DeepSurface®

CASE STUDY

One of the largest law firms in the Pacific Northwest **strengthens its cybersecurity program** thanks to DeepSurface Security.

Challenge:

The law firm needed a cost-effective cybersecurity tool that would help objectively prove that its risk containment efforts were successful and could be easily communicated to its executive staff and customers.

Law firms often house sensitive client information, making them a prime target for cyber criminals.

"Cybersecurity is table stakes for a law firm," said the Chief Information Security Officer (CISO) at one of the top Pacific Northwest law firms. "That's because law firms like ours host data that could contain proprietary company information, personally identifiable information, and protected health information. Also, law firms often hold some of the most valuable information on some of the world's largest companies."

It's imperative that every law firm protects this sensitive data from hackers.

"Hackers see a law firm as a potential opportunity to take advantage of large quantities of valuable, quality documents," said the CISO. "If you're a law firm and you get breached, and you had a poor cybersecurity program, it is going to impact your reputation and could result in serious fallout with your clients."

Solution

The law firm partnered with DeepSurface Security, which visualized and reported all known vulnerabilities, the business risk associated with each vulnerability, and the status of patching all assets across the firm's network.

DeepSurface also provided the law firm with a "pathways" map that identified chained vulnerabilities that weren't readily apparent. This allowed the firm to visualize how cyber criminals could exploit those vulnerabilities and cause maximum damage or access to a network. Reviewing chaining is crucial, since many vulnerabilities may have low CVSS scores on their own, but when chained together, they pose a real risk. CONTINUED

> Law firms often hold some of the most valuable information on some of the world's largest companies. Hackers see a law firm as a potential opportunity to take advantage of large quantities of valuable, quality documents.

CISO,
one of the largest law firms in the Pacific Northwest

DeepSurface®

CASE STUDY

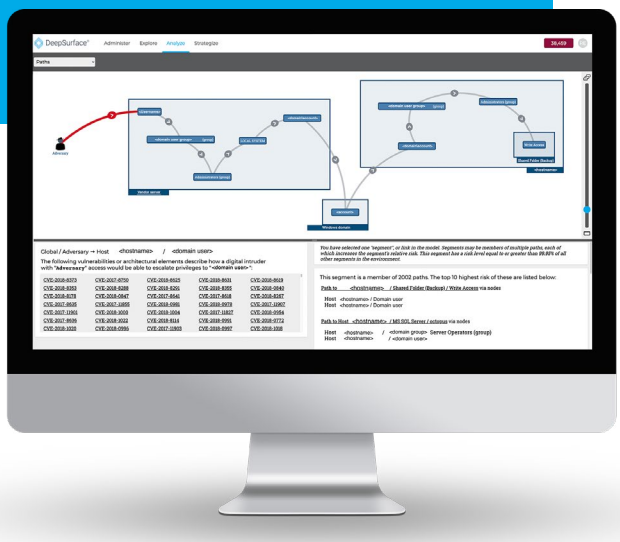
Solution CONTINUED

"With Deep Surface, we can prioritize treating each vulnerability based not just on its CVSS score, but on the actual likelihood of it being exploited," said the CISO. "It lets me pinpoint where in our environment we can focus energy and get the most impact on risk remediation versus just pushing out patches to all assets every month."

In addition to aiding in the prioritization of vulnerabilities, DeepSurface is a valuable validation tool for the CISO when it comes to proving to internal and external stakeholders that cybersecurity is managed responsibly.

"I can produce evidence for an auditor, our board, or our management that shows our risk map," said the CISO. "I can prove that we are not only managing critical patches per a schedule and a quantitative rating system, I also have this report that can quantitatively show either an increase or decrease in cumulative business risk. It shows we are paying attention to a wider set of related factors that could be leveraged in attacks, and not just relying on individual vulnerability scores."

> As environments get more complex, assets are more interconnected, so there are more risks to worry about," said the CISO. "DeepSurface provides a visualization of different access levels of user and system accounts relative to asset patching status, so that we can see where a hacker might go, and which vulnerabilities—even low-rated ones—might be exploited if a particular account is compromised."



RESULTS

- Comprehensive view of what risk each vulnerability poses to critical business assets, along with a remediation plan
- Reduced business risk as a result of faster prioritization and remediation of the vulnerabilities or chained vulnerabilities that matter most
- Executive reports that provide visual and quantitative evidence to stakeholders that cybersecurity risk is responsibly managed

> I can produce evidence for an auditor, our board, or our management that shows our risk map.

CISO,
one of the largest law firms in the Pacific Northwest