide the organization a starting point for awareness of current vulnerabilities, with recommended actions for remediation and follow-on services to help improve their security profile.

Our cybersecurity intelligence is backed by CyPROsecure, which is made up of security professionals and data scientists who analyze and rapidly respond to cyber threats across Cyproteck's global network.

### Security Assessment features

Quickly understand your biggest vulnerabilities and prioritize your security risks. No matter the size or maturity of your organization, you can benefit from implementing a process to regularly review your security posture and identify risks. This is a common best practice recommended by NIST, SOC 2, ISO 27001,

CYPROTECK

FedRAMP and others. Accelerate your security process by partnering with Cyproteck Security to conduct thorough assessments with clear recommendations in accordance with security best practices.

Align security strategy to business objectives. Only through a thorough understanding of your security risks and gaps months of the engagement. This is to provide continuity and show improvement.

## Ransomware Assessment

Ransomware is the most persistent cyber-threat businesses face today. The Cyproteck Ransomware Assessment program helps you strengthen your processes and technology to mitigate the threat of ransomware. Using the latest scanning and threat intelligence tools, Cyproteck consultants will provide you with ongoing support to help you minimize your organization's risk exposure and facilitate a fast recovery time.

You will be partnered with one of our tenured group of security professionals with decades of cybersecurity experience to help you assess your current state of readiness and develop a ransomware playbook to expertly manage ransomware attacks.

Ransomware capabilities

Regular vulnerability scanning: A designated Cyproteck security consultant will conduct a review of your security architecture and design to gain a better understanding of your business and what technical controls are already in place. Cyproteck security experts identify vulnerabilities that may be targeted in attacks through black box, white box or gray box scanning, with periodic re-scans of internal and external IPS to monitor progress over time. Once gaps are identified, we help customers track and make progress on resolving those deficiencies.

Tabletop Incident Response Exercise: Cyproteck will lead two incident response tabletop exercises to highlight process gaps, and help you establish ongoing practices to manage vulnerabilities and minimize your attack surface. The first exercise will occur during the first three months of the engagement with the second exercise being conducted during the last three

can you plan confidently for future security investments and initiatives. If you are migrating areas of your network to the cloud, storing large amounts of sensitive data, or consolidating IT systems, you need to know where all of your network vulnerabilities are or risk an attack that leads to decline in shareholder value, customer confidence, and increased business downtime.

Evaluation of security controls: After the initial vulnerability scan and tabletop IR exercise, Cyproteck security experts will recommend which critical security policies and procedures should be improved to achieve maximum effectiveness.

Visibility & reporting: Throughout the engagement, a designated Cyproteck security consultant will provide ongoing reporting of their findings. Together, the Cyproteck security consultant works with you in partnership to create a roadmap to how you can address those vulnerabilities. Cyproteck's process includes regular Vulnerability Management meetings, you are provided with regular status updates and recommendations for remediation.

Ongoing delivery management: Throughout the program, a Cyproteck project manager will help ensure these activities are on-track and will communicate start and completion dates of the program phases.

Ransomware Assessment features

The Cyproteck ransomware assessment helps you maximize their security resources, decrease risk exposure, and facilitates faster recovery times. Cyproteck's approach is designed to improve customer's overall risk management program.

- Protect and maintain data recovery.
- Undertake preventative measures before an event to ensure data is always recoverable.

- Optimize your support recovery time (.RTO) and recovery point objectives (RPO)

CYPROTECK