

USE CASES

Improving Cyber Resilience with Trace3 and Deepwatch

Trace3's security consulting and tooling experience combined with Deepwatch's managed security platform capabilities provides a strengthened cyber security posture.

Use Case #1 – Alro Steel

Summary: Following the performance of a NIST assessment by Trace3, two security gaps were identified - Managed Detection and Response (MDR) and Managed VM. Alro recognized Deepwatch's data portability and security experts would be the true extension of the team that they were looking for. Alro also identified that our Security Index is unique from our peers and sees a lot of value in our ability to help assess and continue to improve their security program.

Challenge:

- Lack of internal SOC talent
- Lack of environment visibility to detect threats
- Desire for 24x7x365 SOC coverage

Key Initiative:

- MDR Project - desire to engage a 3rd party to acquire 24x7x365 coverage
- SOC Maturity - augment existing SOC for better coverage, visibility, and/or analytics

Solution(s):

- Managed Detection & Response
- Vulnerability Management

Business Impact:

- Initially purchased to bolster their security posture and gain 24/7/365 coverage

Use Case #2 – Paragon28

Summary: Paragon 28 was looking to elevate their security posture by replacing their existing Managed Security Service Provider (MSSP). They turned to Deepwatch because of the remarkable ROI and value we were able to tailor to their unique business needs. They were seeking enhanced threat detection capabilities and SOC functionality.

Challenge:

- Desire to mature their sec ops center
- Lack of environment visibility to detect threats
- Lack of internal SOC talent

Key Initiative:

- SOC Maturity - augment existing SOC for better coverage, visibility, and/or analytics
- MDR Project - desire to engage a 3rd party to acquire 24x7x365 coverage
- SIEM Project - renewal, refresh, or transition to cloud

Solution(s):

- Managed Detection and Response
- Endpoint Detection and Response
- Vulnerability Management

Business Impact:

- Maturity in tech stack for SIEM, Endpoint, and VM, all bundled within services; Ease of communication versus prior MDR.

Use Case #3 – Presbyterian Church

Summary: PCUSA was looking to stand-up a SOC, but did not have the people, process, or technology in place. As building this out internally was not a realistic option, they began to research MSSPs and chose the Deepwatch Managed Security Platform to provide them with a holistic approach to cybersecurity. Deepwatch provided industry-leading technologies, dedicated security experts and patented processes to improve their organization's cyber resiliency, as well as key reporting and metrics for their non-technical stakeholders.

Challenge:

- Lack of internal SOC talent
- Lack of environment visibility to detect threats
- Desire for SOC reporting metrics

Key Initiative:

- MDR Project - desire to engage a 3rd party to acquire 24x7x365 coverage
- SIEM Project - renewal, refresh, or transition to cloud
- SOC Maturity - augment existing SOC for better coverage, visibility, and/or analytics

Solution(s):

- MDR Essentials

Business Impact:

- Provide visibility via Splunk, 24/7/365 SOC coverage and maturity, business reviews & reporting for executive leadership

Use Case #4 – Trace3

Summary: Trace3 was not receiving value from their existing Managed Security Service Provider (MSSP) as alerts often lacked context and were duplicates or false positives. The combination of Deepwatch Experts and our dynamic risk scoring has resulted in high-fidelity, low-volume alerts. Since the initial engagement, Deepwatch has also taken on the management of its Endpoint Detection & Response (EDR) platform. The outcome freed up the Trace3 team to tackle the most important business priorities.

Challenge:

- Lack of internal SOC talent
- Desire to mature their security operations center
- Desire for 24x7x365 SOC coverage

Key Initiative:

- MDR Project - desire to engage a 3rd party to acquire 24x7x365 coverage
- SIEM Project - renewal, refresh, or transition to cloud

Solution(s):

- Managed Detection and Response

Business Impact:

- Trace3 sought a true partnership with a preferred MDR provider. As part of a revamped partnership, Trace3 trusted Deepwatch to lead their SOC and fully manage the Splunk environment.

ABOUT TRACE3

Trace3 delivers business transformation. We consult on, integrate, and operate convergent solutions across data, security, and cloud that embrace emerging technology and drive measurable value.

info@trace3.com

7505 Irvine Center Drive, Suite 100

Irvine, CA 92618

www.trace3.com



ABOUT DEEPWATCH

Deepwatch® is the leading managed security platform for the cyber resilient enterprise. Our platform combines comprehensive threat management capabilities, expert practitioners, and precise automated actions. Embrace preventative actions to improve your security posture and enhance your speed of response. Join leading global brands relying on Deepwatch for cyber resiliency and security peace of mind.

CONTACT US

sales@deepwatch.com

[GET STARTED](#)

4030 W Boy Scout Blvd. Suite 550
Tampa, FL 33607

www.deepwatch.com