deepwatch™

The Deepwatch Managed Security Platform

The Hybrid Security Approach to Cyber Resilience

www.deepwatch.com

Table Of Contents

01. Executive Summary

The **Deepwatch Managed Security Platform** is our holistic approach to cybersecurity, combining industry leading technology, security experts, and patented processes to improve your organization's cyber resiliency.

Our managed security platform combines the technology, people, and processes for a hybrid, collaborative approach to measuring and improving your security program. It consists of three key components:

- **Threat Management Capabilities** encompass the security technology stack utilized by Deepwatch to proactively identify and address cyber threats.
- **The Deepwatch Security Center** provides an advanced engagement window to facilitate strategic and tactical conversations between you and your squad of Deepwatch Experts, providing improved visibility for proactive protection.
- **Deepwatch Experts,** including named analysts, engineers, and threat hunters do more than cover shifts 24/7/365, they become an extension of your organization.

The journey starts with inputs from your organization's unique environment, using existing security investments, to understand your dynamic attack surface to establish your distinct risk profile.

- **Your Security Data** - The unique telemetry generated across your enterprise.
- **Your Attack Surface** - The various ways an attacker could gain access to any asset in your environment.
- **Your Risk Profile** - The risks you face today against the current threat landscape.

The result of this collaborative, proactive approach to security is a more resilient organization with outcomes that include:

- **High Fidelity, Low Volume Alerting** - With Deepwatch Experts and our unique dynamic risk awareness, you see lower volume, higher fidelity alerts that matter.
- **Precision Response** - Deepwatch combines automation with manual expertise in customized threat response plans.
- **Improved Security Posture** - our patented Deepwatch Security Index offers clear metrics to measure security program performance.

02.

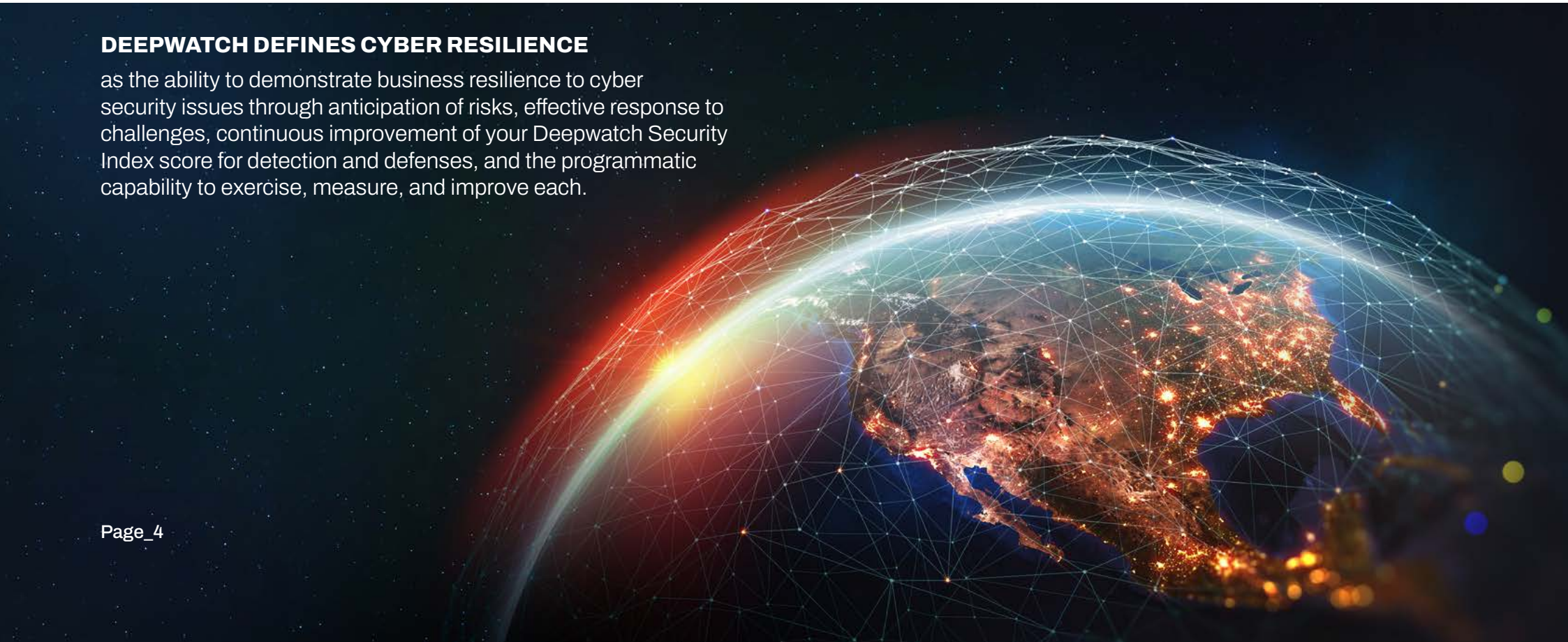
What is Cyber Resilience?

The National Institute of Standards and Technology (NIST) defines cyber resiliency as 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 800-172.)

