deepwatch™

WHITEPAPER

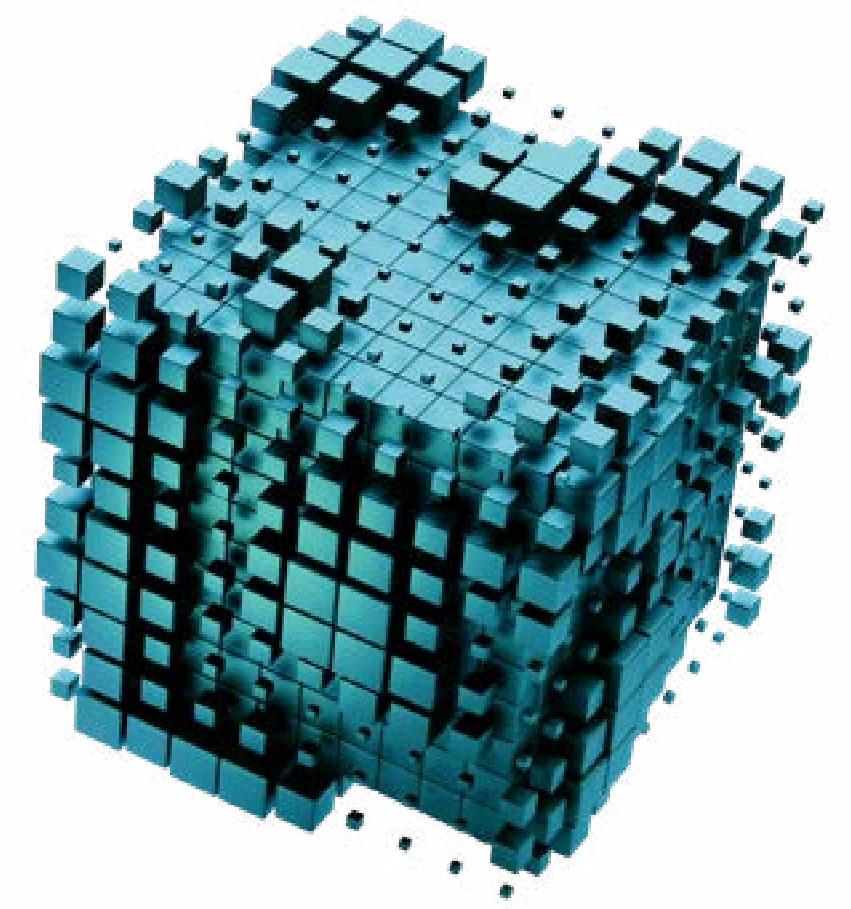
Move Beyond Detection & Response to Accelerate Cyber Resilience

Advantages of Managed Security and the Deepwatch Managed Security Platform

www.deepwatch.com

TABLE OF CONTENTS

deepwatch™



Cyber Resiliency is the ability to **anticipate, withstand, recover from,** and **adapt to** adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

(Source: NIST SP 800-160.)

Accelerate Cyber Resilience

Executive Summary

Cyber Resilience is not a tool, nor is it a solution. Cyber Resilience is a collection of continuing outcomes.

Since its inception, cybersecurity (or information security, going back a bit further) has focused on preventing a negative cybersecurity event. But we've learned you can no more prevent a cybersecurity attack from occurring than you can prevent a tornado in Kansas. You can prepare, you can study the weather, but on a long enough timeline, a storm occurs.

Cyber resilience is the admission of this fact, and the recognition that while we can prevent many attacks from being successful, we need the capability to anticipate and prepare for successful attacks, weather attacks with a minimum blast radius, and ultimately learn something, to improve our cybersecurity posture to ensure that the next attack does even less damage than the one before.

The cyber resilient enterprise is one that understands how its business relies on the operation of their cyber and IT infrastructure. They have identified the magnitude of risk to their business that interruptions in that infrastructure represent, and they are focused not simply on prevention, but on minimizing the impact of what they cannot prevent and hardening their environments against being impacted in the future.

