Why Your Organization's Endpoints Are Your Greatest Source of Risk

Presented @ North Carolina Cybersecurity Summit

Josh Frank, Regional Vice President,
Technical Account Management, Tanium

Tuesday, October 4th, 2022
What is IT Risk?

Gather and analyze data to improve security posture and compliance
Organizations face daunting challenges that significantly increase risk exposure

- Distributed Workforce
- Security Staff Shortage
- Rapid Migration to Cloud
- Lack of Visibility
Many CISOs can’t answer basic questions about the state of risk and compliance in their environment.

- Is my organization compliant with regulatory frameworks?
- How should our organization prioritize remediation efforts?
- Which endpoints present the greatest risk to my enterprise?
- How can I demonstrate the impact we’ve had on risk posture to the Board?
Traditional Risk Mitigation Approaches Are Siloed

Are there critical vulnerabilities?

Is software updated?

What are my compliance exposures?

Are security agents properly installed?
Why do organizations struggle to assess endpoint risk?

IT leaders can’t make informed decisions quickly when data is limited and disconnected.

55% of organizations use more than 20 tools across IT Operations and Security.¹

40% of CIOs say silos make it difficult to identify the severity of an issue and minimize business impact.²

89% of IT leaders report data silos are creating business challenges for digital transformation initiatives.³
The Power of Data

Completeness

Accuracy

Timeliness

Automated

Continuous

Data
Key Elements of Risk Management

**Data Collection**
The first process in identifying risk is to gather data. Data resides in multiple, disparate sources.

**Analysis**
Analysis and Risk categorization needs to be automated given the growing data sets.

**Remediation**
Remediation and mitigation efforts need to be aligned with the business impact.

**Reporting**
Gathering comprehensive risk metrics and synthesizing for exec-level reports is important for data-driven conversations.
IT Risk Categorization

Operations
- Business continuity
- Availability of IT systems
- Unmanaged assets
- Misconfigured systems
- Performance issues

Security
- Vulnerabilities
- Sensitive data
- Endpoint defenses
- Missing compensating controls

Regulatory
- Compliance with different regulatory frameworks
Ensure you have a patching and update program. This is critical, especially in today's security environment. Nearly 60% of the CSO/CISOs we work with do not know which systems have been patched, which need to be patched, and most importantly, which should be on their networks in the first place. Firms [need to connect] IT and SecOps in an unrivaled way. Identifying these vulnerabilities requires a combination of security assessments, tools, and software to remediate infrastructure threats.
RISK USE CASES
Reduce Attack Surface

- Identify lateral movement
  - Nearly 100% of attacks take advantage of user privileges to propagate the attack

- Cyber Hygiene
  - Nearly 100% of attacks take advantage of known, unpatched vulnerabilities
Discover Sensitive Data

• Visibility into where sensitive data resides

• Who has access to data

• Automated tools to protect the data
Compliance Reporting

• Choose a framework

• Continuously monitor compliance

• Quickly identify the gaps and compensating controls
Executive and Oversight Reporting

- Overall view of risk posture
- Performance over time
- Identify gaps to align investments
- Data-driven conversations with key stakeholders
Benchmarking

- Compare risk performance with similar organizations
- Measure effectiveness of risk mitigation programs
Prioritization and Automation

- Smart Prioritization based on business impact
- Automate mundane tasks first, to gain confidence in the system
Asset Visibility

How many devices do you have in your environment?
Do you know what or where those devices are?

Tool & Cost Optimization

Are you paying for software you aren’t using?
Do you have a strategy for long-term cost optimization?

Risk & Compliance

How are you assessing risk? Are you in compliance?
What is your patch efficacy across your environment?

Sensitive Data Protection

Do you know which systems are storing critical data?
How are you measuring data privacy risk today?

Response & Remediation

How quickly can you identify and respond to malicious threats?

Risk Management Maturity Model
THANK YOU