DEEPWATCH DEFINES CYBER RESILIENCE

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.



03.
The Deepwatch Managed Security Platform

The Deepwatch Managed Security Platform is our holistic approach to cybersecurity, combining industry leading technology, security experts, and patented processes to improve your organization's cyber resiliency. Our managed security platform combines the technology, people, and processes that create a hybrid, collaborative approach to managed security. Our platform consists of three key components:

Our Threat Management Capabilities extend your in-house security effort, going beyond log collection and alerts. Deepwatch collaborates with your SecOps team to establish a comprehensive profile, then helps you prioritize threats most important to your organization.

The Deepwatch Security Center provides an advanced engagement window to facilitate strategic and tactical conversations between you and your squad of Deepwatch Experts, providing improved visibility for proactive protection.

Deepwatch Experts, including named analysts, engineers, and threat hunters do more than cover shifts 24/7/365, they become an extension of your organization.

04.

A Journey Guided by Your Inputs

Cyber resilience is not an outcome, it is a continuous journey, one with unique paths or choices. The success of Deepwatch Security Platform relies on inputs unique to your environment and critical to your organization's risk tolerance and desired security outcomes. We leverage and enrich your existing data, map your unique, dynamic attack surface, and collaborate with you to establish stronger risk profiles. Your Security Data. Your Attack Surface. Your Risk Profile.

With your inputs, Deepwatch collaborates with your SecOps team to establish a comprehensive baseline profile, then helps you prioritize your most critical assets and threats most important to your organization.

05.

Threat Management Capabilities

Deepwatch Threat Management Capabilities accelerate improvements to your overall security posture, extending your existing team's capabilities, or delivering new visibility and productivity in these key areas:

Identity And Asset Risk Profiles

Deepwatch develops risk profiles for your assets and identities, assessing factors such as access levels, external exposure, and business significance. These profiles serve as the foundation for informed decision making in downstream activities, including triage, investigation, response, and communication efforts.

Attack Surface Management

If an attacker can see it, an attacker can exploit it. Deepwatch works with you to map your attack surface while Deepwatch Experts monitor for activity against vulnerabilities or misconfigurations within your attack surface to provide prescriptive recommendations that reduce your risk exposure.

Security Policy Management

Navigating the complexities of implementing effective preventive measures in an ever changing landscape of threats can be challenging. Deepwatch experts simplify this process by offering security and configuration policy management for your crucial security tools, including endpoint, firewall, and vulnerability solutions.

Curated Threat Intelligence

Many publicly available open source and commercial security feeds offer generic and outdated information that may not be applicable to your business. At Deepwatch, we overcome this challenge by leveraging the collective intelligence community alongside our internal and organic intelligence curated by our researchers.

Deepwatch Dynamic Risk Scoring

To achieve early detection you need to go beyond signatures and static alerts. Deepwatch's high fidelity/low volume alerting engine enables risk-adjusted decisions tailored to your customized profile. By incorporating advanced techniques for normalization, correlation, anomaly detection, and leveraging the unique attributes of your environment and relevant threat intelligence, our approach ensures smarter, more dynamic detections with high fidelity and a low volume of alerts.

Complete Detection Coverage

With our industry leading detection catalog, you can instantly deploy detections designed to find threat actors and execute playbooks for a consistent process of triage, investigation, and response. Our dedicated team of experts constantly stays ahead of the latest adversary behaviors, helping you identify gaps and develop tailored plans to enhance coverage across the MITRE ATT&CK Framework.

Active Response

Automation, context, and human interaction enable the execution of the right action at the right moment, which is what truly differentiates Deepwatch Active Response and ensures effective protection. The ability to execute an immediate response to contain and isolate a threat once detected is critical. Taking actions such as isolating a breached host from the network along with disabling a compromised user account in order to sever access and contain the threat actor are not just time sensitive but could also be business impacting. These immediate response actions are executed through a combination of automation and Deepwatch Experts taking a coordinated approach based on contextual awareness.