The Deepwatch commitment to cyber resilience includes not only responding to cyber threats, but also actively preparing and equipping organizations to withstand, adapt, and thrive in the face of evolving security challenges. Proactive cyber resilience encompasses a holistic approach that combines advanced technology, expert analysis, strategic planning, and continuous improvement. In this overview, we discuss:

- The cyber resiliency journey and its importance
- Growing challenges that impact that journey
- Measuring and achieving cyber resilience (based on NIST guidance)
- Improved security outcomes when resilience is made a priority

Beyond Cybersecurity

The Deepwatch Commitment

The Deepwatch Commitment to Cyber Resilience

Cyber attacks and destructive data breaches have become key business risks in the age of remote work, cloud computing, and geopolitical instability. No longer simply tasked to protect the digital perimeter, security leaders must now anticipate threats across a growing attack surface, and withstand attacks that grow in volume and complexity every day. In the event systems are breached, a skilled security team must immediately triage the damage, dissect vulnerabilities to prevent future attacks, and adapt security programs or tools to a changing new normal. In essence, security teams must become more broadly resilient to cyber threats.

Resilience is a concept we understand in other areas of our lives. Businesses seek resilience in the face of recession or fickle consumers. Many seek resilience against the declines inherent in aging. Our structures are built in different areas of the country to be resilient against the prevalent weather threats for their area - hurricanes, tornados, earthquakes, blizzards, extreme heat, extreme cold, and the like. Deepwatch is the measured, managed path to cyber resilience for our customers who recognize this same approach is appropriate for their business.

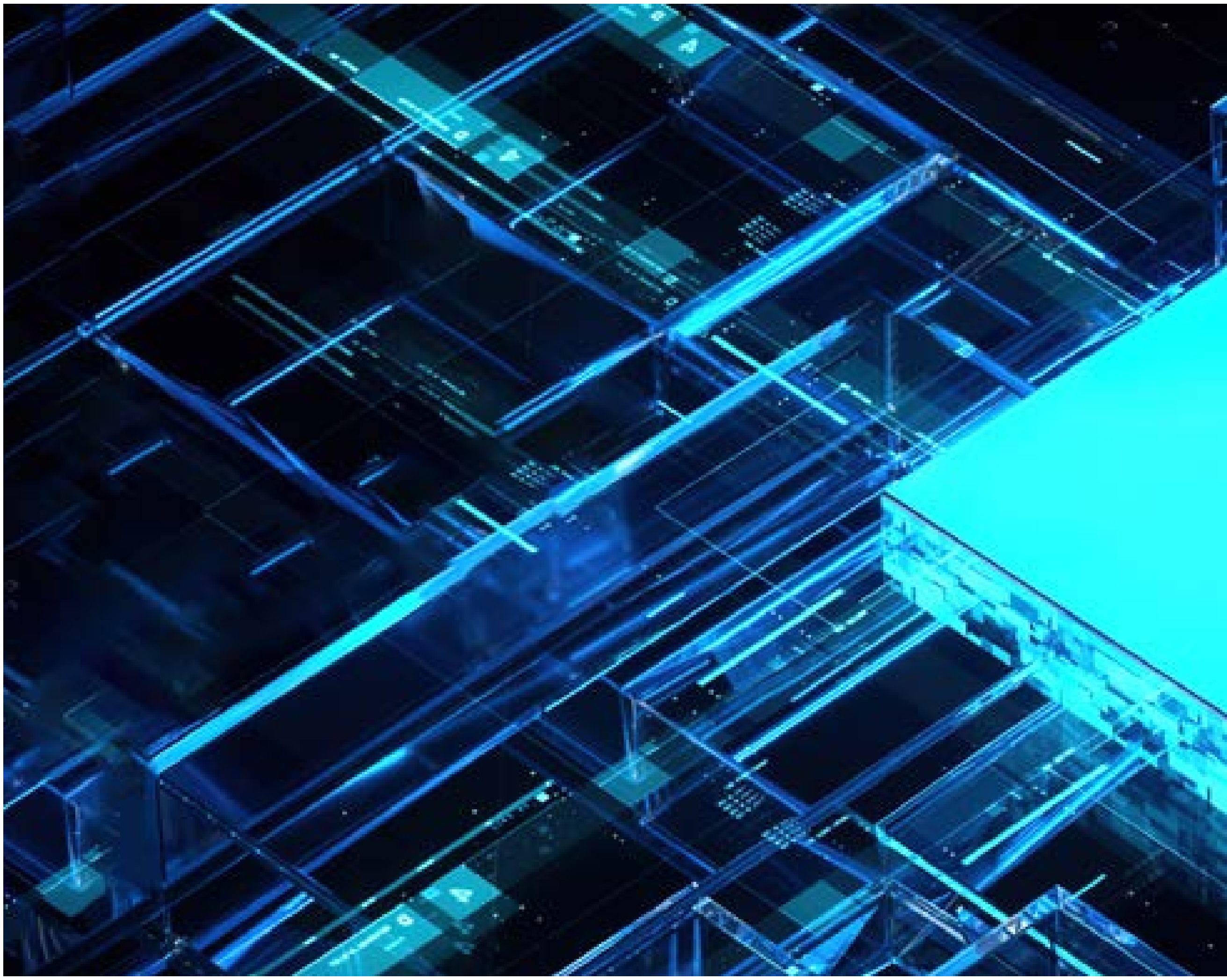
Cyber Resilience is the gold standard approach to enterprise security, establishing a clear, measurable baseline of an organization's capabilities, allowing them to measure progress toward an ultimate goal of reducing business risk.

