Next-Generation Security

In a world where everything is connected, anything can be disrupted!

The threat landscape is continuously evolving as adversaries are increasing the sophistication of cyber-attacks through artificial intelligence and machine learning. The number of potential intrusion points for an attack increases as companies embrace emerging technologies to engage employees and customers better, increase the number of endpoint devices, automate their processes, and shift workloads to the cloud. These combinations of trends drive the criticality for today's business to further harden their security posture across the company to stay ahead of threats and adversaries and minimize the risk of exposure.

Collective Insights Next-Generation Security service helps our clients strengthen their security posture to better:

- Enable a seamless end-user experience
- Protect users' identities and control access to valuable resources
- Protect sensitive data wherever it lives or travels
- Detect incidents using predictive and behavioral analysis
- Respond to incidents via automation
- Promote best practices to manage security-related risk

Facts & Figures

- 68.9 Days, average time to resolve malicious insider attacks (source: Leftronic)
- 69% of IT security leaders said their organizations have a reactive approach to cyber-security (source: CPO magazine)
- 84% of cyber-attacks are caused by human errors, i.e., easy password, physical devices left unsafe, or failing to apply patches (source: MIT Sloan Cybersecurity)

Key Questions

Contact us if you answer "yes" to any of these questions:

- Has your organization experienced a breach or an attack?
- Has your board grown an interest in Cyber Security?
- Do you have multiple point solutions for Cyber Security performing similar functions?
- Has an audit identified security issues that need to be remediated?
- Are you looking to shift identity and access management to the cloud?
- Is your organization lacking minimum security standards?

Collective Insights Delivers Value

- Identity Modernization enabled a Fortune 100 client to securely move 100% of their workloads to the Cloud (first F100 company to do so)
- Increased security posture from the bottom quartile to the top quartile (according to the McKinsey Digital Resilience Assessment) – with several security controls improving enough to reach the top Quartile for Financial Services
- Drove multi-million-dollar savings annually through security tool rationalization, reduced operational overhead and cancellation of data center contracts/leases
- Improved user experience using AAD Seamless Single Sign-On with Conditional Access (faster/less authentication attempts per user along with lowered help desk volume using Self-Service Password Reset)
- Conditional Access allows customer to address risk based on user location, device health, and other factors

Microsoft Gold Partner

For more information, please contact:
James Etzbach
jetzbach@collectiveinsights.com