Extend Your Data Security to the Edge

Spot signs of attack at the perimeter with telemetry from VPN, DNS, and Web Proxies.

- Analyze activity on perimeter devices including DNS and VPN.
- Apply geolocation and threat intelligence to your security telemetry.
- Detect perimeter attacks like malware, APT intrusion, and exfiltration.

"It’s like having an extra staff member that never sleeps always watching over our data."

– Jay Attiya, Director of IT, Toms River Regional Schools
Detect perimeter attacks including DNS attacks, domain hijacking - even stolen credentials on a VPN.

- Detect primary intrusion vectors of malware: email, web, and brute force attacks
- Correlate events and alerts so you can see the full picture and investigate security violations.
- Stop Trojan code from leveraging DNS for botnet campaigns, financial data theft campaigns or targeted attacks

Get more telemetry and context from the core to the perimeter

- Track potential data leaks and attacks at the edges
- Apply perimeter context to internal alerts
- Apply internal context to perimeter alerts
- Monitor perimeter attacks and put them in context with activity and alerts in your core data stores

Detect Attacks on the Edges of the Cyber Kill Chain

- DNS Tunneling
- Access from a suspicious or unexpected geolocation
- Account Hijacking
- Access from a suspicious IP
- Access to known C&C servers
- ....many more

Live Demo
Set up Varonis in your own environment.
info.varonis.com/demo

Risk Assessment
Get your risk report, and identify at-risk data and security vulnerabilities.
info.varonis.com/start

Get in touch
Have more questions? Let us know.
1.877.292.8767
info@varonis.com
Varonis offers a powerful software suite that protects your file, email servers and cloud applications from cyber-attacks and insider threats. We analyze the behavior of the people and machines that access your data, alert on misbehavior, and enforce a least privilege model.

We help thousands of customers prevent data breaches.