> The Deepwatch definition of cyber resilience goes beyond NIST, as the ability to demonstrate business resilience to cyber security issues **through anticipation of risks, effective response to challenges, continuous improvement** of your Deepwatch Security Index score for detection and defenses, and the programmatic capability to **exercise, measure, and improve** each.

Why is Deepwatch Focused on **Cyber Resilience?**

Our approach to cyber resilience comes from a belief that security is a collection of outcomes, not merely tools or solution sets. Businesses have long used the term to discuss resilience in risk management, and a growing number of professionals in IT include cyber resilience in their title. It's an indication of the shift from merely defending the castle to preparing for battle.

What's more, as an industry leading managed detection and response provider for many years, Deepwatch has pioneered our own approach to security, emphasizing not only managed detection and response, but also on the outcomes these endeavors yield throughout the entire security journey. The fact is, bad days come to all security teams. The Deepwatch Experts are there with your security team on those days helping with incident response, forensics and remediation to assist in returning to normal operations as quickly as possible.

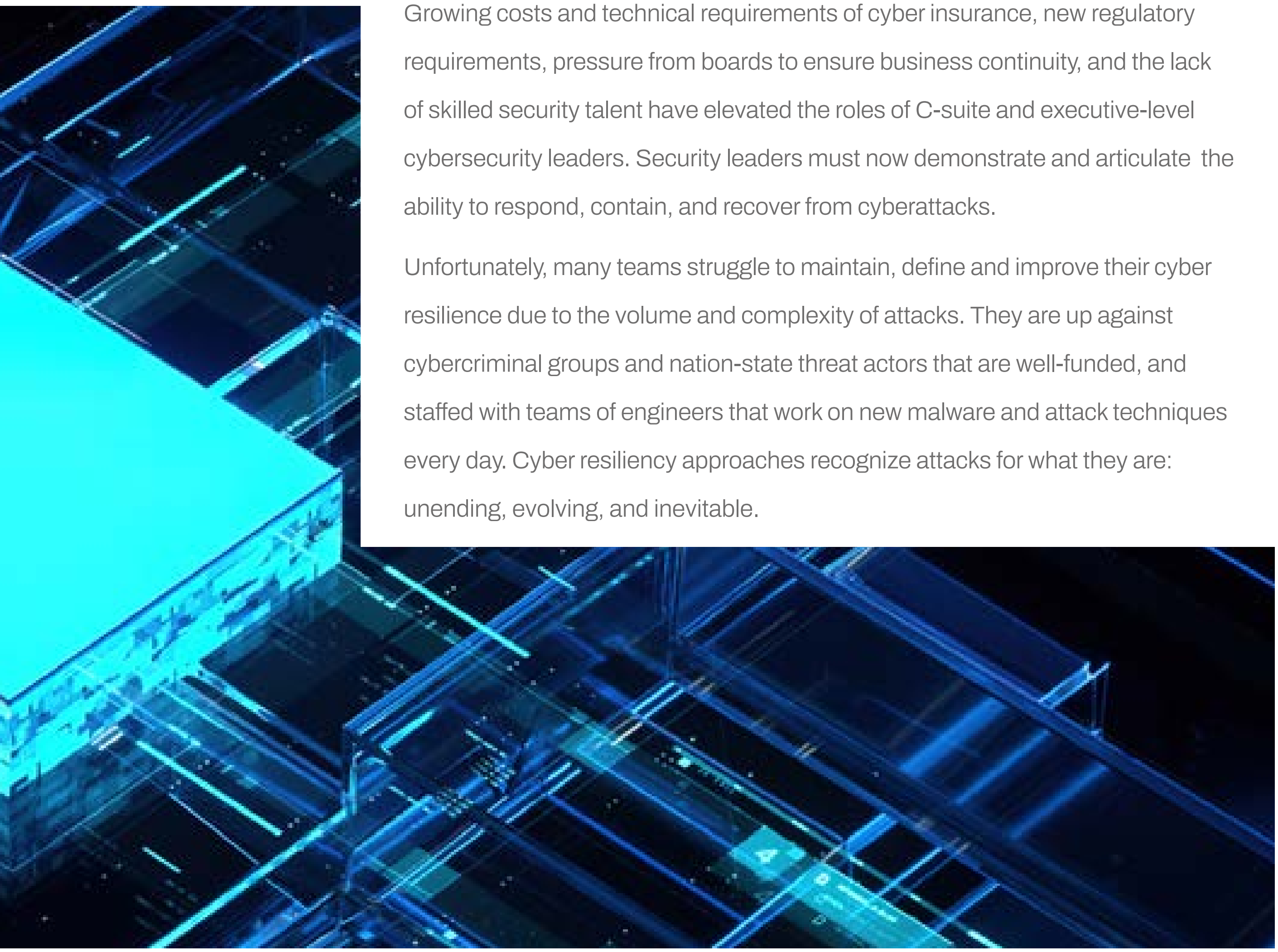


Growing **Challenges,** Mounting **Threats**

Open **Cyber Jobs**

Increase in **New Malware Variants**

Increase in **Cost of a Breach**



Growing costs and technical requirements of cyber insurance, new regulatory requirements, pressure from boards to ensure business continuity, and the lack of skilled security talent have elevated the roles of C-suite and executive-level cybersecurity leaders. Security leaders must now demonstrate and articulate the ability to respond, contain, and recover from cyberattacks.

Unfortunately, many teams struggle to maintain, define and improve their cyber resilience due to the volume and complexity of attacks. They are up against cybercriminal groups and nation-state threat actors that are well-funded, and staffed with teams of engineers that work on new malware and attack techniques every day. Cyber resiliency approaches recognize attacks for what they are: unending, evolving, and inevitable.

