Breach Management

Prevent endpoint attacks. Strike fast to resolve.

BUSINESS CHALLENGE

Business impacts related to cyberattacks and information security breaches cost organizations up to $5 million per attack.[1] To mitigate these risks, organizations must focus on endpoints where potentially sensitive data could be downloaded or consumed. But with endpoint management becoming increasingly complex, security teams are struggling to respond efficiently to incidents, resulting in unprecedented business risks and costs.

A NEW APPROACH

Organizations employ a multitude of specific detective and preventive controls to protect themselves against specific threats, such as malware and data leakages, on their endpoints. However, this patchwork of controls is complex to manage and risks overloading endpoints with multiple agents. Nexthink helps simplify the endpoint security ecosystem with its ability to monitor and respond against multiple threats. Our broad coverages enable organizations to optimize their resources related to endpoint security tools and resources.

OUR SOLUTION

Nexthink offers a comprehensive endpoint approach aligned with standard cyber-security frameworks. We provide a unique approach to detect and report suspicious behaviors on endpoints, coupled with visualization and scoring features to help teams efficiently triage security incidents. Using Nexthink Act, teams can efficiently and rapidly respond to breaches by triggering both manual and automatic remediations across all endpoints.

BUSINESS OUTCOME

- Reduce security risks

CYBER CONTEXT

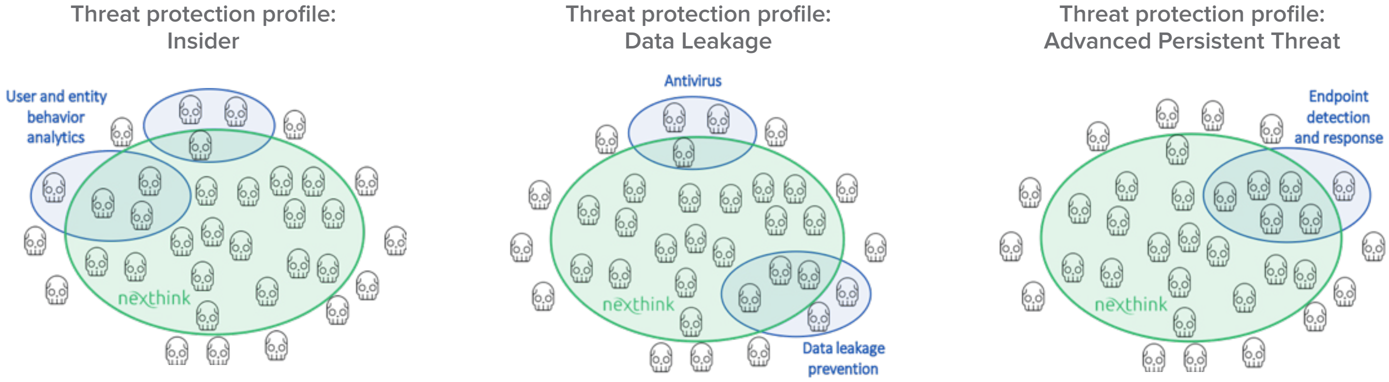
● **PREVENT**
Security awareness

● **PROTECT**
Ensuring compliance

✓ **DETECT**
Threat detection

✓ **RESPOND**
Incident response

With Nexthink: Monitor and respond against multiple threats



Threat protection profile:
Insider

Threat protection profile:
Data Leakage

Threat protection profile:
Advanced Persistent Threat

User and entity behavior analytics
nexthink
Antivirus
nexthink
Data leakage prevention
Endpoint detection and response
nexthink

[1] Ponemon Institute, *Cost of a Data Breach Study 2018*

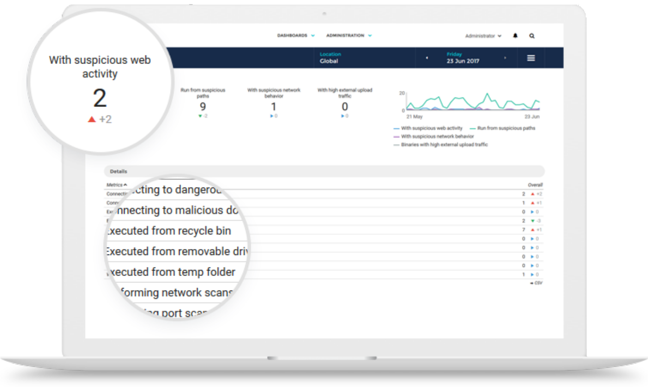
01. Abnormal behavior detection

Quickly identify potential internal/external threats

- Access device activity in real time, including built-in 3rd-party intelligence and external sources
- Define indicators to identify abnormal endpoint/application behaviors
- Get real time alerts when abnormalities are detected

Examples:

- ✓ Detect frequent connection attempts to suspicious URLs
- ✓ Detect high activity during irregular hours
- ✓ Detect binaries executed from a removable drive
- ✓ Identify IOCs across endpoint activity


With suspicious web activity
2
+2
DASHBOARDS
ADMINISTRATION
Administrator
Location
Global
Friday
23 Jun 2017
Run from suspicious paths
9
With suspicious network behavior
1
With high external upload traffic
0
21 May
23 Jun
With suspicious web activity
Run from suspicious paths
With suspicious network behavior
Binaries with high external upload traffic
Details
Metrics
Overall
…cting to dangerou…
…nnecting to malicious do…
…xecuted from recycle bin
…xecuted from removable dri…
…xecuted from temp folder
…forming network scans
…ng port scan…
CSV

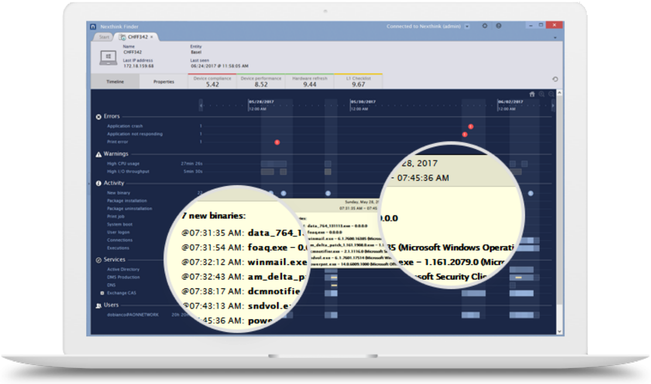
02. Response and post-breach analysis

Close the gap between detection and response

- Collect critical data in real time to prioritize and assess potential impact
- Maintain direct communication with employees during breach containment to ensure optimal experience
- Conduct rapid root cause analysis
- Access historical data and insights

Examples:

- ✓ Remote retrieval of memory dump for post-breach analysis
- ✓ Inform users when a security incident is resolved
- ✓ Initiate complete reinstallation after a device wipeout
- ✓ Isolate device to prevent further infection of leakage



IMPLEMENTATION WITH NEXTHINK SERVICES

We provide risk assessment and implementation services to identify where Nexthink technology will be most effective for breach management.

LEARN MORE

Nexthink provides digital experience management for your enterprise. We combine data collection and monitoring, analysis and intelligence, with automatic remediation and employee engagement to ensure the continuous optimization of your digital workplace. Learn more and schedule a demo at www.nexthink.com