# Cybersecurity Excellence: ServiceNow SecOps, IRM, & Zscaler

'ike (knowledge) level: Novice

Rev. February 6, 2025

## Introduction ↘

In today's digital-first environment, cybersecurity has become more critical than ever. Organizations are grappling with a growing number of cyber threats, evolving compliance requirements, and an increasingly distributed workforce. Traditional security models are no longer sufficient to address these challenges effectively. This white paper explores how organizations can use ServiceNow's Security Operations (SecOps) and Integrated Risk Management (IRM) solutions in combination with Zscaler's Zero Trust architecture to create a comprehensive, proactive cybersecurity strategy that is adaptive, resilient, and agile.

ServiceNow's cloud-based solutions provide the foundation for automating and optimizing security operations, risk management, and compliance. Zscaler complements this with its Zero Trust security approach, which emphasizes the principle of "never trust, always verify" in securing network traffic, regardless of location or device.

### The Cybersecurity Challenge ↘

The growing complexity of cyber threats presents several challenges for organizations:

- **Advanced Persistent Threats (APT)**: Cyberattacks have become more sophisticated and persistent, often bypassing traditional perimeter security measures.
- **Distributed Workforce**: With remote work on the rise, securing users, devices, and data outside the traditional corporate network perimeter has become increasingly difficult.
- **Compliance and Regulations**: Regulatory requirements for data privacy and protection are becoming more stringent, and non-compliance can result in severe penalties.
- **Rising Attack Surface**: The expanding attack surface, fueled by cloud adoption, IoT, and BYOD (Bring Your Own Device) policies, increases the potential for breaches.

Organizations must adopt new approaches that not only address current threats but also build resilience into their IT infrastructure.

### ServiceNow Security Operations (SecOps) and Integrated Risk Management (IRM) ↘

ServiceNow provides a suite of solutions designed to help organizations improve their cybersecurity posture. These solutions enable organizations to respond to threats in real-time, manage risk, and maintain compliance. Let's take a deeper dive into the key ServiceNow capabilities:

#### 1. Security Incident Response (SecOps)

ServiceNow's Security Incident Response (SIR) module helps organizations quickly identify, investigate, and respond to security incidents. It provides:

- **Automated Incident Management**: SecOps automates the creation of security incidents from threat intelligence feeds, alerts, or user reports, enabling faster detection and resolution.
- **Collaboration and Orchestration**: Through integration with other systems and tools, SecOps provides workflows for security teams to collaborate and respond to incidents efficiently.

- **Prioritization and Workflow Automation**: By using advanced machine learning algorithms, ServiceNow can prioritize incidents based on their severity, impact, and potential risk, automating workflows and reducing manual intervention.

### 2. Threat Intelligence Integration

ServiceNow integrates with threat intelligence feeds, enabling teams to gain actionable insights from global threat data. These feeds enhance situational awareness and ensure that the organization stays ahead of evolving threats.

### 3. Vulnerability Response (SecOps)

Security vulnerabilities can expose organizations to significant risk. ServiceNow's Vulnerability Response module integrates with IT and security teams to ensure that vulnerabilities are quickly identified, prioritized, and remediate based on their potential impact.

### 4. Integrated Risk Management (IRM)

ServiceNow's IRM solutions focus on managing risks from a broader organizational perspective. These capabilities help organizations assess and mitigate risks through the following:

- **Risk Management**: By automating risk assessments, creating mitigation plans, and tracking risk mitigation efforts, IRM helps organizations reduce the overall risk to critical assets.
- **Policy and Compliance Management**: ServiceNow automates the enforcement of policies and provides continuous monitoring for compliance with industry standards and regulations.
- **Audit Management**: IRM provides capabilities for tracking and managing audits, ensuring that compliance is maintained across various regulatory frameworks.

## Zscaler and the Zero Trust Security Approach ↘

Zscaler is a leading provider of Zero Trust network security solutions that focus on securing user access and application traffic, regardless of device location or network perimeter. Zscaler provides several key features to strengthen cybersecurity initiatives:

### 1. Zero Trust Access

The Zero Trust approach fundamentally shifts security from relying on a trusted perimeter to a model where trust is never assumed, regardless of where the user or device is located. Zscaler's Zero Trust Network Access (ZTNA) ensures that access to applications is granted based on strict identity verification, device health checks, and context, reducing the risk of breaches.