What is a **Cyber Resilient Enterprise?**

A cyber resilient enterprise is one that **understands their internal and external risks** and **can demonstrate consistent visibility** across its entire attack surface. They are not simply defending themselves, they are continuously fortifying positions and adapting to new tactics and techniques. The cyber resilient enterprise:

Anticipate:
Ability to understand your environment and how it maps to your **RISK** profile

Withstand & Recover
Effectively detecting a threat and executing the right **RESPONSE** at the right time

Adapt
Move responses forward to policies, update controls, and **IMPROVE** security posture

- Understands their current detection, response, and communication capabilities across their entire infrastructure (cloud, network, firewall, endpoints, and related teams).
- Retains and measures metrics to understand the effectiveness of their detection, response, and mitigation plans.
- Practice and refine response and recovery plans, including key business stakeholders, not just IT.
- Communicate metrics and capabilities in clear stakeholder narratives across the business in order to improve capabilities and processes.

Cyber resilient companies look to improve their security posture and response capabilities, while at the same time streamlining security tooling, infrastructure, and processes or policies. From a risk management perspective, cyber resiliency helps reduce the mission, business, organizational, enterprise, or sector risk depending on cyber resources.

The Deepwatch cyber resilience definition includes the ability to anticipate risks based on business objectives. It includes the right responses at the right times. And at its core, includes the mission of continuous improvement. Cyber resilience can only be achieved if there are metrics by which to measure and manage, metrics that matter not only to the effectiveness of security investments, but also to organizational risk reduction.

Cyber Resilience **Goals and Objectives**

Cyber resilience goals combine the risk management decisions at the mission or business process and system levels, and an organization’s risk management strategy.

