Reduce Your Endpoint Attack Surface

There’s no question that end users have become a prime target for cyber criminals. In many organizations, endpoints account for most of the attack surface.

Despite organizations mandating security awareness training for employees and spending a significant portion of their security budgets on modern endpoint protection tools, assessing the security strength of their endpoints remains a major gap.

Optiv Solutions

Optiv’s partnerships with market-leading vendors help organizations select, deploy and integrate endpoint security technologies. But that’s only half the story. It’s also critical to support any endpoint strategy with regular assessments. Optiv’s Endpoint Configuration Review enables clients to apply an informed endpoint strategy with confidence, avoiding unnecessary product deployments and hardening endpoint systems against attacks and weaknesses.

Optiv identifies the baseline security controls that will be used for the configuration review and:

- Collects security tool inventory on endpoints
- Reviews configuration baselines
- Analyzes deployment, patching and update processes
- Assesses OS hardening against industry standards
- Performs automated compliance scans

We then report on significant findings, detailing how an organization’s endpoint images and security tool configurations align with industry best practices, and include recommendations for next steps.

How Do We Do It?

System and Environment Review
Review client endpoint environment, such as software installation, inventory and approval process, patching process, hardening guidelines and endpoint security tools in use

Process Review
Gain an understanding of the associated endpoint processes

Endpoint Hardening Analysis
Scripted and authenticated data collection with additional manual collection and validation of current configuration settings

Targeted Endpoint Security Configuration Review
Review in-scope security tool configurations and compare to the hardening analysis for overlap

Documentation
Provide summary documentation, including the environment overview, analysis procedures, hardening and security tool recommendations and all other detailed findings
The Optiv Advantage

Optiv can help enterprises in every industry connect information security policies, procedures and practices with business goals. Our security leadership experts, backed by our team of consultants, can provide the experience you need to take your program to the next level.

Expert Minds
Optiv’s security professionals are dedicated to helping you achieve results and realize value. Our team of 1,000+ highly skilled client managers and security practitioners work hard to deliver superior results and cutting-edge research to solve your complex, real-world security problems.

Client-First Culture
Optiv’s passion for security and our commitment to quality results means we focus on the right solutions to meet your specific needs.

Proven Methodologies
Optiv has developed proven methodologies to help ensure superior outcomes for your projects and programs.

Leading Best Practices
Our knowledge of leading best practices helps Optiv formulate security recommendations tailored to meet your specific business objectives.

Related Services

Objective Technology Analysis & Validation (OTAV)
Optiv’s OTAV service assists organizations through the process of selecting best-in-class security technology, based on client priorities and requirements, industry expertise, knowledge of security best practices and actively comparing security solutions and validating vendor claims.

Security Information and Event Management (SIEM)
With expertise in a wide range of top SIEM/UEBA solutions and industry best practices, Optiv provides professional service engagements designed to support clients wherever they are in their SIEM journey.

Case Study
North American Travel Retailer Reduces Security Risk Through Endpoint Configuration Review

Customer Profile
With over 10k employees and hundreds of retail locations, the client provides travel retail experiences across North America.

Desired Outcomes
The assessment objective was to detail how endpoint images aligned with industry standards and best practices, and then focus on how the client should configure and implement their new endpoint security software to achieve the most practical and effective security posture.

Solution
Optiv analyzed data gathered from a variety of sources, including access to workstations, servers and Point of Sale (POS) images, then conducted interviews with client staff. Optiv provided a security posture rating to compare to organizations of similar size and industry. Final findings and recommendations were based upon both current and perceived future inadequacies. When clients implement recommendations, they can advance their security posture further.

Client Benefits
With the results of Optiv’s Endpoint Configuration Review, the client was able to reduce their security risk by:

- Identifying strengths and weaknesses of the current desktop and laptop images
- Using best practices to determine if current images contain any gaps
- Validating Risk Controls Self-Assessment against current configurations and processes

Secure greatness™
Optiv Security is the cyber advisory and solutions leader, delivering strategic and technical expertise to more than 7,000 companies across every major industry. We partner with organizations to advise, deploy and operate complete cybersecurity programs from strategy and managed security services to risk, integration and technology solutions. With clients at the center of our unmatched ecosystem of people, products, partners and programs, we accelerate business progress like no other company can. At Optiv, we manage cyber risk so you can secure your full potential.

©2022 Optiv Security Inc. All Rights Reserved. Optiv is a registered trademark of Optiv Inc.