Misconfiguration Increases the Endpoint Attack Surface

The Emerging Era of Configuration Risk Analysis

Endpoints are critical to your business. Any disruption to these systems impacts business operations. When these systems are misconfigured by users or admins, they become vulnerable to cyber-attacks that can affect wholesale system function.

Common endpoint misconfigurations

These can be related to settings, registry settings, risky services that are needlessly activated, access control configurations. These types of attacks are a leading causes of system disruption today.

REGISTRY SETTINGS

RISKY SERVICES

ACCESS CONTROL CONFIGURATIONS

Endpoint Configuration – Challenging but Critical

Most endpoint protection platforms lack the ability to assess the risk associated with misconfiguration.

27%

of ESG research respondents reported that overall configuration and asset management of endpoints is one of their greatest challenges when it comes to the security of their endpoints.

33%

of organizations surveyed indicated that specific access configurations and restrictions are among the most important features or capabilities when it comes to managing endpoint devices.

Endpoint Configuration – Challenging but Critical

PROBLEM:

Attackers target holes in the attack surface via well-known endpoint application and configuration vulnerabilities.

SOLUTION:

With new endpoint risk analytics tools, SecOps teams can continuously reduce the attack surface and safeguard endpoints from attacks by weeding out the most common sources of compromise and breaches.

PROBLEM:

Most SecOps teams are overwhelmed daily with reactive, repetitive tasks such as vulnerability management, incident triage, and patching.

SOLUTION:

Endpoint risk analytics let SecOps teams spend this time more strategically—on risk profiling and proactive risk mitigation of endpoint assets.

New innovations by companies like Bitdefender address attack surface management by providing **fully integrated risk assessment and remediation** capabilities within an endpoint protection platform.

Continuous Visibility into Individual Risk Characteristics

Assessing security risk requires a broad solution that provides continuous visibility into the individual risk characteristics for each system in use.

REDUCE ATTACK SURFACE

Risk analytics - enabled hardening

STOP MALWARE AND FILELESS ATTACKS

Next-gen attack prevention

INVESTIGATE AND RESPOND

Endpoint detection and response

ENDPOINT TELEMETRY

The solution should provide automated capabilities to quickly remediate the most common misconfigurations and monitor for and alert on more unusual configuration issues. These capabilities need to tightly integrate with the broader endpoint protection platform, enabling IT and security teams to share a common mechanism that can provide timely, consistent visibility and remediation of configuration issues.

Ideally, risk assessment would share the same, single agent that is used for prevention, detection, and response.

See how Bitdefender can help

LEARN MORE

Bitdefender

Source: ESG Master Survey Results, *Modern Endpoint Management*, December 2018.