To address cyber resiliency, each organization’s risk management strategy must include threat-framing with respect to cyber threats, strategies for achieving cyber resiliency goals, and strategic approaches to prioritizing and interpreting cyber resiliency objectives. Strategies for achieving cyber resiliency goals include:

Better Evaluation of Risk

- Internal, External, System and Business Risks
- Go beyond prioritization based on scan results
- Dynamic Alerting and prioritization based on internal and external context

Precise Actions

- The right action at the right time.
- Automation is critical, but so is understanding the risk of taking an action.
- Planning and executing the combination of active responses needed, along with policy changes, that enable preventative defenses.
- Precise mix of policy based, automation, and human enabled responses
- Active response capability beyond the detection point

Continuous Improvement

Organizations contend with different security maturity levels, or may have a security posture that leans more towards detection than toward proactive measures. Together we come to understand where the cybersecurity program currently sits and the direction it wants to go, getting buy-in from the business.

Based on these three pillars Deepwatch charts the security journey a company must take to achieve cyber resilience.

Accelerate Cyber Resilience

What to Expect from Cyber Resilience Improvements

Cyber resilience with Deepwatch delivers improved outcomes, reduced alert volume with higher fidelity, precision response, and an improved overall security posture.

Enhanced Security Outcomes

Improved security outcomes are the key result of managing and measuring cyber resiliency. Each organization must determine a security baseline from which to measure and improve efficiency and effectiveness. Beyond metrics of tickets or even number of attacks stopped, security teams must build narratives with both technical and non-technical stakeholders that show improvements in the reduction of risk.

High Fidelity, Low Volume Alerts

With Deepwatch Experts and our unique dynamic risk scoring, teams see lower volume, higher fidelity alerts that matter.

The traditional “alert everything” approach, which remains extraordinarily common across industries, incurs high costs and high alert volumes that waste security teams’ time and lead to alert fatigue. Through collaboration and conversation with your Deepwatch experts and our high fidelity/low volume threat scoring engine, you see only the alerts that matter. We leverage a range of correlation and anomaly driven capabilities based on detection and alerting, context, and trends internal and external to your environment.

The Deepwatch Managed Security Platform correlates every transaction across your enterprise to generate risk profiles for your assets and identities. This framework enables advanced correlation and dynamic assignment of risk values to every alert. Alerts are then generated based on your custom risk threshold. This unique Deepwatch approach results in an average 98% reduction in alert volume compared to traditional security providers while identifying 10 times more threats.

Precision Response

Deepwatch combines automation with manual expertise in customized threat response plans.
The Deepwatch Managed Security Platform enables fast and confident responses to security threats. With proper risk profiling and increased alert fidelity, you and your Deepwatch Experts take a programmatic and consistent approach to threat response, combining automation and manual expertise to execute tailored response plans designed to contain threats faster with minimal disruption to your business.

Improved Security Posture

Our patented Deepwatch Security Index leads you to an improved security posture. The path to cyber resilience is a journey of continuous improvement, day by day and week by week. Deepwatch has developed a patented security index that adapts to your specific environment, guiding you towards an enhanced security posture. This index considers the unique aspects of your environment and offers actionable recommendations for improvement. By tracking your score over time, you can monitor and demonstrate your progress and compare against industry peers.

Enterprise Cyber Resilience

The Deepwatch Advantage

Cyber resilience does not come from a set of tools. It comes from a strategic effort to anticipate threats, ensure timely response capabilities, and the effort to measure security improvements against a rapidly changing and complex threat landscape. Deepwatch is committed to cyber resilience, actively preparing and equipping organizations to withstand, adapt, and thrive in the face of evolving security challenges.

Deepwatch is the leading managed security platform for the cyber resilient enterprise. One of the fastest growing cybersecurity companies, we operate as an extension of our customer's team by providing 24x7x365 comprehensive security management for unparalleled visibility, precision response to threats and the best return on your security investments. With a customer base growing at nearly 75% annually, many of the world's leading enterprises rely on the Deepwatch Managed Security Platform to reduce risk, improve their security posture, and give them peace-of-mind.

deepwatch™

Deepwatch® is the leading managed security platform for the cyber resilient enterprise. Our platform combines patented, innovative technology with Deepwatch expert security practitioners to deliver unmatched threat detection and response capabilities. By operating as an extension of your cybersecurity team, we provide comprehensive security management, 24x7x365 monitoring, and precise automated threat responses. Deepwatch enhances visibility across your attack surface, improves security effectiveness and value through security technology and human security expertise. Join the growing community of leading brands who rely on Deepwatch for peace of mind and cyber resiliency.

THANK YOU