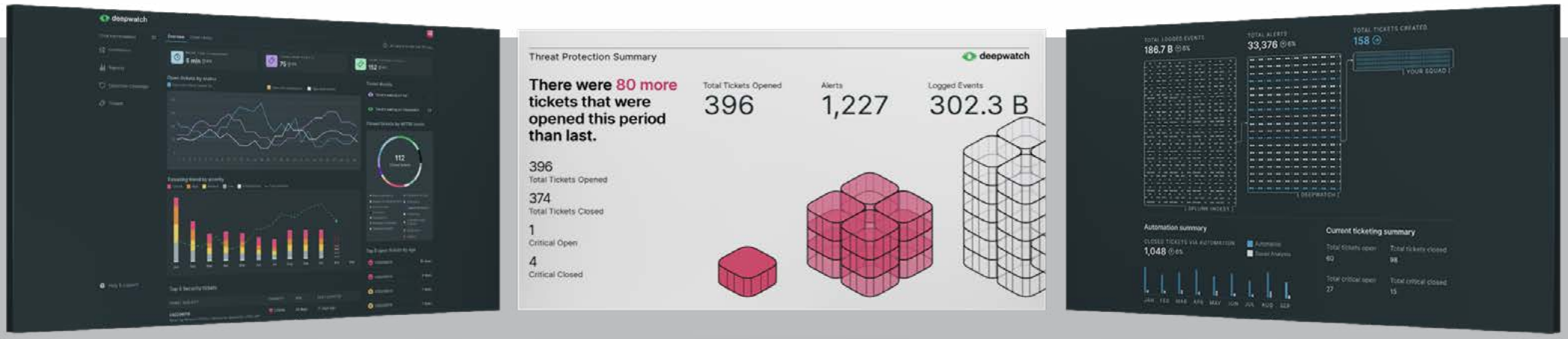
Continuous Threat Hunting

Deepwatch Threat Hunters combine our curated intelligence with contextual, risk aware approaches to identify threats and prioritize needed actions. Threat hunts operate both proactively and reactively to look for relevant behaviors and indicators of compromise from significant cybersecurity events or zero-day vulnerabilities.

06.
The Deepwatch Security Center

The Deepwatch Security Center is the engagement window that facilitates strategic and tactical conversations between you and your Deepwatch Experts. Our comprehensive, agnostic technology consolidates essential elements of our platform, including security data, risk profiles, detection coverage, threat intelligence, ticket management, metrics, and more.

The Deepwatch Security Center correlates security telemetry data from security tools across your environment to enable extended detection capabilities and precision response from Deepwatch managed security services. We see what you see, and help you tune security tools to your unique security posture.



01

Transparency and Engagement

The Deepwatch Security Center offers better transparency and engagement between your security team and Deepwatch Experts. This means you're not alone in your security journey – you have a team of engaged experts guiding you every step of the way.

02

Key Metrics & Reports: Data-Driven Insights

Data-driven decision making means that your security enhancements are rooted in solid information. We leverage environment data, service information, security activity, threat intelligence, and detection information. Every move we make is based on facts and tailored to your unique situation.

03

Self Service Data Transparency

Deepwatch believes that empowered customers with on-demand access to information are more cyber resilient. The Deepwatch Security Center lets you generate reports, review your environment, see available content, and understand what's happening in your environment in near real time.

07.
Deepwatch Experts

One of the most valuable features of the Deepwatch Security Platform is our people, a team of security experts you know by name that help you monitor and respond 24/7/365. Deeepwatch provides human-led, U.S.-based security experts using the latest security tools to gain a deep understanding of the unique nuances and risks present in your environment.

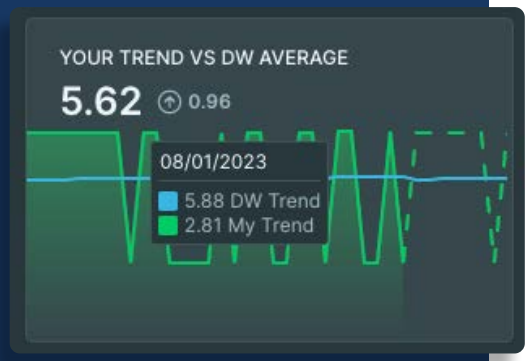
Deepwatch Experts work closely with you and your SecOps team throughout our partnership to fully understand the security dimensions of your organization, foster seamless collaboration, and maximize operational continuity and progression.

Deepwatch goes beyond the staffing of Tier 1 and Tier 2 analysts.
Deepwatch experts include:

- Onboarding Experts
- Security Analysts
- Detection Engineers
- Adversary Tactics & Intelligence team including threat hunters and responders
- Customer Success Managers
- Security Operations Engineers
- Onboarding Engineers
- Subject Matter Expert Engineers
  (Detection, Endpoint, Firewall, Vulnerability and Cloud)

08.
Outputs and Security Outcomes

Deepwatch delivers security outcomes driven by your unique business risk. We help your team prioritize risks based on their potential impact, align security understanding throughout the organization, and drive cost-effective security outcomes including:



The Deepwatch Security Index lets you measure your security program progress against industry peers and your own established security baseline .

High Fidelity, Low Volume Alerting

The Deepwatch platform 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. Our patented Dynamic Risk Scoring engine provides high fidelity, low volume alters, tailored to your organization's unique risk profile and desired outcomes.

Our patented Dynamic Risk Scoring engine provides high-fidelity, low-volume alters, tailored to your organization's unique risk profile and desired outcomes.

Precision Response

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. Deepwatch can take direct action defined by your profile, such as removing access to networks from an endpoint suspected of infection.

Improved Security Posture

The path to cyber resilience is a journey of continuous improvement. We developed the patented Deepwatch 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.

09.

Cyber Resilience Through Collaborative **Managed Security:** A Hybrid Approach

Technology solutions alone are expensive and cumbersome; while staffing solutions alone fill some gaps, but do little to improve security over time. **The Deepwatch Managed Security Platform** provides a collaborative hybrid approach to security, one that allows you to use existing technology investments, while adding critical security personnel and expertise. The result is peace of mind through alert volume reductions, improved precision response, and metrics for measuring and improving your cyber resilience over time.