WOLVERINE M&A SOLUTION

Operational Cybersecurity Intelligence for Mergers & Acquisitions

Reduce risk, accelerate integration,
and optimize cybersecurity spend from day one

THE M&A CYBERSECURITY REALITY

When two organizations merge, their cybersecurity environments rarely align. Tools overlap, licenses pile up, features go unused, and management cant see how security spending reduces risk. Meanwhile, Boards and executive teams demand proof that cybersecurity spending is both effective and fiscally responsible. Traditional dashboards and point analytics often show metrics that don't answer the most relevant questions: Are we spending wisely? Where are the gaps in our defenses? Which tools are redundant or underutilized?

Cyberhill recognizes that complex, mismatched cyber environments are common in M&A. Wolverine provides a unified operational intelligence layer that ensures consistent, governed, and adaptable cybersecurity integration through its AI-driven, ontology-based platform—turning cybersecurity from a post-merger liability into a strategic advantage.

Wolverine minimizes uncertainty, enhances value capture, and simplifies cybersecurity optimization for the newly combined organization.

REDUCE RISK, ACCELERATE INTEGRATION, AND OPTIMIZE SPEND

Wolverine offers the intelligence layer that enables organizations to unify, govern, and optimize cybersecurity immediately after closing.

- Consolidate overlapping tools and features by identifying redundancies across the entire cyber stack.
- Rationalize decisions on licenses and vendors through utilization and cost analysis.
- Enhance visibility into coverage gaps, inefficiencies, and risk exposure
- Establish consistent governance across security domains (network, endpoint, identity, application, cloud, compliance)
- Accelerate post-close integration by aligning controls, reporting, and risk posture.
- Unify the view of tools, features, domains, and costs into a single operational model.

Wolverine helps leadership understand not only what's deployed but also what is unused, redundant, or misaligned with the organization’s risk priorities—providing clarity in defense-in-depth across the merged enterprise.

For M&A, this means cybersecurity integration is no longer reactive or manual—it becomes **self-optimizing from day one.**

THE WOLVERINE CYBERSECURITY LAYER

Wolverine is built on a cybersecurity ontology that maps:

- Tools in Use: SIEM, EDR, IAM, WAF, vulnerability management, DLP, and cloud platforms
- Features of each tool including log correlation, anomaly detection, MFA enforcement, threat hunting, and sandboxing.
- Domain Coverage: network, endpoint, identity, application, cloud, supply chain, and compliance

By mapping these relationships, Wolverine creates a unified cybersecurity model across both organizations. This ontology is what enables AI to deliver actionable intelligence, changing dashboards from static reports into dynamic, decision-making tools.

VISUALIZE, GOVERN, AND OPTIMIZE ACROSS BOTH COMPANIES

Wolverine transforms post-merger cybersecurity into a governed, AI-ready system.

- Visualize relationships, dependencies, and risk across both organizations' security stacks
- Convert due diligence artifacts into connected operational intelligence
- Prioritize tool consolidation and license reduction by identifying overlap and underutilization
- Build a governed, adaptive cybersecurity layer that continuously improves both protection and cost efficiency

FROM DUE DILIGENCE TO EXECUTION

M&A generates large amounts of cybersecurity documentation—vendor lists, licenses, controls, and risk assessments. Wolverine converts that static information into a **dynamic, governed model** of the combined organization's cyber posture.

Conversational, Executive-Level Insight

Instead of static reports, Wolverine enables natural-language queries such as:

- "Which tools overlap in endpoint security coverage?"
- "Which features are we paying for but not using?"
- "What is our year-over-year SIEM spend?"

Dashboards transform into **decision-making hubs**, enabling CISOs and executives to continually optimize both security posture and financial efficiency.

KEY DELIVERABLES

Unified Cybersecurity Ontology

A structured blueprint of all tools, features, domains, and dependencies across the merged enterprise.

Cyber Intelligence Layer

A single operational view of cybersecurity posture, coverage, and cost across Company A, Company B, and the combined organization.

Governance Framework

Standardized visibility into risk, utilization, and financial efficiency across all security domains and directly compare against any regulatory compliance, or governance framework.

AI Optimization & Readiness Roadmap

A forward-looking plan for adaptive defense, predictive analytics, and continuous cybersecurity optimization.

FINANCIAL & OPERATIONAL IMPACT

In addition to managing risk, Wolverine promotes true financial stewardship of cybersecurity—critical in post-merger environments. Its ontology-driven analytics provide executive-level insight into:

- **Cost per tool and per feature**
- **Features in use vs. licensed**
- **Utilization rates across the stack**
- **Coverage cost efficiency by domain**
- **Overlap and redundancy across vendors**
- **Year-over-year and quarterly budget trends**
- **Alignment of spend with organizational risk profile**

Wolverine reduces uncertainty, increases value capture, and ensures that cybersecurity does not become a hidden cost center after a merger—but a strategic advantage.

WHY WOLVERINE FOR M&A

Cybersecurity integration is one of the most complex and costly parts of any merger. Wolverine turns that complexity into a unified, intelligent, and self-healing system—ensuring risks are reduced, resources are optimized, and leadership gains immediate clarity across the combined organization.

Wolverine provides the hidden intelligence layer that makes M&A integration faster, safer, and financially accountable—turning cybersecurity into a strategic advantage from day one.