- **Least Privilege Access**: Users only get access to the resources they need, limiting exposure in the event of a compromised account.
- **Adaptive Authentication**: Zscaler dynamically adjusts access permissions based on risk assessments, ensuring that only authenticated and authorized users can access sensitive data.
- **Encrypted Traffic**: Zscaler encrypts all traffic, ensuring that sensitive data is protected in transit, even across untrusted networks.

### 2. Secure Web Gateway (SWG)

Zscaler's Secure Web Gateway ensures that all web traffic is filtered, inspected, and validated for malicious content, data loss, and other threats. This helps prevent threats from entering the network while allowing users to access the internet securely.

### 3. Cloud Firewall

Zscaler's cloud firewall provides real-time traffic inspection and policy enforcement for all inbound and outbound traffic, regardless of whether it's coming from inside or outside the corporate network. This minimizes attack surfaces and enhances visibility.

### 4. Cloud Sandbox

Zscaler's sandboxing capabilities allow for the safe detonation and inspection of potentially malicious files, ensuring that malware does not enter the corporate environment.

## Combining ServiceNow and Zscaler for a Unified Cybersecurity Strategy ↘

When combined, ServiceNow's SecOps and IRM modules with Zscaler's Zero Trust security approach create a unified and proactive cybersecurity ecosystem. Here's how these solutions work together to strengthen your security posture:

### 1. Integrated Threat Detection and Response

ServiceNow SecOps integrates with Zscaler's threat intelligence and real-time security data to provide a faster, more automated response to cyber incidents. Zscaler's detection capabilities, such as its cloud firewall and secure web gateway, feed into ServiceNow's Security Incident Response system, enabling seamless automation and faster incident resolution.

### 2. Proactive Risk Management

Zscaler's Zero Trust security model ensures that access to critical systems is tightly controlled and constantly monitored. In tandem with ServiceNow's IRM, which provides an integrated view of risk across the organization, teams can identify and mitigate risks early, ensuring that sensitive data and systems are adequately protected at all times.

### 3. Continuous Compliance Monitoring

ServiceNow's compliance management capabilities, paired with Zscaler's granular control over access and traffic, help organizations maintain compliance with regulatory standards such as GDPR, HIPAA, and others. Zscaler enforces access controls while ServiceNow tracks compliance efforts, helping organizations reduce the likelihood of non-compliance and associated penalties.

### 4. Improved Collaboration and Efficiency

Both ServiceNow and Zscaler provide centralized dashboards and insights that enable security teams to collaborate more effectively. ServiceNow's unified platform allows teams to track incidents, vulnerabilities, and risks, while Zscaler ensures that traffic and access are always monitored and protected. This

integration improves operational efficiency and enhances the overall cybersecurity posture of the organization.

## Conclusion ↘

The combination of ServiceNow Security Operations, Integrated Risk Management, and Zscaler's Zero Trust approach offers organizations a comprehensive, modern, and adaptive cybersecurity strategy. By integrating these powerful solutions, organizations can proactively manage security incidents, minimize risk exposure, ensure compliance, and protect their digital assets against the most advanced cyber threats.

In a world where the landscape of cybersecurity threats is constantly evolving, leveraging both ServiceNow and Zscaler provides a powerful foundation for achieving cybersecurity excellence. Through automation, real-time threat detection, and a zero trust approach, organizations can create a more resilient security framework, protecting their data, users, and systems from ever-growing threats.

## About Mana'o Pili ↘

Mana'o Pili is a Hawai'i based technology consulting firm specializing in business automation through ServiceNow.  Mana'o Pili provides its customers with individualized solutions. We reject the notion of one-size-fits-all solutions. Instead, we partner with you to craft a tailored plan that aligns with your unique needs, budget, and objectives. Our approach focuses on optimizing your existing platform while minimizing customization and reducing technical debt.

Here at Mana'o Pili, we treat our customers as 'ohana (family), listen closely to your challenges and deliver tailored attention with exceptional service.